Question #1 *Topic 1*

Physical assets defined in an organization's business impact analysis (BIA) could include which of the following?

A. Personal belongings of organizational staff members

B. Disaster recovery (DR) line-item revenues

C. Cloud-based applications

D. Supplies kept off-site a remote facility

Suggested Answer: *D*

Community vote distribution

D (95%) 5%

01010100 Highly Voted 👍 1 year, 8 months ago

Selected Answer: D

Supplies, especially those kept off-site for disaster recovery or business continuity purposes, are physical assets. If these supplies are essential for the organization to continue its operations after a disruption, they would be considered in a BIA.

upvoted 12 times

honoge_killosa Highly Voted 👍 1 month ago

Selected Answer: D

The correct answer is D.

Thanks to Exam4Lead I successfully cleared my Cissp exam today.

Explanation: Physical assets defined in an organization's business impact analysis (BIA) could include supplies kept off-site at a remote facility. A BIA is a process that identifies an organization's critical business processes and the resources required to support them. Physical assets such as buildings, equipment, and inventory are typically identified in a BIA, as they are critical to the organization's ability to continue operating in the event of a disruption.

upvoted 7 times

hodis Most Recent 🕘 3 days, 4 hours ago

Selected Answer: D

The correct answer is D.

Thanks to Examforsure I successfully cleared my CISSP exam today.

upvoted 1 times

dbartowski 2 weeks, 2 days ago

Selected Answer: D

The correct answer is: D. Supplies kept off-site at a remote facility.
In a Business Impact Analysis (BIA), physical assets refer to tangible resources that support critical business functions. This includes items like servers, backup tapes, hardware, and supplies stored off-site that may be essential during a disruption. These are evaluated for their role in maintaining operations and recovery capabilities.
Let’s break down the other options:
- A. Personal belongings are not considered organizational assets.
- B. DR line-item revenues are financial projections, not physical assets.
- C. Cloud-based applications are digital services, typically categorized under logical or virtual assets.
If you’d like, I can walk you through how organizations typically categorize assets in a BIA. It’s a fascinating process!

upvoted 1 times

bassfunk 2 weeks, 4 days ago

Selected Answer: D

I took the test recently and none of these questions were on it. These are still good as practice but this needs to be updated.

upvoted 1 times

BinuHaneef 3 weeks, 4 days ago

Selected Answer: D

Dont rely on these questions, these are just for practicing but in reality is entirely different

upvoted 1 times

sowoc 3 weeks, 5 days ago

Selected Answer: D

The correct answer is D.

I’m happy to share that I successfully cleared my CISSP exam today! A big thank you to ValidIt_Exams for their helpful resources throughout my preparation. Their study material was well-structured and aligned with the CISSP exam objectives, which really helped me stay focused. The practice questions were especially useful for testing my understanding and getting familiar with the exam format. If you're planning to take the CISSP exam, I definitely recommend checking out ValidIt_Exams study tools for thorough and effective preparation.

upvoted 1 times

AA_Ron 2 months, 4 weeks ago

Selected Answer: D

What is ShaneOrton and sweetykaur are ISC2 plants!??

upvoted 1 times

peterlin01 3 months ago

Selected Answer: A

Do not trust these questions. None of them are from the Real CISSP exam.

upvoted 1 times

BinuHaneef 3 months, 2 weeks ago

Selected Answer: D

Physical Asset

upvoted 1 times

Phfldkdas123 3 months, 2 weeks ago

Selected Answer: D

Are these questions valid?

upvoted 1 times

sweetykaur 3 months ago

No. CISSP actual questions are far serious and tough than this exams.

upvoted 1 times

Saret 3 months ago

Nooooo.

upvoted 1 times

johnyc55 3 months, 3 weeks ago

Selected Answer: D

these are not valid any more from march'25

upvoted 1 times

pg27 6 months ago

Selected Answer: D

Question is specifically asking physical asset.. none of the answer other than Option D is referencing physical asset.

upvoted 1 times

Bietchasup 6 months, 3 weeks ago

Selected Answer: D

now that your're here. Don't rely on these questions. 0 on test

upvoted 7 times

Cyber_Judy 9 months, 1 week ago

The correct answer to question #1 is D. Supplies kept off-site at a remote facility.

Physical assets in the context of a BIA are any tangible resources that are essential to the operation of a business. This can include things like:

Buildings and infrastructure
Equipment and machinery
Inventories and supplies

Data and records
Supplies kept off-site at a remote facility would fall into this category, as they are essential to the business' ability to operate in the event of a disruption at its primary location.

The other answer choices are incorrect:

A. Personal belongings of organizational staff members are not considered business assets, as they are not essential to the operation of the business.
B. Disaster recovery (DR) line-item revenues are not physical assets, but rather financial assets.
C. Cloud-based applications are not considered physical assets, as they are not tangible resources.
upvoted 3 times

⊟ **smithinssia** 11 months, 2 weeks ago
valid examtopics
upvoted 3 times

⊟ **3008** 1 year, 3 months ago
Selected Answer: D
D is answer
upvoted 1 times

Question #2 *Topic 1*

When assessing the audit capability of an application, which of the following activities is MOST important?

A. Identify procedures to investigate suspicious activity.

B. Determine if audit records contain sufficient information.

C. Verify if sufficient storage is allocated for audit records.

D. Review security plan for actions to be taken in the event of audit failure.

Suggested Answer: *C*

Community vote distribution

B (73%) C (27%)

zo24 Highly Voted 1 year, 8 months ago

to me its B, the most important is the scope of the audit, the value it brings, is it sufficient to what the organization need inorder to call or even perform an actual audit. The requirement of disk size we can adjust as we needed, it can only be used to support the content of the information that the application can gather.

upvoted 33 times

aape1 Highly Voted 1 year, 8 months ago

Selected Answer: C

C, the keyword is "Capabilities". Remember the CIA, this question is about availability, not integrity. It would have been B if it was about the accuracy of the application.

upvoted 7 times

cloud29 Most Recent 3 months ago

Selected Answer: B

are these questions still valid on examtopics for CISSP ?

upvoted 1 times

amitsir 3 months, 1 week ago

Selected Answer: B

B is better

upvoted 1 times

cwjchoi 4 months, 2 weeks ago

Selected Answer: B

A (x - first to rule out) Procedures for investigation does not ensure we can audit things
D (x - second to rule out) Plans for audit failures remediates the lack of audit capability, but does not ensure it
C (x) Sufficient storage make sure audit records is available, but if the content is junk, it is no use
D (v) Good information in the audit records ensure it provide relevant information when doing audit, thus ensure audit capability, if compare full junk (C) with partial auditable information (B), B is better

upvoted 1 times

38e51fe 7 months, 3 weeks ago

I choose B

upvoted 1 times

ziyaetuk 7 months, 3 weeks ago

Selected Answer: B

When assessing the audit capability of an application, ensuring that audit records contain sufficient information is most important because without complete and accurate audit data, it would be difficult to trace or investigate any suspicious activities. This sufficiency forms the foundation for all other audit-related activities, such as investigating suspicious activity (Option A) and planning responses to audit failures (Option D).

Additionally, while storage (Option C) is necessary, it is secondary to ensuring that the content of the audit logs is comprehensive and reliable for effective auditing.

upvoted 1 times

celomomo 9 months ago

B. Keyword is "Mostly Important". They are all important but B sounds like the correct answer. To assess an application's audit capability effectively, the most critical activity is determining if the audit records contain sufficient information. Without detailed and comprehensive audit records, it's ALMOST impossible to reconstruct events, detect security incidents, or conduct forensic analysis. This sufficiency directly impacts the ability to monitor and review user activities, system operations, and potential security violations.

upvoted 1 times

celomomo 9 months ago

B. To assess an application's audit capability effectively, the most critical activity is determining if the audit records contain sufficient information. Without detailed and comprehensive audit records, it's ALMOST impossible to reconstruct events, detect security incidents, or conduct forensic analysis. This sufficiency directly impacts the ability to monitor and review user activities, system operations, and potential security violations.

upvoted 1 times

Chibueze 9 months, 1 week ago

Selected Answer: B

Basically in auditing, an auditing tool should be able to capture every important part of the process as input. This determine if the amount of information the application has to work with, and then, enough storage space can then be provision to keep the expected logs. B is the best answer. However, in the absence of B, i'd easily go for C.

upvoted 2 times

IMPERIAL_ACER 9 months, 1 week ago

Its C not B. Its about audit capability not what is in the audit itself. Its like me saying I think what is inside the audit is sufficient to be called an audit... or could be looked at insufficient information to be called an audit... so if you put it in context of what is really insufficient in the audit.... you will see it doesnt make much sense. But in terms of capability now, C makes perfect sense... because I am now as a manager looking to see if this audit assessment capable has enough resources to run based on my company capacity requirements. How long do I have to hold the data and do I have enough for the long term.

How do you audit an application?
Auditing Applications, Part 1
Plan the audit.
Determine audit objectives.
Map systems and data flows.
Identify key controls.
Understand application's functionality.
Perform applicable tests.
Avoid/consider complications.
Include financial assertions.
More items...

Auditing Applications, Part 1 - ISACA

upvoted 4 times

franbarpro 9 months, 1 week ago

I am having a hard time understanding this questions. How is the MOST important thing is to verify storage?
https://www.techtarget.com/searchcio/definition/security-audit
There are several reasons to do a security audit. They include these six goals:
Identify security problems and gaps, as well as system weaknesses.
Establish a security baseline that future audits can be compared with.
Comply with internal organization security policies.
Comply with external regulatory requirements.
Determine if security training is adequate.
Identify unnecessary resources.

upvoted 1 times

cebiko 2 years, 9 months ago

This isn't about security audit. It's about a capability of an app to do audits. Logs are important here, log size and storage.

upvoted 4 times

Jfrei 9 months, 1 week ago

Selected Answer: B

B.

Determine if audit records contain sufficient information is most important.

Verifying storage space is important, but logs stored without the necessary information would be useless.

upvoted 5 times

Logan3003 9 months, 1 week ago

Selected Answer: B

We were planning to roll out a Cloud VDI solution in the organisation where I work. they are providing 6 months retention on all audit logs. They are willing to extend the retention period for a smaller fee. But the project is on-hold because, we are not satisfied with their audit logs because it does not provide us enough audit events to detect security events (Suspicious or malicious activities). They only provide basic admin events in there audit logs. Retention is not a major concern when it comes to level of security events the audit log contain. This is a real world situation I had to dealt with. So answer is “B”

upvoted 3 times

deeden 9 months, 1 week ago

Selected Answer: B

I feel like B is more appropriate because to audit an application, there has to be something to assess. Imagine auditing privileged changes made to an application in the past 3 days and find only login and logout times and that admin modifications are not being logged. I think storage is also important but there was no context of availability mentioned.

upvoted 2 times

Ramye 9 months, 1 week ago

Selected Answer: B

Question is asking, does the application has audit capability? And that is to make sure the application audit logs contain sufficient information.

upvoted 2 times

pigon 1 year, 1 month ago

Though both are important, but if can only choose 1 option, then B is more important. Cos if audit records do not contain sufficient information, then no matter how much storage alloacted also no use. Hence B is more correct.

upvoted 3 times

Question #3 *Topic 1*

An organization would like to implement an authorization mechanism that would simplify the assignment of various system access permissions for many users with similar job responsibilities. Which type of authorization mechanism would be the BEST choice for the organization to implement?

A. Role-based access control (RBAC)

B. Discretionary access control (DAC)

C. Content-dependent Access Control

D. Rule-based Access Control

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **Jfrei** Highly Voted 👍 2 years, 3 months ago

Selected Answer: A

A.

Users with similar responsibilities should always be assigned a role. This simplifies the process of granting access when users join the team as well as move to new teams.

upvoted 39 times

⊟ **jackdryan** 1 year, 8 months ago

A is correct

upvoted 1 times

⊟ **amitsir** Most Recent 3 months, 1 week ago

Selected Answer: A

A is more accurate

upvoted 1 times

⊟ **BuntyBabu** 6 months ago

Selected Answer: A

Keywords are simplify & job responsibilities

upvoted 1 times

⊟ **AZSID** 9 months, 3 weeks ago

Selected Answer: A

A is Correct

upvoted 1 times

⊟ **SKainth** 10 months, 2 weeks ago

Selected Answer: A

Question is talking about Access Permissions with Similar Job Roles.

I will go with answer A.

upvoted 1 times

⊟ **AttahNet** 1 year, 3 months ago

Policy neutral access control mechanism defined around roles and privileges. So

A

Is the answer.

upvoted 2 times

⊟ **wingcheuk** 1 year, 6 months ago

Selected Answer: A

I will pick A for answer.

In domain 5, it says:

RBAC is where access to objects is granted based on the role of the subject.

DAC gives subjects full control of objects they have created or been given access to.

Content-Based Access Control is granted bases on the attributes or content of an object.

Rule Based Access Control is access that's granted based on IF/THEN statements.

As the question is asking an authorization mechanism for many user with similar job responsibilities (role). Only RBAC uses role for authorization, so it is the best option.

upvoted 1 times

wanne 1 year, 7 months ago

Anyone seen RBAC implemented for a lots of users? I would know what I should answer. Reality is a little B with a lot of D, since B is easier to implement and D easier to understand.

upvoted 1 times

jackdryan 1 year, 8 months ago

A is correct.

upvoted 1 times

user009 1 year, 9 months ago

The correct answer is A.

Explanation: The BEST choice for the organization to implement to simplify the assignment of various system access permissions for many users with similar job responsibilities would be Role-based access control (RBAC). RBAC is a widely used authorization mechanism that assigns permissions to users based on their job functions or roles. This simplifies the administration of access control by grouping users based on their job responsibilities, and granting access permissions based on those groups or roles.

upvoted 1 times

Overizzy 2 years, 1 month ago

Selected Answer: A

A RoleBAC

upvoted 1 times

Eltooth 2 years, 2 months ago

Selected Answer: A

A is correct answer. RBAC

upvoted 2 times

franbarpro 2 years, 3 months ago

Selected Answer: A

"A" sounds good to me

upvoted 3 times

Question #4 *Topic 1*

What is the PRIMARY reason for criminal law being difficult to enforce when dealing with cybercrime?

A. Jurisdiction is hard to define.

B. Law enforcement agencies are understaffed.

C. Extradition treaties are rarely enforced.

D. Numerous language barriers exist.

Suggested Answer: *A*

Community vote distribution

A (100%)

Cyber_Judy Highly Voted 9 months, 1 week ago

The correct answer to question #4 is A. Jurisdiction is hard to define.

Cybercrime can take place across borders, making it difficult to determine which jurisdiction has the authority to investigate and prosecute the crime. This can be especially challenging when the attacker is located in a different country than the victim.

The other answer choices are also factors that can make it difficult to enforce criminal law when dealing with cybercrime, but they are not as important as the issue of jurisdiction.

B. Law enforcement agencies are understaffed. This is true, but it is not the primary reason why criminal law is difficult to enforce when dealing with cybercrime.
C. Extradition treaties are rarely enforced. This is also true, but it is not the primary reason why criminal law is difficult to enforce when dealing with cybercrime.
D. Numerous language barriers exist. This is true, but it is not the primary reason why criminal law is difficult to enforce when dealing with cybercrime.

upvoted 8 times

jaber318 1 year, 1 month ago

nice explanation

upvoted 1 times

SangSang 5 months, 3 weeks ago

ChatGPT

upvoted 1 times

amitsir Most Recent 3 months, 1 week ago

Selected Answer: A

A cyber crime can be executed from anywhere in the world

upvoted 1 times

BuntyBabu 6 months ago

Selected Answer: A

All reasons are right but the keyword is 'primary'

upvoted 1 times

user009 9 months, 1 week ago

The correct answer is A.

Explanation: The PRIMARY reason for criminal law being difficult to enforce when dealing with cybercrime is that jurisdiction is hard to define. Cybercrime can occur across international borders, and it may not be clear which law enforcement agency has jurisdiction over the crime. In addition, different countries may have different laws regarding cybercrime, making it difficult to determine which laws apply in a particular case.

upvoted 4 times

hoho2000 1 year, 3 months ago

Selected Answer: A

The question is asking which part of the OS.

The security kernel makes up the main component of the TCB, which is made up of software, hardware, and firmware.

upvoted 1 times

⊟ **hoho2000** 1 year, 3 months ago

Sorry copy and paste wronlgy shoild refer to below

A reference monitor is the abstract machine that holds all of the rules of access for the system. The security kernel is the active entity that enforces the reference monitor's rules. They control the access attempts of any and all subjects; a user is just one example of a subject.

upvoted 1 times

⊟ **AZSID** 1 year, 3 months ago

Selected Answer: A

A looks Correct

upvoted 1 times

⊟ **SKainth** 1 year, 4 months ago

Correct answer is A. Jurisdiction is hard to define.

upvoted 1 times

⊟ **Overizzy** 2 years, 7 months ago

Selected Answer: A

It is hard to know the crime was committed, geographically speaking.

A is correct here.

upvoted 1 times

⊟ **Eltooth** 2 years, 8 months ago

Selected Answer: A

A is correct answer. Jurisdiction.

upvoted 1 times

⊟ **BinuHaneef** 2 years, 9 months ago

Selected Answer: A

Primary reason, yes it is A

upvoted 1 times

⊟ **franbarpro** 2 years, 9 months ago

Selected Answer: A

It's hard to know who's hands-on was on the keaboard...Agree with A

upvoted 3 times

Question #5 *Topic 1*

Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using which protocol?

A. Extensible Authentication Protocol (EAP)

B. Internet Protocol Security (IPsec)

C. Secure Sockets Layer (SSL)

D. Secure Shell (SSH)

Suggested Answer: *A*

Community vote distribution

A (100%)

franbarpro Highly Voted 👍 2 years, 9 months ago

Selected Answer: A

Agree with "A"
I was looking for Advanced Encryption Standard (AES) - I guess that's an algorithm not a "protocol"

upvoted 9 times

jackdryan 2 years, 2 months ago

A is correct

upvoted 1 times

amitsir Most Recent 🕘 3 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

BuntyBabu 6 months ago

Selected Answer: A

IPSec is for VPN; SSL for web applications & email communication, etc; EAP is correct answer

upvoted 1 times

Fouad777 6 months, 1 week ago

Selected Answer: A

he correct answer is A. Extensible Authentication Protocol (EAP).

Here's why:

WPA2 and EAP: WPA2 (Wi-Fi Protected Access 2) utilizes the Extensible Authentication Protocol (EAP) for user authentication. EAP is a framework that allows for various authentication methods

upvoted 1 times

Chibueze 9 months, 1 week ago

Easily A. EAP is the protocol used by WPA2

upvoted 1 times

alokubnisot 1 year ago

I agree, the correct answer is A

upvoted 1 times

SKainth 1 year, 4 months ago

Correct Answer is A.
Extensible Authentication Protocol (EAP) is the protocol used by Wi-Fi Protected Access 2 (WPA2) to provide users with a higher level of assurance that their data will remain protected.

upvoted 1 times

wanne 2 years, 1 month ago

WPA-EAP is broken beyond repair. It's how you still steal passwords today. Just buy ANY certificate and name an accesspoint like one you want to attack. Users will be promted about the certificate change. But they have no possibillity to know if it is a legit change (that has to be made regularly) or not. So the Client will just throw the password at you. But it has Enterprise in its name. So it has to be good!!! So no. It has by magnitudes lower security than the PSK-Variant that does not throw passwords around in algorithms that are broken since 30 years (NTLM). (Unless you are using PWD which is neither supported by Windows/Mac nor GNU-Linux.)

upvoted 2 times

gingasaurusrex 2 years, 2 months ago

Selected Answer: A

A. Extensible Authentication Protocol (EAP) is the protocol used by Wi-Fi Protected Access 2 (WPA2) to provide users with a higher level of assurance that their data will remain protected. EAP provides a framework for transporting authentication protocols that are used in wireless networks, and it is used to authenticate users and devices before they are granted access to the network.

upvoted 2 times

jackdryan 2 years, 2 months ago

A is correct.

upvoted 1 times

user009 2 years, 3 months ago

The correct answer is A.

Explanation: Wi-Fi Protected Access 2 (WPA2) provides users with a higher level of assurance that their data will remain protected by using the Extensible Authentication Protocol (EAP) protocol. EAP is an authentication framework that provides support for multiple authentication methods, including digital certificates, smart cards, and one-time passwords. By supporting EAP, WPA2 enables users to establish a secure connection to a wireless network and ensure that their data is protected.

upvoted 1 times

Eltooth 2 years, 8 months ago

Selected Answer: A

A is correct answer. EAP

upvoted 1 times

Question #6 *Topic 1*

Which part of an operating system (OS) is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system?

A. Reference monitor

B. Trusted Computing Base (TCB)

C. Time separation

D. Security kernel

Suggested Answer: *A*

Community vote distribution

D (80%) A (17%)

Toa Highly Voted 👍 2 years, 10 months ago

Answer D

Security Kernal : In computer and communications security, the central part of a computer or communications system hardware, firmware, and software that implements the basic security procedures for controlling access to system resources.

TCB : The trusted computing base (TCB) of a computer system is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system. By contrast, parts of a computer system outside the TCB must not be able to misbehave in a way that would leak any more privileges than are granted to them in accordance to the security policy.

Reference Monitor: reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are captured by the acronym NEAT

https://en.m.wikipedia.org/wiki/Security_kernel

upvoted 23 times

franbarpro 2 years, 9 months ago

The kernal is close to the hardware and with UEFI we can do secure boot wich give us more security. Agree with "D"

upvoted 3 times

DButtare 2 years, 9 months ago

It is D for me but we are not talking about kernel in the strict form here. Security kernel is part of the OS

upvoted 3 times

jackdryan 2 years, 2 months ago

D is correct

upvoted 2 times

MSKid Highly Voted 👍 2 years, 9 months ago

Kernel relates to relationships between objects in the OS, the Refence Monitor refers to access rights subjects have to those objects so I'm going with D

upvoted 6 times

amitsir Most Recent 🕓 3 months, 1 week ago

Selected Answer: D

Kernal is bridge between hardware and software

upvoted 1 times

BuntyBabu 6 months ago

Selected Answer: D

Security kernal

upvoted 1 times

Fouad777 7 months, 2 weeks ago

Answer is D

The security kernel is the part of the operating system responsible for enforcing security policies and providing secure interfaces among the hardware, operating system, and other parts of the computing system.

It operates within the Trusted Computing Base (TCB) and implements the functionality of the reference monitor, which ensures that access control policies are consistently enforced.

Other Options:

A. Reference monitor:

The reference monitor is a conceptual mechanism that enforces access controls. It is implemented as part of the security kernel but is not itself a specific component of the OS.

B. Trusted Computing Base (TCB):

The TCB includes all components (hardware, software, and firmware) critical to enforcing the system's security policy. The security kernel is a component of the TCB.

C. Time separation:

Time separation is a mechanism for allowing shared resources to be used securely by scheduling access at different times. It is not related to the core function of providing security interfaces.

upvoted 2 times

ziyaetuk 7 months, 3 weeks ago

Selected Answer: D

The security kernel is the component within an operating system responsible for enforcing the security policies and providing security interfaces among the hardware, OS, and other parts of the computing system. It mediates access to all resources and ensures that all interactions comply with security policies.

A. Reference monitor is a theoretical concept that enforces access control policies but is implemented by the security kernel in practice.

B. Trusted Computing Base (TCB) includes all components (hardware, software, and firmware) that enforce security, but it is broader than just the interfaces.

C. Time separation is not related to security interfaces; it refers to how an OS can manage resources over time for different processes.

upvoted 1 times

Chibueze 9 months, 1 week ago

Selected Answer: D

i was actually looking for firmware cos it is part of the security kernel. D

upvoted 2 times

gingasaurusrex 9 months, 1 week ago

Selected Answer: D

D. Security kernel is the part of an operating system (OS) that is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system. The security kernel is the core component of the Trusted Computing Base (TCB) and it enforces the security policy of the system by mediating all access to system resources. The reference monitor is a concept that describes the idealized functionality of the security kernel. Time separation refers to the practice of running different processes or applications at different times to prevent interference or data leakage.

upvoted 2 times

Yokota 9 months, 1 week ago

Selected Answer: D

The security kernel is responsible for providing security interfaces among the hardware, OS, and other parts of the computing system. It is a core component of the operating system that enforces security policies, controls access to system resources, and mediates interactions between different components of the system. The security kernel acts as a trusted boundary, ensuring that only authorized actions are performed and protecting the system from unauthorized access or malicious activities. It is designed to be highly reliable, tamper-proof, and resistant to attacks, making it a critical component for maintaining the security of the overall computing system.

upvoted 2 times

> **cisspisfun2022** 1 year, 8 months ago
>
> You confuse the security kernel with the system kernel. Security kernel is implementation of the RMC thus Reference Monitor Concept. The System kernel is a component of the OS.
>
> upvoted 2 times

3NO5 1 year, 1 month ago

The answer is D because the Security kernel is the part of an operating system responsible for providing security interfaces among the hardware, OS, and other parts of the computing system, not A.

upvoted 1 times

Kampala 1 year, 2 months ago

The answer is A.

A. The reference monitor validates access to every resource prior to granting the requested access. The other options are incorrect. Option D, the security kernel, is the collection of TCB components work together to implement the reference monitor functions. In other words, the security kernel is the implementation of the reference monitor concept. Option B, a TCB partition, and option C, a trusted library, are not valid TCB concept components.

upvoted 1 times

Kampala 1 year, 2 months ago

C. The reference monitor validates access to every resource prior to granting the requested access. The other options are incorrect. Option D, the security kernel, is the collection of TCB components that work together to implement the reference monitor functions. In other words, the security kernel is the implementation of the reference monitor concept. Option A, a TCB partition, and option B, a trusted library, are not valid TCB concept components.

upvoted 1 times

hoho2000 1 year, 3 months ago

Selected Answer: D

Please read what is refernce monitor properly, its an abstract, an idea, (as per CISSP official textbook) the outcome of that abstract is implemente as the security kernel.

upvoted 1 times

Kyanka 1 year, 3 months ago

Selected Answer: D

D Security Kernel looks to be correct for reasons already listed. They're asking about a part of an OS.

upvoted 1 times

iwannapass 1 year, 4 months ago

Selected Answer: D

Security Kernel: The collection of the TCB components that implment the functionality of the reference monitor. The central part of a computer system (hardware, software or firmware) that implements the fundamental security procedures for controlling access to system resources

Reference Monitor: Logical part of the TCB that confirms whether a subject has the right to use a resource prior to granting access. Mediates all access between Subjects and Objects.

upvoted 1 times

Woo7 1 year, 4 months ago

Selected Answer: A

Is the answer a? It is marked as correct.

upvoted 2 times

GPrep 1 year, 5 months ago

Selected Answer: D

D - Reference Monitor is conceptual and TCB is an architecture

This link does a nice job of explaining it in detail

https://www.pearsonitcertification.com/articles/article.aspx?p=1998558&seqNum=3

upvoted 1 times

Question #7 *Topic 1*

What process facilitates the balance of operational and economic costs of protective measures with gains in mission capability?

A. Performance testing

B. Risk assessment

C. Security audit

D. Risk management

Suggested Answer: *D*

Community vote distribution

D (100%)

kazeiya Highly Voted 2 years, 9 months ago

Selected Answer: D

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions.

upvoted 11 times

jackdryan 2 years, 2 months ago

D is correct

upvoted 1 times

Da_xpert Most Recent 2 months, 1 week ago

Selected Answer: D

D is Correct. Risk Management is the correct answer

upvoted 1 times

amitsir 3 months, 1 week ago

Selected Answer: D

At first i thought its risk assesment but risk management is correct byt the definitions

upvoted 1 times

BuntyBabu 6 months ago

Selected Answer: D

Risk assessment & Risk management look relevant. However, Risk assessment is part of risk management

upvoted 2 times

Fouad777 7 months, 2 weeks ago

The correct answer is:

D. Risk management

Explanation:
Risk management is the process of identifying, assessing, and prioritizing risks to balance the operational and economic costs of protective measures with the organization's mission capabilities and objectives.
It involves:
Identifying threats and vulnerabilities.
Evaluating potential impacts and likelihoods.
Implementing safeguards to reduce risks to acceptable levels.
Other Options:
A. Performance testing:

Focuses on evaluating the performance of systems or applications (e.g., speed, reliability) but is not directly related to balancing security costs and mission goals.
B. Risk assessment:

A subset of risk management. It is the process of analyzing threats, vulnerabilities, and potential impacts but does not include implementing or

balancing protective measures.
C. Security audit:

Involves reviewing and assessing security policies, controls, and compliance but does not directly facilitate balancing costs and operational gains.
upvoted 3 times

Overizzy 9 months, 1 week ago

Selected Answer: D

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need.
upvoted 1 times

user009 9 months, 1 week ago

The correct answer is D.

Explanation: The process that facilitates the balance of operational and economic costs of protective measures with gains in mission capability is risk management. Risk management is the process of identifying, assessing, and prioritizing risks, and taking steps to minimize, monitor, and control those risks. This involves balancing the costs and benefits of protective measures with the organization's mission and goals. By identifying and managing risks, an organization can make informed decisions about how to allocate resources and invest in protective measures that provide the greatest benefit to the organization.
upvoted 1 times

gingasaurusrex 9 months, 1 week ago

Selected Answer: D

D. Risk management facilitates the balance of operational and economic costs of protective measures with gains in mission capability. Risk management is a systematic approach to identifying, assessing, and prioritizing risks to organizational operations, assets, or individuals resulting from the operation of information systems and the information processed, stored, or transmitted by those systems. It involves evaluating the likelihood and impact of risks and implementing cost-effective measures to reduce them to an acceptable level. By considering the costs of implementing protective measures against the benefits of mission capability, risk management helps organizations make informed decisions about how to allocate their resources to achieve their security goals. Performance testing, security audit, and risk assessment are all important components of a risk management program.
upvoted 2 times

SKainth 1 year, 4 months ago

Selected Answer: D

Risk Management is correct. The keyword in Question is Balance.
upvoted 2 times

Eltooth 2 years, 8 months ago

Selected Answer: D

D is correct answer. Risk Management.
upvoted 1 times

Question #8 *Topic 1*

Clothing retailer employees are provisioned with user accounts that provide access to resources at partner businesses. All partner businesses use common identity and access management (IAM) protocols and differing technologies. Under the Extended Identity principle, what is the process flow between partner businesses to allow this IAM action?

A. Clothing retailer acts as User Self Service, confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

B. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

C. Clothing retailer acts as Service Provider, confirms identity of user using industry standards, then sends credentials to partner businesses that act as an identity provider (IdP) and allows access to resources.

D. Clothing retailer acts as Access Control Provider, confirms access of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to resources.

Suggested Answer: *B*

Community vote distribution

B (96%)	4%

franbarpro Highly Voted 👍 2 years, 9 months ago

Selected Answer: B

Agree with "B" - "Employees are provisioned with user accounts" sounds like the clothing retailer is an IdP.

Also from crowdstrike:
Identity and access management (IAM) is a framework that allows the IT team to control access to systems, networks and assets based on each user’s identity. IAM consists of two main components:

1. Identity management: Verifies the identity of the user based on existing information in an identity management database.

2. Access management: Uses the requestor’s identity to confirm their access rights to different systems, applications, data, devices and other resources.

An IAM tool’s core functions are to:

Assign a single digital identity to each user
Authenticate the user
Authorize appropriate access to relevant resources
Monitor and manage identities to align with changes within the organization

https://www.crowdstrike.com/cybersecurity-101/identity-access-management-iam/

upvoted 15 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 1 times

gingasaurusrex Highly Voted 👍 2 years, 2 months ago

Selected Answer: B

B. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

The Extended Identity principle is a concept that is used to enable access to resources across partner businesses with different IAM technologies. In this scenario, the clothing retailer acts as an identity provider (IdP), which confirms the identity of the user using industry standards such as SAML, OAuth, or OpenID Connect. The IdP then sends the user's credentials to partner businesses that act as a Service Provider (SP) and allow access to resources.

By using a common IAM protocol, such as SAML, OAuth, or OpenID Connect, the partner businesses can trust the clothing retailer's authentication of the user's identity and grant access to the requested resources. This allows the clothing retailer's employees to access resources at partner businesses without having to maintain separate user accounts for each partner business.

upvoted 6 times

amitsir Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

Fouad777 7 months, 2 weeks ago

B. Clothing retailer acts as identity provider (IdP), confirms identity of user using industry standards, then sends credentials to partner businesses that act as a Service Provider and allows access to services.

upvoted 1 times

[Removed] 10 months, 3 weeks ago

Selected Answer: B

B. Clothing retailer acts as identity provider (IdP), confirms identity, then sends credentials to partner businesses (Service Providers) for access.

upvoted 4 times

deeden 11 months ago

Selected Answer: B

Agree with option B. Employees get their access from Clothing retailer (Idp) to access resources at partner businesses (Service provider).

upvoted 1 times

keithtemplin 1 year, 2 months ago

Selected Answer: C

The key here is that the clothing provider is providing resources. " that provide access to resources at partner businesses"

A Service Provider is an application or service that users want to access, while an Identity Provider authenticates those users and validates their identities. The SP trusts the IdP to securely handle logins.

There for the Retailer "Provides" resources becoming the "Service Provider"

upvoted 1 times

Ivanchun 2 years, 6 months ago

Selected Answer: B

Clothing retailer provide the identity

upvoted 1 times

Nickname53796 2 years, 8 months ago

Selected Answer: B

The SAML 2.0 specification utilizes three entities: the principal, the service provider, and the identity provider

upvoted 1 times

Question #9 *Topic 1*

Which of the following statements BEST describes least privilege principle in a cloud environment?

A. A single cloud administrator is configured to access core functions.

B. Internet traffic is inspected for all incoming and outgoing packets.

C. Routing configurations are regularly updated with the latest routes.

D. Network segments remain private if unneeded to access the internet.

Suggested Answer: *D*

Community vote distribution

D (59%) A (41%)

⊟ **YesPlease** Highly Voted 1 year, 6 months ago

Selected Answer: D

Answer D: Why, glad you asked.... Least privilege extends beyond human access. The model can be applied to applications, systems or connected devices that require privileges or permissions to perform a required task. So internet access is being limited until it is needed to perform a specific task.

A) is incorrect because they are giving 1 admin all the core roles when they may not need all of them to do their job. Of course the argument can be made that they are the only admin and will need all core admin rights, but that is not the same as limiting access for a particular system or person to only have the rights they need to do their job.

upvoted 16 times

⊟ **kurili** Most Recent 2 months, 2 weeks ago

Selected Answer: D

I learnt something new today!! The Principle of Least Privilege is about limiting access to the minimum necessary resources and permissions needed to perform legitimate tasks — and nothing more.

In a cloud environment, this applies not just to user accounts, but also to network resources, services, and workloads.

upvoted 1 times

⊟ **amitsir** 3 months, 1 week ago

Selected Answer: D

A is wrong as administrator access is not a least privilege. D is correct because least access is given to the network segment.

upvoted 2 times

⊟ **Socca** 6 months ago

Selected Answer: A

This statement is closest to the least privilege principle because it implies that administrative access to critical functions is tightly controlled and limited to a specific individual or role. By minimizing the number of administrators with access to core functions, you are following the least privilege principle.

upvoted 2 times

⊟ **somsom** 8 months, 2 weeks ago

a single cloud admin cannot be configured to access core fiction. the risk is high. what if he is not available what will happen to the business? answer is D

upvoted 2 times

⊟ **M_MUN17** 8 months, 3 weeks ago

The correct answer is A. A single cloud administrator is configured to access core functions.

The principle of least privilege refers to granting users, systems, or processes the minimum level of access or permissions necessary to perform their tasks. In a cloud environment, this means restricting administrative access to only those who need it. For example, having a single cloud administrator with access to core functions aligns with this principle, as it limits the potential for unauthorized or unnecessary access.

The other options describe general security practices but do not specifically relate to the principle of least privilege:

B. Internet traffic is inspected for all incoming and outgoing packets refers to traffic monitoring.

C. Routing configurations are regularly updated with the latest routes refers to network routing management.

D. Network segments remain private if unneeded to access the internet relates to network segmentation, not least privilege.

upvoted 2 times

celomomo 9 months ago

Selected Answer: D

I wonder why anyone would even think A is correct. That is a single point of failure and in no way related to PoLP. Least privilege is restricting access to what you or an application need to do its job. A single admin having access to a core service is in no way least privilege. D is the suitable answer.

upvoted 1 times

evilCorpBot7494 9 months, 1 week ago

Selected Answer: D

Correct answer is D.

A doesn't describe least privilege, if you needed to have two cloud administrators access core functions, you would have to give them to the second one and that doesn't relate to least privilege at all. That may be more related to segregation of functions if you decide you only need one cloud administrator for that or if you see that having 2 admins and divide their core functions access would be most secure.

D, on the other hand, is related to least privilege through segregation of the network, ensuring users in an environment don't access other environments they don't need for their work functions.

upvoted 1 times

deeden 11 months ago

Selected Answer: D

D sound more correct. Network is restricted when if Internet is not required. Option A sound more like a demonstration of elevated privilege, which is right for an administrator.

upvoted 1 times

iamlamzzy 1 year ago

Priviledge has to do with access. So, the correct answer is A. Access could've been granted to all the administrators but the key word here is "single".

upvoted 2 times

icebw22 1 year, 1 month ago

Answer D, least privilege principal, provider user/resource enough privilege to perform role/duty.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: D

Preventing unnecessary access is D.

A is a violation of PoLP and is a SPF.

upvoted 1 times

Kyanka 1 year, 3 months ago

Selected Answer: A

Answer: A - I think what they're trying to refer to is how you create one admin account in cloud environments to do the "core" management and then everything is is delegated to other roles. CISSP tries to be vendor agnostic but it looks like they're describing the MS Azure practice of creating one global admin (or as few as possible) to do certain functions.

upvoted 3 times

SKainth 1 year, 4 months ago

Selected Answer: A

Least Privilege is basically based on User roles and privileges. BCD are Security Practices.

upvoted 2 times

Hackermayne 1 year, 5 months ago

Selected Answer: D

I say D, A is close but I don't know if a single admin account that controls the core is the right way to go. Youd likely need one as a
(not truly) global, another as a "break glass account" that no one uses and has a fido key in a safe or something somewhere, and the rest of the admins would be granted permissions under those.

upvoted 1 times

ochijindu0201_ 1 year, 6 months ago

The correct answer is D. "Network segments remain private if unneeded to access the internet."

The least privilege principle in a cloud environment advocates for providing users and systems with the minimum level of access or permissions necessary to perform their tasks or functions. By restricting access to only what is essential, the risk of unauthorized access or potential security breaches is minimized.

Option D reflects the least privilege principle by emphasizing that network segments should remain private unless there is a specific need for them to access the internet. This approach helps limit exposure and potential attack vectors, aligning with the concept of least privilege.

upvoted 4 times

Soleandheel 1 year, 6 months ago

The correct answer is A. The reason option D is not the BEST answer in the context of least privilege is that it specifically refers to network segments and their connectivity to the internet. While it is a valid security practice, the least privilege principle is more commonly associated with user and system access permissions rather than network segmentation.

upvoted 3 times

Question #10 *Topic 1*

An organization has been collecting a large amount of redundant and unusable data and filling up the storage area network (SAN). Management has requested the identification of a solution that will address ongoing storage problems. Which is the BEST technical solution?

A. Compression

B. Caching

C. Replication

D. Deduplication

Suggested Answer: *A*

Community vote distribution

D (71%) A (29%)

Tanzy360 Highly Voted 2 years, 9 months ago

Selected Answer: D

D is the only answer choice that makes sense with the excess data

upvoted 10 times

franbarpro Highly Voted 2 years, 9 months ago

Selected Answer: D

"D" it is.

Data deduplication is a process that eliminates excessive copies of data and significantly decreases storage capacity requirements.

Deduplication can be run as an inline process as the data is being written into the storage system and/or as a background process to eliminate duplicates after the data is written to disk.

https://www.netapp.com/data-management/what-is-data-deduplication/#:~:text=Data%20deduplication%20is%20a%20process,data%20is%20written%20to%20disk.

upvoted 7 times

Da_xpert Most Recent 2 months, 1 week ago

Selected Answer: D

Answer is D: The important part of the question here is "Redundant and unusable data".

upvoted 1 times

kurili 2 months, 2 weeks ago

Selected Answer: D

The problem described is "a large amount of redundant and unusable data" filling up storage.

Deduplication is a storage optimization technique that eliminates redundant copies of data by storing only unique instances of data blocks or files and replacing duplicates with pointers to the original.

This directly addresses storage inefficiency caused by redundant data, reducing overall storage consumption on the SAN.

 Why the others aren't ideal:

A. Compression

→ Reduces the size of data but doesn't remove redundancy. It works on individual files or data streams, not across multiple copies of the same file.

B. Caching

→ Temporarily stores frequently accessed data for performance, not for reducing storage footprint.

C. Replication

→ Actually increases storage use by copying data to other locations for redundancy and availability — the opposite of what's needed here.

upvoted 1 times

amitsir 3 months, 1 week ago

Selected Answer: D

D is more accurate

upvoted 1 times

Skynet08 5 months, 3 weeks ago

Selected Answer: D

the question mentions "redundant" which indicates the answer will be D

upvoted 1 times

Rider2053 6 months, 3 weeks ago

Selected Answer: D

The data deduplication process systematically eliminates redundant copies of data and files, which can help reduce storage costs and improve version control. In an era when every device generates data and entire organizations share files, data deduplication is a vital part of IT operations.

upvoted 1 times

Moose01 6 months, 4 weeks ago

Selected Answer: D

I need to slow down and read it.
it is De-duplication not Duplication, Jesus what a trap.

upvoted 4 times

Eltooth 9 months, 1 week ago

Selected Answer: D

D is correct answer. Redundant can mean multiple (think redundant systems) so if you have multiple versions of the data then dedup would reduce these copies to one main and multiple stubs. Yes there would be a hit on CPU performance once dedup is run for the first time, however long term this speeds up space saving when new (redundant) data is added.

Compression would reference each redundant bit/byte and have pointers to each, filling up the master index record and adding processing overhead each time data was added, searched for or retrieved.

upvoted 2 times

Ezebuike 10 months, 2 weeks ago

Assuming you have a very large file on your desktop and is occupying much storage space, you can zip up the folder and the size of the file will reduce. What dose that mean? you are compressing the file. That same logic can be applied to this quest. Thus, the correct and is A. Compression

upvoted 2 times

3NO5 1 year, 1 month ago

D is the best answer

Deduplication is the best solution for managing excess data, even if it's not just duplicates. It helps remove redundant and unneeded data efficiently.

upvoted 1 times

dm808 1 year, 3 months ago

Selected Answer: A

Deduplication doesnt address unusable data.. so it has to be compression, A

upvoted 1 times

> **dm808** 1 year, 3 months ago
>
> and "redundant" can also mean "unnecessary" as well as "duplicate"
>
> upvoted 3 times

Kyanka 1 year, 3 months ago

Selected Answer: D

D is pretty much the "text book" answer for this question.

upvoted 1 times

andyprior 1 year, 4 months ago

Selected Answer: A

Deduplication is effective in organizations that have a lot of redundant data, such as backup systems that have several versions of the same file.
Compression is effective in decreasing the size of unique files, such as images, videos, and databases

upvoted 1 times

andyprior 1 year, 4 months ago

Deduplication is effective in organizations that have a lot of redundant data, such as backup systems that have several versions of the same file.
Compression is effective in decreasing the size of unique files, such as images, videos, and databases

upvoted 2 times

⊟ **DragonHunter40** 1 year, 4 months ago

I say the answer is A. The question isn't talking about getting rid of the data, and 9 times out of 10, no one is going to go through large amounts of data to see what's a duplicate. Not to mention, you wouldn't know what to keep or delete. A "Compression" is the simplest answer.

upvoted 1 times

⊟ **Bright07** 1 year, 4 months ago

D is the answer. Although both A and D answer look similar. This is simple explanation for both answers. A storage area network (SAN) or storage network is a computer network which provides access to consolidated, block-level data storage. deduplication commonly occurs at the block level; however, compression generally occurs at the file level. Now the difference is that deduplication occurs at the block level according to the question while compression occurs at the file level. so answer is Deduplication.

upvoted 3 times

Question #11 *Topic 1*

Which Wide Area Network (WAN) technology requires the first router in the path to determine the full path the packet will travel, removing the need for other routers in the path to make independent determinations?

A. Synchronous Optical Networking (SONET)

B. Multiprotocol Label Switching (MPLS)

C. Fiber Channel Over Ethernet (FCoE)

D. Session Initiation Protocol (SIP)

Suggested Answer: *B*

Community vote distribution

B (100%)

franbarpro Highly Voted 2 years, 9 months ago

Selected Answer: B

"B" it is!
Multiprotocol label switching (MPLS) is a technique for speeding up network connections that was first developed in the 1990s. The public Internet functions by forwarding packets from one router to the next until the packets reach their destination.

MLPS, on the other hand, sends packets along predetermined network paths. Ideally, the result is that routers spend less time deciding where to forward each packet, and packets take the same path every time.

Consider the process of planning a long drive. Instead of identifying which towns and cities one must drive through in order to reach the destination, it is usually more efficient to identify the roads that go in the correct direction. Similarly, MPLS identifies paths — network "roads" — rather than a series of intermediary destinations.

https://www.cloudflare.com/learning/network-layer/what-is-mpls/

upvoted 13 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 2 times

Jenkins3mol Highly Voted 9 months, 1 week ago

Selected Answer: B

The answer is: B. Multiprotocol Label Switching (MPLS)

Here's why the other options are incorrect:

Synchronous Optical Networking (SONET): SONET is a physical layer technology that deals with the transmission of data over optical fiber. It doesn't handle path determination.
Fiber Channel Over Ethernet (FCoE): FCoE is a protocol for encapsulating Fibre Channel frames over Ethernet networks. It doesn't involve path determination either.
Session Initiation Protocol (SIP): SIP is a signaling protocol for establishing and terminating voice and video communication sessions. It doesn't handle path determination in WANs.
MPLS, on the other hand, is a technology that uses labels to direct packets across a network. The first router in the path assigns a label to the packet, and subsequent routers simply switch the packet based on the label, eliminating the need for them to independently determine the entire path.

upvoted 5 times

06694bf Most Recent 3 months ago

Selected Answer: B

definitely B

upvoted 1 times

Overizzy 9 months, 1 week ago

Selected Answer: B

B is the answer, Multi protocol label switching. Ensures speed and efficiency of data routing. However, it is expensive and encryption must be set up separately. More control and allows for dedicated network paths.

upvoted 2 times

Jamati 9 months, 1 week ago

Selected Answer: B

MPLS is correct, however, technically speaking, with MPLS the first router does not really determine the full path that the packet will traverse, it only determines the next hop info using labels, not the full path. Only Segment Routing, not MPLS, would have this capability to have the 1st router determine the full path.

upvoted 2 times

vavofa5697 2 years, 5 months ago

Selected Answer: B

MPLS (Multiprotocol Label Switching) directs data across a network based on short path labels.

upvoted 2 times

cccispman 2 years, 6 months ago

Total no brainer - B

upvoted 2 times

Jimmyliu0822 2 years, 7 months ago

B,MPLS

upvoted 1 times

Eltooth 2 years, 8 months ago

Selected Answer: B

B is correct answer. MPLS

upvoted 1 times

Cww1 2 years, 9 months ago

Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.

upvoted 4 times

Question #12 *Topic 1*

Which of the following would an information security professional use to recognize changes to content, particularly unauthorized changes?

A. File Integrity Checker

B. Security information and event management (SIEM) system

C. Audit Logs

D. Intrusion detection system (IDS)

Suggested Answer: *A*

Community vote distribution

A (63%) B (37%)

⊟ **franbarpro** Highly Voted 👍 2 years, 9 months ago

File integrity monitoring (FIM) refers to an IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether or not they have been tampered with or corrupted. FIM, which is a type of change auditing, verifies and validates these files by comparing the latest versions of them to a known, trusted "baseline." If FIM detects that files have been altered, updated, or compromised, FIM can generate alerts to ensure further investigation, and if necessary, remediation, takes place.

upvoted 20 times

⊟ **jackdryan** 2 years, 2 months ago

A is correct

upvoted 2 times

⊟ **RawToast** Highly Voted 👍 9 months, 1 week ago

Selected Answer: B

The part that is standing out to me is "particularly unauthorized changes." FIM would tell us if there was a change but a SIEM could contain information about WHO is implementing the changes to the content we are analyzing. Just being sure of a change is not enough to determine if the change was authorized of not. I would lean toward SIEM just because of the ending of the question.

upvoted 11 times

⊟ **celomomo** 9 months ago

If you say SIEM, you can also say Audit log then since the audit log of that file tells you the changes made and that would be the table to query with SIEM. SIEM is not a standalone but relies on logs fed to it to correlate incidents and events. File Integrity checker seems more straightforward IMO.

upvoted 3 times

⊟ **Kyanka** 1 year, 3 months ago

This is a classic cert exam tactic of giving you an almost correct answer and the actual correct answer. Without the 2nd half of the sentence, you wouldn't know SIEM is the BEST answer.

upvoted 2 times

⊟ **RonWonkers** 2 years, 8 months ago

I think you are right

upvoted 4 times

⊟ **jens23** 2 years ago

I've used the exact same reasoning.

upvoted 2 times

⊟ **kurili** Most Recent ⊙ 2 months, 2 weeks ago

Selected Answer: A

□ Why A is correct:

A File Integrity Checker (FIC) is specifically designed to detect changes to files, configurations, or content by comparing the current state of files to a known-good baseline (usually using cryptographic hashes like SHA-256).

If an unauthorized or unexpected change occurs (like a tampered config file, modified system file, or web defacement), the FIC alerts on it.

It's purpose-built for recognizing unauthorized content changes.

 Why the others aren’t a perfect fit:
B. SIEM system
→ Aggregates and correlates logs and alerts from multiple sources, including a file integrity checker, but it doesn’t directly monitor file content changes itself.

C. Audit Logs
→ Record system and user actions. They might show who made a change, but don't detect or monitor what specifically changed in file content.

D. Intrusion Detection System (IDS)
→ Monitors network or system activity for known attack patterns or anomalies, but typically doesn't check for specific file content changes unless integrated with a file integrity tool.

upvoted 1 times

artvark79 2 months, 3 weeks ago

Selected Answer: A

The correct answer is:

A. File Integrity Checker

Explanation:
A File Integrity Checker is specifically designed to monitor and detect changes to files and content, especially unauthorized modifications. It works by comparing the current state of files to a known good baseline (often via cryptographic hashes). If anything changes — such as file tampering, deletion, or unexpected modifications — it alerts the security team.

Other options:

SIEM (B): Collects and analyzes logs for patterns but isn’t focused solely on file integrity.
Audit Logs (C): Records actions/events but does not actively compare file states.
IDS (D): Monitors network or system activity for suspicious behavior but doesn’t focus specifically on content changes like a file integrity checker does.

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: A

Cannot be B. SIEM helps aggregate and analyze logs but does not directly monitor for file content changes.

upvoted 1 times

d7034bf 6 months, 3 weeks ago

Selected Answer: A

Key word is "unauthorized" . While File Integrity Checker (or Monitor) does look for unauthorized changes, SIEM checks for changes whether made on purpose or not.

upvoted 1 times

somsom 8 months, 2 weeks ago

answer is A because unauthorized access is there. siem creates alerts both authorized and non authorized. false positive and false negative

upvoted 1 times

Chibueze 9 months, 1 week ago

Selected Answer: A

This refers to "I" in the CIA triad and the keyword is integrity.

upvoted 1 times

iwannapass 9 months, 1 week ago

Selected Answer: A

Leaning towards A. File Integrity checker.

In the sybex 9th edition book page 1008 it says, " File integrity monitoring tools, also provide a secondary anti virus functionality. These tools are designed to alert ADMINISTRATORS to UNAUTHORIZED FILE MODIFICATIONS."

I'm not sure if Admins are considered security professionals. But this seems to highlight the unauthorized portion of the question.

I did read up on SIEM on page 841. And I had a hard time rationalizing the answer.

upvoted 3 times

Qwertyloopback 9 months, 1 week ago

Selected Answer: A

FIM is correct from all of my research and experience. Take for example the FIM portion of McAfee ESS, you inpu the hash and are alerted if the file is modIfied.

SEIM does not always have the potential for comparing hashes which is what would be necessary to detect file modification.

upvoted 3 times

david124 9 months, 1 week ago

Selected Answer: A

A File Integrity Checker (FIC) is a security tool used to monitor and detect changes to files and directories on a computer system. FIC calculates cryptographic hashes (checksums) of files or directories and compares them to previously recorded checksums to detect changes. If the checksums differ, it indicates that the file or directory has been modified, deleted, or added, and alerts can be generated to inform the security team of potential unauthorized changes.

Security Information and Event Management (SIEM) systems are used to collect, analyze, and correlate security event logs from multiple sources in real-time. Audit Logs also record system activity and can be used to monitor changes, but they are not as effective as FICs for detecting changes in files and directories.

upvoted 3 times

Dash0211 2 years, 2 months ago

As other's said, I think the key word is unauthorized changes. the FIC can show a change happened, doesn't mean it was unauthorized.

upvoted 2 times

vorozco 9 months, 1 week ago

Leaning towards A.

An internet search of "SIEM to detect unauthorized changes to a file" even brings back a bunch of results for FIM, and the results go into integrating FIM with SIEM. So, FIM seems to be the component that would actually be checking for unauthorized changes (it can just be integrated into a SIEM).

upvoted 1 times

Alcpt 9 months, 1 week ago

Selected Answer: A

can only be A

upvoted 1 times

deeden 9 months, 1 week ago

Selected Answer: A

While SIEM solutions can collect and analyze logs from various sources, including file system activity, they might not provide the same level of granular detail and focus as a dedicated file integrity monitoring (FIM) solution

upvoted 2 times

bromings 9 months, 1 week ago

An information security professional would typically use:

A. File Integrity Checker

File Integrity Checkers are tools used to monitor and validate the integrity of files and systems by regularly scanning and comparing the current state of files against a known baseline or reference. They detect unauthorized changes, modifications, or alterations to files by comparing attributes such as file size, timestamps, permissions, and checksums. When unauthorized changes occur, the file integrity checker can generate alerts or notifications to indicate potential security breaches or anomalies.

While the other options (SIEM system, Audit Logs, and IDS) are also valuable security tools, they might not specifically focus on recognizing unauthorized changes to content in the same direct and detailed manner as a File Integrity Checker does.

upvoted 4 times

xxxBadManxxx 9 months, 1 week ago

A:

An information security professional would use a File Integrity Monitoring (FIM) system to recognize changes to content, particularly unauthorized changes.

File Integrity Monitoring is a security technique that involves monitoring and detecting changes to files, directories, and file systems. It helps ensure the integrity of critical system files and sensitive data by identifying any unauthorized or unexpected modifications, deletions, or additions. FIM systems use baseline comparisons or cryptographic hashing techniques to determine if files have been tampered with.

upvoted 1 times

⊟ **1000ba4** 9 months, 1 week ago

Let's say we have a black box solution, such as a firewall, IDS, or IPS. These black boxes can't install a FIM agent or any endpoint solution because they are black boxes. So, the only way to detect unauthorized changes is to integrate these black boxes with a SIEM and monitor the alerts and events related to unauthorized change event IDs.

upvoted 1 times

⊟ **1000ba4** 1 year, 3 months ago

I apologize, actually, there is an agentless File Integrity Checker, so the answer is File Integrity Checker, which is (A).

upvoted 1 times

Question #13 *Topic 1*

Which of the following is included in change management?

A. Technical review by business owner

B. User Acceptance Testing (UAT) before implementation

C. Cost-benefit analysis (CBA) after implementation

D. Business continuity testing

Suggested Answer: *D*

Community vote distribution

B (49%) D (46%) 5%

BinuHaneef Highly Voted 2 years, 9 months ago

Selected Answer: D

A. Technical review by business owner - This is not a Change management

B. User Acceptance Testing (UAT) before implementation - UAT is only testing before implement

C. Cost-benefit analysis (CBA) after implementation - This is not a CM

D. Business continuity testing - This could be after implementing something

upvoted 18 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 2 times

shaitand 8 months, 1 week ago

UAT is the user confirming the change works as expected. That can't happen until AFTER implementation.

upvoted 2 times

Jamati Highly Voted 2 years, 8 months ago

Selected Answer: B

Testing should be done before implementation to ensure no problems will arise after the change.

upvoted 13 times

shaitand 8 months, 1 week ago

If you haven't implemented the change then how do you test the result of implementing the change?

upvoted 1 times

RRabbit_111 7 months ago

because they take a sample group of users to test it on. it's called beta testing in some industries. it'd be very unwise to make big changes and then ahve your entire userbase of millions hate you for it. UAT happens before

upvoted 2 times

Chibueze 9 months ago

Then that is Business continuity test not user acceptance

upvoted 2 times

nisoshabangu Most Recent 2 months, 3 weeks ago

Selected Answer: B

Changes are first tested in a UAT environment, a test manager would then signoff changes , also PM ,architect and senior engineer in a change management doc.

upvoted 1 times

attesco 6 months, 1 week ago

Selected Answer: B

The Technical review is not done by Business Owner, but by the Expert

upvoted 3 times

d7034bf 6 months, 3 weeks ago

Selected Answer: B

In the 5 steps of change management, implementation is the third process where testing is involved to gain feedback and apply changes effectively. B is the more logical answer.

upvoted 2 times

KennethLZK 7 months, 3 weeks ago

Selected Answer: B

Business Continuity Testing is part of the BCP (Business Continuity Planning) and disaster recovery. It is not directly related to CM process. Therefore B is the best answer here.

upvoted 2 times

shaitand 8 months, 1 week ago

Selected Answer: D

I've been implementing changes in ITIL environments for over a decade. A change to the lower environment and the subsequent change to production are two separate changes, not parts of one change. You can't do user testing without first deploying so the user has something to test.

upvoted 1 times

somsom 8 months, 2 weeks ago

D is the answer because you continuously test processes and implement changes where necessary

upvoted 1 times

shaitand 8 months, 1 week ago

So when you hire a contractor to install a door, you test the door BEFORE it is installed? No, you have to test after the contractor has implemented the door installation.

upvoted 1 times

J_Ko 3 months ago

I'm not sure this logic works -so that would mean you'd assume/trust the contractor he/she brought the right door with him/her and installed it correctly. And only then find out e.g. he/she installed the hinges the wrong way around and it won't open?
I'd check the door first, then put the door in the frame and test if it opens the right way around first before proceeding, with the locks, paint, etc, which imho is akin to a test environment or beta test?

upvoted 1 times

celomomo 9 months ago

Selected Answer: B

UAT is always involved in any change management. You have to ensure before implementing, the changes are doing what they are built to do. Why would you do a Business continuity for every change you are carrying out? That option is to catch you out. Unless it is abig change that could cause a big downtime, you would almost never always do Business Continuity testing but UAT is a MUST.

upvoted 2 times

lifesucks44 9 months, 1 week ago

Selected Answer: B

Not sure if the question was changed or what. But it says " Included in the change management process. " This is straight from the book. Test then Implement. I'm going with UAT Testing.

4. Test the change. Once the change is approved, it should be tested, preferably on a
nonproduction server. Testing helps verify that the change doesn't cause an unanticipated
problem.
5. Schedule and implement the change. The change is scheduled so that it can be implemented
with the least impact on the system and the system's customer. This may require
scheduling the change during off-duty
or nonpeak hours. Testing should discover any
problems, but it's still possible that the change causes unforeseen problems. Because of
this, it's important to have a rollback plan. This allows personnel to undo the change
and return the system to its previous state if necessary.

upvoted 4 times

babaseun 2 years, 3 months ago

Even a statement in 4. "Testing helps verify that the change doesn't cause an unanticipated problem" points to business continuity test

upvoted 1 times

dumdada 2 years ago

You're going to do a Business Continuity failover test every time you change a line of code? UAT test is plenty enough

upvoted 2 times

shaitand 8 months, 1 week ago

business continuity is not a failover test, it is simply a test to make sure business operations aren't impacted. This happens BEFORE closing the change. User acceptance merely confirms the user who requested the change is happy, that occurs AFTER implementation.

upvoted 1 times

celomomo 9 months ago

It is so funny that anyone thinks Business continuity test is done for every change lol. UAT is inevitable in Change manegement else, what are you changing if you are not sure it works the way it should? I agree with you Dumdada

upvoted 1 times

InclusiveSTEAM 9 months, 1 week ago

B is the answer.

B

Change management is a process that involves planning, controlling, and implementing changes to a system or process in a structured and controlled manner. User Acceptance Testing (UAT) is a critical component of change management because it ensures that proposed changes have been thoroughly tested and approved by end-users or stakeholders before they are implemented. UAT helps ensure that the changes will meet the business requirements and expectations.

While the other options (A, C, and D) may also be important in various aspects of IT and project management, they are not specific to change management.

Technical review by a business owner (Option A) may be part of the change approval process,

cost-benefit analysis (CBA) after implementation (Option C) may be part of post-implementation evaluation, and

business continuity testing (Option D) may be related to disaster recovery planning

upvoted 1 times

BestCommentorNA 9 months, 1 week ago

Selected Answer: B

I am a change manager.

B. User Acceptance Testing sometimes called beta testing or end-user testing, is a phase of software development in which the software is tested in the "real world" by the intended audience or business representative

D. Business Continuity Testing (or Business continuity planning) is related to disaster recovery. We perform validation testing after implementation. I think D is worded to trick you.

upvoted 1 times

bromings 1 year, 7 months ago

There's no BCT in change management

upvoted 1 times

bromings 9 months, 1 week ago

Change management involves a systematic approach to managing changes within an organization's IT infrastructure, processes, or systems. Among the options provided:

B. User Acceptance Testing (UAT) before implementation

User Acceptance Testing (UAT) is a critical phase within change management. It involves testing changes in a controlled environment to ensure that they meet business requirements and are acceptable to end-users or stakeholders before the changes are implemented into the production environment. UAT helps identify potential issues, gather feedback, and validate that the changes will perform as intended, minimizing risks associated with implementation.

While the other options mentioned (technical review by the business owner, cost-benefit analysis after implementation, business continuity testing) might be part of various stages in the change management process, UAT specifically focuses on testing changes before their deployment to ensure they meet user expectations and requirements.

upvoted 2 times

Kelly8023 9 months, 1 week ago

Selected Answer: B

My understanding is that change management includes request control, change control, release control, and configuration control. UAT before implementation is a key component included in release control. I would go with B.

upvoted 1 times

629f731 9 months, 1 week ago

Selected Answer: B

It is B. The question refers to what elements are part of change management, the elements are:

Schedule and communication plans.
Find project champions
User Acceptance Training (UAT)
Other types of training
Live communication
Support and feedback
Continuous learning
Success analysis

Therefore UAT is the correct answer. If the question were referring to what elements are necessary to maintain a BCP, these elements are:

Change management
Version control
Error accounting
upvoted 2 times

⊟ **deeden** 9 months, 1 week ago

Selected Answer: B

User Acceptance Testing (UAT)

is a crucial component of change management. It ensures that the change (new system, feature, or process) meets the end-users' requirements and expectations before it is fully implemented
upvoted 2 times

⊟ **Chris** 9 months, 1 week ago

Selected Answer: B

B. User Acceptance Testing (UAT) before implementation: UAT is a critical step in the change management process. It involves testing by the end-users to ensure that the system or changes meet their requirements and function correctly in a real-world scenario. This step is essential to validate that the changes will work as expected once deployed.
whiles Business continuity testing is part of business continuity planning and disaster recovery rather than the change management process. It ensures that critical business functions can continue during and after a disaster.

#ShadTech
upvoted 2 times

Question #14 *Topic 1*

A company is enrolled in a hard drive reuse program where decommissioned equipment is sold back to the vendor when it is no longer needed. The vendor pays more money for functioning drives than equipment that is no longer operational. Which method of data sanitization would provide the most secure means of preventing unauthorized data loss, while also receiving the most money from the vendor?

A. Pinning

B. Single-pass wipe

C. Multi-pass wipes

D. Degaussing

Suggested Answer: *C*

Community vote distribution

C (95%) 5%

franbarpro Highly Voted 2 years, 9 months ago

Selected Answer: C

I agree with given answer here "C"

Degaussing - once a drive has been degaussed, it can no longer be used.

Single Pass - replacing 0s and 1s might not be enough. With the right tools "in theory" some of the data can be recover

Muti-Pass - Gives us that "peace of mind" the data has been permanetly deleted.

upvoted 12 times

jackdryan 2 years, 2 months ago

C is correct

upvoted 2 times

Tau Most Recent 2 months, 2 weeks ago

Selected Answer: B

In this scenario, the goal is to securely remove data while preserving the drive's functionality to get the maximum resale value.

Single-pass wipe:

Overwrites all data once with random or fixed patterns.

Meets many regulatory standards for data sanitization.

Leaves the drive intact and operational, making it ideal for resale.

Why not the other options?
A. Pinning: Refers to mobile device security, like keeping apps or screens in view. Not related to data sanitization.

C. Multi-pass wipes:

More secure than single-pass but also more time-consuming and can stress the drive, reducing its lifespan.

Not necessary for most modern drives due to how data is stored.

D. Degaussing:

Uses a magnetic field to destroy data — but it also renders the drive inoperable.

So, you can’t resell it as functioning equipment.

upvoted 1 times

easyp 5 months ago

Selected Answer: B

B. Single-pass wipe

Explanation:

Security:

A single-pass wipe overwrites the data on the hard drive with random or specified data (e.g., all zeroes). This ensures the data is effectively erased and makes it virtually impossible for unauthorized recovery using standard techniques.

Drive Functionality:

Unlike degaussing or physically destroying the drive, a single-pass wipe preserves the operational integrity of the drive. This allows the hard drive to remain functional, maximizing the resale value to the vendor.

Efficiency:

A single-pass wipe is faster than multi-pass wiping methods, which perform multiple overwrites. Most modern studies suggest that a single overwrite is sufficient to prevent data recovery on modern drives.

Multi-pass wipes:

While multi-pass wipes offer slightly higher security, they are overkill for most modern hard drives, as a single-pass wipe is sufficient. Multi-pass wiping also takes significantly more time and could cause unnecessary wear on the drive.

upvoted 1 times

J_Ko 3 months ago

The question specifically states "most secure" -even if not by much, multiple passes are more secure than single pass. There is no time element in the question so C seems more appropriate in the given context. (they probably give the intern that thankless job :D)

upvoted 1 times

Whitehorse69 6 months, 3 weeks ago

Selected Answer: B

A single-pass wipe securely overwrites all data on a hard drive, rendering it unreadable, while preserving the functionality of the drive. This ensures the prevention of unauthorized data access while allowing the company to resell the drives in working condition for the maximum value.

upvoted 1 times

Moose01 6 months, 4 weeks ago

Selected Answer: C

Degaussing - the HDD can NOT be reused.

Single or Multi-Pass that data is erased and the HDD is reusable.

upvoted 1 times

KennethLZK 7 months, 3 weeks ago

Selected Answer: C

Degaussing is the best option if we are no longer using the drive but since the question i asking "reuse program" therefore C is the best option here.

upvoted 1 times

Chibueze 9 months ago

Selected Answer: D

Degaussing

upvoted 1 times

Vasyamba1 9 months, 1 week ago

Selected Answer: C

From the official study guide:

Degaussing a hard disk will normally destroy the electronics used to access the data. However, you won't have any assurance that all the data on the disk has actually been destroyed. Someone could open the drive in a clean room and install the platters on a different drive to read the data.

Purging is a more intense form of clearing that prepares media for reuse in less secure environments. It provides a level of assurance that the original data is not recoverable using any known methods. A purging process will repeat the clearing process multiple times and may combine it with another method, such as degaussing, to completely remove the data.

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: C

Degaussing basically disabled the drive

upvoted 1 times

⊟ **boxu03** 1 year, 3 months ago

D, most secure and the company still get the money

upvoted 2 times

⊟ **maawar83** 1 year, 5 months ago

Multi Pass might work for HDD.. but SSD and others does not...

for More Money, and IT Security Professional would rather get the money that it takes but keep data safe, therefore Degaussing should always be the answer.

Answer D.

upvoted 1 times

⊟ **InclusiveSTEAM** 1 year, 8 months ago

The most secure method of data sanitization in this scenario would typically be:

D. Degaussing

Degaussing involves exposing magnetic storage media to a strong magnetic field to completely erase the data. It's highly secure but renders the drives unusable for data storage.

While multi-pass wipes (Option C) can also provide a high level of data sanitization, they may still leave traces of data on the drive, which might be recoverable with specialized techniques

upvoted 2 times

⊟ **Vince_F_Fang** 1 year, 10 months ago

Selected Answer: C

I agree with given answer here "C".

Because Question has a limit "The vendor pays more money for functioning drives than equipment that is no longer operational". Degaussing make it can not be used, vendor must magnetizing before reuse. Otherwise I will choose D.

upvoted 2 times

⊟ **vorozco** 2 years ago

Selected Answer: C

Answer is C

upvoted 1 times

⊟ **BituBaba** 2 years, 2 months ago

degaussing, which uses a powerful magnetic field to erase data. Degaussing is generally considered the most secure form of data erasure, as it is impossible to recover any data once it has been degaussed.

upvoted 1 times

⊟ **1Kbit** 2 years, 6 months ago

C- Multi-pass wipes = data sanitization that involves writing over the data on a hard drive multiple times using a specific pattern of data.

upvoted 2 times

⊟ **Jamati** 2 years, 8 months ago

Selected Answer: C

Agreed, C

upvoted 1 times

Question #15 *Topic 1*

When reviewing vendor certifications for handling and processing of company data, which of the following is the BEST Service Organization Controls (SOC) certification for the vendor to possess?

A. SOC 1 Type 1

B. SOC 2 Type 1

C. SOC 2 Type 2

D. SOC 3

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **dev46** Highly Voted 👍 2 years, 3 months ago

C is correct - sharing my notes from Prabh Nair (check out his coffee shot video)

There is no type 1 or 2 for SOC 3, and it's used high-level report generally available on public domain/ website.

SOC 1 & 2 has type 1 and type 2. Type 1 is the design of control while Type 2 is the effectiveness of the control.

SOC 1 is good for financial/ books of account.

SOC 2 talks about IT

upvoted 14 times

⊟ **jackdryan** 1 year, 8 months ago

C is correct

upvoted 2 times

⊟ **36dd0ae** Most Recent ⏲ 1 month, 1 week ago

Selected Answer: C

SOC2 Type 2, it details that security controls were assessed by an external entity

upvoted 1 times

⊟ **AZSID** 7 months, 2 weeks ago

Selected Answer: C

SOC 2 Type 2

upvoted 2 times

⊟ **Jenkins3mol** 8 months ago

Selected Answer: C

C is the most detailed one and can validate that in the previous year the vendor performs fine according to soc 2 type 1 requirements

upvoted 1 times

⊟ **BituBaba** 1 year, 8 months ago

Answer is C:

When reviewing vendor certifications for handling and processing of company data, the best Service Organization Controls (SOC) certification for the vendor to possess is the SOC 2 Type II certification. This certification is the most stringent in regards to data security and privacy, and is the most highly sought after by companies. It provides assurance that the vendor has appropriate processes, procedures, and controls in place for the data that they process. It also provides assurance to customers that the vendor is upholding the standards set by the American Institute of Certified Public Accountants (AICPA). The SOC 2 Type II certification is the gold standard in regards to data security and privacy, and is the best certification a vendor can possess.

upvoted 3 times

⊟ **JohnyDal** 1 year, 11 months ago

I think the answer is D (SOC3) because SOC2 reports are always for internal mgmt, not for outsiders. Here, we are the outsiders and the organization will only share SOC3 with us. SOC3 reports are always type-II.

upvoted 2 times

Overizzy 2 years, 1 month ago

Selected Answer: C

C is my answer based on he data protection purposes of SOC 2 type ii

SOC 2 offers a Type 1 and Type 2 report.

The Type 1 report is a point-in-time snapshot of your organization’s controls, validated by tests to determine if the controls are designed appropriately.

The Type 2 report looks at the effectiveness of those same controls over a more extended period - usually 12 months.

upvoted 3 times

Eltooth 2 years, 2 months ago

Selected Answer: C

C is correct answer.

upvoted 1 times

DButtare 2 years, 3 months ago

Selected Answer: C

Data handling is SOC2 type 1 or 2 but type 2 is prefered.
SOC 2 Type II (3 - 12 months monitoring period).
Assesses the effectiveness of security processes by observing operations for at least three months. 6 - 12 months recommended.

upvoted 2 times

franbarpro 2 years, 3 months ago

Selected Answer: C

Yep - I like C

upvoted 2 times

kazeiya 2 years, 3 months ago

Selected Answer: C

C is correct

upvoted 3 times

Question #16 *Topic 1*

Which application type is considered high risk and provides a common way for malware and viruses to enter a network?

A. Instant messaging or chat applications

B. Peer-to-Peer (P2P) file sharing applications

C. E-mail applications

D. End-to-end applications

Suggested Answer: *B*

Community vote distribution

B (80%) 10% 10%

36dd0ae 1 month, 1 week ago

Selected Answer: C

Went with C (email applications) but after rereading the question agree that B (P2P) is the right answer since no where in the question it mentions corporate network, keywords are high risk, network and common way

upvoted 1 times

tsummey 9 months, 3 weeks ago

Selected Answer: C

I'm going with C. The question does not mention anything about corporate or business. Using P2P isn't as common as Chat or Email. Email has a larger attack surface than Chat.

upvoted 1 times

KennethLZK 7 months, 3 weeks ago

But in the modern security we have email security measures to detect and block malicious email. Whereas P2P still quite high-risk even now.

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: B

I believe I read this from our code of conduct

upvoted 1 times

Koko4Kosh 1 year, 4 months ago

Selected Answer: A

The key word here (I believe) is Common. Not common for business to have P2P installed on corp devices. But chat sure is.

upvoted 1 times

febd35a 1 year, 3 months ago

but it doesn't say the application is common, it says the application provides a common way for malware to enter a network.

upvoted 1 times

vorozco 2 years ago

Selected Answer: B

B is correct

upvoted 1 times

cccispman 2 years, 6 months ago

Agreed B is highly likely to be correct. I was tempted to select email.
Another reason why I go with B is because option D is positioned to trick the candidate.

"D. End-to-end applications" closest match to P2P, so answer is B

upvoted 3 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 1 times

Ivanchun 2 years, 6 months ago

Selected Answer: B

Same as Torrent -> P2P

upvoted 3 times

Eltooth 2 years, 8 months ago

Selected Answer: B

B is correct answer. P2P file sharing.

upvoted 1 times

JAckThePip 2 years, 9 months ago

Answer is B

"Eliminating unsecured file shares, which are a common way for malware to spread"

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf

upvoted 3 times

> **febd35a** 1 year, 3 months ago
>
> I believe eliminating unsecured file shares in that context would be like a shared drive on the network that isn't secure. If you have a SAN that doesn't require authentication (isn't secured) that would be a problem.
>
> upvoted 2 times

dev46 2 years, 9 months ago

P2P sounds good

The question ask about application type. The keyword is "type". So, D will be eliminated straight away.

Among A, B and C - PGP can be used for email protection and I can't recall but there is protection for chat app too.

P2P such as torrent is the risky one.

upvoted 3 times

DButtare 2 years, 9 months ago

Selected Answer: B

P2P is a vehicle of spyware, viruses, Trojan horses, worms

upvoted 3 times

franbarpro 2 years, 9 months ago

P2P file sharing is the process of sharing and transferring digital files from one computer to another.

If you aren't careful, P2P file sharing can subject you to spyware, viruses, Trojan horses, worms and identity theft. Some P2P applications can even modify or penetrate your computer's firewall without detection.

upvoted 2 times

Question #17 *Topic 1*

An organization is looking to include mobile devices in its asset management system for better tracking. In which system tier of the reference architecture would mobile devices be tracked?

A. 0

B. 1

C. 2

D. 3

Suggested Answer: *A*

Community vote distribution

B (45%) D (25%) C (16%) 14%

mark9999 Highly Voted 2 years, 8 months ago

Selected Answer: B

Although I went for B:
I assume they're talking about the IT Asset Management(ITAM) Tiers of which there are three:
So there is no Tier 0
Tier 1 - Asset Data Collection - method to inventory every software application and virtual OS that runs on the hardware you have in your inventory
Tier 2 - Asset Data Intelligence - normalize the information, to map the assets to relevant information, and to link the assets to their contracts, projects, departments, and people.
Tier 3 - Asset Lifecycle management - processes that control how you purchase, procure, and dispose of IT assets. This includes virtual devices and software, along with the associated software licenses.

NIST has it as
Tier 1 - Reporting, Analytics, Data storage
Tier 2 - Data collection ie location/HW/SW
Tier 3 - Enterprise assets - Servers, workstations, Laptops etc

So for tracking mobile devices, according to these it could be Tier 3 as the diagrams seem to work backwards to what you would expect (devices at level 1 etc)

upvoted 17 times

jackdryan 2 years, 2 months ago

D is correct

upvoted 3 times

djedwards Most Recent 1 week, 5 days ago

Selected Answer: A

Tier 0: Physical Layer
. - This layer includes the actual mobile devices (smartphones, tablets, etc.) and other physical assets that need to be tracked. It's where the initial data about the asset is collected, such as its identification, location, and status.

upvoted 1 times

Dean1403 3 weeks, 4 days ago

Selected Answer: B

When you include mobile devices to your Asset management system they are included as part of your organization's IT infrastructure, which change how they're classified in the reference architecture. In most reference architectures (such as NIST, DOD, or enterprise IT models), moblie devices fall under Tier1 = Client Trier (or Endpoint tier)

upvoted 1 times

36dd0ae 1 month, 1 week ago

Selected Answer: A

Tier	**Description**	**Examples**
0	**Physical process / field devices**	Sensors, actuators, **mobile devices**, physical equipment

| **1** | **Basic control** | PLCs, embedded controllers |

| **2** | **Supervisory control** | SCADA, HMI |

| **3** | **Operations management** | MES (Manufacturing Execution Systems), batch management |

| **4** | **Enterprise level** | ERP systems, business planning |

upvoted 2 times

b0145c1 1 month, 3 weeks ago

Selected Answer: B

Tier 1 generally deals with primary assets that require direct management and oversight. Mobile devices, as part of the organization's core IT infrastructure, would be tracked here for better visibility, security, and lifecycle management.

A. 0: This tier is typically reserved for core infrastructure or foundational components that form the backbone of the system, like servers or core network devices.
C. 2: This tier may represent secondary systems or systems that interface with Tier 1 systems but aren't directly responsible for asset management.
D. 3: Tier 3 is typically used for external or peripheral systems such as user devices that don't require the same level of management as primary assets.

upvoted 1 times

Tau 2 months, 2 weeks ago

Selected Answer: A

In reference architecture models (like those used in industrial control systems or enterprise IT architecture), the tiers typically represent layers of control and responsibility. Here's how Tier 0 fits:

Tier 0 includes the physical assets and endpoints — such as:

Servers

Workstations

Mobile devices

Sensors and field devices (in ICS environments)

Tracking mobile devices as physical assets places them in Tier 0, where asset management and inventory control operate at the device level.

upvoted 1 times

46f752c 2 months, 4 weeks ago

Selected Answer: D

In the reference architecture model (like the Purdue Enterprise Reference Architecture, often used in cybersecurity and ICS/SCADA environments), the tiers or levels are generally defined as:

Level 0: Physical processes (sensors, actuators)

Level 1: Intelligent devices (PLCs, RTUs)

Level 2: Control systems (SCADA, HMIs)

Level 3: Operations and asset management (production workflows, tracking, data collection)

Level 4: Business planning and logistics (ERP, corporate IT)

Since the question involves tracking mobile devices using an asset management system, that clearly places it in:

□ Level 3 – the Operations and Supervisory level, which is responsible for asset tracking, monitoring, and management systems.

So again, the correct answer is: D. 3

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: B

There is no mention of NIST tiers, so assuming ITAM tiers, the answer is B.

Mobile devices would be tracked starting from ITAM Tier 1 (for basic discovery) and continue through Tier 2 (for ongoing management and lifecycle tracking).

upvoted 1 times

5daa92f 6 months ago

Selected Answer: A

Explanation:
In reference architectures, Tier 0 typically represents the physical layer of the architecture, which includes devices such as sensors, actuators, and mobile devices. This layer is responsible for directly interacting with the physical environment and providing data to higher tiers for processing and analysis.

For mobile devices, they are considered part of the asset layer that needs to be tracked and managed, making them belong to Tier 0 in most reference architectures.

Breakdown of Tiers:
Tier 0: Physical devices and endpoints (e.g., mobile devices, sensors, and other assets).
Tier 1: Edge processing, where data from Tier 0 is collected, processed, or aggregated locally.
Tier 2: Centralized systems for data management and processing, like enterprise servers.
Tier 3: Business and analytics applications that leverage processed data for decision-making.
Tracking mobile devices in an asset management system starts at the Tier 0 level, where their identification, status, and usage data are collected.

upvoted 1 times

attesco 6 months, 1 week ago

Selected Answer: D

You guys should stop confusing people. The Right Answer is D. Read the NIST pub below

upvoted 1 times

Tuhaar 6 months, 2 weeks ago

Selected Answer: D

Tier 3 as per NIST: Explanation:
According to the NIST SP 1800-5 Vol B guidelines, Tier 3 is where mobile devices are actively tracked and managed using Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) systems. This tier is responsible for managing the devices, monitoring their status, ensuring compliance with security policies, and making real-time decisions regarding their security posture.

upvoted 3 times

Ravnit 6 months, 2 weeks ago

Selected Answer: B

n the context of a reference architecture for tracking assets, mobile devices would typically be tracked in System Tier 1. This tier focuses on managing all end-user devices, including mobile devices, ensuring they are properly configured, secured, and monitored. So B is the right response

upvoted 1 times

Moose01 6 months, 4 weeks ago

Selected Answer: B

Per Google search: In a typical reference architecture, mobile devices would be tracked within the "Access" or "Presentation" tier as this layer represents the user interface and directly interacts with end-user devices like smartphones and tablets, where data is accessed and displayed.
Key points about the access tier:
Direct user interaction:
This tier is where users interact with applications through their mobile devices, sending requests and receiving responses.
Data presentation:
The access tier is responsible for presenting data in a user-friendly format on the mobile device screen.
Security considerations:
Due to the direct user interaction, this tier requires robust security measures to protect sensitive data on mobile devices.

upvoted 1 times

Tuhaar 7 months ago

Selected Answer: B

According to the NIST (National Institute of Standards and Technology) reference architecture, mobile devices would be tracked in Tier 1.

Here's a brief overview of the tiers:

Tier 0: This tier typically includes the physical infrastructure, such as hardware and network components.

Tier 1: This tier includes the platform infrastructure, which encompasses operating systems, middleware, and mobile devices.

Tier 2: This tier focuses on the application infrastructure, including applications and software services.

Tier 3: This tier involves the business processes and information systems that support organizational operations.

upvoted 2 times

Fouad777 7 months, 2 weeks ago

Answer id B

Tier 0: Facilities, power systems, and environmental controls.

Tier 1: Hardware and software supporting IT infrastructure.

Tier 2: Shared services like email, directories, and collaboration tools.

Tier 3: Business-critical systems and databases.

upvoted 1 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: D

NIST ITAM Reference Architecture clearly states these would fall into Tier 3 systems.

Tier 3 - Enterprise assets - Servers, workstations, Laptops etc

upvoted 2 times

M_MUN17 8 months, 3 weeks ago

The correct answer is A. 0.

In a typical reference architecture, Tier 0 refers to the physical devices or endpoints, including mobile devices, that interact directly with the environment. Mobile devices, as physical assets, would be tracked in this tier because they represent the lowest level in the architecture, where the hardware and direct interfaces with the system occur.

Tiers 1, 2, and 3 typically deal with higher levels of abstraction, such as applications, data processing, and overall system management.

upvoted 2 times

Question #18 *Topic 1*

Which of the following is the BEST way to protect an organization's data assets?

A. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.

B. Monitor and enforce adherence to security policies.

C. Require Multi-Factor Authentication (MFA) and Separation of Duties (SoD).

D. Create the Demilitarized Zone (DMZ) with proxies, firewalls and hardened bastion hosts.

Suggested Answer: *A*

Community vote distribution

B (52%) A (48%)

⊟ **godchild** Highly Voted 👍 2 years, 9 months ago

policy vs encryption = management vs technical staff. Which is more important?

I choose policy because CISSP needs you to think like a manager..

upvoted 39 times

⊟ **wins34** 1 year, 4 months ago

in option B . There is no clear indication as they are secure policies. So can't trust those policies if they are outdated.

upvoted 2 times

⊟ **Cosy** 2 months, 1 week ago

Thats why you should "monitor"

upvoted 2 times

⊟ **jackdryan** 2 years, 2 months ago

B is correct

upvoted 4 times

⊟ **franbarpro** 2 years, 9 months ago

Having a hardtime to understand how "Security Policies" could be the BEST way to protect an organization's data assets.
If we don't have technical controls in place - users tend to just do whetervar. Imagine having a policy that says change your password every 90 days. How many people will do that? But if GPO expires their password.... they will change it right way.

upvoted 7 times

⊟ **Yohanes411** 5 months, 3 weeks ago

For you to have the technical controls in place, you must have already developed policies and procedures which lay the foundation for how the technical controls are to be implemented. Technical control implementation is the reflection of your policies.

upvoted 1 times

⊟ **FredDurst** 9 months, 1 week ago

SOLID B .... it's more like changing the culture . Even if you use encryption at rest or in transit they can write the data down on a a sticky note , share their screen with third parties , use their cellphone and take snaps of their work computer with confidential data displayed , get hooked on a social engineering scam etc . It all boils down to the the people at the end of the day and their respect for the policy either through pure logic or out of fear of disciplinary actions (enforcement) .

upvoted 9 times

⊟ **N0Ob1e** 2 years, 9 months ago

But if you don't have any policy to say when passwords should expire, would they never expire?

Policy > Standards > Guidelines > Procedure

upvoted 8 times

⊟ **DButtare** Highly Voted 👍 2 years, 9 months ago

Selected Answer: B

I'm for the "B", encryption is part of the policy.

upvoted 12 times

T_dawg Most Recent 4 weeks, 1 day ago

Selected Answer: B

Protecting data is not only protecting the confidentiality (encryption). It does not guarantee availability or integrity.

upvoted 1 times

cjace 1 month, 2 weeks ago

Selected Answer: A

A. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.

Here's why:

While all the options listed are important components of a comprehensive security strategy, encryption directly protects the confidentiality and integrity of data, even if other defenses fail. It ensures that:

Data in transit (e.g., over networks) is protected from interception.

Data at rest (e.g., on servers or storage devices) is protected from unauthorized access.

Modern cryptographic algorithms reduce the risk of data being compromised due to outdated or weak encryption.

upvoted 1 times

SH_ 3 months, 2 weeks ago

Selected Answer: B

B encompasses the others.

upvoted 2 times

CKaraf 3 months, 3 weeks ago

Selected Answer: A

A is the proactive method. B the reactive. A is preferred

upvoted 1 times

HazRic 3 months, 3 weeks ago

Selected Answer: A

Encrypting data in transit and at rest ensures that even if attackers intercept or access the data, they cannot read or misuse it without the decryption keys. This directly protects the confidentiality and integrity of the data itself, which is the core of safeguarding data assets.

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: A

While monitoring and enforcing security policies (option B) is crucial for overall security, encryption directly protects the confidentiality and integrity of data by ensuring that unauthorized individuals cannot access or alter the data. Encryption of both data in transit and data at rest provides a robust layer of protection, especially in case of data breaches or unauthorized access.

In contrast, enforcing security policies (option B) helps manage and guide actions, but without encryption, data might still be vulnerable even if policies are in place.

Therefore, option A is the best choice

upvoted 1 times

karincauk 4 months, 3 weeks ago

Selected Answer: A

The best answer is:

A. Encrypt data in transit and at rest using up-to-date cryptographic algorithms.

Explanation:

While all the options contribute to security, encryption is the most fundamental and effective way to protect data assets from unauthorized access, even if other security controls fail. Proper encryption ensures data confidentiality and integrity, whether it is stored (at rest) or transmitted (in transit).

- B (Monitor and enforce adherence to security policies): This is important but does not directly protect data assets—it's more about governance and compliance.
- C (Require MFA and Separation of Duties): These measures strengthen access control but do not directly protect data at rest or in transit.
- D (Create a DMZ with proxies, firewalls, and bastion hosts): This helps protect network boundaries but does not directly safeguard stored or transmitted data.

Encryption remains the most effective safeguard for data security across various attack vectors.

upvoted 2 times

Bau24 4 months, 3 weeks ago

Selected Answer: A

Encryption only PROTECTS data

upvoted 1 times

easyp 5 months ago

Selected Answer: B

Think like a manager

upvoted 2 times

Yohanes411 5 months, 3 weeks ago

Selected Answer: B

Policies lay the groundwork for all the other options mentioned.

upvoted 1 times

imather 6 months ago

Selected Answer: B

B. A, C, and D are all valid ways to protect data assets. B is the one solution that can implement all of them.

upvoted 1 times

Scheds 6 months ago

Selected Answer: B

When choosing answers, the order of priority should be People, Processes, Technology....Technology usually goes last. Think like a manager on this one.

upvoted 1 times

V_raven 6 months, 2 weeks ago

Selected Answer: B

Choose b as security policies may include using encryption. B in all encompassing and is a managerial selection vs a technical one.

upvoted 2 times

Moose01 6 months, 4 weeks ago

Selected Answer: A

you put your gold in the safe and then you make sure who can have access to safe , when and how.

secure, safe guard and enforce

A is the right answer.

upvoted 1 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: B

Think like a CEO, it's B - policy

upvoted 2 times

Question #19 *Topic 1*

Within a large organization, what business unit is BEST positioned to initiate provisioning and deprovisioning of user accounts?

A. Training department

B. Internal audit

C. Human resources

D. Information technology (IT)

Suggested Answer: *C*

Community vote distribution

C (86%) 14%

DButtare Highly Voted 2 years, 9 months ago

Selected Answer: C

Initiate not create / grant

upvoted 22 times

> **jackdryan** 2 years, 2 months ago
>
> C is correct
>
> upvoted 1 times

franbarpro Highly Voted 2 years, 9 months ago

Selected Answer: C

Agreed

upvoted 6 times

HazRic Most Recent 3 months, 3 weeks ago

Selected Answer: D

The Information Technology (IT) department is best positioned to handle provisioning and deprovisioning of user accounts because it has the technical expertise, tools, and responsibility for managing access to systems and data. IT ensures accounts are created, modified, or removed securely and efficiently. While HR may notify IT of employee changes, IT executes the technical aspects of account management.

upvoted 2 times

RVP20 6 months, 3 weeks ago

Selected Answer: D

While Human Resources (HR) plays a critical role in managing employee lifecycle information (such as hiring, role changes, and terminations), the Information Technology (IT) department is ultimately responsible for the technical execution of user account provisioning and deprovisioning in most organizations. This aligns with CISSP principles of managing access control and system security, which falls under IT's domain.

So, I think :) IT is the better choice from a CISSP perspective.

upvoted 1 times

Bietchasup 7 months, 1 week ago

D. since when did HR create user accounts? yes the onboard but once they have been cleared by HR. Paperwork is sent to IT DEP to create a user account through IAM and can then be assigned access control or GPO, yay or nay?

upvoted 1 times

Dtony66 1 year, 1 month ago

If the criterion is HR is "initiating", would it not actually be the hiring manager of the department deciding to hire or fire the employee. Poor question.

upvoted 2 times

suspense 1 year, 4 months ago

In THORS questions it was similar question and the answer was IT Administrator. Reason that HR doesnt touch creaetion of IT accounts. Now it is HT as correct answer... How can I answer correctly???

upvoted 2 times

shmoeee 1 year, 7 months ago

It's C...a hard C

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: D

The business unit that is BEST positioned to initiate provisioning and deprovisioning of user accounts within a large organization is the Information Technology (IT) department (option D).

Provisioning and deprovisioning of user accounts involve managing access to various systems, applications, and resources within an organization. This process typically involves creating user accounts, granting appropriate permissions, and ensuring access is provided based on business requirements and security policies.

The IT department is responsible for managing the organization's technology infrastructure, including user accounts and access controls.

while other business units may have a role in the overall user account lifecycle (e.g., the HR department may provide employee information to initiate account creation), the IT department is typically responsible for implementing and enforcing access controls, managing user accounts, and ensuring the proper provisioning and deprovisioning of user accounts based on organizational policies and procedures.

upvoted 5 times

vorozco 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

Ivanchun 2 years, 6 months ago

Selected Answer: C

First slight D, but it say initiate not perform change to C

upvoted 2 times

Eltooth 2 years, 8 months ago

Selected Answer: C

C is correct answer. HR

upvoted 1 times

Cww1 2 years, 9 months ago

Correct

upvoted 2 times

Question #20 *Topic 1*

Which of the following is the PRIMARY purpose of installing a mantrap within a facility?

A. Control traffic

B. Control air flow

C. Prevent piggybacking

D. Prevent rapid movement

Suggested Answer: *C*

Community vote distribution

C (100%)

kurili 2 months, 2 weeks ago

Selected Answer: C

detects more than one person in the mantrap, sounds audible alarm and instructions, and will not open secure door until the second 'piggybacking' user has exited the mantrap through the public door, allowing the first user to access the secure area. Once the secure door has closed, the system will allow the second person to enter the mantrap and provide their credentials

upvoted 1 times

somsom 8 months, 2 weeks ago

A is correct

upvoted 1 times

Bach1968 9 months, 1 week ago

Selected Answer: C

The main objective of a mantrap is to prevent piggybacking, which refers to unauthorized individuals following closely behind an authorized person to gain entry to a restricted area without proper authentication. By allowing only one person at a time, the mantrap ensures that each individual must present their credentials, such as an access card or biometric identification, before proceeding further into the secure area.

upvoted 3 times

> **Chibueze** 9 months ago
>
> what you defined here is tailgating, not piggybacking
>
> upvoted 2 times

> **Hackermayne** 1 year, 5 months ago
>
> Your description isn't entirely correct, you're describing tailgating. Piggybacking is similar except its generally an unauthorized person allowing someone in, assuming they're supposed to be there. i.e. its the difference between scurrying in while the doors open (tailgating) and having a staff member hold the door open because you're carrying a large box of donuts (piggybacking)
>
> upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: C

ain't that obvious?

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: C

Control traffic and Prevent Rapid Movement are not a final specific end goal, the concepts are too vague.

upvoted 1 times

shmoeee 1 year, 7 months ago

If you see piggybacking or tailgating, choose that

upvoted 2 times

vorozco 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

⊟ **Ivanchun** 2 years, 6 months ago

Selected Answer: C

Piggybacking, no other option

upvoted 1 times

⊟ **jackdryan** 2 years, 2 months ago

C is correct

upvoted 1 times

⊟ **Eltooth** 2 years, 8 months ago

Selected Answer: C

C is correct answer. Piggybacking.

upvoted 1 times

⊟ **DButtare** 2 years, 9 months ago

Selected Answer: C

Tight space

upvoted 1 times

⊟ **MSKid** 2 years, 9 months ago

Selected Answer: C

Agreed

upvoted 2 times

⊟ **franbarpro** 2 years, 9 months ago

Selected Answer: C

piggybacking, similar to tailgating, refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.

upvoted 4 times

Question #21 *Topic 1*

In the "Do" phase of the Plan-Do-Check-Act model, which of the following is performed?

A. Maintain and improve the Business Continuity Management (BCM) system by taking corrective action, based on the results of management review.

B. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.

C. Ensure the business continuity policy, controls, processes, and procedures have been implemented.

D. Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established.

Suggested Answer: *C*

Community vote distribution

C (63%) B (34%)

Joey456 Highly Voted 2 years, 9 months ago

Plan = Plan

Do = Perform

Act = Improve

Check = Monitor

PLAN - D. Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established.

DO - C. Ensure the business continuity policy, controls, processes, and procedures have been implemented.

ACT - A. Maintain and improve the Business Continuity Management (BCM) system by taking corrective action, based on the results of management review.

Check - B. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.

upvoted 40 times

jackdryan 2 years, 2 months ago

C is correct

upvoted 4 times

SF_NERD Highly Voted 2 years, 9 months ago

Selected Answer: B

PLAN:

• D. Ensure that business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity have been established.

Do

• B. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.

Check

• C. Ensure the business continuity policy, controls, processes, and procedures have been implemented.

Act

• A. Maintain and improve the Business Continuity Management (BCM) system by taking corrective action, based on the results of management review.

Plan

This is the ONLY sensical flow of these steps giving "B" as the Do step/answer

upvoted 5 times

somsom Most Recent 8 months, 2 weeks ago

C is very correct. Monitoring is same check or analyze or examine.

upvoted 1 times

celomomo 9 months ago

Selected Answer: C

option C. It focuses on the implementation of the plans and processes that were developed, which is the core purpose of this phase in the model.

Layer 0: The most trusted layer, where the operating system kernel resides

Layer 1: Contains nonprivileged parts of the operating system

Layer 2: Contains I/O drivers, low-level operations, and utilities

Layer 3: Contains applications and processes

upvoted 1 times

robervalchocolat 10 months ago

Plan: This phase involves defining the problem, setting goals, and creating a plan to address the issue.

Do: This phase is where the plan is implemented and executed. In the context of business continuity management, this involves ensuring that the established policies, controls, processes, and procedures are put into action.

Check: This phase involves monitoring and reviewing the results of the implementation to determine if the plan is working as intended.

Act: This phase involves taking corrective action based on the findings of the check phase, and making improvements to the plan.

upvoted 1 times

deeden 11 months ago

Selected Answer: C

1. **Plan.** Decide what needs to be done, establish the objectives, and determine the processes needed to implement the change.

2. **Do.** Execute the plan.

3. **Check.** Evaluate the results of the plan. This may happen through the use of statistical measures of performance, observations, or evaluations.

4. **Act (or Adjust).** Based on the information generated in the **Do** and **Check** phases (i.e., root causes of failure identified), risk is re-evaluated — and the baseline is determined to measure performance of future changes (adjust).

upvoted 1 times

JazzF 11 months ago

Selected Answer: C

Do: Implementing the ISMS

This phase is where an organisation implements the ISMS policy, controls, processes, and procedures. In the Do phase, an organisation conducts a risk assessment and evaluates the reasons behind each structure. They must prepare procedures indicating the risks and their treatment. Ensuring that the procedure and policy documents are available, adequately protected, distributed, and stored in a managed system is crucial. Documents of external origin must also fall under the scope of ISMS 27001. This is how the Do phase is accomplished.

upvoted 1 times

rami_mma 11 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

rami_mma 11 months, 1 week ago

Plan -> D

Do -> C

Act -> A

Check -> B

upvoted 1 times

susmit683 1 year, 5 months ago

Selected Answer: C

Implement following the Security Policies is "DO"

upvoted 1 times

[Removed] 1 year, 7 months ago

Is this even in the OSG?

upvoted 1 times

AlexJacobson 1 year, 7 months ago

No, it's not, but it's in Official Guide to CISSP CBK Reference (5th edition). I only used Sybex book and Destionation CISSP book (along with their mind maps on YT), but I think that's not enough. I'm seeing questions here that are more and more referencing the Official CBK.

upvoted 1 times

⊟ **J_Ko** 3 months ago

FWIW it is in the McGraw-Hill AIO 9th edition ch. 19.

upvoted 1 times

⊟ **74gjd_37** 1 year, 9 months ago

Selected Answer: B

B is the correct answer.

See https://www.mindtools.com/as2l5i1/pdca-plan-do-check-act

2. Do

Once you've identified a potential solution, test it safely with a small-scale pilot project. This will show whether your proposed changes achieve the desired outcome – with minimal disruption to the rest of your operation if they don't. For example, you could organize a trial within a department, in a limited geographical area, or with a particular demographic.

As you run the pilot project, gather data to show whether the change has worked or not. You'll use this in the next stage.

upvoted 1 times

⊟ **Sledge_Hammer** 1 year, 9 months ago

B is the correct answer.
The next step is to test your hypothesis (i.e., your proposed solution). The PDCA cycle focuses on smaller, incremental changes that help improve processes with minimal disruption.

Test your hypothesis with a small-scale project, preferably in a controlled environment, so you can evaluate the results without interrupting the rest of your operation. You might want to test the solution on one team or within a certain demographic.

upvoted 1 times

⊟ **Demo25** 1 year, 11 months ago

Selected Answer: B

1
The answer is B. Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.

The Do phase of the Plan-Do-Check-Act model is the second phase of the cycle. In this phase, the plan is implemented and the results are monitored. The goal of the Do phase is to ensure that the plan is working as expected and that it is meeting the organization's objectives.

upvoted 1 times

⊟ **Bach1968** 1 year, 12 months ago

Selected Answer: C

in the "Do" phase of the PDCA model, option C is performed, which focuses on the implementation of business continuity policies, controls, processes, and procedures.

upvoted 1 times

⊟ **KelvinYau** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

⊟ **RVoigt** 2 years, 5 months ago

Selected Answer: C

Look at the verbs:
Plan - Established
DO - IMPLEMENTED
Act - Maintain and improve
Check - Monitor and review

upvoted 3 times

Question #22 *Topic 1*

What industry-recognized document could be used as a baseline reference that is related to data security and business operations or conducting a security assessment?

A. Service Organization Control (SOC) 1 Type 2

B. Service Organization Control (SOC) 1 Type 1

C. Service Organization Control (SOC) 2 Type 2

D. Service Organization Control (SOC) 2 Type 1

Suggested Answer: *D*

Community vote distribution

D (83%) C (17%)

Toa Highly Voted 👍 2 years, 9 months ago

Answer D:
The difference between SOC 2 Type i and Soc 2 Type ii reports lies in the period of time each covers.

SOC 2 Type 1, often an organization's first-ever SOC 2 report, looks at internal controls governing data security and privacy at the time of the audit.
SOC 2 Type 2 reports discuss the effectiveness of your organization's information security and privacy controls since your last SOC audit, which typically means one year.
The two types of reports are used differently by organizations:

SOC 2 Type 1 takes a "snapshot-in-time" approach, setting a baseline for future audits of your service organization's system.
SOC 2 Type 2 asks how well your data security and privacy controls have worked since your last SOC 2 audit.
So, the audit procedure most organizations follow is:

Type 1 for the first SOC 2 audit
Type 2 for subsequent SOC 2 audits.

https://reciprocity.com/resources/what-is-a-soc-2-type-2-audit/

upvoted 17 times

jackdryan 2 years, 2 months ago

D is correct

upvoted 1 times

MSKid Highly Voted 👍 2 years, 9 months ago

Selected Answer: D

SOC 2 Audits are not shared publicly unless a NDA is given, so this would work for an internal audit that would not be shared outside the organization | Type 1 report would cover a point in time providing a baseline per the question

upvoted 8 times

b0145c1 Most Recent ⏱ 1 month, 3 weeks ago

Selected Answer: C

SOC 2 Type 2 sounds more accurate

upvoted 2 times

Tau 2 months, 2 weeks ago

Selected Answer: C

C. Service Organization Control (SOC) 2 Type 2

SOC 2 Type 2 reports are focused on data security and privacy and are often used as a baseline reference when conducting a security assessment. These reports assess the effectiveness of a service organization's controls related to security, availability, processing integrity, confidentiality, and privacy over a period of time (usually 6-12 months), making it highly relevant for evaluating data security and business operations.

upvoted 2 times

BigITGuy 2 months, 4 weeks ago

Selected Answer: D

Keyword is 'baseline'.

upvoted 1 times

ziyaetuk 7 months, 1 week ago

Selected Answer: D

The word is "baseline reference". So it's D. It was an elaborate request that will take time, I will go with C. Say you need to demonstrate compliance ASAP because an important enterprise prospect requires it to close the deal. But your company is too young to have formal systems in place, or you've recently made major changes to your data security systems. Instead of waiting for a Type 2 report, a Type 1 report that evaluates your information security controls as they stand today can act as a short-term solution, which defines the base-line.

upvoted 2 times

M_MUN17 8 months, 3 weeks ago

The correct answer is C. Service Organization Control (SOC) 2 Type 2.

SOC 2 Type 2 is an industry-recognized report that focuses on an organization's controls related to data security, availability, processing integrity, confidentiality, and privacy over a period of time. It provides detailed insights into how an organization maintains security and compliance in these areas, making it an ideal baseline reference for conducting a security assessment or evaluating data security practices.

The other options focus on different aspects:

SOC 1 reports are primarily concerned with the internal controls over financial reporting (ICFR), not data security.

SOC 2 Type 1 assesses the design of controls at a specific point in time, while SOC 2 Type 2 covers both the design and operating effectiveness of controls over an extended period, which is more comprehensive for security assessments.

upvoted 3 times

robervalchocolat 10 months ago

Given that the question asks for a document related to data security and business operations, SOC 2 Type 2 is the most appropriate choice. It provides evidence of the effectiveness of controls related to security, availability, processing integrity, confidentiality, or privacy, which are all critical aspects of data security and business operations.

upvoted 1 times

isaphiltrick 10 months, 2 weeks ago

Selected Answer: C

SOC 2 Type 2 reports provide a more comprehensive evaluation of an organization's controls related to security, availability, processing integrity, confidentiality, and privacy. Unlike SOC 2 Type 1, which only assesses the design and implementation of controls at a specific point in time, SOC 2 Type 2 evaluates the operating effectiveness of these controls over an extended period, typically six months to a year. This ongoing assessment offers greater assurance about the reliability and consistency of the controls, making it a better baseline for evaluating data security and business operations.

upvoted 1 times

deeden 11 months ago

Selected Answer: D

Agree with D because of the key word "baseline" Type I can be use as a point in time reference, then observe the system for 6-12 months to complete a Type II report.

upvoted 1 times

Vaneck 1 year, 3 months ago

For a basic reference related to data security and business operations or conducting a security assessment, the industry-recognized document that could be used is :

C. Service Organization Control (SOC) 2 Type 2.

SOC 2 reports are designed to assess an organization's controls over the security, availability, processing integrity, confidentiality and privacy of the systems used to process user data. A SOC 2 Type 2 report not only provides a description of the controls in place, but also assesses the effectiveness of these controls over a period of time, offering substantial assurance on how well a company secures data against established trust criteria.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: D

Answer D) SOC 2 Type I

Sets a baseline for future audits

Describes the organization’s system and the suitability of controls

Takes a “snapshot-in-time” approach

upvoted 3 times

⊟ **Bach1968** 1 year, 12 months ago

Selected Answer: C

Among the options provided, the industry-recognized document that could be used as a baseline reference related to data security, business operations, and conducting a security assessment is option C, Service Organization Control (SOC) 2 Type 2.

SOC reports are a set of independent audit reports created by the American Institute of Certified Public Accountants (AICPA) to assess the controls and security practices of service organizations. SOC 2 specifically focuses on the Trust Services Criteria, which include security, availability, processing integrity, confidentiality, and privacy.

upvoted 2 times

⊟ **jackdryan** 2 years, 2 months ago

D is correct

upvoted 1 times

⊟ **rootic** 2 years, 8 months ago

Selected Answer: D

Answer is D.

upvoted 1 times

⊟ **DButtare** 2 years, 9 months ago

Baseline -> Type 1

upvoted 3 times

⊟ **jon1991** 2 years, 9 months ago

Selected Answer: D

The answer should be - D - Baseline reference seems to be the keyword here, At specific point in time.

upvoted 5 times

Question #23 *Topic 1*

A criminal organization is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the organization?

A. Organization loses control of their network devices.

B. Network is flooded with communication traffic by the attacker.

C. Network management communications is disrupted.

D. Attacker accesses sensitive information regarding the network topology.

Suggested Answer: *A*

Community vote distribution

A (79%) D (21%)

JAckThePip Highly Voted 2 years, 9 months ago

ATTENTION the attacker is planning . If we consider that iy is need know the network to attack, the correct answer is D

"attackers act like detectives, gathering information to truly understand their target. From examining email lists to open source information, their goal is to know the network better than the people who run and maintain it. They hone in on the security aspect of the technology, study the weaknesses, and use any vulnerability to their advantage."

https://www.graylog.org/post/cyber-security-understanding-the-5-phases-of-intrusion

upvoted 15 times

Mgz156 Highly Voted 2 years, 9 months ago

Selected Answer: A

Answer is A

Losing control of their network devices to Criminal organization is the Highest risk

upvoted 7 times

jackdryan 2 years, 2 months ago

A is correct

upvoted 1 times

b0145c1 Most Recent 1 month, 3 weeks ago

Selected Answer: D

it is planning phase! D is the correct one.

upvoted 1 times

Tau 2 months, 2 weeks ago

Selected Answer: D

This is because gaining access to the network topology provides the attacker with crucial information about how the network is structured, which devices and systems are critical, and how to exploit vulnerabilities in the network. It allows the attacker to plan more targeted and effective attacks, potentially causing widespread damage or taking control of key systems.

The other options present risks, but they don't provide the attacker with as much valuable or strategic information as access to the network topology does.

upvoted 1 times

Senthil1982 3 months, 1 week ago

Selected Answer: D

D (Accessing Network Topology) is higher risk because it provides an immediate blueprint of the network, allowing an attacker to plan highly targeted and strategic attacks, even if they don't control the devices immediately. It gives them insight into which devices to target, where vulnerabilities may exist, and how to move through the network with minimal detection.

A (Losing Control of Network Devices), while still very serious, is a tactical step that requires the attacker to first gain control over individual devices and then figure out the network layout, which is a slower and potentially more detectable process.

So, the direct access to sensitive topology information provides an attacker with a much faster and more effective path to compromise the entire network, making D the higher risk in the scenario. I believe "D" is the right answer

upvoted 1 times

Isebarry 5 months ago

Selected Answer: A

Once an attacker takes control of the network, all other attacks listed from B to D can be easily perpetrated. So, the most important of the options is A

upvoted 2 times

fathermora 6 months, 4 weeks ago

Selected Answer: A

My initial thought was D but on a second thought, I agree the answer is A. You may have sensitive information about the network topology (not people or sensitive government data), yet unable to break the network security.

upvoted 3 times

Fouad777 7 months, 2 weeks ago

A. Organization loses control of their network devices.

When an organization loses control of their network devices, it means the attackers can potentially take over the entire network infrastructure. This scenario allows for a wide range of malicious activities, including the possibility of shutting down services, stealing sensitive data, deploying malware, and causing extensive damage. The other scenarios are certainly serious, but losing control of network devices represents a more comprehensive and critical threat.

upvoted 1 times

KennethLZK 7 months, 3 weeks ago

Selected Answer: A

Although D can be used to plan further attacks, it is not as immediately damaging as losing control of the network devices. Therefore A is better option here.

upvoted 1 times

deeden 11 months ago

Selected Answer: D

Agree with option D. Sensitive information sound to have higher risk than loosing control of network devices. You can always shutdown the hardware at the expense to operation, but it's like taking away their only advantage. You can always replace the devices, but sensitive or critical network architecture sound more expensive to overhaul.

upvoted 2 times

somsom 1 year ago

When you know about the information in the network, it will make you leverage it and have access to the network, thereby making the organization lose control of the network. Once you know the organization's Main IP of the network is very risky, you can use it to flood traffic to gain control of the network.

upvoted 2 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: A

Reconnaissance
Weaponising
Delivery
Installation
Exploitation <--- D when knows about sensitive information
Command and control <--A is at this stage
Action

upvoted 2 times

CCNPWILL 1 year, 2 months ago

IF you think its NOT A.... you are not reading the question closely enough. The answer is A.

upvoted 2 times

Rumor19 1 year, 5 months ago

Why not B?
If we consider that, we have to answer the question "What is the highest risk for the (attacking) organization?" It should be B.
A is easy to solve for an attacker. "Their network devices" means their own network devices like a internet router.
Not the ones in the goverment network. Just use a new internet access or hardware.

But if they flood the goverment network with (unnaturally) communication traffic, they get flagged by IDS/IPS and easily detected.

upvoted 1 times

⊟ **Soleandheel** 1 year, 6 months ago

Guys you have to read the question again. Try to understand the question better. The organization being refered to with regard to the highest risk is the Criminal Organization not the government network. A CRIMINAL ORGANIZATION is planning an attack on a government network. Which of the following scenarios presents the HIGHEST risk to the ORGANIZATION? (To the criminals organization) - A: Will compromise the criminal organization, cannot carry out planned attack. I agree with Markrlucas

upvoted 4 times

⊟ **AlexJacobson** 1 year, 7 months ago

Selected Answer: D

It's a GOVERNMENT network! I think this is the key hint that decides whether the answer is A or D. In my opinion, A can come as a consequence of D. By gaining access to sensitive information about the network topology, criminal organization would basically know everything about the network making the attacks on the network more effective and more dangerous.

So for me, it's D.

upvoted 2 times

⊟ **Law88** 1 year, 9 months ago

Selected Answer: D

The scenario that presents the highest risk to the organization is D. Attacker accesses sensitive information regarding the network topology.
The network topology is the arrangement and configuration of the network devices, such as routers, switches, firewalls, servers, etc., and the connections between them, such as cables, wireless links, protocols, etc. The network topology defines how the network operates, communicates, and performs.

upvoted 1 times

Question #24 *Topic 1*

Which reporting type requires a service organization to describe its system and define its control objectives and controls that are relevant to users' internal control over financial reporting?

A. Statement on Auditing Standards (SAS) 70

B. Service Organization Control 1 (SOC1)

C. Service Organization Control 2 (SOC2)

D. Service Organization Control 3 (SOC3)

Suggested Answer: *B*

Community vote distribution

B (82%) C (18%)

⊟ **CuteRabbit168** Highly Voted 👍 2 years, 3 months ago

Selected Answer: B

B (SOC 1) is the correct answer. Misread the question earlier.

upvoted 7 times

⊟ **jackdryan** 1 year, 7 months ago

B is correct

upvoted 1 times

⊟ **Temiii** Most Recent 🕘 2 weeks, 2 days ago

Selected Answer: B

B is correct

upvoted 1 times

⊟ **CCNPWILL** 8 months, 2 weeks ago

Financial... internal... SOC1 !

upvoted 1 times

⊟ **vorozco** 1 year, 6 months ago

Selected Answer: B

System and Organization Controls 1, or SOC 1 (pronounced "sock one"), aims to control objectives within a SOC 1 process area and documents internal controls relevant to an audit of a user entity's financial statements.

https://www.techtarget.com/searchsecurity/definition/SOC-1-System-and-Organization-Controls-1?Offer=abMeterCharCount_var2

upvoted 1 times

⊟ **KelvinYau** 1 year, 7 months ago

Selected Answer: B

No other choose only B is Financial.

upvoted 1 times

⊟ **KelvinYau** 1 year, 7 months ago

No other choose only B is Financial.

upvoted 1 times

⊟ **jegga** 1 year, 7 months ago

B is correct - The SOC1 audit focuses on a description
of security mechanisms to assess their suitability.

upvoted 1 times

⊟ **Firedragon** 2 years, 1 month ago

B is the answer.
https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report
SOC 1 - SOC for Service Organizations: ICFR
Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ICFR)

upvoted 1 times

rootic 2 years, 2 months ago

Selected Answer: B

Financial, so B.

upvoted 1 times

Eltooth 2 years, 2 months ago

Selected Answer: B

B is correct answer. SOC Type 1

upvoted 1 times

stickerbush1970 2 years, 3 months ago

Selected Answer: B

SOC 1
Used to address internal controls that relate to a vendor's financial reporting. It essentially looks at the quality of the vendor's bookkeeping by disclosing its financial and accounting controls.

1. Report evaluates controls within a single point in time (a single date) and often doesn't test controls.

2. Report is considered the ideal option because it tests control effectiveness over a period of time, thereby giving you better insight into patterns or recurring issues.

upvoted 2 times

CuteRabbit168 2 years, 3 months ago

The question is asking about: "control objectives and controls that are relevant to users' internal control over financial reporting". (i.e. NOT financial reporting). Hence, shouldn't the answer be "C" ?

upvoted 1 times

dev46 2 years, 3 months ago

No. it's B
Two keywords here. "internal" + "financial" = SOC 1.

upvoted 2 times

franbarpro 2 years, 3 months ago

Selected Answer: B

I am going with "B" on this one.
SOC 1 report. Evaluates how your services impact your customers' financial reporting control environment

SOC 1 matters for both financial transactions and the things that can impact financial transactions

SOC 2 report is more operational and broadly related to security and governance matters. Not only does it describe how your services remain secure and how you protect the data entrusted to you, but it also notes how well your organization keeps its commitments to the same.

https://www.schellman.com/blog/2016/01/what-are-service-organization-controls-soc-reports/

upvoted 2 times

CuteRabbit168 2 years, 3 months ago

Selected Answer: C

SOC 1 focuses on financial reporting, whereas SOC 2 focuses on compliance and operations.

upvoted 3 times

Question #25 *Topic 1*

Which of the following is the BEST method to validate secure coding techniques against injection and overflow attacks?

A. Scheduled team review of coding style and techniques for vulnerability patterns

B. The regular use of production code routines from similar applications already in use

C. Using automated programs to test for the latest known vulnerability patterns

D. Ensure code editing tools are updated against known vulnerability patterns

Suggested Answer: *C*

Community vote distribution

C (75%) A (25%)

Temiii 2 weeks, 2 days ago

Selected Answer: C

Automated code review

upvoted 1 times

EKP 1 month, 1 week ago

Selected Answer: A

The key is to validate secure coding techniques.

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: C

Code reviews are good practice but may miss subtle injection and overflow flaws without tool assistance.

upvoted 1 times

d7034bf 6 months, 3 weeks ago

Selected Answer: C

A and C are both correct, but what is the BEST option? I believe it would be C.

upvoted 1 times

somsom 8 months, 2 weeks ago

Answer is A. conduct a team review to discus about patterns for code review. in CISSP you think like a manager not like and analyst

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: A

We are asking to validate coding techniques, not to scan our code for vulnerabilities.

upvoted 3 times

Soleandheel 1 year, 6 months ago

C. Using automated programs to test for the latest known vulnerability patterns.....security testing tools like dynamic and static analysis are automated and can help detect injection attacks and buffer overflow attacks among others.

upvoted 2 times

vorozco 2 years ago

Selected Answer: C

C is correct. It's the BEST option because it's automated. I'm thinking of something like a SonarQube scan which provides code hotspots to be reviewed.

I would say it's NOT option A because code can get longggg and really complex. Having a team of people review coding styles and techniques against injection and overflow attacks would take a long time. If anything, the team could get together and review the results from the automated program (making option C necessary FIRST, for option A to be more beneficial).

upvoted 2 times

BLADESWIFTKNIFE 2 years, 1 month ago

Selected Answer: A

I thought we would have to think like a manager. Wouldn't it be "Scheduled team review of coding style and techniques for vulnerability patterns." Since scheduling would be the indicator for manager resposibilities.

upvoted 2 times

dumdada 2 years ago

As a manager you wouldnt want your team to spend their time doing manual reviews that can automated using the right tools.

upvoted 4 times

NodummyIQ 2 years, 4 months ago

Why it is not Option C, "Using automated programs to test for the latest known vulnerability patterns," is a useful method for identifying potential security vulnerabilities in code, but it is not the best method for validating secure coding techniques against injection and overflow attacks. Automated programs can only detect known vulnerabilities, and may not be able to identify new or unknown injection or overflow attacks. A combination of automated testing and human review, such as in option A, is often considered the best method for identifying and mitigating these types of attacks.

upvoted 1 times

jackdryan 2 years, 2 months ago

C is correct

upvoted 2 times

rootic 2 years, 8 months ago

Selected Answer: C

Agree with C.

upvoted 2 times

Eltooth 2 years, 8 months ago

Selected Answer: C

C is correct answer. Application pentest.

upvoted 2 times

franbarpro 2 years, 9 months ago

Selected Answer: C

Agree with "C"

I thought A first... but application pentesting can get expensive fast and human makes mistakes.

upvoted 3 times

Nickolos 2 years, 9 months ago

It might be expensive, but the question asks for 'best', not 'most efficient' or 'cost effective'

upvoted 6 times

dev46 2 years, 9 months ago

yeah, B and D are easy to eliminate but A and C both sound right. But, with A, a human would not be updated with the latest vulnerability all the time. Hence, the automation sound right.

upvoted 1 times

Question #26 *Topic 1*

When resolving ethical conflicts, the information security professional MUST consider many factors. In what order should the considerations be prioritized?

A. Public safety, duties to individuals, duties to the profession, and duties to principals

B. Public safety, duties to principals, duties to the profession, and duties to individuals

C. Public safety, duties to principals, duties to individuals, and duties to the profession

D. Public safety, duties to the profession, duties to principals, and duties to individuals

Suggested Answer: *B*

Community vote distribution

C (64%) 14% 11% 11%

Toa Highly Voted 2 years, 9 months ago

Answer C

Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals and the profession in that order.

https://resources.infosecinstitute.com/certification/the-isc2-code-of-ethics-a-binding-requirement-for-certification/

upvoted 17 times

jackdryan 2 years, 2 months ago

C is correct

upvoted 1 times

franbarpro Highly Voted 2 years, 9 months ago

Selected Answer: C

Going with "C" on this one:

Code of Ethics Preamble:

The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

Act honorably, honestly, justly, responsibly, and legally.

Provide diligent and competent service to principals.

Advance and protect the profession.

https://www.isc2.org/Ethics

upvoted 12 times

Temiii Most Recent 2 weeks, 2 days ago

Selected Answer: C

Option C

upvoted 1 times

easyp 5 months ago

Selected Answer: A

The correct answer is A:

Public safety, duties to individuals, duties to the profession, and duties to principals.

Explanation:

When resolving ethical conflicts, information security professionals must prioritize their responsibilities based on the (ISC)² Code of Ethics. The hierarchy outlined emphasizes the following:

Public safety: The highest priority is always to protect the safety and welfare of society and the public.

Duties to individuals: After public safety, consideration should be given to the rights and welfare of individuals who may be impacted by the decision.

Duties to the profession: The integrity and reputation of the information security profession must be upheld.

Duties to principals: Finally, responsibilities to employers, clients, and other stakeholders come after the previous considerations.

This hierarchy ensures that ethical decision-making focuses first on broader societal impacts and progresses toward more specific obligations.

upvoted 2 times

d7034bf 6 months, 3 weeks ago

Selected Answer: C

Its the PAPA method - Code of Ethics Canons:

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

Act honorably, honestly, justly, responsibly, and legally.

Provide diligent and competent service to principals.

Advance and protect the profession.

upvoted 1 times

Bietchasup 6 months, 3 weeks ago

Selected Answer: A

Honestly feel its A. Thorough all my lectures and studying the topic of the importance of protecting the public and society from harm should be a top priority.

upvoted 1 times

celomomo 8 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Public safety, duties to principals, duties to individuals, and duties to the profession.

This aligns with the standard prioritization for resolving ethical conflicts:

1. Public safety comes first.
2. Duties to principals (such as the organization or clients) follow.
3. Duties to individuals (including protecting personal privacy and ensuring fairness).
4. Duties to the profession (upholding professional standards and integrity) come after the others.

upvoted 1 times

martin451 8 months, 3 weeks ago

Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.

upvoted 1 times

ima_test_taker 1 year, 1 month ago

Selected Answer: C

The Canons are actually listed in order or importance with protecting people as #1 most important. Answer is C.

1. Protect society, the commonwealth and the infrastructure.
2. Act honorably, honestly, justly, responsibly and legally.
3. Provide diligent and competent service to principals.
4. Advance and protect the profession

upvoted 2 times

robervalchocolat 1 year, 2 months ago

https://www.infosecinstitute.com/resources/cissp/the-isc2-code-of-ethics-a-binding-requirement-for-certification/

upvoted 1 times

AshStevens 1 year, 2 months ago

Selected Answer: B

A number of people here seem to be overestimating the importance of individuals. There is no mention of individuals in PAPA. Public safety, principals, and profession are the only three points here to put in order. As "individuals" does not have its own section in PAPA, it comes AFTER we've put those others in order.

upvoted 2 times

NuwanCha 1 year, 3 months ago

C is the correct answer.

upvoted 1 times

sphiwe 1 year, 6 months ago

The official four canons are as follows:

Protect society, the commonwealth and the infrastructure.
Act honorably, honestly, justly, responsibly and legally.
Provide diligent and competent service to principals.
Advance and protect the profession.

Answer is D

upvoted 1 times

Ashsax 1 year, 8 months ago

public safety and duties to principals, individuals and the profession in that order.

upvoted 2 times

Law88 1 year, 9 months ago

Selected Answer: A

According to the ISC2 code of ethics, the order of the ethical considerations for information security professionals is A. Public safety, duties to individuals, duties to the profession, and duties to principals.

upvoted 4 times

hp6721 1 year, 9 months ago

Selected Answer: B

B
Both CISSP official study guide and https://www.isc2.org/Ethics state the following:
Protect SOCIETY, the common good, necessary public trust and confidence, and the infrastructure.
Act honorably, honestly, justly, responsibly, and legally.
Provide diligent and competent service to PRINCIPALS.
Advance and protect the PROFESSION.
Observe, there is no reference to individuals. I speculate most of us selected option C as we are part of the individuals who make the profession and society at large. We want to be included in the factors of consideration; however, there is no mention to individuals in the Code of Canons.

upvoted 4 times

LoboMau 2 years ago

Selected Answer: C

C is correct - Basic ISC2 canon

upvoted 1 times

Question #27 *Topic 1*

Which service management process BEST helps information technology (IT) organizations with reducing cost, mitigating risk, and improving customer service?

A. Kanban

B. Lean Six Sigma

C. Information Technology Service Management (ITSM)

D. Information Technology Infrastructure Library (ITIL)

Suggested Answer: *D*

Community vote distribution

D (68%) C (32%)

⊟ **N00b1e** Highly Voted 👍 2 years, 9 months ago

I've just checked the Official Student Guide, and ITSM isn't mentioned once. ITIL is mentioned 16 times!

upvoted 12 times

⊟ **jackdryan** 2 years, 2 months ago

D is correct

upvoted 1 times

⊟ **kasiya** Highly Voted 👍 2 years, 9 months ago

Selected Answer: D

AIO 8th

ITIL is the de facto standard of best practices for IT service management.

upvoted 8 times

⊟ **cjace** Most Recent ⏲ 1 month ago

Selected Answer: C

While ITIL supports ITSM with best practices, ITSM is the best overall answer because it is the process that directly helps with reducing cost, mitigating risk, and improving customer service.

upvoted 1 times

⊟ **cjace** 1 month, 2 weeks ago

Selected Answer: C

ITSM (Information Technology Service Management) is a strategic and process-based approach to designing, delivering, managing, and improving the way IT is used within an organization. It is explicitly focused on aligning IT services with business needs.

✅ ITSM helps organizations:

Reduce cost by optimizing processes and resources

Mitigate risk through structured change, incident, and problem management

Improve customer service with defined service levels, continuous improvement, and user-centric practices

ITSM frameworks encompass many best practices (including ITIL), making it a comprehensive approach to service management.

D. ITIL (Information Technology Infrastructure Library):

A framework within ITSM — it guides ITSM but is not the process itself.

ITIL is often used to implement ITSM.

upvoted 1 times

⊟ **Rider2053** 4 months, 3 weeks ago

Selected Answer: D

think like a CEO, ITIL is correct answer

upvoted 1 times

⊟ **ayadmawla** 5 months, 1 week ago

Selected Answer: C

While ITSM (or Agile) is a methodology, ITIL (or Scrum) is a framework for implementing that methodology. The connection between the two is strong; ITIL was created with ITSM in mind.

upvoted 1 times

tsummey 9 months, 3 weeks ago

Selected Answer: D

ITIL focuses on aligning IT services with business needs, providing frameworks for service management that help reduce operational costs, mitigate risk through efficient processes, and improve customer service through continual improvement and standardization. ITSM (C) also aims to manage and improve IT services, but ITIL specifically provides the detailed processes and best practices that support comprehensive IT service management.

upvoted 1 times

deeden 11 months ago

Selected Answer: C

ITSM is the most comprehensive framework among the options provided. It encompasses a structured approach to aligning IT services with the needs of the business.

Here's a breakdown of why ITSM is the best choice:

Cost reduction: ITSM focuses on optimizing IT services, identifying inefficiencies, and eliminating waste, leading to cost savings.
Risk mitigation: By establishing clear processes and controls, ITSM helps identify and manage risks effectively.
Improved customer service: ITSM emphasizes customer satisfaction and service delivery, leading to better customer experiences.
While Kanban and Lean Six Sigma can be valuable tools for specific process improvements, ITSM provides a broader framework for managing IT services as a whole.

upvoted 1 times

deeden 11 months ago

Key ITIL Processes
ITIL is divided into several core processes that guide ITSM practices:

Service Strategy: Defines the role of IT services in enabling business objectives.
Service Design: Develops the technical design of IT services to meet business requirements.
Service Transition: Implements new or changed IT services into production.
Service Operation: Manages day-to-day IT service delivery and support.
Continual Service Improvement: Continuously evaluates and improves IT services.

upvoted 1 times

deeden 11 months ago

Service Operations and ITSM
Yes, Service Operations is a critical component of ITSM.

It encompasses the day-to-day activities involved in delivering and supporting IT services.

Key activities within Service Operations include:

Event Management: Detecting, logging, and responding to events within the IT infrastructure.
Incident Management: Restoring normal service operations as quickly as possible to minimize the impact of incidents.
Request Fulfillment: Managing and fulfilling user requests for standard IT services.
Access Management: Controlling access to IT services and resources.
Problem Management: Identifying and resolving underlying causes of incidents.

upvoted 1 times

deeden 11 months ago

Key words:
- service management
- reducing cost
- mitigating risk
- improving customer service

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: D

From the OSG - ITIL, initially crafted by the British government, is a set of recommended best practices for optimization of IT services to support business growth, transformation, and change.

upvoted 1 times

BestCommentorNA 1 year, 7 months ago

Selected Answer: D

The service management process that best helps IT organizations with reducing cost, mitigating risk, and improving customer service is ITIL (Information Technology Infrastructure Library). ITIL is a widely adopted framework for IT service management that provides best practices and guidelines to align IT services with the needs of the business.

Within ITIL, several processes contribute to these objectives, but one of the most crucial ones is Service Level Management (SLM). SLM is responsible for defining, negotiating, documenting, monitoring, measuring, reporting, and reviewing the level of IT services provided to customers. By effectively managing service levels, IT organizations can ensure that they meet customer expectations, reduce costs by optimizing service delivery, and mitigate risks by proactively addressing issues and vulnerabilities.

upvoted 1 times

thanhlb 1 year, 8 months ago

Selected Answer: C

ITIL is a framework of best practices for ITSM, but it is not a service management process itself

upvoted 1 times

Law88 1 year, 9 months ago

Selected Answer: C

The best service management process that helps information technology (IT) organizations with reducing cost, mitigating risk, and improving customer service is C. Information Technology Service Management (ITSM).

ITSM is a set of practices and processes that aim to align the IT services with the business needs and objectives, and to deliver value to the customers and stakeholders. ITSM covers the entire lifecycle of IT services, from planning, designing, developing, deploying, operating, to improving.

upvoted 1 times

4vv 1 year, 10 months ago

27. d => ITIL is a framework for ITSM, prescribing a specific set of processes and guidelines for the provisioning of IT services, but ITSM is the overall, could be c too.

upvoted 2 times

vorozco 2 years ago

Selected Answer: D

D is correct.

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: C

ITIL is a standard practice framework for ITSM. The difference between ITSM and ITIL can be further understood by looking at how the two concepts have evolved. ITSM has changed from its beginnings and developed with the need for standardization across organizations. As ITSM developed, so did several different ITSM frameworks from across different industries and parts of the world. ITIL is just one of those frameworks and happens to be the most comprehensive and popular.
Reference : https://www.teamdynamix.com/itsm-vs-itil-whats-the-difference/

upvoted 2 times

> **vorozco** 2 years ago
>
> So, since ITIL is the most comprehensive and most popular it's probably the BEST process under ITSM to use. This seems to support that the answer is D: ITIL.
>
> upvoted 1 times

Billy235 2 years, 7 months ago

ITSM is the general term used for service management. Options A, B and D are all practices for process improvement. The BEST one that addresses cost, risk and service is ITIL. Answer is D.

upvoted 2 times

rootic 2 years, 8 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

Question #28 *Topic 1*

A company is attempting to enhance the security of its user authentication processes. After evaluating several options, the company has decided to utilize Identity as a Service (IDaaS). Which of the following factors leads the company to choose an IDaaS as their solution?

A. In-house team lacks resources to support an on-premise solution.

B. Third-party solutions are inherently more secure.

C. Third-party solutions are known for transferring the risk to the vendor.

D. In-house development provides more control.

Suggested Answer: *A*

Community vote distribution

A (62%) C (31%) 8%

EKP 1 month, 1 week ago

Selected Answer: B

The question is asking to enhance the security of user authentication processes. Third-party is kind of segregation of tasks, can the security of user authentication processes.

upvoted 1 times

BigITGuy 2 months, 4 weeks ago

Selected Answer: A

Not C at least not in Canada - IDaaS does not completely transfer risk; the organization still retains responsibility for correct integration and usage.

upvoted 1 times

tsummey 9 months, 3 weeks ago

Selected Answer: A

A is about operational necessity, while C is about a strategic advantage. Most organizations first choose IDaaS because they lack the resources to build and maintain an on-premises solution. The risk transfer factor (C) adds value but isn't usually the core reason for the decision.

upvoted 2 times

jieaws 1 year, 2 months ago

The question is asking "...enhance the security of its user authentication processes...". Also, I remind myselft to confine my thoughts within the provided context.

A? "Lack resources and On premise solution" I do not see any wording in the context associated with this assumption. So A is out.
C? " transferring the risk.." Again, does this transferring risk enhances authentication security? Am I answering the question at all?
D? "In house ..." Similar to A and C. These options try to add buffer overflow info which are not within the questions context.

The closest option is B. It exactly echos "...enhance the security of its user authentication processes..."

upvoted 1 times

Yokota 1 year, 2 months ago

Selected Answer: C

A is wrong because they DO have the resources. The company wants to ENHANCE the security. The only option is C

upvoted 2 times

radagon 1 year, 8 months ago

A: answer C is wrong because the question says " to enhance the security of its user authentication processes", transferring risk does not enhance security of the user

upvoted 1 times

Yokota 1 year, 2 months ago

they are not "enhance security of the user" they are enhance security of the PROCESS.

upvoted 1 times

A1nthem 1 year, 8 months ago

Selected Answer: A

A: as lack of resources.

upvoted 1 times

LalithW 1 year, 9 months ago

"A company is attempting to enhance the security of its user authentication processes" means that the company already has an on-premises solution. For enhancement, they lack resources, hence moving with IDaaS. Answer A.

upvoted 3 times

Vince_F_Fang 1 year, 10 months ago

I didn't find any cost related options. I chose B and after seeing the answer, I reevaluated A. Option A is actually equivalent to reducing costs

upvoted 1 times

vorozco 2 years ago

Selected Answer: A

Best answer is A.

I think people choosing option C are thinking about "risk transfer" as part of risk management, but (1) this question isn't really about RM and (2) risk transfer USUALLY is centered around insurance.

upvoted 1 times

atif95 1 year, 10 months ago

Outsourcing services and insurance both are the examples of risk transference (by AIO shon Harris 9th edition)

upvoted 2 times

Azurefox79 2 years, 3 months ago

Selected Answer: A

A is the only answer that makes sense. Transferring risk, C, does not make sense. There is always risk and that's not a driving factor here.

upvoted 1 times

jackdryan 2 years, 2 months ago

A is correct

upvoted 1 times

s_n_ 2 years, 5 months ago

Corp.com chose Identity as a Service (IDaaS) as their solution because of its inherent security benefits, its ability to transfer risk to the vendor, and its scalability and affordability. IDaaS is a third-party authentication solution that uses cloud-based software to provide authentication services, such as user authentication, single sign-on, and multi-factor authentication. This type of solution is often more secure than an on-premise solution because it is hosted by a trusted third-party, who is responsible for maintaining the security of the system. Additionally, IDaaS solutions are known for transferring the security risk to the vendor, which can be beneficial for companies that lack the resources to support an on-premise solution. Finally, IDaaS solutions are known for their scalability and affordability, as they are often much cheaper than developing an in-house authentication solution and can easily be scaled up or down, depending on the company's needs.

Resources:

1. What is Identity as a Service (IDaaS)? - https://www.techopedia.com/definition/31761/identity-as-a-service-idaas
2. Why IDaaS is the Best Choice for

upvoted 2 times

RVoigt 2 years, 5 months ago

Selected Answer: C

From the ISC Official Study Guide:
"Risk Assignment - Assigning risk or transferring risk is the placement of the responsibility of loss due to a risk onto another entity or organization. Purchasing cybersecurity or tradition insurance and outsourcing are common forms of assigning risk or transferring risk. Also known as assignment of risk and transference of risk.

upvoted 2 times

Delab202 2 years, 6 months ago

Selected Answer: B

Enhance the security- Objective

upvoted 2 times

cccispman 2 years, 6 months ago

Just joined - some of these questions are great !
I just want to know which b@5t4rd wrote them !!

'A' doesn't sound sensible because there's an assumption that the company doesn't have a team for managing IDaaS.

Upon viewing Pete Zeger's 7.5hr youtube classic, I am leaning towards B, third party solutions are better, mostly :-)

The business wished to enhance, not because of some in-house skills shortage, but because there's something out there that can do a better job.

This question is actually quite tough and we can fall into the trap of reading too much into it, and that is the crux of the problem !

upvoted 3 times

somkiatr 2 years, 6 months ago

Selected Answer: A

This is not about risk transfer purpose. We select vendor because they are secured enough to match our requirements and we don't have enough resources to support the on premise system.

upvoted 2 times

oudmaster 2 years, 6 months ago

Now what if the company has enough resources to support on-prem solution?
How we would know that?

upvoted 1 times

Question #29 *Topic 1*

An organization recently suffered from a web-application attack that resulted in stolen user session cookie information. The attacker was able to obtain the information when a user's browser executed a script upon visiting a compromised website. What type of attack MOST likely occurred?

A. SQL injection (SQLi)

B. Extensible Markup Language (XML) external entities

C. Cross-Site Scripting (XSS)

D. Cross-Site Request Forgery (CSRF)

Suggested Answer: *C*

Community vote distribution

C (100%)

HazRic 3 months, 3 weeks ago

Selected Answer: C

As an OSCP, CRT, CRTP, CRTO certified, I can confirm that the correct answer is C. Mic drop!

upvoted 1 times

ShefAZ 6 months, 2 weeks ago

Selected Answer: D

browser executed a script upon visiting a compromised websit

A Cross-Site Request Forgery (CSRF) attack occurs when a malicious web site, email, blog, instant message, or program tricks an authenticated user's web browser into performing an unwanted action on a trusted site.

upvoted 2 times

A1nthem 8 months, 3 weeks ago

Selected Answer: C

XXS: </sript> to load on browser

upvoted 1 times

kandegama 1 year, 2 months ago

Selected Answer: C

XSS happen on client side. CSRF happening on web server side.therefore Answer is C

upvoted 3 times

jackdryan 1 year, 2 months ago

C is correct

upvoted 2 times

Arunlab 1 year, 7 months ago

Ignore my comment. I will go with C

upvoted 1 times

Arunlab 1 year, 7 months ago

Answer is D

CSRF uses the authentication cookie.

Cross site request forgery (CSRF) is a web application security attack that tricks a web browser into executing an unwanted action in an application to which a user is already logged in. The attack is also known as XSRF, Sea Surf or Session Riding.

upvoted 2 times

Jamati 1 year, 7 months ago

Selected Answer: C

XSS injects a malicious script into a vulnerable website in order to get a user's session cookies when they visit the compromised website. XSRF/CSRF on the other hand only targets the user directly, it does not compromise any website and does not get session cookies.

upvoted 3 times

rootic 1 year, 8 months ago

Selected Answer: C

Definetely C.

upvoted 1 times

Eltooth 1 year, 8 months ago

Selected Answer: C

C is correct answer.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/attacks/csrf

upvoted 3 times

explorer3 1 year, 8 months ago

Selected Answer: C

Correct answer is C - Cross-site script attack

The attacker can compromise the session token by using malicious code or programs running at the client-side. The example shows how the attacker could use an XSS attack to steal the session token. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker. The example in figure 3 uses an XSS attack to show the cookie value of the current session; using the same technique it's possible to create a specific JavaScript code that will send the cookie to the attacker.

https://owasp.org/www-community/attacks/Session_hijacking_attack

upvoted 2 times

franbarpro 1 year, 9 months ago

Selected Answer: C

Agree with C - If is a scrypt (JavaScript) in the browser. Def XSS.

upvoted 1 times

Cww1 1 year, 9 months ago

its C, the stolen session cookie information part of the question is trying to trick you into picking CSRF

upvoted 3 times

Toa 1 year, 9 months ago

Answer C

https://www.fortinet.com/resources/cyberglossary/cross-site-scripting

upvoted 3 times

Question #30 *Topic 1*

An attack utilizing social engineering and a malicious Uniform Resource Locator (URL) link to take advantage of a victim's existing browser session with a web application is an example of which of the following types of attack?

A. Clickjacking

B. Cross-site request forgery (CSRF)

C. Cross-Site Scripting (XSS)

D. Injection

Suggested Answer: *C*

Community vote distribution

B (88%) 13%

Mgz156 Highly Voted 2 years, 9 months ago

Selected Answer: B

Answer is B

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application

upvoted 16 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 2 times

Toa Highly Voted 2 years, 9 months ago

Answer B

A CSRF attack hinges on the use of social engineering. An attacker fools their victim by sending a link through a chat or email. When a victim is a user without admin privileges, the CSRF attack can make them do things like change an email address as it appears in the target site's system, transfer funds from an account, change username information, and more. If the victim has administrator privileges, the CSRF attack can be used to alter the function of the web application itself

https://www.fortinet.com/resources/cyberglossary/csrf

upvoted 9 times

Cww1 2 years, 9 months ago

I agree

upvoted 2 times

somsom Most Recent 8 months, 2 weeks ago

B is correct it uses social engineering and and web application to trick users

upvoted 1 times

deeden 11 months ago

Selected Answer: B

Hacker was able to steal cookies, then sending forged request to the server and pretending to be the actual user.

upvoted 1 times

GuardianAngel 1 year, 4 months ago

Answer: Cross site Request forgery

https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/#:~:text=CSRFs%20are%20typically%20conducted%20using,request%20from%20a%20forged%20one.

CSRFs are typically conducted using malicious social engineering, such as an email or link that tricks the victim into sending a forged request to a server. As the unsuspecting user is authenticated by their application at the time of the attack, it's impossible to distinguish a legitimate request from a forged one.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: B

Answer B) https://owasp.org/www-community/attacks/csrf

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

upvoted 1 times

A1nthem 1 year, 8 months ago

Selected Answer: B

existing browser session

upvoted 2 times

74gjd_37 1 year, 9 months ago

Selected Answer: B

The Answer is B.
According to OWASP https://owasp.org/www-community/attacks/csrf
Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

upvoted 3 times

The_Green 2 years, 1 month ago

Answer is B

upvoted 1 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 1 times

oudmaster 2 years, 6 months ago

XSS attack does not take advantage of a victim's existing browser session. But CSRF does.

upvoted 4 times

somkiatr 2 years, 6 months ago

Selected Answer: B

B not C. The success of an XSS attack isn't based on the session activation. Corrupted payloads are delivered whenever the user accesses the website. CSRF demands an active session be completed. It mentions that "existing browser session" then should be CSRF attack.

upvoted 1 times

Ncoa 2 years, 7 months ago

Selected Answer: C

I meant C doh!

upvoted 1 times

Ncoa 2 years, 7 months ago

Selected Answer: B

Sounds like a reflected XSS attack to me

Check out the mindmap video on it from efficient learning

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: B

XSS injects a malicious script into a vulnerable website in order to get a user's session cookies when they visit the compromised website. XSRF/CSRF on the other hand targets the user directly, it does not compromise any website and does not get session cookies. Hacker simply sends a URL of cute puppies and cats (for example) with invisible malicious code embedded. While you're scrolling through pictures of cute puppies the code is busy transferring funds from your account to the hacker.

upvoted 2 times

rootic 2 years, 8 months ago

Selected Answer: B

I agree with B

upvoted 1 times

Eltooth 2 years, 8 months ago

Selected Answer: B

B is correct answer. CSRF

https://owasp.org/www-community/attacks/csrf

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

upvoted 2 times

Question #31 *Topic 1*

Which of the following encryption technologies has the ability to function as a stream cipher?

A. Cipher Block Chaining (CBC) with error propagation

B. Electronic Code Book (ECB)

C. Cipher Feedback (CFB)

D. Feistel cipher

Suggested Answer: *C*

Community vote distribution

C (100%)

Mgz156 Highly Voted 1 year, 9 months ago

Selected Answer: C

Answer is C

Cipher feedback mode allows a block cipher with block size n bits to be used as a stream cipher with a data encryption unit of m bits, for any m ≤ n.

In CFB mode, the block cipher operates on a register of n bits. The register is initially filled with an initialization vector.

upvoted 8 times

6c201b2 Most Recent 3 months, 3 weeks ago

Selected Answer: C

Cipher Feedback (CFB) mode is the streaming cipher version of CBC

upvoted 1 times

Bach1968 12 months ago

Selected Answer: C

The encryption technology that has the ability to function as a stream cipher among the options provided is option C: Cipher Feedback (CFB).

Stream ciphers are encryption algorithms that encrypt data one bit or one byte at a time, providing a continuous stream of encrypted output. They are typically used for real-time applications or when encrypting large amounts of data.

upvoted 3 times

vorozco 1 year ago

Selected Answer: C

Answer is C

upvoted 1 times

Ivanchun 1 year, 6 months ago

Selected Answer: C

C, CFB no other for stream cipher

upvoted 1 times

jackdryan 1 year, 2 months ago

C is correct

upvoted 1 times

rootic 1 year, 8 months ago

Selected Answer: C

100% C.

upvoted 1 times

Eltooth 1 year, 8 months ago

C is correct answer.

https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/amp/

upvoted 2 times

franbarpro 1 year, 9 months ago

Selected Answer: C

Agree with C

upvoted 2 times

⊟ **Toa** 1 year, 9 months ago

Answer C

https://www.geeksforgeeks.org/difference-between-block-cipher-and-stream-cipher/?ref=lbp

upvoted 2 times

Question #32 *Topic 1*

In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

A. Process

B. Anticipate

C. Strategic

D. Wide focus

Suggested Answer: *B*

Community vote distribution

A (45%) B (38%) D (17%)

Demo25 Highly Voted 1 year, 11 months ago

Selected Answer: B

The answer is B. Anticipate.
Crisis management is the process of planning and responding to unexpected events that can have a negative impact on an organization. One of the key traits of crisis management is the ability to anticipate potential problems and develop plans to mitigate their impact. This means being able to think ahead and identify potential risks, as well as having a plan in place to deal with them if they do occur.

upvoted 13 times

fuzzyguzzy Most Recent 2 months, 3 weeks ago

Selected Answer: A

The answer if A, especially if this is a test excercise, per the study guide:

If a disaster strikes your organization, panic is likely to set in. The best way to combat this is with an organized disaster recovery plan. The individuals in your business who are most likely to first notice an emergency situation (such as security guards and technical personnel) should be fully trained in disaster recovery procedures and know the proper notification procedures and immediate response mechanisms.

upvoted 1 times

46f752c 2 months, 4 weeks ago

Selected Answer: B

In a disaster recovery (DR) test, which of the following would be a trait of crisis management?

A. Process
B. Anticipate Most Voted
C. Strategic
D. Wide focus

upvoted 1 times

Senthil1982 3 months ago

Selected Answer: C

Crisis management in a disaster recovery (DR) test focuses on the strategic approach to addressing the crisis. This includes making high-level decisions, prioritizing actions, managing resources, and ensuring that the organization can continue operations or recover from the disaster efficiently. It involves leadership, communication, and coordination at the top levels of the organization to minimize impact and guide the response efforts.

Process (A) typically refers to the specific procedures or steps taken during a recovery, not the high-level decision-making that happens during a crisis.

Anticipate (B) is more about preparation and planning, which are part of disaster recovery but not the immediate response to a crisis.

Wide focus (D) refers to addressing many aspects of a disaster but doesn't necessarily capture the strategic nature of crisis management, which typically has a broader focus on high-level decisions.

In short, crisis management is strategic because it requires careful decision-making to navigate the disaster and steer the organization towards recovery.

upvoted 1 times

Imranbhatti 3 months, 3 weeks ago

Selected Answer: B

In the context of crisis management during a disaster recovery (DR) test, the trait that stands out is B. Anticipate. Crisis management involves anticipating potential issues and preparing for them in advance to mitigate their impact.

upvoted 2 times

tama_tama 5 months ago

Selected Answer: D

D. Wide focus
Crisis management is broader in scope compared to disaster recovery (DR). It involves handling high-impact, unpredictable events that require strategic decisions and communication with stakeholders, not just restoring IT systems.
Crisis management includes public relations, legal implications, business continuity, and coordination with authorities, meaning it has a wide focus beyond just the IT processes.

For the other options i think!
A. Process → More relevant to DR, which follows predefined steps for system recovery.
B. Anticipate → While anticipation is part of risk management, crisis management deals with reacting to unfolding events.
C. Strategic → While crisis management involves strategy, "wide focus" better describes its overarching role.
Thus, wide focus (D) is the best choice as crisis management addresses not just IT recovery but also organizational resilience.

upvoted 2 times

easyp 5 months ago

Selected Answer: D

The correct answer is:

D. Wide focus

Explanation:
In disaster recovery (DR), crisis management involves a wide focus because it addresses the overall impact of a disaster on the organization. Crisis management goes beyond the technical aspects of recovery (like restoring IT systems) and considers the broader implications, such as communication with stakeholders, legal and regulatory requirements, public relations, and ensuring business continuity at a high level.

upvoted 1 times

stefan 6 months, 3 weeks ago

Selected Answer: D

The best answer is:

D. Wide focus

Explanation:
• Crisis management during a disaster recovery test typically involves a wide focus because it requires addressing the broader, organizational-wide impacts of a disaster. This includes not only the technical aspects but also coordinating various teams, communication strategies, and ensuring overall business continuity. Crisis management looks at the big picture, which is crucial during a disaster recovery event.

Here's why the other options are less appropriate:
• A. Process Most Voted: This is unclear and not relevant to crisis management in disaster recovery.
• B. Anticipate: While anticipating potential issues is part of disaster recovery planning, crisis management is more about responding effectively when the crisis is happening.
• C. Strategic: While crisis management requires strategic decisions, a wide focus captures the urgency and broad scope of the situation better.

upvoted 2 times

Moose01 6 months, 4 weeks ago

Selected Answer: B

the question is - would be a trait of crisis management?
to anticipate or expect the unexpected possibilities and potential problems that were not accounted for in the plan.

upvoted 1 times

Fouad777 7 months, 2 weeks ago

C. Strategic
Crisis management typically involves making high-level decisions and setting priorities to manage the situation effectively. It is strategic because it

focuses on ensuring that the organization's overall mission and critical operations are maintained or restored as quickly as possible during a disaster. It involves coordinating response efforts, allocating resources, and ensuring leadership oversight during the crisis.

upvoted 2 times

aaminenaji 8 months, 1 week ago

Selected Answer: D

Wide focus encloe it all

upvoted 1 times

somsom 8 months, 2 weeks ago

B is the answer; when you anticipate an event, it may go wrong or better.

upvoted 1 times

M_MUN17 8 months, 3 weeks ago

The correct answer is C. Strategic.

In a disaster recovery (DR) test, crisis management involves taking a strategic approach to handle unforeseen events and ensure business continuity. Crisis management focuses on high-level decision-making, prioritization of resources, and long-term planning to mitigate the impact of a disaster.

The other options refer to different aspects:

A. Process refers to the structured steps or procedures, which are more tactical than strategic.
B. Anticipate is related to proactive risk management but doesn't capture the broader, high-level focus of crisis management.
D. Wide focus refers to considering multiple aspects, but the core of crisis management in DR is strategic planning and leadership.

upvoted 1 times

martin451 8 months, 3 weeks ago

Selected Answer: B

Anticipating potential issues and challenges is a key aspect of effective crisis management, allowing organizations to prepare and respond proactively to minimize impact.

upvoted 1 times

celomomo 9 months ago

Selected Answer: C

crisis management refers to the overall coordination of an organization's response to a disruptive event. Strategy is more important than the process.

upvoted 1 times

robervalchocolat 10 months ago

Crisis management involves identifying potential risks and developing strategies to mitigate them. This is a unique trait of crisis management, as it focuses on proactive measures to prevent or minimize the impact of crises.

upvoted 1 times

deeden 11 months ago

Selected Answer: D

Wide focus best characterizes crisis management in a disaster recovery test.

Process: While important, simply having a process in place is not enough for effective crisis management.
Anticipate: This is a critical component, but it doesn't fully capture the dynamic nature of crisis management.
Strategic: While strategy is essential, it's only one aspect of crisis management.
Wide focus encompasses the broader scope of crisis management, including:

Coordination: Managing multiple stakeholders and resources.
Decision-making: Making rapid and informed decisions under pressure.
Communication: Effective internal and external communication.
Problem-solving: Addressing unexpected challenges and finding solutions.
A wide focus ensures a comprehensive approach to managing a crisis effectively.

upvoted 2 times

Question #33 *Topic 1*

Which of the following BEST describes the purpose of the reference monitor when defining access control to enforce the security model?

A. Strong operational security to keep unit members safe

B. Policies to validate organization rules

C. Cyber hygiene to ensure organizations can keep systems healthy

D. Quality design principles to ensure quality by design

Suggested Answer: *B*

Community vote distribution

B (61%) D (21%) A (18%)

Nickname53796 Highly Voted 2 years, 8 months ago

Selected Answer: B

The reference monitor is much like the bouncer at a club because it stands between each subject and object. Its role is to verify the subject meets the minimum requirements for access

upvoted 12 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: B

The reference monitor is a conceptual security component in access control models that enforces the security policy by mediating all access between subjects (users, processes) and objects (files, resources). Quality by design refers to software development principles, not directly to the function of a reference monitor.

upvoted 1 times

Fouad777 7 months, 2 weeks ago

he correct answer is:

B. Policies to validate organization rules

Explanation:
The reference monitor is a concept in access control that enforces a system's security policy by validating every attempt to access resources according to defined rules. It ensures that all access requests conform to the organization's security policies, such as access permissions and data classification levels.

The reference monitor acts as a mediator between subjects (users or processes) and objects (resources like files, databases, or systems), ensuring that only authorized interactions occur. It is a critical component of security models like the Bell-LaPadula or Clark-Wilson models.

upvoted 2 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: D

It's called the reference monitor CONCEPT - because it is NOT an implementation of any system or policy. When it is implemented it would be called the Security Kernel.

upvoted 2 times

robervalchocolat 10 months ago

A reference monitor is a security kernel that enforces access control policies for a system. It acts as an intermediary between subjects (users or processes) and objects (resources) and ensures that subjects have the necessary permissions to access objects.

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: D

Reference monitor could be applied to a TCB only.

upvoted 1 times

finallink 1 year, 4 months ago

The question is asking what is the "purpose of the reference monitor" its D

upvoted 1 times

susmit683 1 year, 5 months ago

Selected Answer: D

Reference Monitor is a design principle

upvoted 2 times

74gjd_37 1 year, 9 months ago

Selected Answer: D

According to NIST

https://csrc.nist.gov/glossary/term/reference_monitor

reference monitor is "A set of design requirements on a reference validation mechanism that, as a key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism is always invoked (i.e., complete mediation), tamperproof, and small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable)."

1) reference monitor is a design principle, therefore D correct

2) reference monitor is needed to validate whether subjects can access objects; it is used to validate access using access rights defined in a policy; it is not used to validate organization rule, therefore, B is incorrect

upvoted 3 times

Vince_F_Fang 1 year, 10 months ago

Selected Answer: A

I chose A, the policy seems to be at a higher level, and the reference monitor should be controlled at more specific levels of each operation (unit operation)

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: B

The purpose of the reference monitor when defining access control to enforce the security model is BEST described by option B: Policies to validate organization rules.

The reference monitor is a concept in computer security that represents an abstract machine or component responsible for enforcing access control policies. It is an essential component of the security model used to ensure that access to system resources is granted or denied based on predefined rules and policies.

The reference monitor validates and enforces these organization-specific rules and policies regarding access control. It acts as a trusted authority that mediates all access requests and determines whether they should be permitted or denied based on the established security policies.

upvoted 3 times

s_n_ 2 years, 5 months ago

B. Policies to validate organization rules. The reference monitor is a security mechanism that controls and mediates the access of programs, processes, or users to resources or objects in a system. It enforces the security policy for the system by validating and controlling access requests according to the rules specified in the security policy. Resources such as https://searchsecurity.techtarget.com/definition/reference-monitor and https://www.academia.edu/25732717/Reference_Monitor_and_Security_Policies provide more information on the purpose of the reference monitor.

upvoted 2 times

Firedragon 2 years, 7 months ago

Selected Answer: B

Bad wording questions. Pick B.

A core function of the kernel is running the reference monitor, which mediates all access between subjects and objects. It enforces the system's security policy, such as preventing a normal user from writing to a restricted file, such as the system password file.

upvoted 1 times

RonWonkers 2 years, 7 months ago

Selected Answer: B

I think B

upvoted 1 times

Jamati 2 years, 8 months ago

Selected Answer: A

I believe A is the answer. B cannot be correct coz the TCB and reference monitor having nothing to do with the organization but have everything do with the Operating system, hardware, and other units / modules of the system as a whole. D is also out because the goal of the reference monitor is more about security than design.

upvoted 4 times

somkiatr 2 years, 6 months ago

+1 agreed.

upvoted 1 times

rootic 2 years, 8 months ago

Selected Answer: B

Think it's B.

upvoted 2 times

krassko 2 years, 9 months ago

Selected Answer: D

I vote for D, without explanation

upvoted 1 times

Question #34 Topic 1

Which of the following is security control volatility?

A. A reference to the impact of the security control.

B. A reference to the likelihood of change in the security control.

C. A reference to how unpredictable the security control is.

D. A reference to the stability of the security control.

Suggested Answer: *C*

Community vote distribution

B (96%) 4%

SongOTD Highly Voted 2 years, 9 months ago

Selected Answer: B

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf
It says Security control volatility is a measure of how frequently a control is likely to change over time subsequent to its implementation. So I would choose B.

upvoted 12 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 2 times

Fouad777 Most Recent 6 months, 1 week ago

Selected Answer: B

volatility = Changes up and down

upvoted 1 times

Fouad777 7 months, 2 weeks ago

The correct answer is:

B. A reference to the likelihood of change in the security control.

Explanation:
Security control volatility refers to the likelihood or frequency of change in a security control over time. Some controls, such as policies or procedures, tend to be more stable and change less frequently. Others, like technical controls (e.g., firewall rules or antivirus definitions), may change often to respond to evolving threats, updates, or operational requirements.

Understanding the volatility of a control helps in planning and prioritizing maintenance, audits, and updates to ensure the control remains effective over time.

upvoted 1 times

robervalchocolat 10 months ago

Security control volatility refers to the likelihood that a security control will need to be changed or updated in the future. This can be due to various factors, such as changes in technology, threats, or organizational needs.

upvoted 1 times

25cbb5f 1 year, 2 months ago

The correct answer is B. A reference to the likelihood of change in the security control.

Here's what security control volatility means:

Definition: Security control volatility refers to how frequently a security control might need to be changed or updated over time. This could be due to factors like:
Evolving threats and vulnerabilities
Changes in technology
New regulations or compliance requirements

Organizational shifts in business needs
Why other options are not correct:

A. A reference to the impact of the security control: Impact refers to the potential consequences or effects of the security control itself, not its volatility.
C. A reference to how unpredictable the security control is: Unpredictability implies randomness or a lack of reliability, which is not the focus of volatility.
D. A reference to the stability of the security control: Stability is the opposite of volatility. A control with low volatility would be considered more stable.
upvoted 2 times

Vaneck 1 year, 3 months ago
Selected Answer: D
The correct answer is D. A reference to the stability of the safety control. The volatility of a safety control refers to its stability and ability to remain effective and constant over time without the need for frequent modifications.
upvoted 1 times

DarkHorseVIII 1 year, 4 months ago
Answer is C. ---Kinda like stocks: Penny stocks are very volatile; they go up and down very fast because of how cheap they are. They are very unpredictable.
upvoted 1 times

Demo25 1 year, 11 months ago
Selected Answer: B
The other options are incorrect. A. Impact of the security control refers to the severity of the impact that a security control can have on an organization if it is not properly implemented or maintained. C. Unpredictability of the security control refers to how difficult it is to predict how a security control will behave in a given situation. D. Stability of the security control refers to how resistant a security control is to change.

Therefore, the correct answer is B. A reference to the likelihood of change in the security control.
upvoted 3 times

Bach1968 1 year, 12 months ago
Security control volatility refers to the likelihood of change in the security control. Therefore, option B: A reference to the likelihood of change in the security control is the correct description of security control volatility.
Options A, C, and D are not accurate descriptions of security control volatility:

Option A: A reference to the impact of the security control does not relate directly to volatility but rather focuses on the effect or effectiveness of the control.

Option C: A reference to how unpredictable the security control is does not capture the essence of volatility, which pertains more to the likelihood of change rather than the unpredictability of the control itself.

Option D: A reference to the stability of the security control is not synonymous with volatility. Stability refers to the consistent performance and reliability of the control over time, whereas volatility specifically refers to the potential for changes.
upvoted 1 times

jackdryan 2 years, 2 months ago
B is correct
upvoted 1 times

s_n_ 2 years, 5 months ago
Answer B:
Security control volatility is a term used to refer to the likelihood of change in security control. This is an important concept to consider, as it can impact the effectiveness of a security control over time. Resources that provide further information on security control volatility include the National Institute of Standards and Technology (NIST) Security Control Volatility Framework and the International Organization for Standardization (ISO) 27000 series of standards.
upvoted 1 times

Dee83 2 years, 5 months ago
B. Correct answer
A reference to the likelihood of change in the security control is security control volatility.

Security control volatility refers to the likelihood of change in the security control. It represents how frequently a security control may change or need to be updated to reflect new security threats or business requirements. Security controls that are volatile, such as firewalls, intrusion detection systems, and antivirus software, require more frequent monitoring and updating to ensure that they continue to provide adequate protection. High volatility controls may require more resources and effort to maintain their effectiveness. On the other hand, low volatility controls, such as security policies, may not require as much attention, but still need to be reviewed periodically to ensure that they are still effective and aligned with the organization's needs.

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: B

Security control volatility is a measure of how frequently a control is likely to change over time subsequent to its implementation.
Reference --> NIST SP 800-137, Information Security Continuous Monitoring.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

upvoted 1 times

Firedragon 2 years, 7 months ago

Selected Answer: B

B.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf
Security control volatility is a measure of how frequently a control is likely to change over time subsequent to its implementation.

upvoted 1 times

rootic 2 years, 8 months ago

Selected Answer: B

Going with B.

upvoted 1 times

Eltooth 2 years, 8 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

DragonHunter40 2 years, 8 months ago

Volatility means unpredictable.

upvoted 2 times

Question #35 *Topic 1*

When auditing the Software Development Life Cycle (SDLC) which of the following is one of the high-level audit phases?

A. Planning

B. Risk assessment

C. Due diligence

D. Requirements

Suggested Answer: *C*

Community vote distribution

A (44%) D (41%) Other

⊟ **franbarpro** Highly Voted 👍 2 years, 9 months ago

Selected Answer: D

I am thinking "D" - I don't like this question.

DLC Phases
The entire SDLC process divided into the following SDLC steps:

Phase 1: Requirement collection and analysis
Phase 2: Feasibility study
Phase 3: Design
Phase 4: Coding
Phase 5: Testing
Phase 6: Installation/Deployment
Phase 7: Maintenance

The requirement is the first stage in the SDLC process. It is conducted by the senior team members with inputs from all the stakeholders and domain experts in the industry. Planning for the quality assurance requirements and recognization of the risks involved is also done at this stage.

This stage gives a clearer picture of the scope of the entire project and the anticipated issues, opportunities, and directives which triggered the project.

Requirements Gathering stage need teams to get detailed and precise requirements. This helps companies to finalize the necessary timeline to finish the work of that system.

https://www.guru99.com/software-development-life-cycle-tutorial.html#3

upvoted 16 times

⊟ **1460168** 11 months ago

Requirements are part of the "Planning"-Phase.

upvoted 2 times

⊟ **dumdada** 2 years ago

Read the question again

upvoted 2 times

⊟ **jackdryan** 2 years, 2 months ago

A is correct.

upvoted 2 times

⊟ **explorer3** Highly Voted 👍 2 years, 8 months ago

Selected Answer: A

Planning is an audit phase

upvoted 11 times

⊟ **CKaraf** Most Recent ⊙ 3 months, 3 weeks ago

Selected Answer: D

You check the requirements before starting to Plan.

upvoted 1 times

tama_tama 5 months ago

Selected Answer: B

B. Risk assessment

When auditing the Software Development Life Cycle (SDLC), risk assessment is a key high-level audit phase.

The purpose of an SDLC audit is to evaluate risks in software development, including security vulnerabilities, compliance issues, and operational risks.

Risk assessment helps determine whether security controls and compliance measures are adequately incorporated at each SDLC phase.

For the other options I think!

A. Planning → Planning is an SDLC phase, but it's not specifically a high-level audit phase.

C. Due diligence → Due diligence is more related to business risk management rather than SDLC auditing.

D. Requirements → Requirements gathering is part of SDLC but not a distinct audit phase.

Thus, risk assessment (B) is the best choice as it aligns with SDLC audit objectives.

upvoted 1 times

Fouad777 7 months, 2 weeks ago

The answer is A. Planning.

Here's a breakdown of the high-level audit phases within an SDLC audit:

Planning: This phase involves defining the audit's scope, objectives, and methodology. It includes identifying the specific areas of the SDLC to be audited, such as requirements gathering, design, development, testing, and deployment.

Execution: This phase involves conducting the actual audit, which may include reviewing documentation, interviewing stakeholders, and performing tests.

Reporting: This phase involves documenting the audit findings, including any identified issues or risks. The report is typically shared with management and other relevant stakeholders.

While risk assessment and due diligence are important aspects of software development, they are not typically considered high-level audit phases.

Requirements are part of the SDLC but are not an audit phase.

upvoted 1 times

celomomo 9 months ago

Selected Answer: A

In the context of auditing the SDLC, Planning is a high-level audit phase that is critical for setting the direction and scope of the audit. It lays the groundwork for the audit team's approach and ensures that all subsequent activities are aligned with the audit objectives.

upvoted 2 times

robervalchocolat 10 months ago

The high-level audit phases typically include:

Planning: This phase involves defining the scope of the audit, identifying objectives, and developing an audit plan.

Execution: This phase involves collecting evidence, conducting interviews, and reviewing documentation.

Reporting: This phase involves analyzing the evidence, drafting the audit report, and communicating findings to management.

Therefore, planning is one of the high-level audit phases when auditing the SDLC.

upvoted 1 times

Ramye 1 year ago

The question is - which of the following is a high level audit phase? So Due Diligence appears to be high-level. So the given answer probably correct but would like to confirm this.

upvoted 1 times

CCNPWILL 1 year ago

Selected Answer: D

D. documentation supports D as the correct answer.

upvoted 1 times

duplexjay 1 year, 1 month ago

D is correct. Read page 767 of the Official CISSP CBK Reference, (6th editon).

upvoted 1 times

GuardianAngel 1 year, 4 months ago

Answer: Planning
GENERAL SDLC AUDIT PROCEDURE: plan/prepare, describe process, evaluate/report, followup Slide 17
https://s3.amazonaws.com/kajabi-storefronts-production/file-uploads/sites/69255/themes/2154025622/downloads/50fa5a8-d4c-27cf-08cb-023ecccc54e3_Monica_Chis-SDLC-AUDIT-AUGUST-9.pdf
upvoted 1 times

Kugan 1 year, 5 months ago
Selected Answer: C
A/D are the same meaning, Planning is part of requirement. Answer is C because its part of Due diligence in auditing process
upvoted 2 times

GPrep 1 year, 5 months ago
Selected Answer: A
A - Plan is the only one listed - https://aws.amazon.com/what-is/sdlc/#:~:text=The%20software%20development%20lifecycle%20(SDLC,expectations%20during%20production%20and%20beyond.
upvoted 2 times

AlexJacobson 1 year, 7 months ago
Selected Answer: D
It is ABSOLUTELY D:

Official CISSP CBK (6th edition):

Software Development Auditing phases:
- Requirements phase
- Requirements phase
- Implementation phase
- Verification phase
- Operation and maintenance phase
upvoted 5 times

duplexjay 1 year, 1 month ago
D is correct
upvoted 1 times

NameisAlreadyTaken 1 year, 7 months ago
Selected Answer: C
Every option is under the due diligence
upvoted 1 times

bluerock2k 1 year, 7 months ago
"A" Question is for "Audit phases" not SDLC steps:

Phase 1: Requirement collection and analysis
Phase 2: Feasibility study
Phase 3: Design
Phase 4: Coding
Phase 5: Testing
Phase 6: Installation/Deployment
Phase 7: Maintenance
upvoted 1 times

Moose01 1 year, 9 months ago
A. Planning
Planning phase also includes requirements, a wish list of the stakeholders/senior management and experts, which at this point the audit will gather all items the will audit as SDLC moves from one phase to the next.
upvoted 3 times

Question #36 *Topic 1*

What is the term used to define where data is geographically stored in the cloud?

A. Data privacy rights

B. Data sovereignty

C. Data warehouse

D. Data subject rights

Suggested Answer: *B*

Community vote distribution

B (100%)

Fouad777 7 months, 2 weeks ago

The answer is B. Data Sovereignty.

Data sovereignty refers to the legal jurisdiction and control over data, including where it is stored and processed. It's a crucial consideration for organizations, especially those dealing with sensitive data, as it impacts compliance with various data protection laws and regulations.

upvoted 1 times

somsom 8 months, 2 weeks ago

B is correct where data resides in the cloud

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: B

Answer B) Data Sovereignty

The real answer should be "DATA RESIDENCY", but "B" is the closest answer among the choices given.

Definition: Data residency refers to the physical or geographical location where data is stored and processed.

upvoted 2 times

Bach1968 1 year, 12 months ago

Selected Answer: B

The term used to define where data is geographically stored in the cloud is option B: Data sovereignty.

Data sovereignty refers to the legal and regulatory requirements that determine the physical location or jurisdiction in which data is stored, processed, and managed. It relates to the concept that data is subject to the laws and regulations of the country or region in which it resides.

When data is stored in the cloud, organizations must consider data sovereignty to ensure compliance with applicable laws and regulations, as different countries may have different requirements regarding data privacy, security, and access. Data sovereignty addresses concerns about data protection, data privacy rights, and the control and ownership of data.

i again stress that i do not like sensitive data to leave the premises.

upvoted 2 times

Eltooth 2 years, 8 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 1 times

franbarpro 2 years, 9 months ago

Selected Answer: B

Agree with B

Data sovereignty is a country-specific requirement that data is subject to the laws of the country in which it is collected or processed and must remain within its borders. Therefore, organizations must pay close attention to how they are managing their data in different locations.

https://www.virtru.com/resource/data-sovereignty-laws-and-the-cloud#:~:text=Data%20Sovereignty%20in%20the%20Cloud&text=Data%20sovereignty%20is%20a%20country,their%20data%20in%20different%20locations.

upvoted 2 times

Question #37 *Topic 1*

Which of the following does the security design process ensure within the System Development Life Cycle (SDLC)?

A. Proper security controls, security objectives, and security goals are properly initiated.

B. Security objectives, security goals, and system test are properly conducted.

C. Proper security controls, security goals, and fault mitigation are properly conducted.

D. Security goals, proper security controls, and validation are properly initiated.

Suggested Answer: *D*

Community vote distribution

A (73%) D (27%)

krassko Highly Voted 2 years, 9 months ago

Selected Answer: A

It can't be D or anything where testing or validation is mentioned.
as validation or testing are not part of the design but part of the next phase - implementation.

upvoted 6 times

RedMartian Most Recent 2 months, 3 weeks ago

Selected Answer: A

Not D. Validation is a later phase. Security design focuses on initialization rather than testing or validation.

upvoted 1 times

Fouad777 6 months, 1 week ago

Selected Answer: A

In the context of the security design process within the System Development Life Cycle (SDLC), both option A and option D have their merits, but it ultimately depends on the specific needs and requirements of the organization.

upvoted 1 times

Fouad777 7 months, 2 weeks ago

he answer is A. Proper security controls, security objectives, and security goals are properly initiated.

The security design process in the SDLC is focused on ensuring that security is baked into the system from the very beginning. This includes:

Initiating security objectives and goals: Clearly defining the security objectives and goals for the system.
Defining security controls: Identifying and implementing appropriate security controls to protect the system and its data.
Ensuring proper initiation: Making sure that these security measures are properly initiated and integrated into the development process.
While other options may involve important aspects of the SDLC, they do not accurately capture the core focus of the security design process, which is to establish a strong security foundation from the outset.

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: A

In the context of the security design process within the System Development Life Cycle (SDLC), both option A and option D have their merits, but it ultimately depends on the specific needs and requirements of the organization.

Option A: Proper security controls, security objectives, and security goals are properly initiated emphasizes the importance of ensuring that the appropriate security controls, objectives, and goals are identified and initiated during the security design process. This option highlights the need for a proactive approach in implementing security measures from the early stages of system development.

Option D: Security goals, proper security controls, and validation are properly initiated adds the aspect of validation to the mix. It emphasizes the importance of not only setting security goals and implementing security controls but also ensuring that these controls are validated to ensure their effectiveness and alignment with the desired security objectives.

both are valid, as i said earlier, it all depend on the requirements or the need of the company/organization.

upvoted 2 times

KelvinYau 2 years ago

Selected Answer: A

I think A...

upvoted 1 times

Dee83 2 years, 5 months ago

A. Proper security controls, security objectives, and security goals are properly initiated.

The security design process within the System Development Life Cycle (SDLC) ensures that proper security controls, security objectives, and security goals are properly initiated. This includes identifying and assessing risks, and implementing controls to mitigate those risks. The security design process is a critical step in ensuring the security and integrity of a system throughout its lifecycle.

upvoted 2 times

> **jackdryan** 2 years, 2 months ago
>
> A is correct
>
> upvoted 1 times

Billy235 2 years, 7 months ago

Eliminate options B and C as system test and fault mitigation are not security specific and already done somewhere in SDLC. Option D is better than A as it validates security which ends a process. Answer is D.

upvoted 2 times

FredDurst 2 years, 7 months ago

Selected Answer: A

Poorly worded question . The key differentiator here is the term "Objectives" that makes A a winner .

upvoted 2 times

rootic 2 years, 8 months ago

Think it's A.

upvoted 2 times

Eltooth 2 years, 8 months ago

Selected Answer: A

A is correct answer imo.

upvoted 1 times

krassko 2 years, 8 months ago

Selected Answer: A

It's A, all others are from "Implementation" phase

upvoted 1 times

dev46 2 years, 9 months ago

A & D are "initiated"
B & C are "conducted"

The secure design process relates to some kind of initiation, so I eliminate B and C

A - Aren't security goals and objectives are same?
B - but how can validation be part of the process?

Thoughts?

upvoted 2 times

franbarpro 2 years, 9 months ago

Selected Answer: D

MAAAAAAAAAYYYBBBBEEEEE "D" - Only because it has validation in it. I am thinking as they develop the software they will keep validating and testing the software for bugs and fixing them as the go.

https://snyk.io/learn/secure-sdlc/

Implementing SDLC security affects every phase of the software development process. It requires a mindset that is focused on secure delivery, raising issues in the requirements and development phases as they are discovered. This is far more efficient—and much cheaper—than waiting for these security issues to manifest in the deployed application. Secure software development life cycle processes incorporate security as a component of every phase of the SDLC.

While building security into every phase of the SDLC is first and foremost a mindset that everyone needs to bring to the table, security considerations and associated tasks will actually vary significantly by SDLC phase.

upvoted 4 times

⊟ **franbarpro** 2 years, 8 months ago

Changed my answer to "A"

upvoted 1 times

⊟ **DERCHEF2009** 2 years, 9 months ago

really?

upvoted 1 times

Question #38 *Topic 1*

Which of the following is MOST important to follow when developing information security controls for an organization?

A. Use industry standard best practices for security controls in the organization.

B. Exercise due diligence with regard to all risk management information to tailor appropriate controls.

C. Review all local and international standards and choose the most stringent based on location.

D. Perform a risk assessment and choose a standard that addresses existing gaps.

Suggested Answer: *C*

Community vote distribution

B (48%) D (30%) C (22%)

JAckThePip Highly Voted 2 years, 9 months ago

Answer is D

"To assess risk, you need to think about threats and vulnerabilities. Start by making a list of any potential threats to your organization's assets, then score these threats based on their likelihood and impact. From there, think about what vulnerabilities exist within your organization, categorize and rank them based on potential impact. These vulnerabilities can consist of people (employees, clients, third parties), processes or lack thereof, and technologies in place. "

https://www.barradvisory.com/roadmap-to-implementing-a-successful-information-security-program/

upvoted 9 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 4 times

Loveguitar Highly Voted 2 years, 9 months ago

Performing risk assessment covers answer C, for example, if you need to be PCI DSS compliant, you first assess the risk in your environment and compare it with what the standard says, your ISA can help you do that before the external assessor (QSA) comes in and assesses your controls (again the PCI DSS standard) to see your gaps.

upvoted 6 times

Dean1403 Most Recent 3 weeks, 4 days ago

Selected Answer: B

Start with a thorough risk assessment and build security controls that are business aligned, compliant, layered, and adaptable

upvoted 1 times

fuzzyguzzy 2 months, 3 weeks ago

Selected Answer: B

While all the options have merit, the most critical factor is ensuring that security controls are risk-based and tailored to the organization's specific needs.

upvoted 1 times

AjitZavade 2 months, 3 weeks ago

Selected Answer: B

This question is about developing information security controls, and the focus is on what's most important — which means we're looking for the most foundational and risk-based approach.

✅ "Exercise due diligence with regard to all risk management information to tailor appropriate controls"
means:

You use risk-based thinking

You evaluate the organization's specific threats, vulnerabilities, and requirements

You customize controls accordingly, rather than blindly applying standards

This aligns with both:

CISSP best practices

NIST, ISO, and risk-based frameworks like ISO 27005, NIST SP 800-30

upvoted 1 times

RedMartian 2 months, 3 weeks ago

Selected Answer: B

Not C. Review all local and international standards and choose the most stringent based on location. Might lead to unnecessary complexity or cost without addressing specific organizational needs.
Not D. Perform a risk assessment and choose a standard that addresses existing gaps. Valuable, but it emphasizes choosing a standard, not tailoring individual controls based on due diligence and comprehensive risk understanding.

upvoted 1 times

dra3m 3 months ago

Selected Answer: B

B is more detail and specific, although D can be good , standard is not everything when developing controls. some standard are non prescriptive, some need to be tailored as no standard fits all.

upvoted 1 times

Fouad777 6 months, 1 week ago

Selected Answer: B

B. Exercise due diligence with regard to all risk management information to tailor appropriate controls.

When developing information security controls, due diligence ensures that the chosen controls are appropriate and effective based on the specific risks and needs of the organization. By considering all risk management information—such as the organization's risk profile, potential threats, vulnerabilities, and the impact of a security breach—security controls can be tailored to address the unique risks the organization faces. This approach helps ensure that the controls are both effective and proportionate to the risks.

upvoted 2 times

somsom 8 months, 2 weeks ago

The answer is obviously D, risk assessment, gap analysis (Full, partial and non-compliance with ISO Controls) the implementation of Security controls in compliance with ISO 27001

upvoted 1 times

celomomo 9 months ago

Selected Answer: D

Starting point is always review the existing plan and identify gaps. Also the same in ITIL v4. D

upvoted 1 times

adc9365 10 months, 1 week ago

Selected Answer: D

Risk assessment is most important to event start to know which controls are needed then you determine the rules and regulations.

upvoted 1 times

JohnBentass 1 year ago

Selected Answer: B

B. Exercise due diligence with regard to all risk management information to tailor appropriate controls.

This approach ensures that the security controls are specifically tailored to the unique risks and needs of the organization. By exercising due diligence, you can identify and assess the specific threats and vulnerabilities that the organization faces, and implement controls that are most effective in mitigating those risks. This method aligns with best practices in risk management and ensures that resources are allocated efficiently to address the most critical security concerns.

upvoted 1 times

1ee7bdb 1 year, 2 months ago

D is the answer

upvoted 1 times

Hardrvkllr 1 year, 2 months ago

B:
Always need to do your "Due Diligence, and Due Care." While a stringent policy and rules need to be in place, you need to remember, when implementing said controls, they need to be within reach in order to make it an effective control. Due diligence should cover the expectation of cover the local and international standards. It "SHOULD" be implied that it is being looked into, or has been looked into.

upvoted 1 times

AshStevens 1 year, 2 months ago

Selected Answer: D

D. You need to know what you are doing before you can implement A. Due dilligence means nothing if you picked the wrong thing and don't know what you are doing it for. C is partly covered by D and you may not even want the "most stringent" depending on your organisation. Think like a manager!

upvoted 2 times

homeysl 1 year, 3 months ago

Selected Answer: D

You need to identify the risk to make an informed decision

upvoted 1 times

Vaneck 1 year, 3 months ago

Selected Answer: D

The most important option to follow when developing information security controls for an organization is D. Perform a risk assessment and choose a standard that addresses existing gaps. This ensures that security controls are specifically tailored to the organization's needs and vulnerabilities, providing more effective protection against identified threats.

upvoted 2 times

Question #39 *Topic 1*

When recovering from an outage, what is the Recovery Point Objective (RPO), in terms of data recovery?

A. The RPO is the minimum amount of data that needs to be recovered.

B. The RPO is the amount of time it takes to recover an acceptable percentage of data lost.

C. The RPO is a goal to recover a targeted percentage of data lost.

D. The RPO is the maximum amount of time for which loss of data is acceptable.

Suggested Answer: *D*

Community vote distribution

D (91%) 9%

Bach1968 Highly Voted 1 year, 12 months ago

Selected Answer: D

The Recovery Point Objective (RPO) is the maximum amount of time for which loss of data is acceptable in the event of an outage or disaster.

The RPO defines the point in time to which data must be recovered after a disruption, indicating the acceptable level of data loss. It represents the maximum tolerable period during which data may be lost without causing significant impact or harm to the business operations or objectives.

For example, if a company has an RPO of 1 hour, it means that in the event of an outage, the organization can accept a maximum data loss of up to 1 hour's worth of data. The data must be restored or recovered to a state no older than 1 hour before the incident occurred.

upvoted 11 times

MShaaban 1 year, 11 months ago

Thank you. Great explanation.

upvoted 2 times

scoobysnack209 Most Recent 8 months, 1 week ago

RPO - The amount of data to back up. 24 hours? 48 hours and so on.
RTO - The maximum amount of time it takes to restore the network. Nothing to do with data

upvoted 1 times

omarin25 2 years, 4 months ago

Selected Answer: A

Minimum amount of data we need to recover

upvoted 3 times

jackdryan 2 years, 2 months ago

D is correct

upvoted 1 times

dirtmcderp 2 years, 5 months ago

There is 2 important parts to consider here.
1. "When RECOVERING from an outage"
2. "In terms of data recovery"
They are not asking for the definition of RPO, which is the amount of data the business can lose, it's asking about the requirements for recovery.

So if a business has an RPO of lets say 10 GB... That means that the business needs to recover those 10 GB. It's not asking what is acceptable in terms of how much data can be lost.

D is incorrect. . I'm going with A.

upvoted 1 times

Jamati 2 years, 8 months ago

Selected Answer: D

Answer is D

Page 123 of the official study guide 9th edition:
An organization might perform database transaction log backups every 15 minutes. In that case, the RPO would be 15 minutes, meaning that the organization may lose up to 15 minutes' worth of data after an incident. If an incident takes place at 8:30 a.m., the last transaction log backup must have occurred sometime between 8:15 a.m. and 8:30 a.m. Depending on the precise timing of the incident and the backup, the organization may have irretrievably lost between 0 and 15 minutes of data.

upvoted 4 times

Eltooth 2 years, 8 months ago

Selected Answer: D

D is correct answer.

upvoted 2 times

stickerbush1970 2 years, 9 months ago

Selected Answer: D

RPO recovery point objective is a time-based measurement of the maximum amount of data loss that is tolerable to an organization. Also called backup recovery point objective, RPO is additionally important to determining whether the organization's backup schedule is sufficient to recover after a disaster.

upvoted 3 times

franbarpro 2 years, 9 months ago

Selected Answer: D

I am doing with D as well.

Recovery point objective (RPO) is defined as the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization. An RPOs determines the maximum age of the data or files in backup storage needed to be able to meet the objective specified by the RPO, should a network or computer system failure occur.

An organization's loss tolerance, or how much data it can lose without sustaining significant harm, is related to RPO and is set forth in the organization's business continuity plan (BCP). This also dictates procedures for disaster recovery planning, including the acceptable backup interval, because it refers to the last point when the organization's data was preserved in a usable format. For example, an RPO of 60 minutes requires a system backup every 60 minutes.

https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/

upvoted 4 times

kasiya 2 years, 9 months ago

Selected Answer: D

The RPO defines the point in time before the incident where the organization should be able to recover data from a critical business process. For example, an organization might perform database transaction log backups every 15 minutes. In that case, the RPO would be 15 minutes, meaning that the organization may lose up to 15 minutes' worth of data after an incident. If an incident takes place at 8:30 a.m., the last transaction log backup must have occurred sometime between 8:15 a.m. and 8:30 a.m. Depending on the precise timing of the incident and the backup, the organization may have irretrievably lost between 0 and 15 minutes of data.

upvoted 3 times

CuteRabbit168 2 years, 9 months ago

Selected Answer: D

Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance."

upvoted 3 times

Mgz156 2 years, 9 months ago

Selected Answer: D

Answer is D
The recovery time objective (RTO) is the targeted duration of time between the event of failure and the point where operations resume. A recovery point objective (RPO) is the maximum length of time permitted that data can be restored from, which may or may not mean data loss.

upvoted 4 times

Cww1 2 years, 9 months ago

D is describing RTO, Im going A

upvoted 4 times

⊟ **lin** 2 years, 9 months ago

Accidentally upvoted this item but it is wrong. Right answer is definitely 1000% A.

upvoted 1 times

⊟ **Cww1** 2 years, 9 months ago

Changing to D, ty.

upvoted 1 times

Question #40 *Topic 1*

Which of the following attacks, if successful, could give an intruder complete control of a software-defined networking (SDN) architecture?

A. A brute force password attack on the Secure Shell (SSH) port of the controller

B. Sending control messages to open a flow that does not pass a firewall from a compromised host within the network

C. Remote Authentication Dial-In User Service (RADIUS) token replay attack

D. Sniffing the traffic of a compromised host inside the network

Suggested Answer: *B*

Community vote distribution

B (49%) | A (46%) | 5%

N00b1e Highly Voted 👍 2 years, 9 months ago

Selected Answer: A

If you can get control of the controller, do you not own the network?

upvoted 11 times

1460168 11 months ago

Brute-Forcing the SSH __PORT__... You aren't bruting the "port", you are bruting the service.

upvoted 2 times

franbarpro 2 years, 8 months ago

"YES" but how are you going to brute force the SSH password.

upvoted 3 times

ccKane 1 year, 9 months ago

Not the question. It is stated: "If successful..." therefore no matter how.

upvoted 5 times

dev46 2 years, 9 months ago

I will go with A too, the SDN controller is the heart. Compromising controller can initiate other attacks defined in B, C and D.

https://www.routerfreak.com/9-types-software-defined-network-attacks-protect/

upvoted 3 times

jackdryan 2 years, 2 months ago

A is correct

upvoted 1 times

franbarpro Highly Voted 👍 2 years, 9 months ago

Agree with B

https://www.networkworld.com/article/2840273/sdn-security-attack-vectors-and-sdn-hardening.html#:~:text=SDN%20Attack%20Vectors,new%20paradigm%20for%20network%20virtualization.

upvoted 5 times

RedMartian Most Recent 🕘 2 months, 3 weeks ago

Selected Answer: A

"if successful"

upvoted 1 times

Imranbhatti 3 months, 3 weeks ago

Selected Answer: A

Answer is A

Option B, "Sending control messages to open a flow that does not pass a firewall from a compromised host within the network," is incorrect because it does not necessarily give an intruder complete control over the SDN architecture.

While sending control messages from a compromised host can bypass certain security measures like firewalls, it typically affects only specific flows or segments of the network. This action does not compromise the central SDN controller itself, which is the core component managing the entire network. Without access to the controller, the attacker cannot gain full control over the SDN architecture12.

In contrast, a successful brute force attack on the SSH port of the controller (Option A) would allow the attacker to take over the controller, giving them comprehensive control over the entire network. Answer is A

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: A

A successful brute-force attack on the SSH port of the SDN controller is the more dangerous scenario. The controller is the central brain of the SDN architecture. If an attacker gains control of it, they effectively gain control of the entire network. They can manipulate flows, reroute traffic, isolate devices, and perform any action imaginable within the network.

While B (sending control messages to open a flow) is a serious attack, its scope is more limited. Even if successful, the attacker's control is generally restricted to the specific flow they manipulate. They might be able to intercept or modify traffic for that particular flow, but they don't automatically gain complete control of the entire SDN architecture. The controller still retains overall management. Compromising the controller itself, however, grants the attacker that complete control.

upvoted 1 times

martin451 8 months, 3 weeks ago

Selected Answer: A

Gaining access to the SDN controller through a brute force attack on the SSH port would allow the attacker to manipulate the entire network, as the controller is the central point of control in an SDN architecture.

upvoted 1 times

robervalchocolat 10 months ago

A brute force password attack on the SSH port of the SDN controller, if successful, could give an intruder complete control of the controller. This is because the controller is responsible for managing the network's configuration and traffic flows. If an attacker gains control of the controller, they can manipulate the network's behavior to their advantage.

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: A

I agree with A. If you could somehow bypass a firewall from a compromised host, then there's still a question of privileges and authorization of control messages to gain complete control. Unless you're sending it from a compromised admin host/account, which you might have potentially bruteforced (presumably). lol

upvoted 1 times

CCNPWILL 1 year ago

Selected Answer: B

Most of these SDN questions and compromising it CISSP exam usually looks for controller related answer ive come to notice. compromising the controller gives you access to the fabric.

upvoted 1 times

duplexjay 1 year, 1 month ago

A gives complete control while B gives complete access.

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: A

My AI told me that A is correct. So that is it.

upvoted 2 times

25cbb5f 1 year, 2 months ago

Out of the options provided, the attack most likely to give an intruder complete control of an SDN architecture is:

A. A brute force password attack on the Secure Shell (SSH) port of the controller

Here's why:

Why SDN Controllers are Critical Targets: SDN separates the control plane (where network configuration happens) from the data plane (where traffic flows). The controller is the central, highly privileged component that orchestrates the entire network. Compromising it would grant an attacker substantial power.

Brute Force and SSH: A brute force attack attempts to guess the controller's administrative credentials through repeated login attempts. SSH is a common remote management protocol, and if its protection is weak, a successful brute force attack can lead to control plane takeover.

upvoted 1 times

Parikshitcyber 1 year, 3 months ago

While gaining SSH access to the controller through a brute force password attack option A is indeed a serious security concern and could potentially allow an attacker to gain administrative access to the SDN controller, it may not necessarily result in complete control of the entire SDN architecture.

On the other hand, option B describes an attack scenario where a compromised host within the network sends control messages to the SDN controller to open a flow that bypasses the firewall. This attack directly targets the SDN architecture itself and could potentially give the intruder complete control over network traffic flows, allowing them to manipulate traffic and potentially compromise other network devices or services.

Thats why it is B

upvoted 1 times

Ukpes 1 year, 8 months ago

Selected Answer: B

This type of attack, known as a flow rule modification attack, can allow an attacker to inject malicious traffic into the network or bypass security controls, giving the attacker complete control over the network.

upvoted 2 times

homeysl 1 year, 8 months ago

Selected Answer: A

easy one. A is my answer.

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: B

The attack that could give an intruder complete control of a software-defined networking (SDN) architecture is option B: Sending control messages to open a flow that does not pass a firewall from a compromised host within the network.

In software-defined networking, the SDN controller is responsible for managing and controlling the network infrastructure. By sending control messages to open a flow that bypasses the firewall from a compromised host within the network, an attacker can gain unauthorized access and manipulate the network's behavior.

B

upvoted 3 times

HughJassole 2 years ago

A. "By compromising the SDN controller, a hacker could have total control of the network."
I googled B and C and those don't come up, so I don't think they are valid.
D. is just sniffing traffic. This seems too easy, but based on all my research A it is.

upvoted 1 times

HughJassole 1 year, 11 months ago

I researched this more and thought about it, A doesn't make sense because once you ssh into a system you need to become root to do any damage, otherwise it's pointless.
B. is absolutely correct:
"If an attacker could create a flow that bypasses the traffic steering that guides traffic through a firewall the attacker would have a decided advantage."

"The attacker would want to instantiate new flows by either spoofing northbound API messages or spoofing southbound messages toward the network devices. If an attacker can successfully spoof flows from the legitimate controller then the attacker would have the ability to allow traffic to flow across the SDN at their will and possibly bypass policies that may be relied on for security."
https://www.networkworld.com/article/2840273/sdn-security-attack-vectors-and-sdn-hardening.html

upvoted 5 times

Question #41 *Topic 1*

Which of the following is the BEST option to reduce the network attack surface of a system?

A. Disabling unnecessary ports and services

B. Ensuring that there are no group accounts on the system

C. Uninstalling default software on the system

D. Removing unnecessary system user accounts

Suggested Answer: *A*

Community vote distribution

A (100%)

franbarpro Highly Voted 2 years, 9 months ago

Selected Answer: A

The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect.

https://www.fortinet.com/resources/cyberglossary/attack-surface

upvoted 8 times

jackdryan 2 years, 2 months ago

A is correct

upvoted 2 times

0211e3f Most Recent 8 months, 4 weeks ago

Selected Answer: A

Reducing attack surface will best protect the network.

upvoted 1 times

dimosatteia 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: A

or the use of revers proxy

upvoted 1 times

Ivanchun 2 years, 6 months ago

Selected Answer: A

A, because talking about network attack

upvoted 2 times

Jamati 2 years, 7 months ago

Selected Answer: A

I'll go with A.

upvoted 2 times

Eltooth 2 years, 8 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

Question #42 *Topic 1*

The security architect is designing and implementing an internal certification authority to generate digital certificates for all employees. Which of the following is the
BEST solution to securely store the private keys?

A. Physically secured storage device

B. Trusted Platform Module (TPM)

C. Encrypted flash drive

D. Public key infrastructure (PKI)

Suggested Answer: *B*

Community vote distribution

B (57%) | D (29%) | 14%

oudmaster Highly Voted 2 years, 6 months ago

Every employee will have a digital certificate. That means every of the them will have a private key stored in his device.
The private keys will be stored in the TPM of the users' devices.
PKI is a framework and irrelevant to storing the keys.

upvoted 12 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: B

Not D - PKI is the overall framework for managing keys and certificates, but it does not specify or implement the storage mechanism for private keys itself.

upvoted 1 times

robervalchocolat 10 months ago

Trusted Platform Module (TPM): A TPM is a hardware-based security module that is typically embedded on the motherboard of a computer system. It provides secure storage for cryptographic keys and other sensitive data. TPMs are designed to be tamper-resistant and can be used to protect against various attacks, including cold boot attacks and physical tampering.

upvoted 1 times

isaphiltrick 10 months, 2 weeks ago

Selected Answer: B

A Trusted Platform Module (TPM) is a dedicated hardware chip designed to securely store cryptographic keys, including private keys. It provides hardware-based security by protecting the keys from unauthorized access and tampering. TPMs are widely recognized as one of the most secure options for storing private keys, especially within an internal certification authority (CA) environment, where the security of private keys is critical.

upvoted 1 times

Hardrvkllr 1 year, 2 months ago

B:
The key word is, "Store..."

upvoted 2 times

eboehm 1 year, 2 months ago

For key storage its pretty much always going to be a TPM or HSM.
Ima go with A as I think a Physically secure storage device is just another name for HSM

upvoted 1 times

8b48948 1 year, 3 months ago

The question states nothing to do with the devices being laptops. VMs dont have TPMs neither do desktops, so how could it be TPM.

upvoted 1 times

> **eboehm** 1 year, 2 months ago
>
> ummm pretty much all modern desktops have tpms
>
> upvoted 1 times

8b48948 1 year, 3 months ago

If you issue certs from AD CS to Windows devices the private user key is not stored on the TPM of the laptop. This would have to be PKI IMO.

upvoted 2 times

GPrep 1 year, 5 months ago

Selected Answer: B

B - from CISSP Official Study Guide (Sybex) - Trusted Platform Module Modern computers often include a specialized cryptographic component known as a Trusted Platform Module (TPM). The TPM is a chip that resides on the motherboard of the device. The TPM serves a number of purposes, including the storage and management of keys used for full-disk encryption (FDE) solutions. The TPM provides the operating system with access to the keys only if the user successfully authenticates. This prevents someone from removing the drive from one device and inserting it into another device to access the drive's data.

Chapple, Mike; Stewart, James Michael; Gibson, Darril. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (Sybex Study Guide) (p. 286). Wiley. Kindle Edition.

upvoted 1 times

abenall 1 year, 7 months ago

The best answer is B. Trusted Platform Module (TPM) because TPMs provide hardware-based security that is more resilient to external software attacks than software-based encryption solutions. They are designed to protect and store cryptographic keys securely within the hardware, making it a suitable option for securing the private keys of a certification authority.

upvoted 1 times

Ukpes 1 year, 8 months ago

Selected Answer: B

A Trusted Platform Module (TPM) is a cryptographic processor embedded into a computer. It provides authentication and full-disk encryption.

upvoted 1 times

dimosatteia 1 year, 9 months ago

Selected Answer: B

TPM is correct.

upvoted 1 times

Sledge_Hammer 1 year, 9 months ago

B is the correct answer!
A Trusted Platform Module (TPM) is a specialized chip on a laptop or desktop computer that is designed to secure hardware with integrated cryptographic keys. A TPM helps prove a user's identity and authenticates their device.
In this case, the employees each own a TPM compliant device.

upvoted 1 times

KelvinYau 2 years ago

Selected Answer: B

I think should be A vs B.
the question asking internal certification <- so i choose B

upvoted 1 times

A1nthem 2 years, 2 months ago

Selected Answer: B

designing and implementing an "internal" certification authority

upvoted 2 times

4study 2 years, 5 months ago

Selected Answer: B

I vote B as well

upvoted 1 times

> **jackdryan** 2 years, 2 months ago
>
> B is correct
>
> upvoted 1 times

JohnyDal 2 years, 5 months ago

Selected Answer: B

TPM and HSM are the best options to store crypto keys

upvoted 3 times

Question #43 *Topic 1*

The existence of physical barriers, card and personal identification number (PIN) access systems, cameras, alarms, and security guards BEST describes this security approach?

A. Access control

B. Security information and event management (SIEM)

C. Defense-in-depth

D. Security perimeter

Suggested Answer: *D*

Community vote distribution

C (47%) | D (42%) | 11%

RVoigt Highly Voted 2 years, 4 months ago

Selected Answer: D

CISSP Official Study Guide pg 73 - Defense in depth includes administrative, technical (logical) and physical controls. What's listed is only physical controls. Answer is D.

upvoted 15 times

CCNPWILL 1 year ago

So a PIN number is a physical control? The correct answer is C my guy.

upvoted 2 times

Ramye 1 year ago

Yes , the PIN for the card that you need to use to get into the building.

upvoted 1 times

jens23 2 years ago

Exactly!

upvoted 2 times

GenesisTech Highly Voted 2 years, 8 months ago

Selected Answer: C

MFA + physical layer. (defense in depth)

upvoted 7 times

jackdryan 2 years, 2 months ago

C is correct

upvoted 3 times

Privacy2024 Most Recent 1 week, 5 days ago

Selected Answer: C

CISSP wants you to think like a manager and identify strategy over tools. Therefore the answer should be C - Defense in Depth.

upvoted 1 times

AjitZavade 2 months, 3 weeks ago

Selected Answer: C

The question lists multiple, layered security controls:

Physical barriers

Card and PIN access systems

Cameras

Alarms

Security guards

This clearly represents a multi-layered approach to security, which is the core concept behind:

✅ Defense-in-depth — the use of multiple types of security controls at different layers (physical, technical, administrative) to protect assets.

Defense-in-depth ensures:
If one layer fails, others are still in place

Both preventive and detective controls are used

Covers different attack surfaces (physical, digital, human)
upvoted 1 times

RedMartian 2 months, 3 weeks ago

Selected Answer: C

Defense-in-depth is a layered security strategy that uses multiple controls (physical, technical, administrative) to protect assets.
upvoted 1 times

Imranbhatti 3 months, 3 weeks ago

Selected Answer: D

The correct answer is D. Security perimeter.

A security perimeter involves the use of physical and logical measures to protect the boundaries of a secure area. This includes physical barriers, card and PIN access systems, cameras, alarms, and security guards, all of which are designed to prevent unauthorized access and detect any security breaches.
Option C, "Defense-in-depth," is incorrect in this context because it refers to a layered security strategy that employs multiple security measures to protect information and systems. While defense-in-depth can include physical security measures, it also encompasses a wide range of other controls, such as technical, administrative, and procedural safeguards.

The scenario described focuses specifically on physical security measures like barriers, access systems, cameras, alarms, and security guards, which are best categorized under the concept of a security perimeter. This term specifically addresses the physical boundaries and measures used to protect a secure area.
upvoted 1 times

CKaraf 3 months, 3 weeks ago

Selected Answer: D

D. Not C as there is no mention for network security for example
upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: D

While defense-in-depth includes perimeter security, the description focuses specifically on the outer layer of security: physical barriers, card/PIN access, cameras, alarms, and guards. These elements work together to control and monitor access to a secured area, which is the core concept of a security perimeter. Defense-in-depth would encompass multiple layers of security beyond just the perimeter.
upvoted 1 times

easyp 5 months ago

Selected Answer: C

The correct answer is:

C. Defense-in-depth

Explanation:
The scenario describes multiple layers of security controls designed to protect an organization's assets. This approach is known as defense-in-depth, which involves implementing various types of security measures at different levels to create overlapping defenses. The goal is to ensure that if one security measure is bypassed, others remain in place to mitigate the risk.

Breakdown of Components in the Scenario:
Physical barriers: Prevent unauthorized access to facilities.
Card and PIN access systems: Provide an additional layer of authentication.
Cameras and alarms: Detect and deter unauthorized activities.

Security guards: Act as a human layer of enforcement and monitoring.

Each of these components contributes to an overall strategy of layering security to protect against a range of threats.

upvoted 1 times

lifre 5 months, 2 weeks ago

Selected Answer: A

In my opinion, the correct answer is “A” – Access control.

SIEM is not dealing with physical controls and instead focuses on data collection and analysis, regarding a completely different layer.

Defense-in-depth describes a concept of multiple layers of security controls that provides security in case of the failure of one or more layers. I can’t see this approach here.

Security perimeter would describe the subset of physical access controls that are described here (e.g. physical barriers), but overall I’d say that “Access control” would be the broader definition to include all of the mentioned measurements.

upvoted 1 times

Fouad777 6 months, 1 week ago

Selected Answer: C

Defense-in-depth is a comprehensive security strategy that employs multiple layers of security controls across various levels of an organization to protect against threats. The idea is to create a layered defense, so if one security measure fails, other layers still provide protection.

The components mentioned—physical barriers, card and PIN access systems, cameras, alarms, and security guards—are all elements of physical security and access control, which are part of a broader defense-in-depth strategy. These measures work together to provide redundancy, so even if one layer is bypassed, others are still in place to protect the organization.

upvoted 1 times

SangSang 5 months, 2 weeks ago

Stop using ChatGPT, use you brain please.

upvoted 1 times

Zapepelele 6 months, 2 weeks ago

Selected Answer: C

Defense-in-depth, does indeed encompass the elements described in option D, Security perimeter, along with additional layers of security measures.

upvoted 1 times

somsom 8 months, 2 weeks ago

C is the correct answer, A security perimeter example is a firewall,

upvoted 1 times

M_MUN17 8 months, 3 weeks ago

Selected Answer: C

Defense-in-depth is a security strategy that employs multiple layers of security controls to protect an organization's assets. The use of physical barriers, card and PIN access systems, cameras, alarms, and security guards exemplifies this approach, as it combines various security measures to provide a comprehensive defense against unauthorized access or threats.

The other options are less accurate in this context:

A. Access control focuses specifically on the policies and procedures for granting or denying access to resources.

B. Security information and event management (SIEM) refers to systems that aggregate and analyze security data from various sources, which is not directly related to physical security measures.

D. Security perimeter typically refers to the boundary around an organization’s physical or network environment but does not encompass the multi-layered nature of defense-in-depth.

upvoted 2 times

deeden 10 months, 4 weeks ago

Selected Answer: C

I feel like C is most appropriate. A perimeter is just one layer, more like a fence. Imagine walking in to a facility with all these controls mentioned as you approach from the gate, to the parking lot, and finally the building entrance.

upvoted 2 times

iamlamzzy 1 year ago

Selected Answer: C

A. Access control: This refers specifically to mechanisms that manage who or what is allowed to access resources, which would include card and PIN systems but not necessarily the broader range of physical security measures mentioned.

B. Security information and event management (SIEM): This involves the collection, analysis, and reporting of security data from various sources, primarily focused on digital events rather than physical security measures.

C. Defense-in-depth: This is a comprehensive strategy that integrates multiple layers of security, including both physical and logical controls. The description given fits this approach as it includes multiple layers of physical security measures.

D. Security perimeter: This generally refers to the boundary that separates a secured area from a non-secured area. While it can include some of the elements mentioned, it does not fully encapsulate the range of security measures described.

upvoted 2 times

⊟ **1460168** 11 months ago

D: Is boundary, correct.

C: Is physical and logical (PIN Number), correct.

upvoted 1 times

⊟ **CCNPWILL** 1 year ago

Selected Answer: C

Def in depth. physical barrier and knowing a PIN number is already different controls.

upvoted 1 times

Question #44 *Topic 1*

A hospital enforces the Code of Fair Information Practices. What practice applies to a patient requesting their medical records from a web portal?

A. Purpose specification

B. Collection limitation

C. Use limitation

D. Individual participation

Suggested Answer: *A*

Community vote distribution

D (84%) A (16%)

dirk_gentley Highly Voted 2 years, 3 months ago

Selected Answer: D

and usual residence of the data controller.
(7) The Individual Participation Principle. An individual should have the right:
b) to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him;

https://iapp.org/resources/article/fair-information-practices/

upvoted 19 times

waleogere 1 year, 6 months ago

Agree! The answer is D.

upvoted 1 times

jackdryan 1 year, 8 months ago

D is correct

upvoted 2 times

GuardianAngel Most Recent 11 months ago

D. Individual participation
https://www.dhs.gov/sites/default/files/2024-01/Fair%20Information%20Principles_12_2008.pdf
Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use,
dissemination, and maintenance of PII. DHS should also provide mechanisms for
appropriate access, correction, and redress regarding DHS's use of PII.

upvoted 1 times

YesPlease 1 year ago

Answer D) Individual Participation

https://itlaw.fandom.com/wiki/Fair_Information_Practice_Principles#Access/Participation

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: D

The practice that applies to a patient requesting their medical records from a web portal, within the context of the Code of Fair Information Practices, is option D: Individual participation.

Individual participation refers to the right of individuals to access and participate in the management of their personal information. It empowers individuals to have control over their data and allows them to exercise their rights, such as requesting access to their personal information or requesting corrections or updates to their records.

In the given scenario, when a patient requests their medical records from a web portal, they are exercising their right to access their personal information. The hospital, by providing a web portal for such requests, enables individual participation and facilitates the patient's access to their medical records.

upvoted 1 times

vorozco 1 year, 6 months ago

Selected Answer: D

Answer is D.

https://simson.net/ref/2004/csg357/handouts/01_fips.pdf

upvoted 2 times

Dee83 1 year, 11 months ago

D. Individual participation applies to a patient requesting their medical records from a web portal.

Individual participation refers to the ability of an individual to have control over what information is collected about them, and how it is used. In the context of a hospital, this would include patients having the right to access their own medical records and request any necessary corrections or deletions.

upvoted 1 times

Delab202 2 years ago

Selected Answer: D

Code of Fair Information Practices led to Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, first published by the OECD in 1980.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.

upvoted 1 times

somkiatr 2 years ago

Selected Answer: D

Individual Participation Principle.

Under General Data Protection Regulation (GDPR) and other related regulations, individuals have the right to enquire, at any point in time, about the information we hold on file about them. This principle can be applied to all participating countries if required.

Reference : https://www.cemplicity.com/data-protection-principles/

upvoted 1 times

oudmaster 2 years ago

Selected Answer: D

Purpose Specification Principle Subjects should be notified of the reason for the collection of their personal information at the time that it is collected, and organizations should only use it for that stated purpose.

!

Individual Participation Principle Subjects should be able to find out whether an organization has their personal information and what that information is, to correct erroneous data, and to challenge denied requests to do so.

!

I vote for D (Individual Participation)

upvoted 1 times

RonWonkers 2 years, 1 month ago

Selected Answer: D

Answer is D

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: D

Definitely D

upvoted 2 times

rootic 2 years, 2 months ago

Selected Answer: D

Going with D.

upvoted 1 times

ItsBananass 2 years, 2 months ago

https://www.fpc.gov/resources/fipps/

Individual Participation. Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

upvoted 2 times

SongOTD 2 years, 3 months ago

Selected Answer: D

The patient is requesting his/her own info. So I would choose D

upvoted 2 times

wyerock 2 years, 3 months ago

Selected Answer: D

A is why the have the information, D is what they have.

upvoted 1 times

bmaheux 2 years, 3 months ago

Selected Answer: D

https://iapp.org/resources/article/fair-information-practices/

(7) The Individual Participation Principle. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;

upvoted 4 times

stickerbush1970 2 years, 3 months ago

Selected Answer: A

The 'purpose specification principle', that is, the principle that a citizen needs to be informed why the personal data is being collected and the specific purposes for which it will be processed and kept

upvoted 2 times

Question #45 *Topic 1*

A colleague who recently left the organization asked a security professional for a copy of the organization's confidential incident management policy. Which of the following is the BEST response to this request?

A. Access the policy on a company-issued device and let the former colleague view the screen.

B. E-mail the policy to the colleague as they were already part of the organization and familiar with it.

C. Do not acknowledge receiving the request from the former colleague and ignore them.

D. Submit the request using company official channels to ensure the policy is okay to distribute.

Suggested Answer: *C*

Community vote distribution

D (55%) C (45%)

⊟ **franbarpro** Highly Voted 👍 2 years, 9 months ago

They are no longer with the organization. So, ignore them.

upvoted 11 times

⊟ **CKaraf** 3 months, 3 weeks ago

Dont be a jerk... that is what CISSP wants us. Correct is D

upvoted 1 times

⊟ **franbarpro** 2 years, 8 months ago

I agree with "D" though

upvoted 1 times

⊟ **jackdryan** 2 years, 2 months ago

D is correct

upvoted 1 times

⊟ **dev46** Highly Voted 👍 2 years, 9 months ago

Why D?

Policy is confidential and no question to responding to ex-employees. I would ignore.

upvoted 6 times

⊟ **Yadster** 2 years, 8 months ago

You wont be providing them the policy unless that request is approved, which you first push up to management for a approval and also to make aware that a request for the policy has been requested by an outsider. Also what if the outsider goes and ask someone else as well. You organization should be made aware that such inquires are being requested.

upvoted 13 times

⊟ **EKP** Most Recent 🕒 1 month ago

Selected Answer: D

Someone is asking a security professional for confidential documents, of cause cannot distribute. But the security professional doesn't need to reply directly and seek official channel instead.

upvoted 1 times

⊟ **fuzzyguzzy** 2 months, 4 weeks ago

Selected Answer: D

I agree with other answers that simply ignoring them is a lie. Your organization needs to know they made the request, so go through the proper channels (let your company know).

upvoted 2 times

⊟ **ServerBrain** 3 months, 2 weeks ago

Selected Answer: C

"a copy of the organization's CONFIDENTIAL incident management policy"

upvoted 2 times

⊟ **deeden** 10 months, 4 weeks ago

Selected Answer: D

sounds like a question of ethics and professionalism. agree with option D

upvoted 2 times

64elpaso 1 year, 1 month ago

What if asked in person or over the phone, question doesn't specify how he asked, bad question.

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: D

C just sounds like a remission to me.

upvoted 1 times

73f8ac3 1 year, 2 months ago

Selected Answer: D

Ideally, answer should be "Reply that this document is confidential and that he has no more access privilege to it". Since that is not possible, let's consider.

A and B are out (you do not 'declassify' confidential documents informally)

C is... unprofessional and as pointed out leaves possibility open for other colleagues to answer with A or B and compromize the document.

With D, you are certain that

- If he has legitimate reason to access it, then it will be authorized and traced
- If he has none, then it will be properly denied (and traced again)

C is

D

upvoted 2 times

NuwanCha 1 year, 3 months ago

D. Submit the request using company official channels to ensure the policy is okay to distribute.

Explanation:

Option D is the most appropriate response because it ensures that proper procedures are followed for distributing sensitive organizational policies, especially after the colleague has left the organization. By submitting the request through official channels, such as contacting the appropriate personnel in the organization's administration or legal department, it allows for proper review and authorization before sharing the policy.

upvoted 1 times

Parikshitcyber 1 year, 3 months ago

Selected Answer: D

Options A and B may compromise the confidentiality of the policy by potentially exposing it to unauthorized individuals or distribution channels. Option C is not a proactive or professional approach to handling the request and could lead to misunderstandings or potential legal issues. Therefore, option D is the most appropriate and responsible course of action in this situation.

upvoted 2 times

homeysl 1 year, 3 months ago

Selected Answer: C

At a minimum, that data is classified as Sensitive. Which means that it is for internal user only.

upvoted 1 times

Kyanka 1 year, 3 months ago

Selected Answer: D

These answers are all bad but D makes the most sense because you should always report these kinds of requests to someone.

upvoted 1 times

xxxBadManxxx 1 year, 4 months ago

Selected Answer: C

As the colleague is no longer part of the organization, they no longer have a legitimate need to access the confidential incident management policy. Ignoring the request and not acknowledging receipt helps maintain the confidentiality and security of the policy.

upvoted 1 times

IntheZone 1 year, 5 months ago

Selected Answer: C

Answer is C, always think like a manager as you know these are confidential and are red line.

For D, you would look bad since your employees expect you to know what can be shared and what is not. If this wasn't a CISSP exam question, D might be on the table for a normal employee.

upvoted 2 times

⊟ **ddjkl** 1 year, 7 months ago

Selected Answer: C

it's confidential

upvoted 2 times

⊟ **thanhlb** 1 year, 8 months ago

Selected Answer: D

Not acknowledging receiving the request from the former colleague and ignoring them may be rude or unprofessional, and may also raise suspicion or resentment from the former colleague

upvoted 1 times

Question #46 *Topic 1*

Which of the following BEST describes when an organization should conduct a black box security audit on a new software protect?

A. When the organization wishes to check for non-functional compliance

B. When the organization wants to enumerate known security vulnerabilities across their infrastructure

C. When the organization is confident the final source code is complete

D. When the organization has experienced a security incident

Suggested Answer: *C*

Community vote distribution

C (73%) A (20%) 7%

⊟ **rootic** Highly Voted 👍 2 years, 8 months ago

Selected Answer: C

Question asks about BEST moment for performing pentest. There is no any sense to perform BlackBox pentest (and pay for it, of course) when the product is in development.
100% sure it's C - BlackBox pentest should be performed only when 1st version of product is ready.

upvoted 11 times

⊟ **jackdryan** 2 years, 2 months ago

C is correct

upvoted 1 times

⊟ **RedMartian** Most Recent ⊙ 2 months, 3 weeks ago

Selected Answer: C

Not A. Non-functional compliance relates to things like performance, reliability, and scalability — not security. A black box audit wouldn't focus on this.

upvoted 1 times

⊟ **ServerBrain** 3 months, 2 weeks ago

Selected Answer: C

" on a new software protect "

upvoted 1 times

⊟ **robervalchocolat** 10 months ago

A. When the organization wishes to check for non-functional compliance: While a black box security audit can help identify non-functional compliance issues, it's not the best time to conduct it. A black box audit is more effective when the software is complete and ready for testing.

upvoted 1 times

⊟ **Jenkins3mol** 1 year, 2 months ago

Selected Answer: C

According to procedure, c looks like a correct option. The thing is this question composer seems to have very poor language skills to clearly and fully describe what the situation is.

upvoted 3 times

⊟ **maawar83** 1 year, 6 months ago

Answer Should be B:
Conducting a black box security audit is particularly beneficial during the testing phase of a software development lifecycle or just before the software goes into production. This allows security professionals to simulate real-world attacks and identify potential vulnerabilities before the software is deployed in a live environment.

upvoted 2 times

⊟ **InclusiveSTEAM** 1 year, 8 months ago

C is the best answer.
A black box security audit tests the externally visible behavior of a system without knowledge of its internal structure and implementation.
It is most useful when the final source code is complete, to check for unknown vulnerabilities before deployment.

upvoted 2 times

⊟ **InclusiveSTEAM** 1 year, 8 months ago

A is the answer
Option A - When the organization wishes to check for non-functional compliance - is the best answer for when a black box security audit should be conducted on a new software product.
A black box audit analyzes an application from an external perspective with no knowledge of internal code or structure.
It focuses on functionality, usability, and other non-functional aspects.
B describes a vulnerability scan, not a black box audit.
C - black box audits do not require or use source code access.
D refers to incident response, not proactive software auditing.
upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: C

The BEST description of when an organization should conduct a black box security audit on a new software product is option C: When the organization is confident the final source code is complete.

A black box security audit is a type of security assessment where the auditor has no prior knowledge of the internal workings of the software being tested. The audit is performed from an external perspective, simulating the approach of an attacker who does not have access to the source code or internal details of the software.

Conducting a black box security audit is typically done when the organization believes that the development of the software is complete or nearing completion. The organization should have confidence that the final source code is available, as the audit will focus on assessing the security of the software as a whole, without considering the internal details or implementation.
upvoted 1 times

RVoigt 2 years, 4 months ago

Selected Answer: C

CISSP Official Study Guide pg 969 "Black-Box Testing Black-box testing examines the program from a user perspective by providing a wide variety of input scenarios and inspecting the output. Black-box testers do not have access to the internal code. Final acceptance testing that occurs prior to system delivery is a common example of black-box testing."
upvoted 4 times

irEd1 2 years, 4 months ago

C, just means there should be no more revisions to the source code, so technically that means the first beta test can begin.
upvoted 2 times

s_n_ 2 years, 5 months ago

Answer: B
When the organization wants to enumerate known security vulnerabilities across their infrastructure. This type of security audit involves assessing the existing security measures of a system, such as firewalls, antivirus, and access control, to identify any potential vulnerabilities or weaknesses.
The organization should conduct a black box security audit on a new software product when they want to identify known security vulnerabilities and assess the current security measures to identify any potential weaknesses. Resources include OWASP's guide to Security Auditing, SANS Institute's guide to Security Auditing, and NIST's guide to Security Auditing.
upvoted 2 times

somkiatr 2 years, 6 months ago

Selected Answer: C

Should be C. Answer A mentions about non-functional compliance which may not be necessary about security.
upvoted 1 times

oudmaster 2 years, 6 months ago

Selected Answer: C

Black Box Testing is conducted with Application Runtime, so the source code should be completed to execute the application.
upvoted 1 times

sec_007 2 years, 8 months ago

Selected Answer: C

C
Black box security audit = Pentest (conducted by independent 3rd party)
For a NEW product, usually done after all functionality is coded and complete to investigate security flaws in the product.
upvoted 2 times

Humongous1593 2 years, 8 months ago

Selected Answer: A

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied virtually to every level of software testing: unit, integration, system and acceptance.

upvoted 4 times

Nickolos 2 years, 7 months ago

You may be mixing up black box testing with a penetration test type (black box) which simulates a situation where the attacker doesn't know anything about the infrastructure or code being tested.

This type of test aims to simulate the real-world scenario of external attackers targeting and attempting to compromise your systems. Black Box testing has the benefit of perfectly simulating a motivated external attacker that has zero-knowledge of your operations and IT infrastructure.

upvoted 1 times

GenesisTech 2 years, 8 months ago

Selected Answer: A

black box testing does not imply known vulnerabilities.

upvoted 2 times

Nickolos 2 years, 7 months ago

Yes it does. Penetration testing involves attempting to exploit all known and possibly unknown vulnerabilities.

upvoted 1 times

Question #47 *Topic 1*

In software development, which of the following entities normally signs the code to protect the code integrity?

A. The organization developing the code

B. The quality control group

C. The developer

D. The data owner

Suggested Answer: *A*

Community vote distribution

A (67%) C (33%)

⊟ **BigITGuy** 2 months, 4 weeks ago

Selected Answer: A

Not C. Individuals don't sign code.. the organization does to maintain centralized trust.

upvoted 1 times

⊟ **martin451** 8 months, 3 weeks ago

Selected Answer: A

The organization responsible for developing or building the software typically manages the keys used to sign the code, ensuring both data integrity and source authentication.

upvoted 1 times

⊟ **deeden** 10 months, 4 weeks ago

Selected Answer: A

option A sounds more appropriate for code signing certificates.

upvoted 1 times

⊟ **Jenkins3mol** 1 year, 2 months ago

Selected Answer: A

If A is not there, then I would vote for C. But A is here, then obviously the code belongs to the company, but not individuals. We have all signed a document clarifying this point with us as employees, right?

upvoted 1 times

⊟ **john_boogieman** 1 year, 3 months ago

Selected Answer: C

OSG, pag. 1029. Code Signing

Code signing provides developers with a way to confirm the authenticity of their code to end users. Developers use a cryptographic function to digitally sign their code with their own private key, and then browsers can use the developer's public key to verify that signature and ensure that the code is legitimate and was not modified by unauthorized individuals.

upvoted 2 times

⊟ **homeysl** 1 year, 3 months ago

Selected Answer: A

Integrity = OEM

upvoted 1 times

⊟ **Vasyamba1** 1 year, 3 months ago

Selected Answer: A

From the OCG v9 - The developer signing the code does so using a private key,
whereas the corresponding public key is included in a digital certificate that is distributed
with the application. Users who download the application receive a copy of the certificate
bundled with it and their system extracts the public key and uses it in the signature verification process.
Yes, it is written "the developer", but I think it means "the developer company", not the individual. If the key is incuded in the digital certificate - the certificate is obviouusly issued for the company.

upvoted 2 times

⊟ **Hackermayne** 1 year, 5 months ago

Selected Answer: A

When you guys install a driver. Is it signed by Joe Whoever or is it signed by the company? You want uniformity in things like this, and any dev shouldn't be able to just sign anything the company puts out.

upvoted 3 times

YesPlease 1 year, 6 months ago

Selected Answer: A

Answer A)

The developer is the entity responsible for writing, building, and/or submitting the code that will be signed. This entity maintains a secure development environment, including the source code repository, and will submit code to the signer after it has completed the organization's software development and testing processes.

The signer is the entity responsible for managing the keys used to sign software. This role may be performed by the same organization that developed or built the software, or by an independent party able to vouch for the source of the code.

https://csrc.nist.gov/files/pubs/shared/itlb/itlbul2018-05.pdf

upvoted 4 times

thanhlb 1 year, 8 months ago

Selected Answer: A

it will conflict of interest if developer sign the code

upvoted 2 times

ljkesmeer 1 year, 8 months ago

I think the company is the right answer cause what if you have more than one developer working on the code?

upvoted 2 times

williom 1 year, 9 months ago

I think C. reasons below:

in software development, the 'source code' is signed by the developer: https://docs.github.com/en/authentication/managing-commit-signature-verification/signing-commits

in software distribution, the organisation would sign their 'software'. e.g. Nvidia would 'release sign' their drivers for the public download: https://learn.microsoft.com/en-us/windows-hardware/drivers/install/release-signing

upvoted 4 times

Bach1968 1 year, 12 months ago

Selected Answer: C

n software development, the entity that normally signs the code to protect the code integrity is option C: The developer.

Code signing is a process in which a digital signature is applied to software code to verify its authenticity and integrity. The digital signature is created using a private key owned by the developer. By signing the code, the developer provides assurance that the code has not been tampered with and originates from a trusted source.

upvoted 2 times

> **ccKane** 1 year, 9 months ago
>
> Usually code signing is done at organizational level rather than by individuals. E.g., when you download and install software, you rather trust code that is signed by a well-known and trusted organization than an individual developer. I go with A.
>
> upvoted 2 times

MRK019 2 years ago

think like a manager... the developer signing the code may switch his job...thus it is the Organization's responsibility to sign the code.
A is correct

upvoted 4 times

KelvinYau 2 years, 1 month ago

Code signing is a security measure that involves digitally signing the code with a cryptographic signature that verifies the identity of the code author and ensures that the code has not been tampered with or altered since it was signed. This helps to protect users from running malicious or unauthorized code.

In most cases, the developer signs the code using a private key, which is kept secure and only accessible to authorized personnel. The organization developing the code (Option A) may also be involved in managing the signing process and ensuring that the code meets the organization's security and quality standards. However, the actual act of signing the code is typically performed by the developer.

upvoted 1 times

A1nthem 2 years, 2 months ago

Selected Answer: A

Its Organization responsibility to protect the data be NDA from individual of Developer and implement the Due care to protect the data.

upvoted 1 times

ACunningPlan 2 years, 3 months ago

Selected Answer: C

Of these Developer is the most accurate and used to be true but now it is really the Build or DevOps process that signs, and then it can go to media or deployed to environments as a signed artifact.

upvoted 1 times

ACunningPlan 2 years, 2 months ago

Uhg, I know for this exam it is A even though in real world the organization doesn't if know if their code is signed or not. But legally owner is signing, even if subcompany writes and compiles.

upvoted 1 times

jackdryan 2 years, 2 months ago

A is correct

upvoted 1 times

Question #48 *Topic 1*

Which of the following technologies can be used to monitor and dynamically respond to potential threats on web applications?

A. Field-level tokenization

B. Web application vulnerability scanners

C. Runtime application self-protection (RASP)

D. Security Assertion Markup Language (SAML)

Suggested Answer: *B*

Community vote distribution

C (89%) 11%

⊟ **Mekd** Highly Voted 👍 2 years, 9 months ago

Selected Answer: C

C
https://www.crowdstrike.com/cybersecurity-101/cloud-security/runtime-application-self-protection-rasp/

Application protection: Detecting and blocking security vulnerabilities and malicious activity within the application during runtime
Threat intelligence: Providing deep, code-level visibility within the application and producing insights that help the security team understand who is attacking their organization, their methods and motivations

upvoted 14 times

⊟ **jackdryan** 2 years, 2 months ago

C is correct

upvoted 1 times

⊟ **acacia318** Most Recent 🕘 3 months, 1 week ago

Selected Answer: C

IMHO, thinking like a manager is arriving to the correct solution with having gaps in your knowledge. The first step is to read the question carefully -- you know you have accomplished this when you've identified the modifiers for the nouns and verbs. The 2nd step is to eliminate the wrong or distracting answers. I happen to know what SAML is, but am unsure what is "Field-Level Tokenization -- but being a token, probably not appropriate for the question. From the remaining two, I'm guessing a vulnerability scanner would not "dynamically respond" to a threat but ID and report vulnerabilities. This leave "C" as something that can monitor and respond.

upvoted 1 times

⊟ **robervalchocolat** 10 months ago

Runtime application self-protection (RASP) is the technology that best fits the description. RASP agents are embedded within web applications and can monitor application behavior in real time, detecting and responding to potential threats as they occur. This makes RASP a powerful tool for protecting web applications from attacks like SQL injection, cross-site scripting, and others

upvoted 1 times

⊟ **Ezebuike** 10 months, 2 weeks ago

Web application vulnerability scanners find vulnerabilities before an attacker can exploit them, but Runtime Application Self-Protection (RASP) is technology that incorporates security functionality within software applications to prevent malicious attacks while the application is running. RASP focuses on the application itself, using sensors embedded within the software, as well as contextual information, to monitor the application during runtime, address specific vulnerabilities that exist within each piece of software, and stop threats automatically and in real time. Based on this I will go for C

upvoted 1 times

⊟ **Jenkins3mol** 1 year, 2 months ago

Selected Answer: C

RASP and Cloud Security
RASP is an important component within the organization's cloud security strategy, more particularly for cloud application security. As companies increasingly leverage the cloud to advance business transformation efforts, enable new business models and activate a remote workforce, they must also ensure that all business conducted in a cloud or hybrid environment is safe and secure.

Traditional security measures are not equipped to deliver protection in the cloud, which means that organizations must craft a new strategy and adopt new tooling, including application-level policies, tools, technologies and rules — chief among them RASP — to maintain visibility into all cloud-based assets, protect cloud-based applications from cyberattacks and limit access only to authorized users.

upvoted 1 times

25cbb5f 1 year, 2 months ago

The BEST technology for monitoring and dynamically responding to potential web application threats is:

C. Runtime application self-protection (RASP)

Here's why RASP is the most suitable choice:

Real-time Defense: RASP operates within the application itself, meaning it can detect and block attacks in real-time as they're happening, unlike other options that are often more focused on pre-deployment checks.
Behavior-Based Detection: RASP analyzes application behavior and looks for anomalies or malicious code execution attempts. This allows it to catch attacks that traditional signature-based tools might miss.
Dynamic Response: A key feature of RASP is its ability to dynamically respond to attacks. It can block the malicious request, send an alert, or even quarantine suspicious code, preventing harm.

upvoted 1 times

e58c193 1 year, 2 months ago

Selected Answer: C

RASP, vulnerability scanners do not respond

upvoted 1 times

GuardianAngel 1 year, 4 months ago

Vulnerabiity scanners just scan for vulnerabilities, they dont respond to vulnerabilities

upvoted 2 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C) Runtime Application Self-Protection (RASP)

https://en.wikipedia.org/wiki/Runtime_application_self-protection

upvoted 1 times

aape1 1 year, 8 months ago

Selected Answer: C

C. Runtime Application Self-Protection (RASP) is a security technology that is designed to protect web applications and APIs by monitoring and defending against attacks in real-time while the application is running. RASP solutions are typically integrated directly into the application or its runtime environment.

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: C

The technology that can be used to monitor and dynamically respond to potential threats on web applications is option C: Runtime application self-protection (RASP).

Runtime application self-protection (RASP) is a security technology that is integrated directly into an application's runtime environment. It is designed to monitor the application's behavior and detect and respond to potential security threats in real-time. RASP solutions have the ability to detect and prevent attacks such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities.

upvoted 1 times

Azurefox79 2 years, 3 months ago

Selected Answer: C

RASP for the same reasons provided by Dee83 and mekd

upvoted 1 times

Dee83 2 years, 5 months ago

C- correct answer
Runtime application self-protection (RASP) can be used to monitor and dynamically respond to potential threats on web applications.
Runtime Application Self-Protection (RASP) is a security technology that provides real-time monitoring of web applications and dynamically responds to potential threats. RASP is integrated into the web application and runs alongside the application code, providing visibility into the application's runtime environment and the ability to detect and respond to threats in real-time. RASP can detect and block attacks such as SQL injection, cross-site

scripting (XSS), and file inclusion vulnerabilities.

Web application vulnerability scanners are tools that automate the process of identifying security vulnerabilities in web applications, but it does not provide real-time monitoring and dynamic response to potential threats.

upvoted 2 times

Delab202 2 years, 6 months ago

Selected Answer: C

Web application vulnerability scanners are a specialised type of vulnerability scanner which focus on finding weaknesses in web applications and websites.

Run Time Application Self-Protection is designed to detect attacks on an application in real time. When an application is running, RASP can protect application from malicious attacks by analyzing both the app's behavior and the context of that behavior. App can continuously monitor its real time behavior pattern of traffic, where attacks can be identified and mitigated immediately without human intervention.

upvoted 2 times

Jamati 2 years, 7 months ago

Selected Answer: C

RASP is the answer

upvoted 1 times

rootic 2 years, 8 months ago

Selected Answer: C

Web scan obviously can't dynamicly respond to threats.

It's C.

upvoted 2 times

[Removed] 2 years, 8 months ago

B = Detect

C = Respond

upvoted 2 times

Question #49 *Topic 1*

A security architect is developing an information system for a client. One of the requirements is to deliver a platform that mitigates against common vulnerabilities and attacks. What is the MOST efficient option used to prevent buffer overflow attacks?

A. Access control mechanisms

B. Process isolation

C. Address Space Layout Randomization (ASLR)

D. Processor states

Suggested Answer: *C*

Community vote distribution

C (93%) 7%

Mekd Highly Voted 2 years, 3 months ago

Selected Answer: C

Answer C
Address space layout randomization (ASLR) is a memory-protection process for operating systems (OSes) that guards against buffer-overflow attacks by randomizing the location where system executables are loaded into memory.

upvoted 14 times

jackdryan 1 year, 8 months ago

C is correct

upvoted 1 times

Hackermayne Most Recent 11 months, 3 weeks ago

Selected Answer: C

It is nothing other than C. What this specifically does is randomize addresses so you can't figure them out. Its been a while since I've done this but in a typical SIMPLE buffer overflow, the process is something like this:
1. Find a place to input something, send it a ton of data to see what happens i.e. plugging thousands of characters into something that expects maybe 20 max.
2. App crashes, you now have to figure out where it crashes
3. Use metasploit or something to generate a list of non-repeat characters, it crashes on a specific area of that so you know it crashed on say character 1687. That likely means you've found a spot to input some type of shellcode into the heap or stack. There's a lot of other steps and not much room, but essentially just think of ASLR as randomizing that location where you're trying to put your shellcode, since it isn't consistent, it'll never take because you haven't put it on the exact line its supposed to be on.

upvoted 2 times

Bach1968 1 year, 5 months ago

Selected Answer: B

The MOST efficient option used to prevent buffer overflow attacks is option B: Process isolation.

Buffer overflow attacks occur when a program writes data beyond the bounds of a buffer, leading to potential memory corruption and unauthorized access to the system. Process isolation is an effective defense mechanism against such attacks. By isolating processes from each other, each process is allocated its own memory space, and the buffer overflow in one process does not affect the memory of other processes. This prevents the attacker from exploiting the vulnerability in one process to gain unauthorized access to other parts of the system.

upvoted 1 times

4vv 1 year, 4 months ago

B. Process isolation: This is a method that keeps processes separate so that the failure or compromise of one process doesn't affect others. While it can limit the impact of a buffer overflow by preventing it from affecting other processes, it doesn't directly prevent buffer overflow attacks.
C. Address Space Layout Randomization (ASLR): ASLR randomizes the memory addresses used by processes. This makes it difficult for an attacker to predict the location of specific functions or buffers, thereby making buffer overflow exploits (particularly return-to-libc or ROP attacks) much harder to execute successfully.

upvoted 4 times

Bhuraw 2 years, 2 months ago

Am surprised ASLR has no mention in the official study guide

upvoted 3 times

Jamati 2 years, 1 month ago

Noticed that too

upvoted 2 times

ADeAngelo 1 year, 11 months ago

Could be one of those 50 test questions.

upvoted 1 times

Question #50 *Topic 1*

In a quarterly system access review, an active privileged account was discovered that did not exist in the prior review on the production system. The account was created one hour after the previous access review. Which of the following is the BEST option to reduce overall risk in addition to quarterly access reviews?

A. Implement bi-annual reviews.

B. Create policies for system access.

C. Implement and review risk-based alerts.

D. Increase logging levels.

Suggested Answer: *B*

Community vote distribution

C (54%) B (44%)

N00b1e Highly Voted 2 years, 9 months ago

Selected Answer: B

I agree with B. If you create a policy on when system accounts can be created, they would have to be logged or someone would have to actively break policy. Think like a manager!

upvoted 24 times

1460168 11 months ago

Think like a Manager. Do not touch anything, tell others how to do it.

upvoted 1 times

Jamati 2 years, 7 months ago

I agree, the key here is to think like a manager.

upvoted 2 times

jackdryan 2 years, 2 months ago

B is correct

upvoted 1 times

thomass Highly Voted 2 years, 9 months ago

sorry, should be C?

upvoted 11 times

Ramye 1 year, 1 month ago

Why though?

Without the established policy, there won't be any concern of creating accts, hence there should not be any trigger or anything like that. So answer most likely B.

But if anyone has confirmed answer I'll be happy to take that. Thx

upvoted 2 times

cysec_4_lyfe Most Recent 2 months, 3 weeks ago

Selected Answer: C

Implement and review risk-based alerts: This option is the best because it focuses on proactive detection. Risk-based alerts can notify administrators when unusual or potentially dangerous activity occurs, such as the creation of a new privileged account outside the regular review cycle. This helps identify and address issues in a more timely manner.

upvoted 2 times

AjitZavade 2 months, 3 weeks ago

Selected Answer: C

▯ Why C is the BEST Option

The scenario describes a privileged account that was created right after a quarterly review and went unnoticed until the next one — suggesting a gap in real-time or near-real-time monitoring.

✅ Implementing and reviewing risk-based alerts would:

Detect suspicious or high-risk events (e.g., new privileged account creation)

Allow for faster incident detection and response

Reduce the time window between when a risky event occurs and when it's discovered

This significantly reduces overall risk, especially when paired with quarterly access reviews.

✖ Why the Other Options Are Less Effective (in this context)
Option Why Not the Best
A. Implement bi-annual reviews ✖ This reduces review frequency (from quarterly to twice a year), increasing risk instead of reducing it.
B. Create policies for system access ✅ Good foundational step, but policies alone don't enforce or detect violations.
D. Increase logging levels ✅ May help gather more data, but useless without alerting or active monitoring — doesn't reduce risk by itself.
upvoted 2 times

Senthil1982 3 months ago

Selected Answer: C

Implementing and reviewing risk-based alerts (option C) is the most effective way to reduce overall risk in this scenario, as it ensures that suspicious activities, like the creation of unauthorized privileged accounts, are detected promptly and acted upon before they escalate. This complements quarterly access reviews by adding continuous monitoring and immediate notifications.

B. Create policies for system access: Policies for system access are essential for defining acceptable access controls and procedures. However, having policies in place without the ability to actively monitor access and account changes will not prevent unauthorized access or provide early detection of suspicious activity. Policies must be coupled with monitoring and real-time alerts for effective risk management.
upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: C

While B (Create policies for system access) is important and should already be in place, it doesn't directly address the specific issue of a rogue privileged account being created between reviews. Policies are guidelines, but they don't actively prevent or detect this type of activity in real-time.

Risk-based alerts, on the other hand, do address this gap. By implementing alerts for specific high-risk actions (like the creation of new privileged accounts, especially outside of normal change windows), the security team can be notified immediately when such an event occurs. This allows for rapid investigation and mitigation, significantly reducing the window of opportunity for malicious activity. It complements the quarterly reviews by providing continuous monitoring and detection capabilities.
upvoted 1 times

Isebarry 5 months ago

Selected Answer: B

Creating policies for system access is more important than increasing logging levels in this case. The policies created should actually include logging. That way, policy drives system access and logging levels.
upvoted 1 times

Fouad777 6 months, 3 weeks ago

Selected Answer: C

C. Implement and review risk-based alerts.

Here's why:

Risk-based alerts provide real-time or near-real-time monitoring and alerting for unusual or suspicious activities, such as the creation of new privileged accounts. This enables a more proactive approach to security, allowing the organization to quickly identify and respond to potential threats.

Implementing bi-annual reviews (A) would reduce the frequency of reviews, potentially increasing the risk of unnoticed issues.

Creating policies for system access (B) is important, but on its own, it may not provide the necessary real-time detection and response capabilities.

Increasing logging levels (D) can be helpful, but without active monitoring and alerting, it might not effectively reduce risk.

Risk-based alerts enhance your security posture by providing timely information and enabling swift action to mitigate potential risks.

upvoted 1 times

Bietchasup 7 months ago

Selected Answer: B

nobody ever comes back on here after failing or passing lol

upvoted 4 times

KennethLZK 7 months, 1 week ago

Selected Answer: B

From a managerial standpoint, establishing clear policies is fundamental. Policies provide a framework for consistent and secure access management, ensuring that all actions are governed by well-defined rules. This helps in maintaining control and accountability, which are key managerial responsibilities.

upvoted 1 times

GabrielVillamizar 11 months ago

Selected Answer: C

En base a la pregunta, al C es la correcta

upvoted 1 times

Nithstar 11 months, 1 week ago

answer c is correct sinc alerts can detect changes

upvoted 2 times

CCNPWILL 1 year ago

Selected Answer: C

B is a good answer, but C is better.

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: C

Well, this is quite contentious a question, huh. But as you can see, you will have to change the policy along the way, anyway, every time after you have done a quarterly check. So B would be out of the question very necessary, fundamental and routine; however, C is directly resolving the problem depicted in the question body, so C is more relevant an answer which is heavily implied by the question composer. And C is the conclusion that you should have as a manager after adopting doubleloop thinking method.

upvoted 4 times

jieaws 1 year, 2 months ago

B policies encompasses C alert implementation. B enforces C and holds the stake holders (usually Sr professionals) accountable for implementation alignment with the police B.

I finally understand why CISSP exam emphasizes managerial view. B takes precedence C. In order words, B must be in place first. I choose B.

upvoted 1 times

AshStevens 1 year, 2 months ago

Selected Answer: C

C. The trick here is that it was created immediately after the previous check. The implication is that the user is very aware that it wouldn't be allowed UNDER THE POLICIES THEY ALREADY HAVE, and are choosing to ignore that. A new policy does not enforce compliance, but setting up alerts to monitor would immediately detect non-compliance regardless of the users intent or timing.

upvoted 2 times

Vaneck 1 year, 3 months ago

Selected Answer: C

The best option for reducing overall risk in addition to quarterly access reviews is :

C. Implement and review risk-based alerts.

Implementing and reviewing risk-based alerts would enable early detection of suspicious or unauthorized activity, such as the creation of new privileged accounts, and react accordingly. This proactive approach helps to identify and mitigate potential risks in real time, rather than relying solely on periodic reviews.

upvoted 1 times

Question #51 *Topic 1*

A corporation does not have a formal data destruction policy. During which phase of a criminal legal proceeding will this have the MOST impact?

A. Sentencing

B. Trial

C. Discovery

D. Arraignment

Suggested Answer: *C*

Community vote distribution

C (85%) Other

Bach1968 Highly Voted 12 months ago

Selected Answer: C

Option C:
The lack of a formal data destruction policy would have the MOST impact during the discovery phase of a criminal legal proceeding.

During the discovery phase, both the prosecution and defense exchange relevant information and evidence related to the case. This includes providing documents, records, and other forms of evidence that are pertinent to the case.

In the context of a criminal legal proceeding, if a corporation does not have a formal data destruction policy, it may lead to the unintentional or intentional destruction of potentially relevant evidence. This could include deleting or disposing of electronic records, documents, or other forms of data that could be crucial to the case.

The discovery phase relies on the principle of transparency and providing all relevant information to both parties involved. If data destruction occurs without a formal policy in place, it can raise concerns about the integrity of the evidence and potentially impact the fairness and credibility of the legal proceeding.

upvoted 10 times

Madamcyber2025 Most Recent 2 months, 2 weeks ago

Selected Answer: C

The absence of a formal data destruction policy would have the most impact during the Discovery phase of a criminal legal proceeding.

During discovery, both parties exchange information and evidence relevant to the case. If a corporation lacks a data destruction policy, it may lead to difficulties in managing and producing required documents, potentially resulting in legal complications or sanctions

upvoted 1 times

Madamcyber2025 2 months, 2 weeks ago

Selected Answer: C

Anyone with the best answer please share

upvoted 1 times

Ivanchun 1 year, 5 months ago

Selected Answer: C

Vote C

upvoted 1 times

jackdryan 1 year, 1 month ago

C is correct

upvoted 1 times

JohnyDal 1 year, 5 months ago

Selected Answer: C

Keeping data longer than necessary would result in more effort and expense during the discovery phase to search for relevant material. Answer is C.

upvoted 1 times

Delab202 1 year, 6 months ago

Selected Answer: C

Sentencing
If the judge or jury finds the defendant guilty, the court will determine the punishment. Federal sentencing guidelines and similar state guidelines often define minimum and maximum sentences and identify factors the court may consider. The court may hold a separate sentencing hearing, at which the state may present evidence in support of a harsh sentence, and the defendant may request leniency by presenting evidence of mitigating factors.

upvoted 1 times

cccispman 1 year, 6 months ago

Selected Answer: A

Lets think about this question a little bit ...
A company does not have any formal data destruction policy in place !
Which means the company is culpable as they have breached privacy laws. So in the criminal proceedings the judge will take this into account when passing down sentence (i.e. penalty), so I'm voting A contrary to my previous comment.

upvoted 1 times

lifre 5 months, 2 weeks ago

I had the same thought. But maybe we are overthinking?

upvoted 1 times

cccispman 1 year, 6 months ago

There's no such terms as 'Discovery' in criminal law. There's a trial which is normally held in a court where the evidence is tested before a jury or judge or both. Therefore, the answer should be trial.

upvoted 1 times

somkiatr 1 year, 6 months ago

Selected Answer: C

In a criminal law case, the term “discovery” refers to the process of discovering and obtaining evidence the other side plans to present. Both the prosecutor and the criminal defense lawyer engage in discovery. Each side can make a criminal discovery request. When the criminal defense attorney and asking to obtain copies of the destruction policy can cause many impact.

upvoted 1 times

Billy235 1 year, 6 months ago

Keeping data longer than necessary would result in more effort and expense during the discovery phase to search for relevant material. Answer is C.

upvoted 1 times

Jamati 1 year, 7 months ago

Selected Answer: C

I agree with the given answer. Company might have destroyed the data already by the time the cops come asking for it.

upvoted 1 times

RonWonkers 1 year, 7 months ago

Selected Answer: B

Would this not be B?

upvoted 1 times

Nickolos 1 year, 7 months ago

Are you asking or stating?

Because if you're stating, it would be preferable if you provide an explanation or citation. And if you're asking, then you shouldn't vote.

upvoted 10 times

Question #52 *Topic 1*

What is considered the BEST explanation when determining whether to provide remote network access to a third-party security service?

A. Contract negotiation

B. Supplier request

C. Business need

D. Vendor demonstration

Suggested Answer: *A*

Community vote distribution

C (84%) A (16%)

⊟ **stickerbush1970** Highly Voted 👍 2 years, 9 months ago

Selected Answer: C

Third party accessing company assets will need a business need.

upvoted 17 times

⊟ **jackdryan** 2 years, 1 month ago

C is correct

upvoted 1 times

⊟ **Bach1968** Highly Voted 👍 1 year, 12 months ago

Selected Answer: C

While contract negotiation (option A) is an important aspect of engaging with a third-party security service, it is not the BEST explanation when determining whether to provide remote network access to that service. The question specifically asks for the BEST explanation, and in this context, the primary consideration should be the business need (option C).

Contract negotiation typically occurs after assessing the business need and deciding to proceed with engaging a third-party security service. During contract negotiation, the terms and conditions of the engagement are discussed and agreed upon, including aspects such as service levels, pricing, confidentiality, liability, and legal obligations.

Therefore, while contract negotiation is relevant, option C (business need) is the BEST explanation for deciding whether to provide remote network access to a third-party security service.

upvoted 6 times

⊟ **Jenkins3mol** 1 year, 2 months ago

I agree with this explanation.

upvoted 1 times

⊟ **Nithstar** Most Recent ⊙ 11 months, 1 week ago

without a contract in place business need cannot suffice the requirement to grant network access so, A should be the correct answer

upvoted 1 times

⊟ **Moose01** 1 year, 9 months ago

A. all business requirements are addressed during contact negotiation. business needs falls under the one of the many terms in the contact.

upvoted 2 times

⊟ **MD806** 1 year, 10 months ago

Who determines the correct answer ? Seems like Most Voted is C but correct answer is A

upvoted 2 times

⊟ **KelvinYau** 2 years, 1 month ago

Selected Answer: C

Providing remote network access to a third-party security service is a decision that should be made based on the specific business needs and the risks involved. It is important to evaluate the requirements for the service and whether it is critical for the business operations.

upvoted 1 times

⊟ **s_n_** 2 years, 5 months ago

The best explanation when determining whether to provide remote network access to a third-party security service is Business Need. Remote network access should only be provided if there is a specific business need that cannot be met without the service. It is important to consider the security implications of providing remote access and to ensure that the third-party service adheres to the organization's security policies and practices.

upvoted 1 times

Joadeika 2 years, 5 months ago

Selected Answer: A

All business need is addressed in contract negotiation

upvoted 2 times

dumdada 2 years ago

You can have an unnecessary remote access in the contract even without a real business need. Business need is the key here

upvoted 2 times

cccispman 2 years, 6 months ago

Selected Answer: A

Surely, business need !

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: A

I will select A.
Third-Party Security Services Provider (TPSSP)
The security roles and responsibilities of TPSSPs for:
- Identity and access management
- Cloud Workload Protection Platform
- Network Security
- Data & Storage Security
- Assessment
- Security Analytics as a Service
- Application Security
- Security Support Services
Normally we need to negotiate roles & responsibilities of TPSSP. Service Level Agreement(SLAs) and types of support (On-site or Remote Access) have to be clarified.

Reference : https://www.lexology.com/library/detail.aspx?g=3ed47921-2cfa-4d1b-8615-ad468a1cbc81

upvoted 1 times

KayChan 2 years, 6 months ago

Business need is a justification

upvoted 1 times

rootic 2 years, 8 months ago

Selected Answer: C

Vote for C.

upvoted 1 times

DButtare 2 years, 9 months ago

Selected Answer: C

Is there a real need

upvoted 2 times

stickerbush1970 2 years, 9 months ago

Once the business need is determined, then a connection policy will be made.

upvoted 2 times

kptest12 2 years, 9 months ago

Answer is A

For e.g , When working with a 3rd party on an internal project , if they need VPN access to meet the business need , the access is granted a part of contract negotiation .

upvoted 4 times

Joey456 2 years, 8 months ago

Disagree. Cyber policy dictates business needs for access. Not any element of the business contract. The 3rd party has NO RIGHTS to be on the network.

upvoted 2 times

Question #53 *Topic 1*

The acquisition of personal data being obtained by a lawful and fair means is an example of what principle?

A. Collection Limitation Principle

B. Openness Principle

C. Purpose Specification Principle

D. Data Quality Principle

Suggested Answer: *A*

Community vote distribution

A (93%) 7%

noh_ssiw_l Highly Voted 1 year, 9 months ago

Selected Answer: A

It's crylstal clear on OECD's privacy guidelines and I don't know what they are talking about hahaha
Collection limitation principle - limit the collection of personal data to only what is needed to provide a service, obtain the personal data lawfully and, where appropriate, with the knowledge or consent of the data subject.

upvoted 7 times

kjfdhfkjh Most Recent 7 months ago

Selected Answer: A

A is correct.

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: A

The acquisition of personal data being obtained by a lawful and fair means is an example of the Collection Limitation Principle.

The Collection Limitation Principle is one of the fundamental principles of data protection and privacy. It states that personal data should be collected by lawful and fair means and, where appropriate, with the knowledge or consent of the individual concerned.

upvoted 2 times

RVoigt 2 years, 3 months ago

Selected Answer: B

CISSP Official Study Guide pg 166 "The key provisions of the GDPR include the following:
- Lawfulness, fairness, and transparency says that you must have a legal basis for processing personal information, you must not process data in a manner that is misleading or detrimental to data subjects, and you must be open and honest about data processing activities.
- Purpose limitation says that you must clearly document and disclose the purposes for which you collect data and limit your activity to disclosed purposes.
..."

upvoted 1 times

RVoigt 2 years, 3 months ago

- Data minimization says that you must ensure that the data you process is adequate for your stated purpose and limited to what you actually need for that purpose.
- Accuracy says that the data you collect, create, or maintain is correct and not misleading, that you maintain updated records, and that you correct or erase inaccurate data.
- Storage limitation says that you keep data only for as long as it is needed to fulfill a legitimate, disclosed purpose and that you comply with the "right to be forgotten" that allows people to require companies to delete their information if it is no longer needed
- Security says that you must have appropriate integrity and confidentiality controls in place to protect data.
- Accountability says that you must take responsibility for actions you take with protected data and that you must be able to demonstrate your compliance."

upvoted 1 times

cccispman 2 years, 6 months ago

Selected Answer: A

The only answer which makes logical sense, limitation !

upvoted 1 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

Jamati 2 years, 7 months ago

Agreed, answer is A

upvoted 1 times

franbarpro 2 years, 8 months ago

Selected Answer: A

"A" - (1) The Collection Limitation Principle. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

upvoted 4 times

N00b1e 2 years, 9 months ago

Selected Answer: A

I think A

upvoted 1 times

bherto39 2 years, 9 months ago

Selected Answer: A

A is correct..

reference https://itlaw.fandom.com/wiki/Fair_Information_Practice_Principles

upvoted 2 times

Question #54 *Topic 1*

Which of the following is the MOST appropriate control for asset data labeling procedures?

A. Categorizing the types of media being used

B. Logging data media to provide a physical inventory control

C. Reviewing off-site storage access controls

D. Reviewing audit trails of logging records

Suggested Answer: *A*

Community vote distribution

A (60%) D (36%) 4%

⊟ **stickerbush1970** Highly Voted 👍 2 years, 9 months ago

Selected Answer: A

Data categorization is a must for any organization.

upvoted 10 times

⊟ **jackdryan** 2 years, 1 month ago

A is correct

upvoted 1 times

⊟ **BigITGuy** Most Recent ⊙ 2 months, 4 weeks ago

Selected Answer: A

Not D - Reviewing audit trails is part of monitoring, not directly about labeling asset data.

upvoted 1 times

⊟ **robervalchocolat** 10 months ago

most appropriate control for asset data labeling procedures because it helps to ensure that data is appropriately labeled and protected based on its sensitivity and value. Different types of media may require different levels of security, and categorizing them allows organizations to implement appropriate controls.

upvoted 1 times

⊟ **deeden** 10 months, 4 weeks ago

Selected Answer: B

Option B sounds more logical to me. Assets can easily get lost without inventory, and you can't protect what you don't have.

I think there's a grey area here because labeling requires both classification and categorization of data.

By classifying data based on sensitivity, value, and criticality, organizations can apply appropriate security controls and protection measures. This approach ensures that sensitive information is handled with the necessary care, REGARDLESS OF THE MEDIA ON WHICH IT IS STORED.

Categorizing media types is still important for physical security and access controls, but it's a secondary consideration compared to data classification.

Review is important during audits, not necessarily during data labeling.

upvoted 3 times

⊟ **CCNPWILL** 1 year, 2 months ago

A has to happen first before B. A is priority.

upvoted 1 times

⊟ **YesPlease** 1 year, 6 months ago

Selected Answer: A

Answer A)

Classification versus Categorization:

Classification by itself is simply a system of classes set up by an organization to differentiate asset values and, therefore, protection levels. The act of assigning a classification level to an asset is called categorization. Ideally, all assets should be categorized into a classification system to allow them to be protected based on value.

https://destcert.com/resources/domain-2-asset-security/

upvoted 1 times

Vince_F_Fang 1 year, 10 months ago

Selected Answer: D

Isn't this issue about the control of the program itself

upvoted 4 times

50e940e 1 year ago

correct, it is the control of PROCEDURE, instead of asset management

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: A

The MOST appropriate control for asset data labeling procedures is option A: Categorizing the types of media being used.

Asset data labeling procedures involve labeling and categorizing different types of media (such as physical storage devices, electronic media, or documents) to effectively manage and track data assets. Categorizing the types of media being used helps in identifying and distinguishing between different storage devices and media types, allowing for better organization and control.

By categorizing the types of media, organizations can implement appropriate security controls and procedures tailored to each category. This includes assigning different levels of sensitivity or classification to data stored on specific media, implementing access controls based on media types, and applying specific handling and disposal procedures.

upvoted 3 times

HughJassole 2 years ago

The question is asking "control for asset data labeling". So how to label data that is an asset, for example an application or a database with customer info. A CMDB does that, that's where you store all this info, and everything is a Configuration Item and has all relevant info. So the answer is B.

upvoted 2 times

Rollingalx 2 years, 3 months ago

I go with B.
While categorizing the types of media being used and reviewing audit trails of logging records are important controls, it may not be as directly relevant to asset data labeling procedures as logging data media to provide a physical inventory control.

upvoted 3 times

s_n_ 2 years, 5 months ago

The most appropriate control for asset data labeling procedures is B. Logging data media to provide physical inventory control. By logging the data media, organizations can keep track of all of the different types of media being used, such as CDs, USBs, hard drives, etc. Organizations can also use the logs to track the movement of data media within the organization, including any off-site storage access controls. Additionally, by logging data media, organizations can review audit trails of logging records to ensure that all data media is properly labeled and accounted for. Resources include National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and The National Archives, Guidance on the Management of Data Media Labeling.

upvoted 3 times

Billy235 2 years, 6 months ago

Question is asking about labeling procedures. Options B, C and D have nothing to do with a labeling procedure. Answer is A.

upvoted 2 times

Firedragon 2 years, 7 months ago

Selected Answer: A

official study guide P190, Marking Sensitive Data and Assets
labeling has nothing to do with audit logs

upvoted 3 times

Jimmyliu0822 2 years, 7 months ago

Assestment

upvoted 1 times

Bhuraw 2 years, 8 months ago

Selected Answer: D

Others seem irelevant

upvoted 1 times

⊟ **DButtare** 2 years, 9 months ago

Selected Answer: D

We are talking about the data itself not the medium

upvoted 4 times

Question #55 *Topic 1*

What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment?

A. Swapping data

B. Randomizing data

C. Encoding data

D. Encrypting data

Suggested Answer: *D*

Community vote distribution

B (55%) A (29%) D (16%)

⊟ **somkiatr** Highly Voted 👍 2 years, 6 months ago

Selected Answer: A

Should be A.

Techniques of Data Anonymization

1. Data masking
2. Pseudonymization
3. Generalization
4. Data swapping
5. Data perturbation
6. Synthetic data

Reference : https://corporatefinanceinstitute.com/resources/business-intelligence/data-anonymization/

upvoted 14 times

⊟ **deeden** 10 months, 4 weeks ago

I think this question equates Randomizing data to masking, such as replacing values with random meaningless characters (e.g., # , / $) which is a stronger anonymization option than just shuffling values around. I know, it's weird right. lol

upvoted 2 times

⊟ **DERCHEF2009** Highly Voted 👍 2 years, 9 months ago

Selected Answer: B

B is much better

upvoted 6 times

⊟ **stickerbush1970** 2 years, 9 months ago

anonymizing - remove identifying particulars or details, how is B doing this?

upvoted 4 times

⊟ **CharlesL** 2 years, 8 months ago

How do you get the testing result in from encrypted content?

upvoted 4 times

⊟ **jackdryan** 2 years, 1 month ago

B is correct

upvoted 1 times

⊟ **RedMartian** Most Recent ⊙ 2 months, 3 weeks ago

Selected Answer: B

Not A. Means shuffling PII between records. This preserves real data in the system and could still expose PII if re-identified. Not true anonymization.

upvoted 1 times

⊟ **Imranbhatti** 3 months, 3 weeks ago

Selected Answer: B

The best approach to anonymizing personally identifiable information (PII) in a test environment is B. Randomizing data.

Randomizing data involves altering the original data in such a way that it cannot be traced back to the individual, ensuring privacy and compliance

with data protection regulations like GDPR12. This method is effective because it maintains the structure and format of the data while making it impossible to identify the original individuals.
Option A, "Swapping data," is incorrect because it involves exchanging data values between different records. While this can obscure the original data, it does not fully anonymize it. Swapped data can sometimes be re-identified if the swapping pattern is discovered or if there are other data points that can be correlated12.

Randomizing data, on the other hand, alters the data in a way that makes it impossible to trace back to the original individuals, providing a higher level of anonymity and security

upvoted 2 times

cysec_4_lyfe 4 months, 2 weeks ago

Selected Answer: B

Swapping data may not provide sufficient protection against re-identification if the dataset is small.

upvoted 2 times

Fouad777 6 months, 2 weeks ago

Selected Answer: B

What is the BEST approach to anonymizing personally identifiable information (PII) in a test environment? A. Swapping data B. Randomizing data C. Encoding data D. Encrypting data
The BEST approach to anonymizing personally identifiable information (PII) in a test environment is:

B. Randomizing data

Here's why:

Randomizing data effectively removes the association between the data and the individuals it represents, making it difficult to re-identify the individuals from the anonymized dataset. This approach ensures that the data cannot be traced back to specific individuals, which is crucial for maintaining privacy and confidentiality in a test environment.

Swapping data (A) and encoding data (C) may help in anonymization, but they are generally less effective than randomization in ensuring data cannot be traced back. Encrypting data (D) secures the data but doesn't anonymize it, as the original data can still be accessed with the appropriate decryption keys.

upvoted 4 times

Verm12 10 months ago

Selected Answer: B

OSG states "Randomized masking can be an effective method of anonymizing data" pg 203

upvoted 2 times

Ezebuike 10 months, 2 weeks ago

I am not sure if an encrepted data casn be used in a test environment. But I will go for option B

upvoted 1 times

JohnBentass 1 year ago

Selected Answer: A

A. Swapping data

Data swapping involves exchanging values between different records in a dataset, which helps preserve the confidentiality of individual data entries while maintaining the overall statistical distribution and relationships within the data.

This technique is more effective than some other common anonymization methods:

Randomizing data alters values with random, mock data but doesn't maintain the exact statistical distribution, which can compromise data utility for complex datasets.
Data swapping, on the other hand, provides a straightforward way to anonymize PII while preserving data integrity and statistical accuracy appropriate for testing needs. It enables realistic datasets for software development and testing without exposing sensitive information

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: B

B. Randomizing data: Randomizing data is a common approach to anonymization. It involves replacing original data values with randomly generated values that do not correspond to any real individuals. This ensures that the data cannot be traced back to its original source while still maintaining its structural and statistical properties for testing.

upvoted 1 times

dm808 1 year, 3 months ago

Selected Answer: B

Only option B refers to anonymization.

A. Swapping Data- Pseudonymization
B. Randomizing Data- Anonymization
C. Encoding Data- Tokenization
D. Encrypting Data- Tokenization

upvoted 1 times

GuardianAngel 1 year, 4 months ago

Answer: B. Randomizing data

A test environment might including needing to test analytics, computations, reports, dashboards - basically processes that have to be tested with unencrypted data.

Randomizing data involves replacing PII with randomly generated values while maintaining the statistical properties of the original data. This ensures that the computations and analytics performed on the anonymized data yield accurate results and reflect the real-world scenarios.

Swapping data involves replacing PII with other data. Swapping data may introduce biases or alter the statistical properties needed for accurate analytics and computations.

Encoding data transforms data into a different representation using encoding schemes.

Encrypting data is not be the best choice for this scenario as encryption aims to protect data rather than anonymize it.

upvoted 2 times

study22024 1 year, 5 months ago

Randomized masking can be an effective method of anonymizing data pg279 cissp study guide

upvoted 2 times

YesPlease 1 year, 6 months ago

Selected Answer: B

Answer B)

Encrypting the data does not remove Pii...it just prevents anyone that stole the data from reading it without the proper credentials. However, someone with proper rights...like a DBA can see the Pii data without a problem.

Also, Page 202-204 in CISSP study guide clear states randomization as the best option to anonymize data in a way that it will even make GDPR a non-issue.

upvoted 2 times

homeysl 1 year, 8 months ago

Selected Answer: A

A is my answer

upvoted 1 times

Sledge_Hammer 1 year, 9 months ago

The correct Answer is A.

There are also some well-known techniques to be applied in a structured database for anonymization:

Masking: removing, encrypting, or obscuring the private identifiers
Pseudonymization: Replace the private identifiers with pseudonyms or false values
Generalization: Replacing a specific identifier value with a more general one
Swapping: Shuffling the attribute values of the dataset so that they are different from the original one
Perturbation: Changing the data by introducing random noises or using random methods

upvoted 3 times

Dann108 1 year, 10 months ago

It is randomization. Even if you remove not only encrypt personal data, in some cases it is still not anonymized. The ideal answer would be "Randomized masking".

upvoted 1 times

Question #56 *Topic 1*

Which of the following departments initiates the request, approval, and provisioning business process?

A. Operations

B. Security

C. Human resources (HR)

D. Information technology (IT)

Suggested Answer: *A*

Community vote distribution

A (71%) C (29%)

N00b1e Highly Voted 2 years, 9 months ago

HR would be the only people to initiate a request, surely?

upvoted 9 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

jackdryan 2 years, 1 month ago

Changing to A

upvoted 2 times

somkiatr Highly Voted 2 years, 6 months ago

Selected Answer: A

A is correct. Operation as a process owner should give requirement to IT. HR is responsible for access control provision not business process provision.

upvoted 6 times

TeeheeShamon Most Recent 2 months, 3 weeks ago

Selected Answer: C

Chat gpt says it's C too.

upvoted 1 times

Imranbhatti 3 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Human resources (HR).

Human Resources (HR) typically initiates the request, approval, and provisioning business process. This department is responsible for managing employee-related processes, including onboarding, access provisioning, and other administrative tasks

Option A, "Operations," is incorrect because the Operations department typically focuses on the day-to-day activities and processes that keep the organization running smoothly. While Operations may be involved in the provisioning process, they are not usually the ones who initiate the request, approval, and provisioning business process12.

Human Resources (HR) is the department that usually initiates these processes, especially when it comes to employee-related activities such as onboarding, access provisioning, and other administrative tasks

upvoted 2 times

CKaraf 3 months, 3 weeks ago

Selected Answer: C

Since when do IT initiate request? Did they hire the person? 100% HR

upvoted 1 times

Rider2053 4 months, 1 week ago

Selected Answer: C

The request, approval, and provisioning business process is typically initiated by the Human Resources (HR) department, especially in relation to employee onboarding, role changes, and termination

upvoted 1 times

Fouad777 6 months, 1 week ago

Selected Answer: C

The Human Resources (HR) department typically initiates the request, approval, and provisioning process for new employees, contractors, or changes in access for existing staff. This is because HR is responsible for managing personnel-related information, including hiring, onboarding, role changes, and terminations, which directly impact access requirements.

upvoted 1 times

Moose01 6 months, 3 weeks ago

Selected Answer: A

A - COO, Chief Operation Office will align Organization's objectives, business objective to IT and Security. not HR, HR will receive certain policies, processes and procedures from COO.

upvoted 1 times

Mrawrrr 8 months ago

Selected Answer: C

It is always HR which initiates the provisioning. HR is responsible for ensuring that new employees have the necessary access and resources to perform their job functions, which includes initiating requests for system access, equipment, and other provisions.
Operations might do it but not initiate.

upvoted 1 times

CaptJanek 10 months, 4 weeks ago

In mot companies there is no Operations department, this is a canned CISSP answer and this is the answer they want for the test, so this is the answer we must use. It does not apply to the real world.

upvoted 1 times

deeden 10 months, 4 weeks ago

This is an example of a badly worded question because there is no context of what a business process could be in reference to; examples of business process could be (not limited to):

Onboarding/Offboarding employees (HR)
Budget allocation/Procurement (Finance)
Marketing campaigns (Marketing)
Strategic Planning (Management)
Hardware and Software Procurement, enhancements, updates, adaptation (IT)
Incident response, Vulnerability management, Security awareness training (Security)

upvoted 1 times

HappyDay030303 1 year, 8 months ago

C. Human resources (HR)

The Human Resources (HR) department typically initiates the request, approval, and provisioning business process for tasks related to employee onboarding, offboarding, access requests, and other personnel-related activities. This process involves requesting access to systems, applications, and resources for new hires or making changes to existing employees' access levels. After HR initiates the request, it is often passed on to the IT department for further action.

upvoted 1 times

xxxBadManxxx 1 year, 11 months ago

A is correct folks are amazing who is answering C lol.

upvoted 2 times

BLADESWIFTKNIFE 1 year, 11 months ago

Selected Answer: C

HR is the home office for all operations approvals and requests. Even CEO need to run things through HR for legal purposes.

upvoted 2 times

Bach1968 1 year, 12 months ago

Selected Answer: C

to me, this answer should be C, why? maybe because i understand the following, in my company the power is withing the HR department, any Process that need to be implemented, must start , regardless who sign it for governing the process even if it is me, if the HR VP say no, i say no.
so i really think this is a gray area question. it is important to note, it depend on the organization, or the bylaws of the company, however, never ever

run a business from an IT perspective, you will brake your company, business has needs, IT is a service provided, they align systems with business needs. this is a golden rule every one keep it in mind.

upvoted 2 times

s_n_ 2 years, 5 months ago

Information technology (IT). In the modern business world, IT departments are typically responsible for initiating, approving, and provisioning business processes. IT departments manage a company's technology resources, such as hardware, software, networks, and data systems. They use these resources to streamline and automate business processes, including requesting, approving, and provisioning. Additionally, IT departments are often responsible for ensuring that the right people have access to the right resources and that the resources are secure. Resources:

- https://www.techopedia.com/definition/25515/business-process-automation
- https://www.globalknowledge.com/us-en/content/what-is-it-department/

upvoted 3 times

Ncoa 2 years, 7 months ago

Selected Answer: A

Initiate, start the process. I would say Operations is the best answer. HR may be an approver and provisioner but the main initiator imo

upvoted 2 times

Question #57 *Topic 1*

An organization is setting a security assessment scope with the goal of developing a Security Management Program (SMP). The next step is to select an approach for conducting the risk assessment. Which of the following approaches is MOST effective for the SMP?

A. Security controls driven assessment that focuses on controls management

B. Business processes based risk assessment with a focus on business goals

C. Asset driven risk assessment with a focus on the assets

D. Data driven risk assessment with a focus on data

Suggested Answer: *D*

Community vote distribution

B (48%) C (36%) Other

FredDurst Highly Voted 2 years, 7 months ago

Selected Answer: B

This is an easy one . The reason we conduct security assessments as part of developing a functional/relevant security program is to generate value to the stakeholders by ensuring that the identified risks to the BUSINESS are optimized and we are left with residuals . Other answers are tactical .As a cybersecurity leaders you must turn tactical observations into strategic insights but first must find out what business process / function is the cash cow or star player and then identify the assets , data etc that enable it and then get tactical and geek out with your security toys .

This question wants to measure your business savvy, savvy ? lol

upvoted 28 times

dirk_gentley Highly Voted 2 years, 9 months ago

Selected Answer: C

First step of Risk Assessment is to identify assets. https://sansorg.egnyte.com/dl/RFrVIbX2oc

upvoted 9 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

djedwards Most Recent 3 weeks, 4 days ago

Selected Answer: C

In everything I've studied it always comes back to identification of the assets

upvoted 1 times

RedMartian 2 months, 3 weeks ago

Selected Answer: B

Not C. Focuses on protecting specific assets. While important, it may miss the bigger picture of how those assets support key business functions.

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: B

When developing a SMP, the "MOST" effective approach is to align the risk assessment with the business processes and business goals. Asset driven assessment focuses on technical assets, but may not capture the full business process impact.

upvoted 1 times

Fouad777 6 months, 1 week ago

Selected Answer: B

When developing a Security Management Program (SMP), the primary objective is to align security efforts with the organization's overall business goals. A business process-based risk assessment ensures that the security strategies directly address and protect critical processes that are essential for achieving organizational objectives. This approach effectively identifies risks in the context of the organization's operations and priorities.

upvoted 2 times

430026f 7 months ago

Selected Answer: C

first thing to do when conducting risk assessment is the identifications of assets , the data is included as an asset , then the control based risk assessment to make sure the security controls are implemented correctly when needed and the B choice it is rarely when security is being an important as business goal ,but thu it is not the first step as the question tells

upvoted 1 times

robervalchocolat 10 months ago

This approach focuses on identifying and assessing risks that could impact the organization's ability to achieve its business goals. This is the most effective approach for developing a Security Management Program (SMP) because it ensures that security controls are aligned with the organization's strategic objectives.

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: C

I agree with the majority in saying that everything needs to align with the business goals i.e., assets, security controls, etc. But I can't get my head around the idea that most risk management framework always starts with discovery and asset identification. You can't protect what you don't know. Now, this question is about the scope of security assessment, and the approach for conducting risk assessment. Personally, I would select a risk-based approach (but it's not an option) and that would just take you back to asset identification.

upvoted 1 times

8e1c45b 11 months, 1 week ago

Selected Answer: C

Security is protecting your crown jewels. What are your assets and why you have to protect them, what are th business goals you have driven. All ties to Assets first.

upvoted 1 times

CCNPWILL 1 year ago

Selected Answer: B

Security strategy needs to be in line with business strategy. Answer is B.

upvoted 2 times

Vaneck 1 year, 3 months ago

Selected Answer: B

The most effective approach for the Safety Management Program (SMP) is :

B. Business process-based risk assessment with a focus on business objectives.

This approach ensures that risk assessment is aligned with business objectives and needs, enabling risk management that directly supports the organization's strategic objectives. By focusing on business processes, the organization can better understand how security risks affect its operations, and make informed decisions to mitigate these risks appropriately.

upvoted 1 times

GuardianAngel 1 year, 4 months ago

ANSWER: B. Business processes based risk assessment with a focus on business goals

https://www.ifc.org/content/dam/ifc/doc/mgrt/p-handbook-securityforces-2017.pdf

https://policy.un.org/sites/policy.un.org/files/files/documents/2020/Oct/spm_-_chapter_iv_-_section_a_-_security_risk_management_2.pdf

https://documents1.worldbank.org/curated/en/962101606403107500/pdf/Security-Management-Plan-Emergency-Locust-Response-Program-P173702.pdf

https://documents1.worldbank.org/curated/en/099530109052230270/pdf/P1767580b5e94b07108eb00a05d98f790d1.pdf

upvoted 2 times

iwannapass 1 year, 4 months ago

Selected Answer: B

B. Security SUPPORTS the Business Goal. Without the business, there is no security, who will be paying security? The Business Goal is most important, Security will support the Business Goal

upvoted 2 times

Hackermayne 1 year, 5 months ago

Selected Answer: B

I'm gonna say the business goals. It just says organization, not a for profit business, there are some situations like governments and nonprofits (and even some instances in normal for profit business) where you won't care about the assets as long as you're meeting the goal.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C) Asset driven risk assessment with a focus on the assets

Security management is the high-level process of cataloguing enterprise IT assets and developing the documentation and policies to protect them from internal, external, and cyber threats.

https://www.hpe.com/us/en/what-is/security-management.html

upvoted 1 times

Soleandheel 1 year, 6 months ago

B. Business processes based risk assessment with a focus on business goals. Think like a manager guys. It's always about the priorities of the business.

upvoted 2 times

Question #58 *Topic 1*

Which technique helps system designers consider potential security concerns of their systems and applications?

A. Threat modeling

B. Manual inspections and reviews

C. Source code review

D. Penetration testing

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **dev46** Highly Voted 2 years, 3 months ago

Threat Modeling such as STRIDE would cover pretty much all the security considerations

S - Spoofing
T - Tampering
R - Repudiation
I - Information Disclosure
D - DDoS Attacks
E - Elevation of privilege

upvoted 11 times

⊟ **Kiplan** Highly Voted 2 years, 3 months ago

Selected Answer: A

A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security

https://owasp.org/www-community/Threat_Modeling#:~:text=A%20threat%20model%20is%20a,through%20the%20lens%20of%20security.

upvoted 9 times

⊟ **jackdryan** 1 year, 7 months ago

A is correct

upvoted 1 times

⊟ **zilm0diafpinc** Most Recent 11 months, 4 weeks ago

A. the rest are simply does not sense

upvoted 1 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: A

Threat modeling is a proactive approach to identify and assess potential threats and vulnerabilities in a system or application during the design phase. It involves systematically analyzing the system architecture, identifying potential threats and attack vectors, and evaluating their potential impact. By understanding the potential threats and their likelihood, system designers can make informed decisions about implementing appropriate security controls and mitigations.

upvoted 2 times

⊟ **ItsBananass** 2 years, 3 months ago

I'm thinking "B". As in, Code Review...etc

upvoted 1 times

Question #59 *Topic 1*

A security professional can BEST mitigate the risk of using a Commercial Off-The-Shelf (COTS) solution by deploying the application with which of the following controls in place?

A. Network segmentation

B. Blacklisting application

C. Whitelisting application

D. Hardened configuration

Suggested Answer: *D*

Community vote distribution

D (58%) A (35%) 6%

Nickolos Highly Voted 2 years, 9 months ago

The risk of what? The application being dangerous to the corporate network or the application being vulnerable to external exploits? Either way segmentation makes more sense imo.

upvoted 11 times

dev46 2 years, 9 months ago

True. Network Segmentation makes sense. It minimize the exposure.

How can you harden COTS? It's a ready-made product.

upvoted 6 times

stickerbush1970 2 years, 9 months ago

I would think this mean hardening the OS, not COTS

upvoted 5 times

Nickolos 2 years, 9 months ago

Exactly - ensuring no unnecessary ports or services are running, access to the internet is configured properly (if at all needed), proper acl is setup, etc.

upvoted 1 times

DeepCyber 2 years ago

Even if you harden the configuration It will not help If there is vulnerability in the software code which is exploited by attacker. Attacker may access your network through legitimate way to exploits your network If network segmentation is not in the place.

upvoted 2 times

AjitZavade Most Recent 2 months, 3 weeks ago

Selected Answer: D

When using a Commercial Off-The-Shelf (COTS) solution, you're dealing with software developed by a third party, over which you have limited control over its code. Therefore, the best way to mitigate risk is by:

✅ Applying a hardened configuration — disabling unnecessary features, services, default accounts, open ports, debug modes, etc.

Hardened configuration helps:
Minimize the attack surface

Reduce vulnerabilities

Ensure secure defaults

Enforce compliance (e.g., CIS Benchmarks, NIST)

❌ Why the Other Options Are Less Appropriate
Option Why It's Not Best for This Scenario
A. Network segmentation Limits lateral movement, but doesn't address vulnerabilities within the COTS app itself. Helpful, but not specific enough.

B. Blacklisting application Blacklisting prevents known bad apps, not a control for mitigating risk of a chosen COTS app.

C. Whitelisting application Whitelisting prevents unapproved software from running — not directly relevant once you've already chosen to run the COTS app.

upvoted 1 times

cysec_4_lyfe 4 months, 2 weeks ago

Selected Answer: D

This is easy to me and the answer is D. Anyone who has configured MS O365 or Entra, etc., knows how unsecure by default these can be. Review best practices and recommendations to harden the COTS products. A.I. - Hardening a COTS application involves configuring it to minimize its attack surface by disabling unnecessary features, removing default accounts, and applying security patches. This approach ensures that the application is set up to operate securely, reducing the likelihood of exploitation by attackers.

upvoted 2 times

cwjchoi 4 months, 2 weeks ago

Selected Answer: D

A vs D

A - it prevent attacker to lateral move to the internal network if the application is compromised

D - It reduce the chance for the application to be compromised

I think it is better to enhance the first line of defense, so D.

upvoted 1 times

humor927 5 months, 1 week ago

Selected Answer: D

The key is what controls you use when you deploy the application.

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: D

I think most confusion comes from the perception of what COTS can be. COTS products can include: motherboards, Windows OS, Microsoft 365, Office, Pfsense, VMware, routers, switches, IoT, etc.

So network and endpoint devices, you can segment, but how about productivity suites and application platforms? network segmentation is a common security practice anyway, regardless of COTS.

I think the best thing is to research CVE and vendor reputation, and then make sure all DEFAULT configuration, credentials, features, etc. are hardened during implementation.

upvoted 3 times

Ramye 1 year ago

Selected Answer: D

Even if you put this in a separate network segment it needs to be hardened because it is off the shelf.

upvoted 1 times

jieaws 1 year, 2 months ago

I remembered OSG recommended D, harderning config. for COTS.

Again, very important, please confine my solution within the context here. A? network segmentation could be an option, but is not the first step I shall do and is out of question context.

I choose D.

upvoted 2 times

ajike 1 year, 3 months ago

The question says control . Hardened configuration will mitigate if there is possibility of an attack. I will go with Network segmentation

upvoted 1 times

Kyanka 1 year, 3 months ago

Answer is D. A COTS application is not necessarily hardened by default. For example, the government uses STIGs to tell admins how to harden some applications.

upvoted 1 times

Hongjun 1 year, 3 months ago

Selected Answer: D

Refer to CISSP official study guide 9th chapter 20- 20.1.11

upvoted 3 times

Hackermayne 1 year, 5 months ago

Selected Answer: D

I'm saying D. As far as risk from attackers goes, I would lean towards network segmentation, however, general risk includes a lot of other factors like user accessibility, interoperability issues, etc. Segmenting it could introduce a much larger and complex workload and ultimately make it risky in that sense.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: D

Answer D) Hardened configuration

This means you remove/change configurations you don't need/want as well as change default usernames/passwords/ports/etc...

Segmenting a network won't help as it would still leave the COTS exposed with defaults readily available to be exploited.

upvoted 1 times

Moose01 1 year, 7 months ago

Selected Answer: A

A. Network Segmentation - when introducing a new pet into your house, you have to learn the behavior and interaction with other pets before you let him loose.
same here, as a security personnel you must know exactly what you introducing before hand and must be on segmented part of the network that shutting an interface can terminate all possible risks on the rest of the network.
trust but verify

upvoted 3 times

homeysl 1 year, 8 months ago

Selected Answer: D

D. Hardened the system that will host the COTS. Segmenting it will kill the functionality of the solution.

upvoted 2 times

Moose01 1 year, 9 months ago

D. Hardening
I am hardening security by segmenting and limit access as needed.
Segmentation is a part of Hardening.

upvoted 4 times

Wz21 1 year, 9 months ago

think like a manager with technical experience and common sense :)

upvoted 1 times

Question #60 *Topic 1*

Which of the following BEST describes centralized identity management?

A. Service providers perform as both the credential and identity provider (IdP).

B. Service providers identify an entity by behavior analysis versus an identification factor.

C. Service providers agree to integrate identity system recognition across organizational boundaries.

D. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.

Suggested Answer: *C*

Community vote distribution

D (36%) A (33%) C (31%)

Marzie Highly Voted 2 years, 2 months ago

Selected Answer: D

Yet another horrible question purely due to ambiguous wording. Centralized IAM doesn't have to be across org boundaries. Which puts me off C and leans me towards D, which I don't like much either tbh

upvoted 8 times

Jenkins3mol 1 year, 2 months ago

Yep, lots of horrible questions.

upvoted 1 times

Jamati Highly Voted 2 years, 7 months ago

Selected Answer: D

Centralized access control implies that a single entity (the IdP) performs all authorization verification.

Decentralized access control (also known as distributed access control) implies that various entities perform authorization verification.

The Identity Provider (IdP) is a third party that holds the user authentication and authorization information. Because centralized identity management is united across all applications, the user only needs to access one console to enable a variety of services and infrastructure. For example, a Service Provider such as a bank can use an IdP like provide customers with seamless access to banking services that are externally managed, like ordering checks, sending money through a cash app, or applying for a loan. If the customer updates their address in one application, it is updated in all applications.

upvoted 7 times

Ramye 1 year, 1 month ago

For the authentication the centralized is ideal as just need to know one ID (use means of SSO) but for authorization it must be individual apps / services as each app/service would authorize based on needs.

So debating Option A or D.

Any confirmed answer would be appreciated. Thx

upvoted 2 times

Sledge_Hammer 1 year, 9 months ago

From your submission here, the answer is A.

upvoted 2 times

RedMartian Most Recent 2 months, 3 weeks ago

Selected Answer: D

Not A. Service providers perform as both the credential and identity provider (IdP). This is a decentralized model, where each provider manages its own identity system — not centralized.

Not B. Service providers identify an entity by behavior analysis versus an identification factor. This refers to behavioral biometrics or continuous authentication, not centralized identity management.

Not C. Service providers agree to integrate identity system recognition across organizational boundaries. This best describes federated identity management, where identity systems work together across domains — not centralized.

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: D

Here's why the other options are less accurate:

A. Service providers perform as both the credential and identity provider (IdP). This describes a more decentralized or federated approach, not centralized. In centralized identity management, the service providers don't handle credential management.

B. Service providers identify an entity by behavior analysis versus an identification factor. Behavioral analysis is a separate security mechanism and isn't the defining characteristic of centralized identity management. Centralized identity management is about who manages the identity, not how it's verified.

C. Service providers agree to integrate identity system recognition across organizational boundaries. This describes federation or identity federation, which is related but distinct from centralized identity management. Federation allows for interoperability between different identity systems, but it doesn't necessarily imply a single, central authority. Centralized identity management can be part of a federated system, but federation itself doesn't define centralized identity management.

upvoted 1 times

easyp 5 months ago

Selected Answer: D

Centralized Identity Management
Definition: In centralized identity management, a single, trusted entity (often called an Identity Provider or IdP) manages all user identities, credentials, and authentication for multiple systems or services within the same organization.

Federated Identity Management
Definition: Federated identity management allows multiple organizations or systems to share identities across boundaries. It enables a user from one organization to authenticate and access services in another organization without needing separate credentials.

I would go with D

upvoted 1 times

easyp 5 months ago

Selected Answer: C

The correct answer is:

C. Service providers agree to integrate identity system recognition across organizational boundaries.

Explanation:
Centralized identity management involves a single identity system being used across multiple services or organizations to authenticate and authorize users. This allows for a more streamlined process of managing user identities and their access across different systems and platforms. When service providers agree to integrate identity system recognition across organizational boundaries, they can rely on a centralized identity provider (IdP) to manage user credentials and access rights consistently.

upvoted 1 times

debig3riw 7 months, 1 week ago

Selected Answer: A

he correct answer is:
D. Service providers rely on a trusted third party (TTP) to provide requestors with both credentials and identifiers.
Explanation:

Centralized identity management involves using a trusted third party (such as an identity provider) to manage user credentials and identifiers. This model consolidates identity and access management to a single authority, which simplifies authentication and ensures consistency across services.

Here's why the other options are incorrect:

A. This describes a situation where the service providers themselves act as identity providers, which is more indicative of a decentralized or isolated identity management model.
B. Behavior analysis does not describe centralized identity management; it relates more to behavioral authentication or continuous authentication.
C. This refers to federated identity management, where multiple organizations agree to recognize each other's identity systems, rather than a centralized approach.

upvoted 1 times

tejas07jain 7 months, 1 week ago

Selected Answer: C

I think C is the right answer. CIM refers to the system where identity data and authentication are handled by a central authority, allowing multiple SPs to recognize and verify identities across different apps, platforms / organizations. It also aligns with Federated Identity management and SSO, where users / services (dispersed across org. boundaries) can authenticate once and get access to the services.

upvoted 1 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: A

The answer is A - answer D refers to Federated Identity Management, which is not the same.

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: C

Horrible... While both options C and D describe centralized identity management, they represent different implementation models.

Key difference:
Option C: Multiple service providers share a common identity repository.
Option D: A trusted third party manages identity information and issues credentials. Federated Identity Management.

Both models aim to achieve the same goal of providing a unified identity management solution across multiple systems and organizations.

upvoted 1 times

8e1c45b 11 months, 1 week ago

Selected Answer: A

Leaning towards A.
This is what the OSG 10e says.
Implementing Identity Management
Identity management (IdM) implementation techniques generally fall into two categories:
Centralized access control implies that a single entity within a system performs all authorization verification.
Decentralized access control (also known as distributed access control) implies that various entities located throughout a system perform authorization verification.
A small team or individual can manage centralized access control. Administrative overhead is lower because all changes are made in a single location, and a single change affects the entire system.

upvoted 2 times

Rachy 11 months, 2 weeks ago

Selected Answer: A

Let's calm down and read the options. If it is centralized, it doesn't need to rely on TPP to provide IAM. The best answer is A which is to one SP is serving as central authority to provide credentials and IDP

upvoted 2 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: A

The most fitting description for centralized identity management would be:

A. Service providers perform as both the credential and identity provider (IdP).

This option accurately portrays the concept of centralized identity management, where a single entity (the service provider) is responsible for both providing credentials (such as usernames and passwords) and verifying identities. This centralization streamlines the authentication process and enhances security by consolidating identity-related functions.

upvoted 2 times

Hardrvkllr 1 year, 2 months ago

Selected Answer: A

I though it was D, but copilot states the answer is A

Centralized identity management is best described by option A: Service providers perform as both the credential and identity provider (IdP). In this model, a single authority (the service provider) is responsible for maintaining and managing the identities and access controls for all users within the system. This central authority acts as the identity provider (IdP), issuing credentials and managing user identities. This approach simplifies administration and improves security by providing a single point of control. However, it can also create a single point of failure and may not scale well for large, distributed systems. Options B, C, and D describe different aspects of identity management but do not accurately define centralized identity management.

upvoted 1 times

eboehm 1 year, 2 months ago

Selected Answer: A

wow soooo many wrong answers here. There is NO mention of federated identities in the question. Centralized just means you are using something like active directly for authentication where decentralized would be a peer-to-peer environment where authentication is handled locally on each system. Dont add extra context to what the question is asking!

upvoted 2 times

AshStevens 1 year, 2 months ago

Selected Answer: D

"C" describes federated identity management, where organizations agree to share identity system recognition across their boundaries. Textbook definitions - that isn't centralised! Consider the danger of blanket statements - if there are any centralised management systems where multiple service providers don't integrate across boundaries, then the answer is too specific to be true.

That leaves A or D to fill in the role of Centralised access - however the service provider would not typically be the one doing this in all cases. D fits the bill.

upvoted 1 times

john_boogieman 1 year, 3 months ago

Selected Answer: D

"Service providers agree to integrate identity system recognition across organizational boundaries" describes a form of federated identity management, not a centralized identity management.

upvoted 1 times

Question #61 *Topic 1*

What is the MOST significant benefit of role-based access control (RBAC)?

A. Reduces inappropriate access

B. Management of least privilege

C. Most granular form of access control

D. Reduction in authorization administration overhead

Suggested Answer: *D*

Community vote distribution

B (62%) D (38%)

Cww1 Highly Voted 2 years, 9 months ago

given answer is correct

upvoted 12 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 3 times

Bach1968 Highly Voted 1 year, 12 months ago

Selected Answer: B

The MOST significant benefit of role-based access control (RBAC) is:

B. Management of least privilege.

RBAC is a widely adopted access control model that provides several benefits, but the management of least privilege is considered its most significant advantage. RBAC ensures that users are assigned only the privileges necessary to perform their specific job functions, known as the principle of least privilege.

By implementing RBAC, organizations can minimize the risk of inappropriate access and unauthorized actions. Users are granted access rights based on predefined roles that align with their responsibilities, eliminating unnecessary privileges that could be exploited. This helps to reduce the attack surface and potential impact of security incidents.

While RBAC also offers other benefits, such as reducing administrative overhead and providing a structured and scalable access control framework, the management of least privilege is considered the most significant because it directly addresses the principle of granting users the minimal privileges required to perform their tasks effectively and securely.

ps. do not forget segregation of duties

upvoted 10 times

TeeheeShamon Most Recent 2 months, 3 weeks ago

Selected Answer: D

Chat gpt says it D

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: B

Must answer from a technical perspective and not an efficiency perspective. Hence, overhead comes second to the principle of least privilege.

upvoted 1 times

easyp 5 months ago

Selected Answer: D

The most significant benefit of Role-Based Access Control (RBAC) is its ability to simplify and reduce administrative overhead by grouping users into roles based on their job functions. These roles are then assigned permissions, instead of managing access for individual users.

upvoted 1 times

easyp 5 months ago

Selected Answer: D

The correct answer is:

D. Reduction in authorization administration overhead

Explanation:
The most significant benefit of Role-Based Access Control (RBAC) is its ability to reduce authorization administration overhead. By assigning access permissions based on roles rather than individual users, administrators can easily manage and update permissions across multiple users who share the same job functions. This simplifies user access management, especially in large organizations, where manually assigning permissions to each user would be time-consuming and prone to errors.

Role-based grouping allows for efficient user management and easier updates, as changes to a role's permissions automatically apply to all users assigned to that role.

upvoted 2 times

humor927 5 months, 1 week ago

Selected Answer: D

D is the MOST significant benefit of role-based access control (RBAC)
B is the General principles of access control

upvoted 1 times

Fouad777 6 months, 1 week ago

Selected Answer: D

Role-Based Access Control (RBAC) is a model for managing user permissions based on their role within an organization. The key advantage of RBAC is that it simplifies access control by grouping permissions into roles and assigning those roles to users, rather than managing individual permissions for each user.

Why Option D is Correct:
Reduction in authorization administration overhead is the most significant benefit of RBAC because it allows for easier management of user access. Instead of assigning individual permissions to each user, administrators can assign users to roles, and those roles automatically inherit the appropriate permissions. This significantly reduces the administrative burden and ensures consistency in access management.

As the organization grows, managing individual permissions becomes more complex and error-prone. RBAC simplifies this by reducing the number of direct assignments needed and ensuring that users only have access to the resources required for their roles.

upvoted 1 times

Ramye 1 year ago

Selected Answer: B

You do not authorize someone some permission/role for reducing administration overhead. Least privilege always needs to be considered.

upvoted 1 times

CCNPWILL 1 year, 2 months ago

Selected Answer: B

B. having a role will put the allowed priv already for the user. easier to manage.

upvoted 1 times

73f8ac3 1 year, 2 months ago

Selected Answer: D

D
RBAC does not guarantee you give the least privilege. It allows you not to spend too much time doing it. Least priviledge is an objective, but RBAC does not guarantee it !

upvoted 3 times

deeden 10 months, 4 weeks ago

I think you're right. It sounds to me like RBAC guarantee's uniformity and consistency based on roles, but not necessarily least privilege. Reduction of admin overhead is the prime advantage.

upvoted 2 times

deeden 10 months, 4 weeks ago

You could potentially use RBAC to give all analysts roles access to engineering, which they don't really need. It's not a benefit, but more like a use/misuse case.

upvoted 1 times

Hongjun 1 year, 3 months ago

Selected Answer: B

Refer to CISSP 9th official guide chapter 14 page 157. RABC helps to implement of the 'least privilege ' policy.

upvoted 3 times

SangSang 5 months, 2 weeks ago

Yes, help to implement, but not guaranteed, nothing prevents you from having 3 separate roles but they all holding the same permissions

upvoted 1 times

OriginalDragon 1 year, 4 months ago

Selected Answer: D

Going with D here, managing least privilege is a subset of admin overhead

upvoted 2 times

dm808 1 year, 3 months ago

100% agree !

and all access controls should manage least privilege.. either by design or by admin overhead

upvoted 1 times

Soleandheel 1 year, 6 months ago

B. Management of least privilege

upvoted 1 times

Zonas 1 year, 7 months ago

I choose D

upvoted 1 times

homeysl 1 year, 8 months ago

Selected Answer: B

B is the correct answer

upvoted 2 times

Moose01 1 year, 9 months ago

D. management and admin overhead work is reduced by put placing ten thousand users into one group if they all need to have access to a particular object.

RBAC is not granular access level, that is where DAC comes into play providing special access to a specific user or group granted by the data owner.

D is the correct answer.

upvoted 3 times

Question #62 *Topic 1*

What is the MOST common security risk of a mobile device?

A. Data spoofing

B. Malware infection

C. Insecure communications link

D. Data leakage

Suggested Answer: *B*

Community vote distribution

D (56%) B (44%)

Joey456 Highly Voted 👍 2 years, 8 months ago

D CISSP 9th ed page 407

upvoted 16 times

> **jackdryan** 2 years, 1 month ago
>
> D is correct
>
> upvoted 1 times

> **shmoeee** 1 year, 7 months ago
>
> This page mentions malware infection/malicious code first in the paragraph.
>
> Then the rest of the paragraph follows with data leakage, then insecure communications.
>
> Not sure which one to choose here since they all are mentioned on page 407
>
> upvoted 1 times

>> **shmoeee** 1 year, 7 months ago
>>
>> As a follow up to my last comment, this page also mentions that on the CISSP exam, "mobile devices" should include smartphones, tablets, laptops, smart watches, and fitness trackers fyi
>>
>> upvoted 3 times

SF_NERD Highly Voted 👍 2 years, 9 months ago

Selected Answer: B

Question is about MOST COMMON, not highest threat. B is correct. Even Kiplan's link says that in the initial paragraph.

upvoted 6 times

RedMartian Most Recent ⊙ 2 months, 3 weeks ago

Selected Answer: D

Not B. Still a concern, but less frequent on mobile compared to PCs due to app store controls and sandboxing.

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: D

While all the options are potential risks, data leakage is the most common security risk associated with mobile devices.

Variety of factors contribute to leakage: Mobile devices are easily lost or stolen, contain sensitive personal and work data, and often connect to untrusted networks. These factors dramatically increase the risk of data leakage.

upvoted 1 times

JAlexander35 6 months, 1 week ago

Selected Answer: D

Malware infection is not that common on mobile devices

upvoted 1 times

somsom 8 months, 1 week ago

Read the question to know what is asked. Risk and not threat . Common threat is malware like phishing however common risk is data leakage. There is different between risk and threats . Answer is D

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: D

I think everyone here would agree that threat and risk have a different definitions. To put it simply: (Risk = Asset x Vulnerability x Threat) So the threat of Malware infecting my phone could lead to the risk of... leaking data. Option D

upvoted 3 times

CCNPWILL 1 year, 2 months ago

Selected Answer: D

Agree with D. That is the biggest concern of a business. not specifically about malware.. malware that is doing what... question doesnt say. D is clear and is the best answer.

upvoted 1 times

dm808 1 year, 3 months ago

Selected Answer: D

The answer is D

A. Data spoofing -Threat
B. Malware infection - Threat
C. Insecure communications link- Vulnerability
D. Data leakage - Risk

upvoted 4 times

hoho2000 1 year, 3 months ago

Selected Answer: B

You must first have malware than follow by data leak.

Also not all mobile have important information to leak. Malware can infect a mobile phone than move to another device when its connected to the office network.

This seems more logical.

upvoted 1 times

ManU145 1 year, 6 months ago

https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

1) Data Leakage

upvoted 1 times

Soleandheel 1 year, 6 months ago

D. Data leakage ......think of all the apps you installed on your phone. On the other hand, how many times have you had a malware on your phone? For me, never! Imagine all the data leakage that happens with all the apps installed on your phone. D. Data leakage is the correct answer. Guys again stop relying too much on chatgpt. Chatgpt says B. malware which is wrong.

upvoted 2 times

ljkesmeer 1 year, 8 months ago

Selected Answer: D

D is correct!

upvoted 1 times

Dagi_D 1 year, 8 months ago

malware infection is a common security risk for mobile devices, data leakage is the impact.

upvoted 2 times

noh_ssiw_l 1 year, 9 months ago

Selected Answer: D

Commingling!!!!!!!!

upvoted 1 times

Vince_F_Fang 1 year, 10 months ago

Selected Answer: D

Data leakage is more common, including device loss, device intrusion, and being seen on the screen, all of which can lead to data leakage

upvoted 1 times

⊟ **xxxBadManxxx** 1 year, 10 months ago

B: Malicious Apps and Websites. Like desktop computers, mobile devices have software and Internet access. Mobile malware (i.e. malicious applications) and malicious websites can accomplish the same objectives (stealing data, encrypting data, etc.)

upvoted 1 times

Question #63 *Topic 1*

What level of Redundant Array of Independent Disks (RAID) is configured PRIMARILY for high-performance data reads and writes?

A. RAID-0

B. RAID-1

C. RAID-5

D. RAID-6

Suggested Answer: *A*

Community vote distribution

A (100%)

Kyanka 9 months, 4 weeks ago

Selected Answer: A

Shouldn't be any debate but a helpful way to remember RAID 0 is the performance based one is because of how often you see it in hybrid with other configs: RAID 10, RAID 50, etc.

upvoted 2 times

Jay327 2 years, 1 month ago

Selected Answer: A

striping=Performance

upvoted 2 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: A

RAID 0

upvoted 1 times

dev46 2 years, 3 months ago

RAID 0 is right

Nice article
https://www.prepressure.com/library/technology/raid

upvoted 4 times

Question #64 *Topic 1*

What type of risk is related to the sequences of value-adding and managerial activities undertaken in an organization?

A. Control risk

B. Demand risk

C. Supply risk

D. Process risk

Suggested Answer: *D*

Community vote distribution

D (100%)

jokijoki Highly Voted 1 year, 8 months ago

D is correct.
Processes are the sequences of value-adding
and managerial activities undertaken by the company.
Process risk relates to disruptions to these processes.

https://globaljournals.org/GJRE_Volume14/3-Risk-Assessment-and-Management.pdf

upvoted 9 times

jackdryan 1 year, 1 month ago

D is correct

upvoted 1 times

somkiatr Highly Voted 1 year, 6 months ago

Selected Answer: D

D.
Process Risk
Processes are the sequences of value-adding
and managerial activities undertaken by the company.
Process risk relates to disruptions to these processes. It
affects a firm's internal ability to produce and supply
goods/services, which results from the consequences of
a breakdown in a core operating, manufacturing or
processing capability. It includes.
• Manufacturing yield variability
• Lengthy set-up times and inflexible processes
• Equipment reliability
• Limited capacity/bottlenecks
• Outsourcing key business processes

Reference : https://globaljournals.org/GJRE_Volume14/3-Risk-Assessment-and-Management.pdf

upvoted 6 times

Soleandheel Most Recent 6 months, 3 weeks ago

D. Process risk

upvoted 1 times

Question #65 *Topic 1*

International bodies established a regulatory scheme that defines how weapons are exchanged between the signatories. It also addresses cyber weapons, including malicious software, Command and Control (C2) software, and internet surveillance software. This is a description of which of the following?

A. International Traffic in Arms Regulations (ITAR)

B. Palermo convention

C. Wassenaar arrangement

D. General Data Protection Regulation (GDPR)

Suggested Answer: *C*

Community vote distribution

C (100%)

Jamati Highly Voted 👍 2 years, 7 months ago

Selected Answer: C

The answer is C. Surprisingly the Wassenaar arrangement can't be found anywhere in the Study Guide so I don't understand why ISC2 would test on this.

upvoted 5 times

ADeAngelo 2 years, 5 months ago

possible one those 50 test questions thrown in and don't count for total score.

upvoted 3 times

Woz 2 years, 7 months ago

Good Question.

upvoted 1 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

somsom Most Recent ⊙ 8 months, 1 week ago

I just know is C

upvoted 1 times

Abakoule 11 months ago

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control regime established on 12 July 1996, in Wassenaar, near The Hague, Netherlands. According to the Wassenaar Arrangement document, it was "established to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

upvoted 3 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: C

I have no idea which one to choose, but I trust the guys below.

upvoted 2 times

Kyanka 1 year, 3 months ago

Selected Answer: C

C: This question is definitely now in the study materials for CISSP. Some people were saying it's not in the Study Guide a year or more ago.

upvoted 1 times

franbarpro 2 years, 8 months ago

The qeustion asks for international bodies...A. ITAR is out (This is US) B. Is also out (Human traficking/orgnize crime) C. Is def the answer established in 1996 between 42 states. D. Is just EU Privacy Law

upvoted 4 times

Joey456 2 years, 8 months ago

C - https://sector.ca/what-the-wassenaar-arrangement-means-for-cybersecurity-pros/

upvoted 2 times

Question #66 *Topic 1*

An organization has implemented a protection strategy to secure the network from unauthorized external access. The new Chief Information Security Officer
(CISO) wants to increase security by better protecting the network from unauthorized internal access. Which Network Access Control (NAC) capability BEST meets this objective?

A. Port security

B. Two-factor authentication (2FA)

C. Strong passwords

D. Application firewall

Suggested Answer: *B*

Community vote distribution

A (61%) B (39%)

⊟ **DERCHEF2009** Highly Voted 2 years, 9 months ago

Selected Answer: A

NAC = Port Security

upvoted 23 times

⊟ **BDSec** Highly Voted 2 years, 9 months ago

“Internal access” is key here. Port security.

upvoted 9 times

⊟ **cccispman** 2 years, 6 months ago

You correctly identify 'internal access' as being key and I agree with you !
But ...
Port 22 is routine open internally for legitimate access. 2FA is standard practice these days for securing access to network infrastructure.

upvoted 3 times

⊟ **dev46** 2 years, 9 months ago

Correct

upvoted 3 times

⊟ **cysec_4_lyfe** Most Recent 2 months, 3 weeks ago

Selected Answer: A

Unauthorized "internal access" would insinuate they include insiders or employees who would already be authenticated. Port security is the best Network Access Control (NAC) capability to protect against unauthorized internal access because it enforces physical and data-link layer restrictions on network ports, preventing rogue devices from connecting to the network. This directly addresses the CISO’s goal of mitigating insider threats and unauthorized internal device proliferation.

upvoted 1 times

⊟ **RedMartian** 2 months, 3 weeks ago

Selected Answer: A

Not B. Enhances user authentication, but doesn’t control device-level access to the internal network.

upvoted 1 times

⊟ **amitsir** 3 months, 1 week ago

Selected Answer: B

How 2FA relates to NAC:
NAC systems can incorporate 2FA as a security measure to verify user identity and grant access to the network.
By requiring users to provide a password and a second factor (like a code from a mobile app or a hardware token), 2FA strengthens the authentication process and makes it more difficult for unauthorized users to gain access.
2FA can be used to control access to specific resources or zones within a network, helping to protect sensitive data and systems

upvoted 1 times

⊟ **WZ1122** 4 months, 1 week ago

Selected Answer: A

I trust deepseek

The BEST Network Access Control (NAC) capability to protect the network from unauthorized internal access is:

A. Port security

Explanation:
Port security is a NAC feature that restricts access to a network by limiting which devices can connect to specific switch ports based on their MAC addresses. This prevents unauthorized devices from gaining access to the network internally, even if they are physically connected to the network.

Two-factor authentication (2FA) and strong passwords are important for securing user accounts but do not directly address unauthorized internal access at the network level.

Application firewalls are designed to protect applications from external threats and are not specifically focused on controlling internal network access.

Port security is the most effective NAC capability for mitigating risks from unauthorized internal access.

upvoted 1 times

easyp 5 months ago

Selected Answer: B

The best option for securing internal network access is:

B. Two-factor authentication (2FA).

While 2FA is typically seen as a defense for external access, it can also be crucial for internal access. In environments where insiders are given access to the network, 2FA ensures that even if an insider's credentials are compromised (for instance, if someone gains access to a user's password), the second factor (like a time-based code or biometric scan) is required to access the system. This significantly reduces the risk of unauthorized internal access.

upvoted 2 times

easyp 5 months ago

Selected Answer: B

The correct answer is:

B. Two-factor authentication (2FA)

Explanation:
Two-factor authentication (2FA) provides an additional layer of security beyond just relying on passwords or credentials. By requiring two separate factors (something the user knows, like a password, and something the user has, like a token or mobile device), 2FA significantly increases protection against unauthorized access, even if an attacker has compromised a user's password.

Internal access control is a major focus here, and 2FA is especially effective in mitigating the risk of unauthorized access by internal users, as it strengthens the authentication process and ensures that access is granted only when both factors are verified.

upvoted 1 times

somsom 8 months, 1 week ago

Always check the protocol involved it will help

upvoted 1 times

somsom 8 months, 1 week ago

It read a NAC the answer is port security . Two factor is part of cloud security .

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: B

In this context, I think Port security is a network security feature that restricts access to a network port by limiting the number of MAC addresses allowed on a specific port. It's a layer-2 security mechanism that helps prevent unauthorized devices from accessing the network. This focus more on unauthorized external access.

Unauthorized internal access is more likely would be coming from insider threats e.g., a disgruntled employee, or social engineering attack, contractors, etc.

upvoted 1 times

Rachy 11 months, 2 weeks ago

Selected Answer: B

To increase the vote and not confuse people, I will go for B anytime any day. Port security is for external access control

upvoted 1 times

Ramye 1 year, 1 month ago

The objective of this question “protecting the network from unauthorized internal access” and to satisfy this requirements it is most likely 2FA (MFA). 2FA / MFA will be used for Authentication / Authorization, hence the answer is: B

upvoted 1 times

MP26 1 year, 2 months ago

MFA is not a capability of a NAC. So it should be A:

upvoted 2 times

marziparzi 1 year, 2 months ago

This says "An organization has implemented a protection strategy to secure the network from unauthorized external access."

If it didn't say that I would have leaned to 2FA. But 2FA is relevant for both external and internal. We need to find something that's exclusive to internal. That's why I think it's Port security

upvoted 1 times

Hongjun 1 year, 3 months ago

Selected Answer: B

The key word - increase . The question told us that control already been implemented. Now they want to increase. B is increase which from 1 to 2 ACD are all basic control which is from 0 to 1.

upvoted 2 times

IntheZone 1 year, 5 months ago

Selected Answer: B

While Port security is good, 2FA is better as there are two steps to bypass. Also for port security, MAC spoofing is a thing which makes me doubt this could be the right answer

upvoted 1 times

Question #67 *Topic 1*

Which section of the assessment report addresses separate vulnerabilities, weaknesses, and gaps?

A. Findings definition section

B. Risk review section

C. Executive summary with full details

D. Key findings section

Suggested Answer: *D*

Community vote distribution

D (54%) A (31%) B (15%)

Joey456 Highly Voted 2 years, 2 months ago

B - https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/how-to-write-vulnerability-assessment-report/#:~:text=Creating%20a%20vulnerability%20assessment%20report,automated%20and%20manual%20testing%20tools.

upvoted 5 times

RedMartian Most Recent 2 months, 3 weeks ago

Selected Answer: A

Key Findings highlight critical issues only, not a comprehensive list.

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: A

In the context of a CISSP exam or security assessment report, "findings" and "key findings" serve different purposes:

Findings: These are the detailed, specific observations and issues discovered during the assessment. They represent all the vulnerabilities, weaknesses, and gaps identified in the system or environment. Findings are often technical and provide a granular view of the security posture.

Key Findings: These are the most significant and critical findings that warrant immediate attention. They are a subset of the overall findings, selected based on their potential impact, severity, and relevance to the organization's security objectives. Key findings are often highlighted in the executive summary or a dedicated "key findings" section of the report to bring them to the attention of senior management and stakeholders.

upvoted 1 times

J_Ko 3 months ago

While I would agree with the above, answer A states "finding definitions", not the findings themselves; so they should consist of terms, definitions, etc that provide definition and context to the (key) findings.

upvoted 1 times

Fouad777 6 months, 2 weeks ago

Selected Answer: A

To best meet the objective of protecting the network from unauthorized internal access, the most suitable Network Access Control (NAC) capability is:

A. Port security

Port security helps prevent unauthorized devices from connecting to the network by limiting access to specific physical ports on network switches. This measure can effectively control internal access to the network, ensuring that only authorized devices and users can connect.

If you have more questions or need further assistance, feel free to ask!

upvoted 1 times

AMANSUNAR 1 year, 1 month ago

Selected Answer: D

The key findings section of an assessment report provides a detailed breakdown of identified vulnerabilities, weaknesses, and gaps. It offers a comprehensive overview of the security issues discovered during the assessment.

upvoted 2 times

InclusiveSTEAM 1 year, 2 months ago

The answer is D

The section of an assessment report that addresses individual vulnerabilities, weaknesses, and gaps is the key findings section.

The key findings provides the detailed technical breakdown of the specific issues uncovered during testing/examination. It outlines and describes each finding.

The executive summary and risk review sections provide higher-level overview and analysis.

The findings definition section explains risk scoring but doesn't cover the vulnerabilities themselves.

upvoted 4 times

VVine 1 year, 3 months ago

Selected Answer: D

Key findings provides detailed info

upvoted 3 times

Bach1968 1 year, 5 months ago

Selected Answer: D

The section of the assessment report that typically addresses separate vulnerabilities, weaknesses, and gaps is the "Findings" or "Key Findings" section. Option D, "Key findings section," is the most appropriate choice.

In this section, the report typically presents a detailed analysis of the identified vulnerabilities, weaknesses, and gaps discovered during the assessment process. It provides specific information about each finding, including the nature of the issue, its impact on the system or organization, and recommendations for remediation or mitigation. This section helps the recipient of the report understand the specific areas of concern that need to be addressed to improve the security posture.

upvoted 2 times

Moose01 1 year, 7 months ago

D. is the correct one (Key findings) - Key means most important and what audit was intended for to begin with.

This section of the report establishes what the audit was about, why the audit risk areas mattered to management, and what the team included in the audit. Next, the report details the issues that were found in the results section.

upvoted 1 times

BennyMao 1 year, 7 months ago

Selected Answer: D

The key findings section is correct.

upvoted 2 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 2 times

Tygrond87 1 year, 7 months ago

Selected Answer: A

The section of the assessment report that addresses separate vulnerabilities, weaknesses, and gaps is the "Findings definition section". This section is where the specific vulnerabilities, weaknesses, or gaps that were discovered during the assessment are documented in detail. It often includes a description of the issue, its potential impact, and recommendations for remediation. The findings definition section is a critical component of the assessment report as it provides a detailed breakdown of the issues that need to be addressed to improve the security posture of the organization.

upvoted 4 times

Mike4649 1 year, 4 months ago

Agree with A

upvoted 1 times

Dee83 1 year, 11 months ago

A. Findings definition section addresses separate vulnerabilities, weaknesses, and gaps. This section of the report typically includes a detailed description of the vulnerabilities, weaknesses, and gaps identified during the assessment, along with their potential impact on the organization's security posture. This section may also include recommendations for mitigating or remediating the identified issues, to help the organization improve its security.

upvoted 3 times

pingundas 2 years, 2 months ago

Using this as an example, the given answer is correct:
https://www.ndlegis.gov/files/committees/67-2021/23_5011_3000appendixb.pdf

upvoted 3 times

Jamati 2 years, 1 month ago

According to this document the answer is Executive Summary

upvoted 1 times

SSimko 11 months, 1 week ago

It is D, it is a sub section of executive summary... it is the "most correct" answer out of the 4.

upvoted 1 times

rootic 2 years, 2 months ago

Selected Answer: B

Agree with B.

upvoted 1 times

franbarpro 2 years, 2 months ago

Def. "B"

upvoted 1 times

sphenixfire 2 years, 2 months ago

Same, b

upvoted 1 times

CharlesL 2 years, 2 months ago

Selected Answer: B

Definitely is B

upvoted 1 times

Question #68 *Topic 1*

Why is data classification control important to an organization?

A. To enable data discovery

B. To ensure security controls align with organizational risk appetite

C. To ensure its integrity, confidentiality and availability

D. To control data retention in alignment with organizational policies and regulation

Suggested Answer: *B*

Community vote distribution

B (50%) C (48%)

Firedragon Highly Voted 2 years, 7 months ago

Selected Answer: B

B.
official study guide, P182. data classification only protects data confidentiality and integrity, it has nothing to do with availability.

A data classification identifies the value of the data to the organization and is critical to protect data confidentiality and integrity.

upvoted 17 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

jackdryan 2 years, 1 month ago

Changing to C

upvoted 1 times

Meowson 1 year, 11 months ago

Your reply can't be more meaningless for the discussion.

upvoted 30 times

Loveguitar Highly Voted 2 years, 8 months ago

C would be right if it aligns with the risk tolerance of the organization, why ensure the CIA if it does not align with your goals? the best choice is B

upvoted 8 times

a88aas 2 years, 5 months ago

Best Answer would be C. You don't perform Data classification to ensure that "security controls" are aligned with the organisational risk appetite. It doesn't make sense.

You implement data classification to ensure that only individuals at specific clearance levels have access to read/write to specific sets of classified data (Confidentiality). Classifying the data would then In-turn, prove to be integral, & the availability piece would then be applicable

upvoted 3 times

RedMartian Most Recent 2 months, 3 weeks ago

Selected Answer: C

Not C. That's the goal of information security as a whole. Classification helps support this, but doesn't directly ensure all three aspects.

upvoted 1 times

amitsir 3 months, 1 week ago

Selected Answer: B

As per my understanding, data classification cannot provide availability or integrity

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: B

Data classification is a critical control in information security because it helps organizations determine how to apply appropriate security measures based on the sensitivity of the data and the associated risk. By classifying data (e.g., public, confidential, highly sensitive), an organization can tailor its security controls to fit the risk appetite of the organization and ensure that the right level of protection is in place. This alignment helps balance security with operational efficiency and compliance requirements.

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: C

Here's a breakdown of how data classification contributes to these principles:

Integrity: Proper classification helps identify data that requires strict controls to prevent unauthorized modifications.
Confidentiality: Sensitive data can be assigned appropriate classification levels to restrict access and protect against disclosure.
Availability: Data classification helps determine which data is critical for business operations and requires robust backup and recovery plans.

upvoted 3 times

1460168 11 months ago

Selected Answer: B

It is B. It has nothing to do with C-I-A. Espacially nothing with availability!

upvoted 1 times

CCNPWILL 1 year ago

Selected Answer: B

Getting us back on the right course.

B. To ensure security controls align with organizational risk appetite
This is correct.

ive seen different flavors of this same question. Data classification is primarily used to determine the appropriate security controls on it that align with the business risk appetite. this is the correct answer every time.

Simply classifying it doesnt ensure jack anything. you need the controls. B

upvoted 1 times

73f8ac3 1 year, 2 months ago

Selected Answer: B

Correct answer is B
you do not need data classification to protect the CIA. But you need it to adapt the appropriate controls to the level of sensitivity you classified the asset

upvoted 1 times

Hongjun 1 year, 3 months ago

Selected Answer: C

Cissp 9th official guide chapter 5.1.2 page 157. The description of classification. It mentioned classification recognize the value of the data. It is important to protect the data integrity and confidentiality.

upvoted 1 times

Ramye 1 year, 1 month ago

So it's not saying anything about availability, and that makes B as the answer.

upvoted 2 times

YesPlease 1 year, 6 months ago

Selected Answer: B

Answer B) Data classification helps you provide the right level of protection based on the data's value, sensitivity, and the risk posed to the organization if that data is lost, stolen, or exposed

upvoted 1 times

Soleandheel 1 year, 6 months ago

C. To ensure its integrity, confidentiality and availability

upvoted 1 times

glenndexter 1 year, 7 months ago

B
Think like a manager, or perhaps a CISO.

upvoted 2 times

InclusiveSTEAM 1 year, 8 months ago

The correct answer is B
Data classification is important to enable security controls that align with an organization's risk appetite, so option B is correct.

Properly classifying data allows applying security controls at levels commensurate with the data's sensitivity and criticality to the business. This ensures controls match the organization's priorities and risk profile.

Option A is a benefit of classification but not the core purpose.
Option C states generic goals rather than strategic alignment.
Option D is also a secondary advantage, not the primary driver.
upvoted 3 times

⊟ **aape1** 1 year, 8 months ago

Selected Answer: B

B. because it's all about Risk when comes to protecting the Data = values. Risk appetite in NIST definition is "The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value."
upvoted 1 times

⊟ **Dann108** 1 year, 10 months ago

though C sounds good, data classification contribute to confidentiality and integrity and less for availability, therefore I think "To ensure security controls align with organizational risk appetite" is the better answer
upvoted 1 times

⊟ **Bach1968** 1 year, 12 months ago

Selected Answer: B

Option B, "To ensure security controls align with organizational risk appetite," is indeed a valid reason for why data classification control is important to an organization.

Data classification helps organizations align their security controls with their risk appetite by enabling them to identify and prioritize the protection of sensitive or critical data. It allows organizations to allocate resources and apply appropriate security measures based on the classification of data and the associated risks.

By classifying data, organizations can determine the level of security controls and safeguards needed for each classification category. This ensures that security measures are proportionate to the level of risk associated with the data. It helps organizations focus their efforts and resources on protecting the most sensitive or high-risk data, while also ensuring that less critical data receives appropriate levels of protection.

So, both option B ("To ensure security controls align with organizational risk appetite") and option C ("To ensure its integrity, confidentiality, and availability") are valid reasons for the importance of data classification control.
upvoted 1 times

Question #69 *Topic 1*

To monitor the security of buried data lines inside the perimeter of a facility, which of the following is the MOST effective control?

A. Fencing around the facility with closed-circuit television (CCTV) cameras at all entry points

B. Ground sensors installed and reporting to a security event management (SEM) system

C. Regular sweeps of the perimeter, including manual inspection of the cable ingress points

D. Steel casing around the facility ingress points

Suggested Answer: *C*

Community vote distribution

B (63%) C (21%) A (16%)

FredDurst Highly Voted 2 years, 1 month ago

Selected Answer: B

https://www.youtube.com/watch?v=zZ3EwOQo6Hw&t=81s

upvoted 8 times

Jamati 2 years, 1 month ago

Great video

upvoted 2 times

oudmaster 2 years ago

I dont think SEM solution (aka SIEM) has anything to do with this.

upvoted 2 times

dm808 9 months ago

Agree.. i think SEM(aka SIEM) is a distractor

upvoted 1 times

RedMartian Most Recent 2 months, 3 weeks ago

Selected Answer: B

Not C. Regular sweeps of the perimeter, including manual inspection of cable ingress points -- useful as a supplemental control, but it’s not continuous and won’t detect real-time tampering.

upvoted 1 times

amitsir 3 months, 1 week ago

Selected Answer: B

Fencing around the facility and survilence with CCTV can not monitor the secuirty of burried line. CCTV can only let us know that who is entring and exiting the facility. It can be legitimate workers as well. But how to monitor if burried lines are being tempered ? only way to get it monitored is by using ground sensors.

upvoted 1 times

SH_ 3 months, 1 week ago

Selected Answer: A

If you could go with ONLY ONE option in real life, wouldn't it be A (i.e. fence + CCTV)? These questions asking for MOST x or y, I typically think ONLY ONE option and leave the rest.

upvoted 1 times

Bau24 4 months, 3 weeks ago

Selected Answer: B

The question is about monitoring

B. Ground sensors installed and reporting to a security event management (SEM) system

upvoted 1 times

CCNPWILL 8 months, 2 weeks ago

there are different sensor types that can indeed report back to a centralized monitoring station. Definitely going with B. makes the most sense.

A and B are addressing the perimeter... D is not better than B.

B is correct.

upvoted 2 times

GuardianAngel 10 months, 3 weeks ago

Selected Answer: B

All three other answers are perimeter security. The only option that is not is B. Ground Sensors.

A. Perimeter security: Installing fences, gates, surveillance cameras, and access control systems to secure the external area around the cable ingress point and the entire data center facility.

D. Perimeter Cable management: Implementing proper cable management practices, including secure enclosures, cable trays and conduits

C. Perimeter Regular inspections and maintenance: Conducting regular inspections and maintenance of the cable ingress point and the surrounding areas to identify and address any potential security vulnerabilities promptly.

upvoted 1 times

maawar83 1 year ago

I believe it is C, this is more tricky question rather than effective control.

"inside the perimeter of a facility" and "most effective", assuming that inside the facility perimeter you already have enough access controls etc... a regular sweeps of the perimeter should be more than enough.

upvoted 2 times

Soleandheel 1 year ago

B. Ground sensors installed and reporting to a security event management (SEM) system

upvoted 1 times

Demo25 1 year, 5 months ago

Selected Answer: B

The MOST effective control to monitor the security of buried data lines inside the perimeter of a facility is B. Ground sensors installed and reporting to a security event management (SEM) system.

Ground sensors are devices that can detect vibrations or other disturbances in the ground. When a ground sensor is triggered, it sends an alert to a security event management (SEM) system. The SEM system can then notify security personnel of the alert, so they can investigate the situation.

upvoted 2 times

Jung1999 1 year, 9 months ago

I think the keyword in this question is "buried data lines" in the facility. It means cable, I think.... so I will go to C

upvoted 2 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

RVoigt 1 year, 10 months ago

Selected Answer: A

There is literally 2 pages dedicated to CCTV cameras in the Official Study Guide. PG 460 includes "Video surveillance, video monitoring, closed-circuit television (CCTV), and security cameras are all means to deter unwanted activity and create a digital record of the occurrence of events. Cameras should be positioned to watch exit and entry points allowing any change in authorization or access level. Cameras should also be used to monitor activities around valuable assets and resources as well as to provide additional protection in public areas such as parking structures and walkways."

upvoted 3 times

JohnyDal 1 year, 11 months ago

Selected Answer: B

Most effective is definitely sensors. It will occur more frequently and reliably than regular manual checks/sec guard

upvoted 1 times

Dee83 1 year, 11 months ago

B.is the likely answer

Ground sensors installed and reporting to a security event management (SEM) system is the most effective control to monitor the security of buried data lines inside the perimeter of a facility. Ground sensors can detect any unauthorized digging or excavation near the buried data lines, and by reporting to a security event management system, the security team will be alerted immediately to any potential threats. CCTV cameras and regular perimeter sweeps can help to detect and deter intruders, but they may not detect digging or excavation near the buried data lines. Steel casing around the facility ingress points can provide a level of physical protection, but it may not detect or deter unauthorized access to the buried data lines.

upvoted 2 times

somkiatr 2 years ago

Selected Answer: C

I agreed with C. Ground sensor is detective control and may generate false positive alert while sweeping the perimeter regularly and inspecting all the cable's ingress points manually would be more preventive and most effective comparing to other choices.

upvoted 4 times

halonsx 2 years ago

keyword in the question being "monitor" - sensors are able of monitoring vs checks.

upvoted 3 times

stickerbush1970 2 years, 3 months ago

Selected Answer: C

Correct

upvoted 1 times

rootic 2 years, 2 months ago

Why C. Why not B? Automated alarm if someone try to do some harm to a line much more effective, isn't it?

upvoted 6 times

Delab202 2 years ago

Alarms can be disabled.

upvoted 1 times

Sledge_Hammer 1 year, 3 months ago

That's why you need sensors to trigger an alert and report to a SEM where buried cables are laid. Having worked for a cable company and Dish Network, I know for sure that you don't start digging without an authorized team that has the ability to scan the ground for buried pipes and cables. That could be automated via sensors that alert a SEM in a data center environment.

upvoted 1 times

Question #70 *Topic 1*

An enterprise is developing a baseline cybersecurity standard its suppliers must meet before being awarded a contract. Which of the following statements is TRUE about the baseline cybersecurity standard?

A. It should be expressed as general requirements.

B. It should be expressed as technical requirements.

C. It should be expressed in business terminology.

D. It should be expressed in legal terminology.

Suggested Answer: *B*

Community vote distribution

B (41%) C (35%) A (24%)

cysec_4_lyfe 2 months, 3 weeks ago

Selected Answer: B

A baseline cybersecurity standard should be expressed in technical requirements to ensure clear and measurable expectations for suppliers. A baseline cybersecurity standard should clearly outline specific technical requirements that suppliers must meet to ensure they adhere to the necessary security controls and best practices. This approach ensures that suppliers implement concrete measures to protect against cyber threats, aligning with recognized industry standards and frameworks such as ISO 27001 and NIST CSF.

upvoted 2 times

RedMartian 2 months, 3 weeks ago

Selected Answer: B

Not C. Business terms help communicate with executives, but a standard for suppliers must include specific technical criteria.

upvoted 1 times

Chimchamp 3 months, 2 weeks ago

Selected Answer: B

Technical

upvoted 1 times

f168100 3 months, 2 weeks ago

Selected Answer: B

I go for Technical

upvoted 2 times

Imranbhatti 3 months, 3 weeks ago

Selected Answer: B

The correct answer is B. It should be expressed as technical requirements.

Baseline cybersecurity standards should be expressed as technical requirements because they need to provide clear, actionable guidelines that suppliers must follow to ensure their systems and processes meet the necessary security criteria. Technical requirements are specific and measurable, making it easier to assess compliance and enforce the standards
Option C, "It should be expressed in business terminology," is incorrect because baseline cybersecurity standards need to provide clear, actionable guidelines that can be directly implemented by technical teams. Expressing these standards in technical requirements ensures that they are specific, measurable, and enforceable, which is crucial for maintaining security and compliance12.

Business terminology might be too broad or vague, making it difficult for technical teams to understand and implement the necessary security measures. Technical requirements, on the other hand, provide the detailed instructions needed to effectively secure systems and data

upvoted 1 times

max58 4 months, 2 weeks ago

Selected Answer: B

The question asks about a baseline cybersecurity standard that suppliers must meet before being awarded a contract. The key here is ensuring that the standard is clear, actionable, and measurable in terms of security expectations.
B. It should be expressed as technical requirements is indeed the best answer. Cybersecurity standards must clearly define the specific security measures, and only technical requirements can ensure the correct implementation of these measures.

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: B

A baseline cybersecurity standard should be expressed in technical requirements to ensure clear and measurable expectations for suppliers. This includes specific controls, technologies, and processes that must be implemented.

While general requirements can provide a high-level overview, technical requirements are essential for effective evaluation and enforcement of the standard.

Here's a breakdown of why the other options are less effective:

A. General requirements: Too vague and difficult to enforce.
C. Business terminology: While understanding business needs is important, the standard should focus on technical implementation details.
D. Legal terminology: While legal considerations are important, the primary focus should be on technical requirements to ensure effective security.

upvoted 2 times

Rachy 11 months, 2 weeks ago

Selected Answer: B

B. Its a cybersecurity standard so I will guess its a cyber Vendors

upvoted 1 times

Chris 11 months, 3 weeks ago

Selected Answer: C

Here's why C. It should be expressed in business terminology is appropriate:

Clarity for Stakeholders: Using business terminology helps ensure that all stakeholders, including suppliers, understand the expectations and the rationale behind them. This approach promotes better alignment and cooperation.

Alignment with Business Objectives: Expressing cybersecurity requirements in business terms ensures that they are seen as integral to achieving business goals, rather than as isolated technical mandates.

Effective Communication: Managers and executives need to communicate security requirements in a way that resonates with the business context, making it easier for suppliers to see the value and necessity of compliance.

upvoted 3 times

Ramye 1 year ago

Selected Answer: C

Standards must be set to meet business goals. If it does not meet business needs then it's useless.

upvoted 2 times

Vasyamba1 1 year, 3 months ago

Selected Answer: B

this is related to SLR before signing the contract.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: A

Baseline is the keyword

upvoted 1 times

Hongjun 1 year, 3 months ago

Selected Answer: C

Refer to chapter 1 the description of SLA and SLR . It talk about the third party or company
of your supply chain shall has minimum security standards. It relates with business. Technical details was developed by third-party company by following your business requirements. You don't give then the details of Technical.

upvoted 2 times

gjimenezf 1 year, 5 months ago

Selected Answer: C

C. Business Terminology

upvoted 3 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C) It should be expressed in business terminology.

Too technical or legal and you may confuse your vendor(s).

upvoted 2 times

Soleandheel 1 year, 6 months ago

C. It should be expressed in business terminology.

upvoted 1 times

Soleandheel 1 year, 6 months ago

Think like a manager guys. Using business terminology to express technical security things to other stakeholders is what a manager would do. You don't want to use too technical or even legal terminology when communicating with other stakeholders like suppliers. Business terminology is what you want to use when communicating security baselines to prospective suppliers. Remember, you want to think like an executive or a manager not an engineer.

upvoted 2 times

Question #71 *Topic 1*

Which access control method is based on users issuing access requests on system resources, features assigned to those resources, the operational or situational context, and a set of policies specified in terms of those features and context?

A. Mandatory Access Control (MAC)

B. Attribute Based Access Control (ABAC)

C. Role Based Access Control (RBAC)

D. Discretionary Access Control (DAC)

Suggested Answer: *B*

Community vote distribution

B (86%) 14%

stickerbush1970 Highly Voted 1 year, 9 months ago

Selected Answer: B

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf

upvoted 6 times

jackdryan 1 year, 1 month ago

B is correct

upvoted 1 times

ServerBrain Most Recent 3 months, 2 weeks ago

Selected Answer: D

A discretionary access control (DAC) system would show how the
owner of the objects allows access, allows owners to determine who can access objects they control.

upvoted 1 times

Bach1968 12 months ago

Selected Answer: B

The access control method that is based on users issuing access requests on system resources, features assigned to those resources, the operational or situational context, and a set of policies specified in terms of those features and context is called Attribute Based Access Control (ABAC).

In ABAC, access decisions are made based on various attributes or characteristics associated with users, resources, and the environment. These attributes can include user roles, job titles, time of day, location, device type, and any other relevant contextual information. Policies are defined using these attributes, and access requests are evaluated against these policies to determine whether access should be granted or denied.

ABAC offers a more flexible and fine-grained access control approach compared to other methods such as Role Based Access Control (RBAC) or Discretionary Access Control (DAC). It allows organizations to define access control policies based on dynamic and contextual factors, providing granular control over resource access and helping to enforce security requirements based on specific conditions.

upvoted 2 times

rajkamal0 1 year, 6 months ago

Selected Answer: B

ABAC is the correct answer
https://techgenix.com/5-access-control-types-comparison/

upvoted 2 times

somkiatr 1 year, 6 months ago

Selected Answer: B

Attribute-based access control (ABAC), also known as policy-based access control for IAM, defines an access control paradigm whereby a subject's authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment attributes.

upvoted 2 times

Jamati 1 year, 7 months ago

Selected Answer: B

From Official study guide 9th edition page 682

Attribute-Based Access Control A key characteristic of the Attribute-Based Access
Control (ABAC) model is its use of rules that can include multiple attributes. This allows
it to be much more flexible than a rule-based access control model that applies the rules
to all subjects equally. Many software-defined networks (SDNs) use the ABAC model.
Additionally, ABAC allows administrators to create rules within a policy using plain language statements such as “Allow Managers to access the WAN using a mobile device.”

upvoted 3 times

rdy4u 1 year, 8 months ago

Attribute-based access control (ABAC) is an authorization model that evaluates attributes (or characteristics), rather than roles, to determine access. The purpose of ABAC is to protect objects such as data, network devices, and IT resources from unauthorized users and actions—those that don’t have “approved” characteristics as defined by an organization’s security policies.

https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/

upvoted 1 times

franbarpro 1 year, 8 months ago

The question is talking about Zero Trust lol. "B" attribute.

upvoted 1 times

Boats 1 year, 8 months ago

Selected Answer: A

Mandatory Access Control

1. Access control policy
2. Classification or sensitivity labels for objects
3. Clearance or privilege labels for subjects

upvoted 2 times

franbarpro 1 year, 8 months ago

MAC is based on lebels - Military fav

upvoted 1 times

Question #72 *Topic 1*

What is a security concern when considering implementing software-defined networking (SDN)?

A. It has a decentralized architecture.

B. It increases the attack footprint.

C. It uses open source protocols.

D. It is cloud based.

Suggested Answer: *B*

Community vote distribution

B (92%) 8%

jokijoki Highly Voted 1 year, 8 months ago

B is correct.
"A significant issue regarding SDN security is that virtualizing every aspect of the network infrastructure increases your attack footprint. "

https://www.networkworld.com/article/3245173/secure-your-sdn-controller.html

upvoted 11 times

jackdryan 1 year, 1 month ago

B is correct

upvoted 1 times

attesco Most Recent 6 months, 1 week ago

Selected Answer: B

SDN security concerns
A significant issue regarding SDN security is that virtualizing every aspect of the network infrastructure increases your attack footprint. The SDN controller is typically the primary target for attackers because it is the central point for decisions in a network and a central point of failure.

Attackers can try to get control of the network by breaking into a controller or pretending to be one. Once a central controller is compromised, an attacker can gain complete control over your network. This would be considered an extreme scenario, but it could be possible as SDN usage continues to grow.

There are new types of denial-of-service attacks that try to exploit potential scaling limits of an SDN infrastructure by locating specific automatic processes that use a significant amount of CPU cycles.

upvoted 1 times

Bach1968 12 months ago

Selected Answer: B

A security concern when considering implementing software-defined networking (SDN) is (B) it increases the attack footprint.

SDN introduces a centralized controller that manages the network infrastructure and allows for dynamic and programmable network configurations. While SDN offers advantages in terms of flexibility and automation, it also expands the attack surface of the network. With SDN, there is a single point of control that, if compromised, can have a significant impact on the entire network.

The centralized nature of SDN makes it an attractive target for attackers. If they can gain unauthorized access to the SDN controller or exploit vulnerabilities in the controller software, they may be able to manipulate network configurations, redirect traffic, or launch attacks on other network components.

upvoted 4 times

somkiatr 1 year, 6 months ago

Selected Answer: B

B is correct. It increases the attack footprint because it utilizes SDN controller and other Network Element devices to create virtual networks increasing points of attack comparing to traditional network.

upvoted 3 times

Jamati 1 year, 7 months ago

Selected Answer: B

By process of elimination, only correct answer is B.

One of the most significant security risk factors is the possibility of a compromised SDN controller attack at the control plane layer. Due to the centralization design of the SDN, the SDN controller becomes the brain of the SDN architecture. Attackers can focus on compromising the SDN controller in an attempt to manipulate the entire network.
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/benefits-and-the-security-risk-of-software-defined-networking#:~:text=In%20fact%2C%20SDN%20is%20exposed,at%20the%20control%20plane%20layer

upvoted 2 times

sphenixfire 1 year, 8 months ago

Selected Answer: C

CISSP gude, s. 526 "SDN offers a new network design that is directly programmable from a central location,
is flexible, is vendor neutral, and is open standards based."

upvoted 1 times

franbarpro 1 year, 8 months ago

Open source protocols are the most secure....bcs they have been tested by the community. I don't think that would be a securing concern. Anything we add to our network becomes at attack surface..... so I go for B on this one.

upvoted 3 times

stickerbush1970 1 year, 9 months ago

Selected Answer: B

correct

upvoted 3 times

Question #73 *Topic 1*

What is the BEST way to restrict access to a file system on computing systems?

A. Use least privilege at each level to restrict access.

B. Restrict access to all users.

C. Allow a user group to restrict access.

D. Use a third-party tool to restrict access.

Suggested Answer: *A*

Community vote distribution

A (100%)

Bach1968 Highly Voted 👍 12 months ago

Selected Answer: A

he correct answer is A. Use least privilege at each level to restrict access.

Least privilege is a principle in information security that states that users should only be granted the minimum level of access necessary to perform their job functions. Applying least privilege to file system access means granting permissions and privileges to users and groups based on their specific needs and roles, and no more. This helps prevent unauthorized access and limits the potential damage that can be caused by compromised accounts.

By implementing least privilege, access to the file system is limited to only those users who require it for their job responsibilities. This approach reduces the risk of accidental or intentional misuse of the file system and helps protect sensitive data and system resources.

upvoted 6 times

amitsir Most Recent 🕓 3 months, 1 week ago

Selected Answer: C

Least priviliage is a principle in information security not a menthod to restric access on file system. only way is to create a user group such as read, write or execute i.e. applicable to a file system of OS.

upvoted 1 times

Firedragon 1 year, 7 months ago

Selected Answer: A

A.

https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/privileges

upvoted 1 times

jackdryan 1 year, 1 month ago

A is correct

upvoted 1 times

franbarpro 1 year, 8 months ago

Thiking about NTFS and It's ACE/ACL capabilities

upvoted 1 times

jokijoki 1 year, 8 months ago

A is correct.

upvoted 1 times

Question #74 *Topic 1*

Which of the following is the PRIMARY reason for selecting the appropriate level of detail for audit record generation?

A. Avoid lengthy audit reports

B. Enable generation of corrective action reports

C. Facilitate a root cause analysis (RCA)

D. Lower costs throughout the System Development Life Cycle (SDLC)

Suggested Answer: *B*

Community vote distribution

C (63%) | B (37%)

⊟ **dev46** Highly Voted 2 years, 9 months ago

A & D - We don't create audit reports to save storage space or cost

B - Audit reports for analysis, it does not have any corrective actions

I would go for C - Audit report helps to find the root cause after the security incident

upvoted 11 times

⊟ **oudmaster** 2 years, 6 months ago

I disagree, Root Cause Analysis (RCA) is more of technical procedures not Audit. Example generate RCA when there is malware infection to see how a system got infected.

And the Audit purpose is for sure to assist correct things.

upvoted 2 times

⊟ **6yrd7fcv97** 1 year, 8 months ago

It's talking about audit records though, not an actual audit. System logs are audit records, so setting the right levels enables RCA. Get it wrong and there's too much or two little, making that more difficult.

upvoted 2 times

⊟ **jackdryan** 2 years, 1 month ago

C is correct

upvoted 1 times

⊟ **johnsandler64** Highly Voted 2 years, 9 months ago

Selected Answer: C

Also agree RCA is the goal

upvoted 7 times

⊟ **BigITGuy** Most Recent 2 months, 4 weeks ago

Selected Answer: C

Unlikely B. Corrective action reports come after root cause analysis, but RCA is the primary driver.

upvoted 2 times

⊟ **robervalchocolat** 9 months, 1 week ago

A. Avoid lengthy audit reports: While storage space can be a concern, it's not the primary reason for detail selection. Having the right information for analysis is more important.

B. Enable generation of corrective action reports: Audit records do contribute to corrective actions, but identifying the root cause (RCA) comes first. The root cause helps determine the most effective corrective actions.

C. Facilitate a root cause analysis (RCA): This is the primary reason. You need detailed audit records to understand the sequence of events, identify weaknesses, and pinpoint the underlying cause of the issue.

D. Lower costs throughout the System Development Life Cycle (SDLC): Although proper audit practices can contribute to cost reduction, it's not the main driver for detail selection.

upvoted 1 times

⊟ **Ramye** 1 year ago

Selected Answer: B

Audit is all about finding out whether you are compliant with standards, policies, controls etc. and shows you where there could be any gaps to be compliant. Those gaps somehow needs to be corrected after talking to management.

upvoted 2 times

hoho2000 1 year, 3 months ago

Selected Answer: B

Ans B. Audit does not do RCA, its purpose is compliance to a standard.

A typical finding would identify the following:
Condition. Statement that describes the results of the audit
Criteria. Standards used to measure the activity or performance of the auditee
Cause. Explanation of why a problem occurred
Effect. Difference between and significance of the condition and the criteria
Recommendation. Action that must be taken to correct the cause

upvoted 1 times

Hongjun 1 year, 3 months ago

Selected Answer: B

This topic is talk about what kinds of standards shall used for audit report. It is SOC knowledge test. No matter SOC 1 or SOC2 . It focus on checking whether the actions is reasonable and suitable for organization. So it is B .

upvoted 1 times

maawar83 1 year, 6 months ago

Answer is C! the PRIMARY Reason is to facilitate the RCA..

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C)

Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems

https://csf.tools/reference/nist-sp-800-171/r2/3-3/3-3-1/#:~:text=Selecting%20the%20appropriate%20level%20of%20abstraction%20is%20a%20critical%20aspect%20of%20an%20audit%20logging%20capability%2

upvoted 1 times

Moose01 1 year, 8 months ago

RCA is not correct - for example Cisco IOS code has enough reporting to enable developers to easily identify with the code numbers what is the cause within the IOS.
B. Enable generation of corrective action reports.
corrective action - NOT reporting, to correct the code

upvoted 1 times

BoyBastos 1 year, 10 months ago

Selected Answer: B

B is correct

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: B

the correct answer is B. Enable generation of corrective action reports.

When audit records are generated with the appropriate level of detail, they provide valuable information that can be used to analyze security events, identify vulnerabilities, and determine the necessary corrective actions. These corrective actions can help address any identified weaknesses or shortcomings in the system's security posture.

By having detailed audit records, organizations can generate comprehensive reports that highlight the specific actions or changes needed to mitigate risks and improve security. These corrective action reports serve as a guide for implementing necessary measures and making improvements to the system's security controls.

upvoted 5 times

Moose01 2 years, 1 month ago

B.

RCA is a report that must be generated after an incident. the RCA will document the Time/Date, Impact, Duration, Cause and How to Prevent this from happening again.

Audit Report is to gain a more general understanding of the environment and to make & take corrective action and make greater improvements.

upvoted 1 times

⊟ **RVoigt** 2 years, 4 months ago

Selected Answer: C

CISSP Official Study Guide pg 10 - "Auditing is the programmatic means by which a subject's actions are tracked and recorded for the purpose of holding the subject accountable for their actions while authenticated on a system through the documentation or recording of subject activities. It is also the process by which unauthorized or abnormal activities are detected on a system. Auditing is recording activities of a subject and its objects as well as recording the activities of application and system functions. Log files provide an audit trail for re-creating the history of an event, intrusion, or system failure. Auditing is needed to

detect malicious actions by subjects, attempted intrusions, and system failures and to reconstruct events, provide evidence for prosecution, and produce problem reports and analysis."

upvoted 1 times

⊟ **Dee83** 2 years, 5 months ago

C. Facilitate a root cause analysis (RCA) is the primary reason for selecting the appropriate level of detail for audit record generation. Root cause analysis (RCA) is an approach used to identify the underlying cause of an incident or problem. In order to conduct an RCA, it is necessary to have detailed information about what occurred during the incident or problem. This includes information about the actions taken, the systems involved, and the data that was accessed. By selecting the appropriate level of detail for audit record generation, organizations can ensure that they have the necessary information to conduct an RCA and understand the underlying cause of a security incident.

upvoted 1 times

⊟ **somkiatr** 2 years, 6 months ago

Selected Answer: C

C would be correct.

Facilitate Root Cause Analysis in Auditing will have benefit

• Focused audit planning

• More insight to findings

• Improved rigor of analysis

• Better recommendations

• More impactful audits

These will generate more detail for the audit record in the audit report.

Reference : https://www.caaf-fcar.ca/images/content/performance-audit/Webinars/SpringWebinarSeries/RCA/RCA-EN_Slides%E2%80%93Apr-14-20.pdf

upvoted 1 times

⊟ **Jamati** 2 years, 7 months ago

Selected Answer: C

Agreed, C

upvoted 1 times

Question #75 *Topic 1*

What is the correct order of execution for security architecture?

A. Governance, strategy and program management, operations, project delivery

B. Governance, strategy and program management, project delivery, operations

C. Strategy and program management, project delivery, governance, operations

D. Strategy and program management, governance, project delivery, operations

Suggested Answer: *C*

Community vote distribution

B (74%) C (26%)

kasiya Highly Voted 2 years, 9 months ago

Selected Answer: B

Governance, strategy and program management, project delivery, operations

upvoted 20 times

> **DERCHEF2009** 2 years, 9 months ago
>
> Why not C?
>
> upvoted 1 times
>
> > **[Removed]** 2 years, 8 months ago
> >
> > Without Governance there is no strategy or program, without a strategy or program, there is no project, and without a project, it cannot transition to operations (day-to-day use, maintenance)
> >
> > upvoted 10 times
>
> > **dev46** 2 years, 9 months ago
> >
> > Read Domain 1 of CISSP. Governance comes first as a stepping stone.
> >
> > upvoted 5 times
> >
> > > **Woz** 2 years, 8 months ago
> > >
> > > Everything starts with a strategy. Governance supports strategy.
> > >
> > > upvoted 3 times
>
> **jackdryan** 2 years, 1 month ago
>
> B is correct
>
> upvoted 1 times

somsom Most Recent 8 months, 1 week ago

Sorry I wanted to say B is correct

upvoted 1 times

somsom 8 months, 1 week ago

C is correct because Governance and strategy = Administrators, program management = tactical = management , project delivery and operations = operations . lol

upvoted 1 times

Ramye 1 year, 1 month ago

Selected Answer: C

A lot of folks here going with B.

But how come a governance comes before strategy? Everything starts with strategy and then along the line governance comes in. This is how we do all the projects.

upvoted 1 times

Soleandheel 1 year, 6 months ago

Another Chatgpt problem. Too many people here are going with misleading chatgpt answers. Governance never comes before strategy. Strategy must be in place before governance can have any relevance. For sure the first 2 answer options are wrong.

upvoted 4 times

AMANSUNAR 1 year, 7 months ago

Selected Answer: B

This sequence aligns with a structured approach to security architecture:

Governance: Establishing policies, roles, responsibilities, and decision-making processes.
Strategy and Program Management: Developing a strategic approach and managing security programs.
Project Delivery: Implementing security measures and controls through projects.
Operations: Ongoing management and maintenance of security measures and controls.
Correct Answer: B. Governance, strategy and program management, project delivery, operations

upvoted 2 times

BoyBastos 1 year, 10 months ago

Selected Answer: C

C is correct

upvoted 1 times

Bach1968 1 year, 12 months ago

apologize for the confusion. You are correct, the correct order of execution for security architecture is: C. Strategy and program management, project delivery, governance, operations

By following this order, organizations can develop a strategic approach to security, effectively implement security initiatives through projects, establish governance structures for oversight, and maintain the security posture through ongoing operations.

upvoted 2 times

Dee83 2 years, 5 months ago

B. is the correct answer
Governance, strategy and program management, project delivery, operations

The correct order of execution for security architecture is typically as follows:

Governance: This is the highest level of decision-making for the organization and it establishes the overall direction for security.
Strategy and program management: This involves developing the overall security strategy and plan for the organization, and managing the implementation of the security program.
Project delivery: This involves executing specific projects that support the security strategy, such as implementing new security technologies or processes.
Operations: This involves ongoing management and maintenance of the security program, including monitoring and incident response.

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: C

Answer is C. Governance function will align with vision, mission, and goals, and ensuring that the strategic direction being taken.

upvoted 2 times

Jamati 2 years, 7 months ago

Selected Answer: B

Answer is B. Everything starts with governance and compliance.

upvoted 2 times

> **Ramye** 1 year, 1 month ago
>
> Wrong. You can't be compliant in dark. You must have some strategy / guidance that guides you to decide what needs to be governed and be compliant with.
>
> upvoted 2 times

rootic 2 years, 8 months ago

Selected Answer: B

I'm with B.

upvoted 1 times

explorer3 2 years, 8 months ago

Selected Answer: C

Establish strategy, then deliver strategy through program of work (becomes operations), but before operations, employ governance controls for successful operations

upvoted 4 times

Question #76 *Topic 1*

An international organization has decided to use a Software as a Service (SaaS) solution to support its business operations. Which of the following compliance standards should the organization use to assess the international code security and data privacy of the solution?

A. Service Organization Control (SOC) 2

B. Information Assurance Technical Framework (IATF)

C. Health Insurance Portability and Accountability Act (HIPAA)

D. Payment Card Industry (PCI)

Suggested Answer: *B*

Community vote distribution

A (96%) 4%

⊟ **25cbb5f** 9 months ago

Selected Answer: A

The most suitable compliance standard for the international organization to assess both code security and data privacy of a SaaS solution is:

A. Service Organization Control (SOC) 2

Here's why SOC 2 is the best fit:

Focus on Security, Availability, and Privacy: SOC 2 reports are specifically designed to evaluate service providers, like SaaS vendors, on controls related to the security, availability, processing integrity, confidentiality, and privacy of the systems they use to process customers' data.
International Applicability: While developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 is widely recognized internationally and often requested by organizations worldwide.
Flexibility: SOC 2 allows specifying the Trust Services Criteria (security, privacy, etc.) that are most relevant to the organization's needs.
B. Information Assurance Technical Framework (IATF): IATF is primarily used within US government agencies. It might have relevance in limited contexts, but it's less common for commercial business purposes.

upvoted 2 times

⊟ **AMANSUNAR** 1 year, 1 month ago

Selected Answer: A

The Information Assurance Technical Framework (IATF) is not a widely recognized standard for assessing the security and privacy aspects of cloud computing or Software as a Service (SaaS) solutions. The IATF is not as commonly associated with international code security and data privacy in the context of cloud services.

For a more widely accepted and relevant standard for assessing the security and privacy of a SaaS solution, Service Organization Control (SOC) 2 is a more appropriate choice.

upvoted 1 times

⊟ **Ukpes** 1 year, 1 month ago

SOC2 standard is based on the following trust services criteria: security, data privacy, confidentiality, process integrity, and availability.

upvoted 1 times

⊟ **BoyBastos** 1 year, 3 months ago

Selected Answer: A

SOC2 is right

upvoted 2 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: B

If the organization is specifically concerned with international code security and data privacy, the Information Assurance Technical Framework (IATF) would indeed be a more appropriate compliance standard to assess the solution.

The IATF is a framework developed by the International Organization for Standardization (ISO) to provide guidelines for assessing the security and privacy aspects of information technology systems. It covers various areas such as risk management, security controls, and data privacy.

While SOC 2 focuses more broadly on the overall security and privacy controls of service providers, the IATF specifically addresses the security and privacy of information technology systems, making it more suitable for assessing the code security and data privacy of the SaaS solution in an international context.

Therefore, the organization should use the IATF to assess the international code security and data privacy of the SaaS solution.

upvoted 1 times

HughJassole 1 year, 6 months ago

D: Payment Card Industry. SOC2 is a report, not a standard.
"The PCI Security Standards Council (PCI SSC) is a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide."
https://www.pcisecuritystandards.org/

upvoted 1 times

dmo_d 1 year, 7 months ago

Selected Answer: A

A it is.
B and C are US only.
D is too specific (to financial businesses).

upvoted 1 times

Dee83 1 year, 11 months ago

A. Service Organization Control (SOC) 2 would be the most appropriate compliance standard for an international organization to use to assess the international code security and data privacy of a Software as a Service (SaaS) solution.

upvoted 2 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

Firedragon 2 years, 1 month ago

Selected Answer: A

A.
The question is asking "international", IATF is US only, SOC2 is the answer.

upvoted 3 times

rootic 2 years, 2 months ago

Selected Answer: A

it's A

upvoted 1 times

pingundas 2 years, 2 months ago

@ Humongous1593, I asked that question the support and got this answer:

____

Our answers are verified by our experts
If the given answer is not correct then you can go with user voted ones.

____

upvoted 3 times

kptest12 2 years, 2 months ago

Selected Answer: A

Its SOC2 which has Privacy, confidentiality , security, availability and process integrity

upvoted 2 times

Humongous1593 2 years, 3 months ago

Selected Answer: A

A, why does this thing choose the wrong answer 90% of the time. I don't get it.

upvoted 3 times

Jay327 2 years, 1 month ago

I thought I only felt this way :)

upvoted 1 times

CharlesL 2 years, 2 months ago

https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA606355.xhtml

upvoted 1 times

DERCHEF2009 2 years, 3 months ago

Selected Answer: A

Yes its A

upvoted 4 times

stickerbush1970 2 years, 3 months ago

Selected Answer: A

Agree with A

upvoted 3 times

CuteRabbit168 2 years, 3 months ago

Selected Answer: A

Obvious SOC 2

upvoted 4 times

Question #77 *Topic 1*

An authentication system that uses challenge and response was recently implemented on an organization's network, because the organization conducted an annual penetration test showing that testers were able to move laterally using authenticated credentials. Which attack method was MOST likely used to achieve this?

A. Hash collision

B. Pass the ticket

C. Brute force

D. Cross-Site Scripting (XSS)

Suggested Answer: *B*

Community vote distribution

B (77%) A (23%)

⊟ **Bach1968** Highly Voted 12 months ago

Selected Answer: B

Based on the given scenario, the attack method that was MOST likely used to achieve lateral movement using authenticated credentials is the "Pass the ticket" attack (Option B). In a Pass the Ticket attack, an attacker acquires a valid ticket-granting ticket (TGT) or session key from a compromised account or system and uses it to authenticate and impersonate a legitimate user. This allows the attacker to gain unauthorized access to other systems and move laterally within the network without the need for further authentication. It is a common technique used in advanced persistent threats (APTs) to maintain persistent access and expand control within a network.

upvoted 5 times

⊟ **BigITGuy** Most Recent 2 months, 4 weeks ago

Selected Answer: A

Not A. Hash collision is more related to compromising cryptographic hashes, not typically used for lateral movement via authentication credentials.

upvoted 1 times

⊟ **HughJassole** 1 year ago

B: Pass the ticket.

"Pass the Ticket is a credential theft technique that enables adversaries to use stolen Kerberos tickets to authenticate to resources (e.g., file shares and other computers) as a user without having to compromise that user's password. Adversaries often use this technique to move laterally through an organization's network to hunt for opportunities to escalate their privileges or fulfill their mission. "

https://www.netwrix.com/pass_the_ticket.html

upvoted 3 times

⊟ **DapengZhang** 1 year, 3 months ago

Selected Answer: A

Didn't see any clue about ticket or Kerberos from question itself. Lateral movement refers to the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. https://www.crowdstrike.com/cybersecurity-101/lateral-movement/

How to get an initial access in a Challenge and response auth? hash collision.

upvoted 1 times

⊟ **J_Ko** 2 months, 4 weeks ago

The CHAP system was installed because of pentest, which implies it was not there when the test was done.

upvoted 1 times

⊟ **jackdryan** 1 year, 1 month ago

B is correct

upvoted 1 times

⊟ **somkiatr** 1 year, 6 months ago

Selected Answer: A

Challenge and response authentication has no ticket. For example, CHAP uses password hashing (MD5) and now is considered broken with hash collision. Kerberos is not challenge and response protocol.

upvoted 2 times

⊟ **somkiatr** 1 year, 6 months ago

Pass-the-ticket is an authentication exploit which involves using stolen Kerberos tickets to authenticate to a domain without the account's password. Also known as the forged ticket attack, it is one of the common and effective techniques to move laterally within a network.

The valid Kerberos tickets can be extracted from the lsass memory on a system. Depending on the level of access in a system, the attacker can get hold of the user's service tickets or ticket granting ticket (TGT) . While the TGT can be used to get the required service tickets from the Ticket Granting Server, the service tickets are the actual key to access specific critical server or service in the network.

The two popular exploits in this technique are Silver ticket and Golden ticket. Silver Tickets are used to generate service tickets to access a particular service like MS SQL and the system that hosts the service . Golden tickets on the other hand, are used to generate TGTs for any account in Active Directory.

upvoted 5 times

⊟ **J_Ko** 2 months, 4 weeks ago

the question states the chap system was installed AFTER the test. So that implies it was not there when the later movement happend.

upvoted 1 times

⊟ **jbell** 1 year, 2 months ago

Kerberos uses a nonce in challenge response process. https://www.ietf.org/rfc/rfc4120.txt . Answer B.

upvoted 1 times

⊟ **sec_007** 1 year, 8 months ago

Selected Answer: B

https://www.qomplx.com/qomplx-knowledge-pass-the-ticket-attacks-explained/

upvoted 2 times

⊟ **franbarpro** 1 year, 8 months ago

"Pass the Hash" beby - Oooh wait is Kerboros, well let's "Pass the ticket" then!

upvoted 1 times

⊟ **kptest12** 1 year, 8 months ago

Selected Answer: B

A common exploit, called pass the ticket, is the process of an attacker forging a ticket and passing it along to authenticate to a resource.

upvoted 4 times

⊟ **Jamati** 1 year, 7 months ago

With pass the ticket the hacker does not forge a ticket, they simply steal existing ones. It's the Silver Ticket attack where tickets are forged.

upvoted 1 times

Question #78 *Topic 1*

Which of the following would qualify as an exception to the "right to be forgotten" of the General Data Protection Regulation (GDPR)?

A. For the establishment, exercise, or defense of legal claims

B. The personal data has been lawfully processed and collected

C. For the reasons of private interest

D. The personal data remains necessary to the purpose for which it was collected

Suggested Answer: *A*

Community vote distribution

A (100%)

Bach1968 12 months ago

Selected Answer: A

An exception to the "right to be forgotten" of the General Data Protection Regulation (GDPR) is: A. For the establishment, exercise, or defense of legal claims.

The right to be forgotten allows individuals to request the erasure of their personal data under certain circumstances. However, this right is not absolute, and there are exceptions where data can be retained even if a request for erasure is made. One such exception is when the personal data is necessary for the establishment, exercise, or defense of legal claims. In such cases, the organization may be required to retain the data to fulfill its legal obligations or protect its legal rights.

upvoted 2 times

xxxBadManxxx 1 year ago

D :The personal data remains necessary to the purpose for which it was collected.

upvoted 1 times

Jung1999 1 year, 3 months ago

How about the D? To be honest, I agree with A, but when I saw this question the first time, I thought the answer was D. Because I thought that the "right to be forgotten" about personal data.

upvoted 3 times

jackdryan 1 year, 1 month ago

A is correct

upvoted 1 times

Firedragon 1 year, 7 months ago

Selected Answer: A

A.

https://gdpr-info.eu/issues/right-to-be-forgotten/

The right to be forgotten is not unreservedly guaranteed. It is limited especially when colliding with the right of freedom of expression and information. Other exceptions are if the processing of data which is subject to an erasure request is necessary to comply with legal obligations, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or for the defence of legal claims.

upvoted 2 times

Jamati 1 year, 7 months ago

Selected Answer: A

Simple - A

upvoted 1 times

franbarpro 1 year, 8 months ago

Yep - "A" You can't just be like "delete everything you know about me" when that information is needed for legal purposes

upvoted 4 times

J_Ko 2 months, 4 weeks ago

The best one-sentence explanation :)

upvoted 1 times

Humongous1593 1 year, 9 months ago

Selected Answer: A

A is the proper answer.

upvoted 1 times

Question #79 *Topic 1*

Dumpster diving is a technique used in which stage of penetration testing methodology?

A. Attack

B. Reporting

C. Planning

D. Discovery

Suggested Answer: *D*

Community vote distribution

D (100%)

somsom 8 months, 1 week ago

Answer is D

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: D

The valid option in this case is option D: Discovery.

The discovery stage is focused on gathering information about the target organization, its systems, and its infrastructure. This information can include both technical and non-technical data. Dumpster diving specifically involves searching through physical trash or waste disposal areas of the target organization to gather potentially sensitive or valuable information.

By examining discarded documents, invoices, printouts, or other materials, an attacker can uncover valuable information such as system configurations, network diagrams, passwords, or even confidential documents. This information can then be used in subsequent stages of the penetration test to exploit vulnerabilities and gain unauthorized access to the target organization's systems.

upvoted 4 times

Jamati 2 years, 7 months ago

Selected Answer: D

Obviously D

upvoted 2 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 1 times

Toa 2 years, 7 months ago

Answer D

Discovery

“The discovery phase of penetration testing includes two parts. The first part is the start of actual testing, and covers information gathering and scanning.

Dumpster diving—gathering info on a target by digging through what they have thrown out

https://www.sciencedirect.com/topics/computer-science/discovery-phase

upvoted 3 times

sec_007 2 years, 8 months ago

More information on dumpster diving:

https://www.techtarget.com/searchsecurity/definition/dumpster-diving

https://crashtest-security.com/penetration-test-steps/

upvoted 1 times

franbarpro 2 years, 8 months ago

Selected Answer: D

I was thinking planning at first.... but then it hit me. If they are doing dumpster diving.....they prob finish the planning stage.

upvoted 4 times

Question #80 *Topic 1*

Which of the following is performed to determine a measure of success of a security awareness training program designed to prevent social engineering attacks?

A. Employee evaluation of the training program

B. Internal assessment of the training program's effectiveness

C. Multiple choice tests to participants

D. Management control of reviews

Suggested Answer: *B*

Community vote distribution

B (80%) 13% 7%

franbarpro Highly Voted 2 years, 8 months ago

Selected Answer: B

Yep "B"

upvoted 7 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

somsom Most Recent 8 months, 1 week ago

Obviously B

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: B

my AI told me that B is correct, and I'm convinced. I chose D previously, and now I felt foolish.

upvoted 1 times

noh_ssiw_l 1 year, 9 months ago

which one is vague ohh i mean which one encompasses the other and that's it!!!!! B. for me

upvoted 3 times

Bach1968 1 year, 12 months ago

Selected Answer: B

The correct answer is option B: Internal assessment of the training program's effectiveness. To determine the measure of success of a security awareness training program designed to prevent social engineering attacks, conducting an internal assessment of the program's effectiveness is essential. This assessment involves evaluating the program's impact on employees' knowledge, behavior, and ability to recognize and respond to social engineering attacks. It helps determine whether the training program is achieving its intended objectives and identifies areas for improvement.

upvoted 3 times

hgamboa 1 year, 12 months ago

Selected Answer: C

B sounds ambiguous to me since it's not stating any kind of KPI to determine the program success. According to the Official Study Guide 9th edition pag 100 " In some circumstances, a quiz or test can be administered to workers inmediately after training session. A follow up quiz should be performed three to six months later to see if they retain the information..."

upvoted 1 times

babaseun 2 years, 1 month ago

Selected Answer: A

Training evaluation is important for a variety of reasons. It can help identify areas where training is needed, assess the effectiveness of training, and determine whether training is having the desired impact. Training evaluation can also help improve the quality of future training programs.

upvoted 2 times

Seron23 2 years, 2 months ago

How will you measure internal effectiveness??

upvoted 1 times

oudmaster 2 years, 6 months ago

What the assessment will do?

!

Every training awareness should include test at the end to evaluate every candidate how well they benefit of the training. This way you can partially measure the effectiveness of the training. The other part is related to how these trained staff react to social engineering attacks.

upvoted 1 times

BoZT 1 year, 10 months ago

Employees can remember or simply take notes on the test answers. Internal assessment can include phishing simulation.

upvoted 3 times

Jamati 2 years, 7 months ago

Selected Answer: B

I'll go with B on this one.

upvoted 2 times

Question #81 *Topic 1*

The security team is notified that a device on the network is infected with malware. Which of the following is MOST effective in enabling the device to be quickly located and remediated?

A. Data loss protection (DLP)

B. Intrusion detection

C. Vulnerability scanner

D. Information Technology Asset Management (ITAM)

Suggested Answer: *D*

Community vote distribution

D (96%) 4%

projtfer Highly Voted 👍 2 years, 8 months ago

Selected Answer: D

Selected D. The detection mechanism has already found out that a device has been infected which means it is too late for a vulnerability scanner. The tool that had detected the malware infection, would have given the hostname/IP address of that device. The question asks about the most effective way to "locate", if we plug in the hostname / IP address in the ITAM system, that would give the actual location (Geographical) location of that device and who to contact in case some boots on the ground is needed. Therefore ITAM is the right answer.

upvoted 18 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 3 times

kptest12 Highly Voted 👍 2 years, 8 months ago

Selected Answer: D

In order to locate the asset we need a tool like ITAM

upvoted 5 times

somsom Most Recent 🕘 8 months, 1 week ago

Except if the ip address was flagged then ITAM can be used to find and remediate

upvoted 1 times

somsom 8 months, 1 week ago

Let me tell yiu o'u a scenario that happened in my laptop. My laptop was infected by malware, I quickly use anti.virus to scan my system just to know the part infected. Immediately I was able to see it and remediate it. So IDS is correct. Snort is also an example of IDS

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

What a terrible question. Asset System? No, you don't.

upvoted 1 times

Hardrvkllr 1 year, 2 months ago

ChatGPT and Copilot give two different answers, as I feel it is a B, Copilot states it is D, and ChatGPT states B

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: C

IDS is correct because we don't know which exact host is infected to find it via ITAM, also ITAM is not mentioned in the OSG.

upvoted 1 times

Bach1968 1 year, 12 months ago

Selected Answer: D

Option D: Information Technology Asset Management (ITAM) can also play a role in enabling the infected device to be quickly located and remediated.

ITAM involves tracking and managing the inventory of IT assets within an organization, including devices such as computers, servers, and network devices. By maintaining an up-to-date record of all devices, their locations, and configurations, ITAM can help identify the specific device that is infected with malware.

Once the infected device is identified through ITAM, appropriate remediation actions can be taken, such as isolating the device, conducting a thorough scan for malware, applying patches or updates, or even physically removing and replacing the device if necessary.

Therefore, both option B (Intrusion detection) and option D (ITAM) can be effective in quickly locating and remedying an infected device. The choice between them may depend on the specific capabilities and implementation of the organization's security infrastructure.

upvoted 1 times

⊟ **KCLung** 2 years ago

I do not understand why it is D. I do not hear any IT inventory system can detect the malware and fix it. Although it can easy to detect location of the device, how can it detect which device has the malware. It sounds does not make sense. I would choose C as the IDS can detect the attack of malware and display the source IP of the attack.

upvoted 3 times

⊟ **Jamati** 2 years, 7 months ago

Selected Answer: D

Answer is D. The rest don't make sense.

upvoted 3 times

⊟ **Vino22** 2 years, 8 months ago

C is the answer

upvoted 2 times

⊟ **franbarpro** 2 years, 8 months ago

How scanning for weaknesses will help you locate and remediate the malware? The answer should Def be "D". If you have an up to date Inventory is should be easy to find the device and fix the issue.

upvoted 3 times

Question #82 *Topic 1*

Which of the following threats would be MOST likely mitigated by monitoring assets containing open source libraries for vulnerabilities?

A. Distributed denial-of-service (DDoS) attack

B. Advanced persistent threat (APT) attempt

C. Zero-day attack

D. Phishing attempt

Suggested Answer: *C*

Community vote distribution

B (54%) C (39%) 5%

CuteRabbit168 Highly Voted 2 years, 9 months ago

Selected Answer: B

Unlikely able to detect and mitigate zero-day attacks. Libraries may contain scripts that APTs can use to perform malicious activities

upvoted 17 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 4 times

irEd1 Highly Voted 2 years, 5 months ago

C. Zero day attacks. A zero day attack means the vulnerability was present from day 0. The only thing that would prevent it is constantly checking your open source libraries to see if there are updates because of a vulnerability. Same as patches and updates.

upvoted 11 times

Ramye 1 year ago

Wrong definition.

Zero Day attack means - any vulnerabilities / threat which is unknown and does not have any solution at this time.

So you don't know you most likely monitor for known issues.

upvoted 4 times

djedwards Most Recent 3 weeks, 4 days ago

Selected Answer: C

Most other sites agree with C

upvoted 1 times

36dd0ae 1 month, 1 week ago

Selected Answer: C

C: Zero-day attack

A zero-day attack exploits a previously unknown or unpatched vulnerability in software (heartbleed/log4j) - often found in open source libraries that are integrated into apps.

upvoted 1 times

fuzzyguzzy 2 months, 2 weeks ago

Selected Answer: C

All these answers are terrible, but zero day attacks exploit vulnerabilities that would show up in a decent threat feed. APTs exploit vulnerabilities, but they require more than just handling and scanning for vulnerabilities.

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: C

Monitoring assets containing open source libraries for vulnerabilities is most effective against the risk of zero-day attacks or emerging vulnerabilities.

upvoted 1 times

iRyae 4 months, 2 weeks ago

Selected Answer: C

A zero-day attack targets previously unknown vulnerabilities in software or systems that the vendor has not yet patched or disclosed. Many open-source libraries and components are widely used across various applications, and they may contain undiscovered vulnerabilities. Monitoring these assets for vulnerabilities, especially in open-source libraries, helps identify and patch these security flaws before they are exploited by attackers in zero-day attacks.

APTs are sophisticated, long-term attacks. While they might leverage a vulnerability in an open-source library, they are more complex and often involve multiple attack vectors. Monitoring libraries is a helpful part of a broader defense against APTs, but it's not the primary mitigation strategy.

upvoted 1 times

easyp 5 months ago

Selected Answer: C

The correct answer is:

C. Zero-day attack

Explanation:
Monitoring assets that contain open-source libraries for vulnerabilities is most likely to mitigate the risk of a zero-day attack, particularly in scenarios where an attacker exploits vulnerabilities in outdated or poorly maintained open-source libraries.

By regularly monitoring these libraries:

Organizations can identify vulnerabilities as they are discovered.
They can apply patches or updates promptly, reducing the likelihood of a zero-day vulnerability being exploited.
Open-source libraries are commonly used in modern applications, and vulnerabilities in these libraries can be targeted by attackers in zero-day scenarios.

upvoted 1 times

Fouad777 6 months ago

Selected Answer: C

Zero-day attacks exploit vulnerabilities that are unknown to the software vendor and for which no patch is available. Open-source libraries, being widely used, are often targets for zero-day exploits. Monitoring these libraries for newly discovered vulnerabilities allows organizations to proactively mitigate the risk of zero-day attacks by:
Quickly identifying when a vulnerability is disclosed.
Applying patches or workarounds as soon as they become available.
Potentially implementing mitigations even before an official patch is released if details of the vulnerability are known.

upvoted 1 times

Ravnit 6 months, 2 weeks ago

Selected Answer: C

Zero-day attacks exploit unknown or unpatched vulnerabilities in software. By monitoring and regularly updating open source libraries for known vulnerabilities, organizations can reduce the risk of zero-day exploits, ensuring that any discovered vulnerabilities are promptly addressed before they can be exploited by attackers.

upvoted 2 times

aaminenaji 8 months, 2 weeks ago

I would go with C and here is why:
monitoring libraries won't typically prevent the full spectrum of an APT, which includes social engineering, lateral movement, and other methods beyond just exploiting software vulnerabilities.

upvoted 2 times

deeden 10 months, 4 weeks ago

Selected Answer: C

Monitoring assets containing open source libraries for vulnerabilities is most effective in mitigating zero-day attacks.

Zero-day attacks exploit vulnerabilities that are unknown to the software vendor and for which no patch exists.
By tracking open-source libraries and their associated vulnerabilities, organizations can identify and address potential risks before they are exploited.
The other options are less likely to be directly impacted by monitoring open source libraries:

DDoS attacks target network availability, not specific vulnerabilities.
APTs are persistent threats that may or may not involve exploiting software vulnerabilities.
While monitoring open source libraries won't prevent all zero-day attacks, it significantly reduces the risk of exploitation.

upvoted 1 times

CCNPWILL 1 year ago

Selected Answer: B

B is the best answer out of all choices.

upvoted 1 times

Ramye 1 year, 1 month ago

A Zero Day means exploiting those vulnerabilities for what there are no solutions yet. And these could be that it was not discovered and known to vendors yet.

So you can't take action for threats that are unknown, so the answer most likely is B.

But anyone has confirmed answer pls confirm. Thx

upvoted 2 times

Jenkins3mol 1 year, 1 month ago

Selected Answer: A

You are never going to beat 0day or apt. Come on.

upvoted 1 times

Jenkins3mol 1 year, 2 months ago

Selected Answer: C

Well, I think you will never be able to mitigate apt risk, because they've got to get you. It's just a question of time. And APT does possessed and developed lots of Zero-day vulnerabilities as well.

upvoted 2 times

CCNPWILL 1 year, 2 months ago

Selected Answer: C

I agree with C as well.

upvoted 1 times

Question #83 *Topic 1*

As a design principle, which one of the following actors is responsible for identifying and approving data security requirement in a cloud ecosystem?

A. Cloud auditor

B. Cloud broker

C. Cloud provider

D. Cloud consumer

Suggested Answer: *C*

Community vote distribution

D (85%) C (15%)

kptest12 Highly Voted 2 years, 2 months ago

Selected Answer: D

https://www.isc2.org/Articles/Responsibility-and-Accountability-in-the-Cloud

Data Security - Customer responsibility

upvoted 14 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 2 times

sbear123 Most Recent 9 months, 1 week ago

Selected Answer: D

In all models of cloud, Data is always Customer's responsibility.

upvoted 4 times

Hongjun 10 months ago

Selected Answer: D

Copy form chapter 3.4: Users often mistakenly assume that their CSP is responsible for all security, but users have responsibility for securing their own storage and processing capabilities. So clear that is D

upvoted 1 times

YesPlease 1 year ago

Selected Answer: D

Answer D) Cloud Consumer is responsible for DATA SECURITY on IaaS - PaaS - SaaS

https://www.isc2.org/insights/2021/02/responsibility-and-accountability-in-the-cloud

upvoted 1 times

Soleandheel 1 year ago

D. is the correct answer. Think of it like this; Who ever owns the data, decides how they want the data they own identified, classified and secured. The data owner always has the ultimate say and in this case, the cloud consumer would be considered the data owner. Imagine if the data being stored contained important propriatory information, would you as the owner of the data (the clod consumer) want the cloud provider deciding on how to classify and secure your data? Absolutely not. So in a very logical way, you can see that the correct answer is undeniably D.

upvoted 1 times

AMANSUNAR 1 year, 1 month ago

Selected Answer: D

The cloud consumer is the entity or organization that utilizes cloud services. In the context of data security, the cloud consumer plays a key role in identifying and specifying the security requirements for their data when using cloud services.

upvoted 1 times

Moose01 1 year, 2 months ago

D is correct - generally cloud provider is responsible for some level of security but the wording here is Requirements and Approval, that is requested and approved by the consumer. cloud providers will make more money by selling different security packages to consumers.

upvoted 2 times

BoyBastos 1 year, 3 months ago

Selected Answer: D

Cloud consumer

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: C

the correct answer is C. Cloud provider.

The Cloud provider is responsible for identifying and approving data security requirements in a cloud ecosystem. They are the ones who offer the cloud services and resources to the Cloud consumers. As part of their role, Cloud providers are expected to implement security measures and controls to protect the data and ensure compliance with applicable regulations and standards.

upvoted 2 times

Dee83 1 year, 11 months ago

D. Cloud consumer is responsible for identifying and approving data security requirements in a cloud ecosystem as a design principle.

A cloud consumer is the organization or individual who utilizes the cloud services offered by a cloud provider. As such, it is the responsibility of the cloud consumer to identify and approve the data security requirements for their specific use case and business needs. This includes assessing the risks and vulnerabilities associated with their data and applications, and determining the appropriate controls and safeguards that are required to protect them. The cloud consumer must also ensure that the cloud provider is able to meet these requirements,

upvoted 4 times

rajkamal0 2 years ago

Selected Answer: D

100% Cloud Consumer.

The cloud service provider does not take any responsibility of security lapse on customer.

upvoted 2 times

oudmaster 2 years ago

Data in any cloud model is always owned by the customer and they are responsible to identifying and approving data security requirement.

!

Consumers must have security consultants who decide the security requirements.

!

I go with D

upvoted 1 times

Toa 2 years, 1 month ago

Answer D

Page 12 of link explain : Because cloud Consumers retain ownership of the data residing in a cloud Ecosystem, they usually keep the security authorization in- house and are responsible for identifying all security requirements pertaining to the cloud Ecosystem's hosting and processing of this data.

Cloud Consumer

A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.

Cloud Provider

A person, organization, or entity responsible for making a service available to interested parties.

Cloud Auditor

A party that can conduct an independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

Cloud Broker

An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

Cloud Carrier

An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=919233

upvoted 1 times

rootic 2 years, 2 months ago

Selected Answer: D

I with D.

upvoted 1 times

⊟ **franbarpro** 2 years, 2 months ago

Selected Answer: D

For data security I am thinking of "D" - No matter if we are in the cloud...... We are still responsible for our data. YES it is stored in the cloud but if anything happens to the data. It's "US" the company in the news - not the cloud provider.

upvoted 2 times

⊟ **stickerbush1970** 2 years, 3 months ago

Selected Answer: C

Cloud providers have multiple offerings that accommodate different information assurance levels.

upvoted 2 times

Question #84 *Topic 1*

Which of the following is the MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network?

A. Network Access Control (NAC)

B. Privileged Access Management (PAM)

C. Group Policy Object (GPO)

D. Mobile Device Management (MDM)

Suggested Answer: *A*

Community vote distribution

A (56%) D (44%)

Bach1968 Highly Voted 1 year, 12 months ago

The MOST effective way to ensure the endpoint devices used by remote users are compliant with an organization's approved policies before being allowed on the network is by using
A. Network Access Control (NAC)

Network Access Control (NAC) solutions provide organizations with the ability to authenticate and validate the compliance of devices before granting them access to the network. NAC solutions typically perform checks on various aspects of the device, such as its operating system, antivirus software, patches, and configuration settings, to ensure they meet the organization's security policies.

By implementing NAC, organizations can enforce policies and control access based on the compliance status of the endpoint devices. Devices that do not meet the required security standards can be prevented from accessing the network or placed in a restricted network segment until they are brought into compliance.

upvoted 5 times

djedwards Most Recent 3 weeks, 4 days ago

Selected Answer: D

Why would they add "...endpoint devices used by remote users..." if it wasn't D?

upvoted 1 times

RedMartian 2 months, 3 weeks ago

Selected Answer: A

Likely A. Not D. MDM manages mobile devices, enforcing policies and configurations, but it’s limited to mobile platforms and does not apply to all endpoint types (e.g., laptops, desktops). Also, MDM is typically used after enrollment, not for pre-access enforcement across all remote endpoints.

upvoted 2 times

Toksss 3 months ago

Selected Answer: D

"...endpoint devices used by remote users..."
NAC does nothing for a remote user. It exists to give or deny a user access to a local network.

upvoted 1 times

amitsir 3 months, 1 week ago

Selected Answer: A

NAC is not limited to authentication, it also does security posture checks like updated antivirus, security policy, updated patches etc.

upvoted 1 times

ServerBrain 3 months, 2 weeks ago

Selected Answer: D

MDM is how you can enforce policy to remote endpoints

upvoted 1 times

Chris 11 months, 3 weeks ago

Selected Answer: A

A. Network Access Control (NAC)

Here’s why NAC is the best choice:

Network Access Control (NAC): NAC solutions provide a comprehensive approach to managing and enforcing security policies for devices attempting to access network resources. They can perform health checks on devices to ensure compliance with security policies (e.g., antivirus presence, up-to-date patches) before granting network access. This makes NAC highly effective for verifying compliance of endpoint devices used by remote users. NAC provides a holistic approach by integrating various checks and balances to ensure all endpoint devices meet the required security policies before accessing the network, making it the most effective solution for this purpose.

upvoted 3 times

iamlamzzy 1 year ago

Selected Answer: A

Correct answer is NAC. How i know it? I Managed a NAC tool for 3 plus years. They are used to verify the posture of an endpoint before allowing them full network access. If they don't meet the requirement the device is isolated to a limited network state.

upvoted 2 times

CCNPWILL 1 year, 2 months ago

Selected Answer: D

MDM. With MDM you can ensure the device is in a good posture before being allowed on the network. Answer is D.

upvoted 3 times

Hongjun 1 year, 3 months ago

Selected Answer: D

I prefer D. Keywords- complain company approved policy. It does mentions what policies. NAC is just policy of access. But MDM includes policies for access, how data was encrypted, what software you can used, which website you can't browse etc. So I chose D.

upvoted 2 times

Hongjun 1 year, 3 months ago

Typo. It does not mention what policies.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: A

Answer A) Key phrase in question is "on network"

NAC can stop devices at Network level (virtual or otherwise).

MDM does apply to mobile devices like laptops, but cell phones are not usually connecting directly to a Network. Also, MDM stops mobile devices even before connecting to a network if they don't meet minimum policy requirements like phone OS version is older than the accepted version.

upvoted 2 times

Ramye 1 year, 1 month ago

Cell phones (mobile devices) can be restricted to connect/consume company resources if are not registered in MDM system.
MDM actually is better solution as it can restrict devices if they’re not compliant with company policies.

upvoted 1 times

Soleandheel 1 year, 6 months ago

A. Network Access Control (NAC)

upvoted 1 times

AMANSUNAR 1 year, 7 months ago

Selected Answer: D

Mobile Device Management (MDM) solutions are designed to manage and enforce policies on mobile devices, including remote users' endpoint devices. MDM allows organizations to ensure compliance with security policies, enforce configuration settings, and remotely manage devices, making it a powerful tool for securing remote endpoints.

upvoted 2 times

waleogere 2 years ago

D. Mobile Device Management (MDM) is the right choice.

upvoted 2 times

DapengZhang 2 years, 3 months ago

Selected Answer: D

For sure it is D, the question is asking effective way to ensure the endpoint devices are compliant to company rules. NAC is only for remote user authentication; but for device that is used by users, shall be MDM.
Quoted from OSG9: Administrators register employee devices with a mobile device management (MDM)
system. Mobile device management (MDM) is a software solution to the challenging task
of managing the myriad mobile devices that employees use to access company resources.
The MDM system monitors and manages mobile devices and ensures that they are kept
up-to-date. The goals of MDM are to improve security, provide monitoring, enable remote
management, and support troubleshooting.

upvoted 4 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

BoZT 1 year, 10 months ago

MDM is for mobile devices, what if the endpoint is a computer? and for a remote user, they definitely need to have a computer to work.

upvoted 2 times

[Removed] 1 year, 7 months ago

A laptop is a mobile device too

upvoted 2 times

marziparzi 1 year, 2 months ago

This is why I think it is not MDM as well, and think it is NAC. It says "remote" not "remote mobile".
However, if it said "remote mobile" that would make this really hard to choose for me.

upvoted 2 times

Ivanchun 2 years, 6 months ago

Selected Answer: A

A, remote user need to meet the NAC requirement to connect

upvoted 2 times

DracoL 2 years, 8 months ago

Selected Answer: A

Network access control (NAC), also known as network admission control, is the process of restricting unauthorized users and devices from gaining access to a corporate or private network. NAC ensures that only users who are authenticated and devices that are authorized and compliant with security policies can enter the network.

upvoted 2 times

Question #85 *Topic 1*

Which one of the following BEST protects vendor accounts that are used for emergency maintenance?

A. Vendor access should be disabled until needed

B. Frequent monitoring of vendor access

C. Role-based access control (RBAC)

D. Encryption of routing tables

Suggested Answer: *C*

Community vote distribution

C (54%) A (46%)

Rollizo Highly Voted 2 years, 9 months ago

it is A for sure. If you have this account enable, you don't know how the third party manages the credentials or protects the computer or the keys. Then it is a security hole and it needs to be enable only during outages or big faults.

upvoted 13 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 2 times

rajkamal0 Highly Voted 2 years, 6 months ago

Selected Answer: C

RBAC is the best answer.

"Emergency" access - means active and available 24/7 - A is incorrect IMHO

upvoted 7 times

nuggetbutts 7 months, 3 weeks ago

No, it is the concept of "Just-in-time" Access which is answer A. This is specifically addressed in the exam outline.

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

Can't be C. RBAC is useful for general user access control, but emergency vendor accounts often need privileged access, which is not strictly controlled by RBAC alone.

upvoted 2 times

ziyaetuk 7 months, 1 week ago

Selected Answer: A

A. Vendor access should be disabled until needed

Explanation:

Disabling vendor accounts until they are explicitly needed for emergency maintenance ensures that these accounts cannot be exploited when not in use. This approach minimizes the attack surface and mitigates risks associated with always-on vendor accounts, such as:

Unauthorized access due to weak or stolen vendor credentials.

Potential misuse by attackers exploiting dormant accounts.

By enabling access only on demand, the organization significantly reduces the likelihood of unauthorized access.

upvoted 2 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: C

This is asking about JIT - not RBAC. Answer A is right.

upvoted 1 times

Mrawrrr 8 months ago

Selected Answer: A

Disabling vendor access until it is needed is the best way to protect these accounts because it minimizes the window of opportunity for unauthorized access or misuse.

upvoted 2 times

deeden 10 months, 4 weeks ago

Selected Answer: C

Role-based access control (RBAC) is the most effective way to protect vendor accounts for emergency maintenance.

By assigning specific permissions based on roles, organizations can ensure that vendors have only the necessary access to perform their tasks. This minimizes the risk of unauthorized actions and data breaches.

Here's a breakdown of why the other options are less effective:

A. Vendor access should be disabled until needed: While this can reduce risk, it can also hinder emergency response time.
B. Frequent monitoring of vendor access: Monitoring is important but doesn't prevent unauthorized access.
D. Encryption of routing tables: Unrelated to vendor account protection.
By implementing RBAC, organizations can establish granular control over vendor access and reduce the risk of security incidents.

upvoted 1 times

8b48948 1 year, 2 months ago

Dont think it would be A, would you want to have to re-enable account access in the event of an emergency.

upvoted 1 times

CCNPWILL 1 year, 2 months ago

A is a better choice than C. Answer is clearly A here. RBAC limits the role of the vendor account. but not enabling it until when its needed is the best way to ensure it gets used properly most of the time.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: A

A for attack surface reduction

upvoted 1 times

Kyanka 1 year, 3 months ago

A: Emergency accounts is commonly a type of temporary accounts that needs to be disabled when not in use. Many SRGs/STIGs require these accounts be accounted for and disabled in a timely manner when not actively needed.

upvoted 2 times

BabaRed 1 year, 4 months ago

Selected Answer: A

"Emergency" should hopefully mean rarely used. If that's the case, then A. It could be a liability to give a third-party vendor RBAC access when they are rarely needed.

upvoted 1 times

stack120566 1 year, 4 months ago

Vendors (not partners) are usaully called upon in an adhoc basis to offer intermittant serivce These vendors are usually delegated certian RBAC access within an application and possibly within a database in support of the application or service that they are vendor of. The best way is to leave the account disabeld when not in use. Partners may have tools to monitor and authorization to provide on-going support an applications, vendors would not. Vendors are much more restricted.

upvoted 2 times

YesPlease 1 year, 6 months ago

Selected Answer: A

Answer A)

According to CIS (Center for Internet Security)
a. Emergency Accounts: Emergency Accounts are intended for short-term use and include restrictions on creation, point of origin, and usage (i.e., time of day, day of week). SEs may establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency accounts must be automatically disabled after 24 hours.

https://www.cisecurity.org/wp-content/uploads/2020/06/Account-Management-Access-Control-Standard.docx

upvoted 5 times

⊟ **Soleandheel** 1 year, 6 months ago

I'm going with C. RBAC as oppossed to A. Disabling until needed. My reason is becuase of the keyword "Emergency". Enabling a disabled account in time of an emergency can be time consuming and challenging whereas in the case of RBAC, the needed access is all set to go. Logically C. RBAC makes more sense. I believe the correct answer here is C.

upvoted 2 times

⊟ **Moose01** 1 year, 8 months ago

A. it is an account that vendor support engineer login and an in house engineer will monitor while he is performing his support work.

account is disabled once the job is completed.

RBAC for everyone - 99% of the time unless its other type of access control.

upvoted 1 times

⊟ **homeysl** 1 year, 8 months ago

Selected Answer: A

A is my answer. It says use for emergency maintenance.

upvoted 1 times

Question #86 *Topic 1*

Which event magnitude is defined as deadly, destructive, and disruptive when a hazard interacts with human vulnerability?

A. Crisis

B. Catastrophe

C. Accident

D. Disaster

Suggested Answer: *C*

Community vote distribution

B (53%) D (42%) 6%

noh_ssiw_I Highly Voted 1 year, 9 months ago

thumbs up for the stupid question it is

upvoted 40 times

Skynet08 5 months, 3 weeks ago

are these question being asked in the exam?

upvoted 2 times

dumdada Highly Voted 2 years ago

What a stupid question .....

upvoted 20 times

BigITGuy Most Recent 3 months ago

Selected Answer: D

A catastrophe is a larger-scale event. The question didn't 'scream'.

upvoted 1 times

Djonzi 7 months ago

Selected Answer: D

Should be D....

upvoted 2 times

debig3riw 7 months, 1 week ago

Selected Answer: D

The correct answer is:
D. Disaster
Explanation:

A disaster is defined as a deadly, destructive, and disruptive event that occurs when a hazard (e.g., natural or man-made) interacts with human vulnerability. It overwhelms local capacity, necessitates external assistance, and results in significant harm to people, property, or the environment.

Here's why the other options are incorrect:

A. Crisis: A crisis is a critical situation that demands immediate attention but may not necessarily involve widespread destruction or loss of life. It can escalate into a disaster if not managed effectively.
B. Catastrophe: While similar to a disaster, a catastrophe is a larger-scale event often associated with extremely widespread devastation, often exceeding the capacity of national and international resources to respond effectively.
C. Accident: An accident is typically an unintended, smaller-scale event that causes harm but does not reach the scale or impact of a disaster.

In summary, disaster is the most appropriate term for an event that is deadly, destructive, and disruptive due to the interplay between hazards and vulnerabilities.

upvoted 2 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: D

CISSP specifically defines Disaster as deadly, destructive, disruptive events combined with human vulnerability. Catastrophe is a different, higher category that involves a much larger scale.

upvoted 2 times

deeden 10 months, 4 weeks ago

Selected Answer: B

In terms of impact to human lives, the hierarchy of event magnitude can be described as follows:

Catastrophe: The most severe, involving widespread destruction and significant loss of life, often affecting large regions and requiring extensive recovery efforts.
Disaster: A serious event causing substantial damage and disruption, impacting a large number of people, but on a smaller scale than a catastrophe.
Crisis: An unstable situation that has the potential to escalate into a disaster if not managed properly.
Accident: Typically localized incidents with limited impact, resulting in injuries or minor disruptions.

> [!important] Earthquakes, hurricanes, or weather conditions that could lead to large-scale wildfires are more properly classed as hazards, rather than threats there is no human intention behind a thunderstorm. Pandemics are also hazards, not threats.

upvoted 2 times

[Removed] 11 months, 1 week ago

Selected Answer: B

According to the CISSP official book, a catastrophe is defined as a major disruption that destroys the facility altogether. This aligns with the question's description of an event magnitude that is deadly, destructive, and disruptive when a hazard interacts with human vulnerability. In contrast, a disaster is described as an event that causes the entire facility to be unusable for a day or longer, but does not necessarily destroy the facility.

upvoted 1 times

Chris 11 months, 3 weeks ago

Selected Answer: D

D. Disaster: This term is specifically used to describe events that cause significant harm, especially when human vulnerability is a key factor. Disasters inherently imply a significant negative impact on humans, making them deadly, destructive, and disruptive.

Considering the emphasis on human vulnerability and the significant impact of the event, D. Disaster remains the most appropriate term to describe an event that is deadly, destructive, and disruptive due to human vulnerability. Disasters are characterized by their severe impact on human lives and infrastructure, aligning closely with the scenario described in the question.

Therefore, the correct answer remains:
D. Disaster.

upvoted 1 times

TheManiac 1 year, 1 month ago

Selected Answer: C

human vulnerability is the key here. Catastrophe or Disaster is based on humans. they are natural. But an accident is what we do.
Crisis doesnt have to be deadly. So, right answer is Accident.

upvoted 1 times

Jenkins3mol 1 year, 1 month ago

Is this a language test though?

upvoted 4 times

e58c193 1 year, 2 months ago

Human vulnerability is the key word in this question, which will make answer C the correct choice.
A catastrophe and a disaster can take place without human vulnerability, think about natural events, or nuclear plant catastrophes.

upvoted 1 times

dm808 1 year, 3 months ago

Selected Answer: D

from
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8630994/#:~:text=Cataclysm%3A%20a%20large%2Dscale%20and,damage%20or%20loss%20of%20life.

Catastrophe: an event causing great and usually sudden damage or suffering; a disaster.
Disaster: a sudden accident or a natural catastrophe that causes great damage or loss of life.

Catastrophe and Disaster are in each other's definition...

But I'd lean more toward D since Disaster specifically mentions loss of life..

upvoted 1 times

hoho2000 1 year, 3 months ago

Selected Answer: C

A hazard is a precondition of a system, workplace or environment that could cause a risk event to happen accidentally, that is, without being the conscious intent of the person involved in that event.

The last key word was Hazard, the other 3 bogs words were smoke screen

upvoted 1 times

Kyanka 1 year, 3 months ago

Answer can't really be defined based on the question. The common difference between disaster and catastrophe based on how most orgs define it, is based on scale. Catastrophe is when a disaster is larger than the local resources can support recovery. So a disaster is when something destroys everything in the server room but a catastrophe is when something destroys the whole building.

upvoted 1 times

Hongjun 1 year, 3 months ago

Selected Answer: B

D refers to nature. Question ask for human. It is B. Such as Covid 19. It is catastrophe not disaster.

upvoted 3 times

GuardianAngel 1 year, 4 months ago

I can't find a definition for disaster or catastrophe that clearly matches the question, but in taking other tests from Wiley and Udemy, the questions that are worded somewhat similar all have the answer as catatrophe. Here's a definition from one of the explainations that seems closer to "deadly, destructive, and disruptive" for a catastrophe than a disaster: Catastrophes have the most significant physical impact on businesses. They can come in the form of earthquakes, tornados, fires, and floods. The distinguishing difference between catastrophes and disasters is that a catastrophe destroys a facility altogether. To resume operations, short- and long-term solutions must be developed. A disaster typically involves the facility only being partially destroyed and the business being affected temporarily.

upvoted 1 times

Question #87 *Topic 1*

Which of the following BEST describes the purpose of software forensics?

A. To analyze possible malicious intent of malware

B. To perform cyclic redundancy check (CRC) verification and detect changed applications

C. To determine the author and behavior of the code

D. To review program code to determine the existence of backdoors

Suggested Answer: *C*

Community vote distribution

C (79%) 14% 7%

dev46 Highly Voted 1 year, 9 months ago

Software forensics is the science of analyzing software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the centerpiece of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets. Software forensics tools can compare code to determine correlation, a measure that can be used to guide a software forensics expert.

Source -Wikipedia

upvoted 8 times

jackdryan 1 year, 1 month ago

C is correct

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: C

Software forensics is the process of analyzing code to determine its origin (authorship). Analyzing malicious intent of malware is part of malware analysis, not software forensics.

upvoted 1 times

georgegeorge125487 10 months, 2 weeks ago

Software forensics: the importance is attribution : review the code to identify the developer when malicious insiders are suspected.

upvoted 2 times

Bach1968 12 months ago

Selected Answer: C

The purpose of software forensics (also known as software reverse engineering) is best described as: C. To determine the author and behavior of the code.

Software forensics involves the analysis of software code to understand its structure, functionality, and behavior. It aims to identify the origin of the code, determine its purpose, and gain insights into its functionality. By examining the code, forensic analysts can gather information about the software's behavior, identify potential vulnerabilities or malicious intent, and assess its overall security.

While software forensics may involve analyzing possible malicious intent of malware (option A), performing cyclic redundancy check (CRC) verification to detect changed applications (option B), and reviewing program code to determine the existence of backdoors (option D), its primary purpose is to understand and investigate the authorship and behavior of the code.

the story never end, too long and too complex

upvoted 3 times

assmaalick 1 year ago

D Forensic analysts may also be called on
to conduct forensic reviews of applications or the activity that
takes place within a running application. In some cases, when
malicious insiders are suspected, the forensic analyst may be
asked to conduct a review of software code, looking for back

doors, logic bombs, or other security vulnerabilities. In other
cases, forensic analysis may be asked to review and interpret
the log files from application or database servers, seeking
other signs of malicious activity, such as SQL injection attacks,
privilege escalations, or other application attacks

upvoted 1 times

somkiatr 1 year, 6 months ago

Selected Answer: C

I choose C. What Is Software Forensics? Software forensics is a branch of science that investigates computer software text codes and binary codes in cases involving patent infringement or theft. Software forensics can be used to support evidence for legal disputes over intellectual property, patents, and trademarks.

upvoted 1 times

rajkamal0 1 year, 6 months ago

Selected Answer: C

C is the correct answer.
Reading the question clearly suggests the forensic analysis of attacker code

upvoted 1 times

Firedragon 1 year, 7 months ago

Selected Answer: C

C.
https://en.wikipedia.org/wiki/Software_forensics

upvoted 1 times

FredDurst 1 year, 7 months ago

Selected Answer: C

Software Science aimed at authorship analysis of computer source code for legal purposes. It involves the areas of author identification, discrimination, and characterization.
https://resources.infosecinstitute.com/topic/computer-forensics-overview-software-forensics/

upvoted 2 times

Bhuraw 1 year, 8 months ago

Selected Answer: A

A seems right

upvoted 3 times

Outdoors 1 year, 8 months ago

Selected Answer: D

D is correct

upvoted 2 times

J_Ko 2 months, 4 weeks ago

I read D as being part of C which is why I went with C.

upvoted 1 times

franbarpro 1 year, 8 months ago

Selected Answer: C

Yep "C" - Let's make sure they didn't copy our code

upvoted 3 times

Question #88 *Topic 1*

A web developer is completing a new web application security checklist before releasing the application to production. The task of disabling unnecessary services is on the checklist. Which web application threat is being mitigated by this action?

A. Session hijacking

B. Security misconfiguration

C. Broken access control

D. Sensitive data exposure

Suggested Answer: *B*

Community vote distribution

B (88%) 13%

amitsir 3 months, 1 week ago

Selected Answer: B

in OWASP top 10 there is no term called broken access control, its called broken authentication. correct answer is security misconfiguration which includes web server, database, application, routers and firewalls as well.

upvoted 1 times

J_Ko 2 months, 4 weeks ago

there is; at least in the 2021 version.

https://owasp.org/Top10/A01_2021-Broken_Access_Control/

I really dislike these kind of questions where you need to infer from the answers that "the checklist" is the OWASP top 10... but it is what it is.

upvoted 1 times

8b48948 8 months, 2 weeks ago

Terrible question - my choice would be B and not really sure any of them are relevant.

upvoted 2 times

dm808 9 months ago

Why not A?

The question is asking which application THREAT is being mitigated.. Session hijacking is the only threat listed..

Security misconfiguration is a vulnerability

Broken access control is a vulnerability

Sensitive data exposure is a risk..

upvoted 3 times

Ramye 7 months, 1 week ago

Not sure but if configured properly then chances of session hijacking is less/minimized.

upvoted 2 times

YesPlease 1 year ago

Selected Answer: B

Answer B) Security Misconfigurations

https://www.balbix.com/insights/security-misconfiguration-impact-examples-and-prevention/

upvoted 3 times

Soleandheel 1 year ago

C. Broken Access Controls is the correct answer. Broken access controls pertain to issues related to improper authorization and access permissions, which are often a key aspect of mitigating threats by disabling unnecessary services. However, B. Security misconfiguration in itself will not be an appropriate answer for the question. I see a lot of people selecting answer B. because they are looking at Chatgpt. Please don't blindly accept chatgpt answers, many of them are wrong and this is one of them.

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: B

The web application threat being mitigated by disabling unnecessary services is:

B. Security misconfiguration.

Disabling unnecessary services helps reduce the attack surface of a web application by eliminating potential entry points for attackers. It helps ensure that only essential services are running, reducing the chances of security vulnerabilities arising from misconfigured or unpatched services. By disabling unnecessary services, the web developer minimizes the risk of security misconfigurations that could be exploited by attackers.

upvoted 2 times

Moose01 1 year, 7 months ago

B.

8 Examples of Security Misconfigurations

1- Sample Applications Vulnerability. ...

2- Directory Listing Vulnerability. ...

3- Error Message Vulnerability. ...

4- Default Privileges Vulnerability. ...

5- Unnecessary Features Vulnerability. ...

6- Improper Data Validation Vulnerability. ...

7- Unpublished URLs Vulnerability. ...

8- Out-of-date Software Vulnerability.

upvoted 3 times

DapengZhang 1 year, 9 months ago

Selected Answer: C

the purpose of "disabling unnecessary services" is to avoid vertical privilege escalation.

upvoted 1 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

sphenixfire 2 years, 2 months ago

Selected Answer: B

not completly clear for me but after googleing cissp security missconfiguration all the articles refere to functions that should be disabled if not needed (no default config on). so B

upvoted 3 times

franbarpro 2 years, 2 months ago

This is application hardening..... so check for that human error of misconfiguring stuff.

upvoted 2 times

dev46 2 years, 3 months ago

A & D can be eliminated as session hijacking and data breach still going to happen after hardening/ disabling unnecessary services

I chose Broken Authentication, but it's not true. I read some articles. Example of broken authentication (https://avatao.com/blog-broken-access-control/) - it can still happen

B seems right - if we don't disable configuration for directory listing, attacker can list the directory (https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration)

upvoted 3 times

ygc 2 years, 3 months ago

B is correct, key word is 'disabling'.

upvoted 3 times

Question #89 *Topic 1*

What is the BEST method to use for assessing the security impact of acquired software?

A. Threat modeling

B. Common vulnerability review

C. Software security compliance validation

D. Vendor assessment

Suggested Answer: *A*

Community vote distribution

A (100%)

Firedragon Highly Voted 👍 2 years, 7 months ago

Selected Answer: A

A.
Official study guide, page26
Threat modeling is the security process where potential threats are identified, categorized, and analyzed. Threat modeling can be performed as a proactive measure during design and development or as a reactive measure once a product has been deployed. In either case, the process identifies the potential harm, the probability of occurrence, the priority of concern, and the means to eradicate or reduce the threat.

upvoted 9 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

RRabbit_111 Most Recent ⏲ 7 months ago

Selected Answer: D

While threat modeling is undoubtedly valuable, vendor assessment aligns more closely with the question's focus on acquired software:

Vendor assessment evaluates the entire security lifecycle of the software, not just static or identified threats. It includes considerations like:

Patch management.
Secure software development practices.
Ongoing support and vulnerability disclosure mechanisms.
The question's emphasis on "security impact" implies a need for broader risk management, which vendor assessments address by evaluating the vendor's ability to mitigate risks holistically, not just identifying specific threats.

upvoted 1 times

KennethLZK 7 months, 1 week ago

Selected Answer: D

Both Threat modeling & Vendor assessment are important, but for assessing the security impact of acquired software, vendor assessment provides a broader evaluation of the vendor's security practices, which is crucial for ensuring the software's overall security.

upvoted 1 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: D

Threat modeling is not the most applicable to the question which is specific to "aquired software". The only options are C and D - and D encompasses C making D the broader "management level" answer. 3rd party vendor assessments are used to validate security and can be distributed to potential customers as proof of their security compliance.

upvoted 1 times

maawar83 1 year, 6 months ago

Answer is C!
Elimination Rule:
- A-Threat Modeling is a process not a method to use for assessing security impact

- B- known vulnerabilities is part of the threat model and security assessment
so It is either C or D..
the best will be C as
Ensure that the acquired software complies with relevant security standards and regulations. This may include industry-specific standards or frameworks, as well as general data protection regulations.
upvoted 3 times

Bach1968 1 year, 12 months ago

Selected Answer: A

The BEST method to use for assessing the security impact of acquired software is:

A. Threat modeling.

Threat modeling is a proactive approach to identify potential security threats and vulnerabilities in software systems. It involves analyzing the software's architecture, components, and interactions to determine possible attack vectors and prioritize security controls accordingly. By conducting a threat modeling exercise for acquired software, organizations can gain insights into potential security risks and make informed decisions on implementing appropriate security measures. It helps in understanding the software's security posture and guides the development of effective mitigation strategies.
upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: A

Answer is A.
Once you've acquired the software you can implement a threat model such as STRIDE. However before purchasing the system you have to ensure it has been subjected to formal evaluation processes in advance and has received some kind of security rating. Often trusted third parties are used to perform security evaluations; one such example being the Common Criteria.
CISSP official Study Guide Volume 9 page 337
upvoted 2 times

Mgz156 2 years, 9 months ago

Selected Answer: A

Answer is A. Security impact of software after being "Acquired " . Threat Modelling is right
upvoted 3 times

krassko 2 years, 9 months ago

Selected Answer: A

B is included in A
upvoted 3 times

ItsBananass 2 years, 9 months ago

I'm going with B, vulnerability assessment should give a vulnerability score which could give you a vulnerability impact assessment score and impact severity. I think you would have to know what the vulnerability is before you can asses the true treat. You can not have a threat w/o a vulnerability.
upvoted 2 times

dev46 2 years, 9 months ago

A seems right to me as we have to included more than vulnerability score to understand security impact of software/ application. Example, PASTA, a threat modeling method has 7 stage. One of the stage includes vulnerability weakness and analysis. So, option A includes B .
upvoted 4 times

Question #90 *Topic 1*

Which of the following ensures old log data is not overwritten?

A. Log retention

B. Implement Syslog

C. Increase log file size

D. Log preservation

Suggested Answer: *C*

Community vote distribution

A (49%) D (41%) 10%

⊟ **Coolwater** Highly Voted 👍 2 years, 8 months ago

For those who are saying "Retention " = retention is something which we define as a date or week or month or year for saving logs or any other kind of data . after the defined period, the data will be overwritten . lets take CCTV data storage as an example. if we are configuring the storage settings for 1 moth , it will only keep 1 month of recent video footage , the old footages will be overwritten . Ans is D

upvoted 10 times

⊟ **DERCHEF2009** Highly Voted 👍 2 years, 9 months ago

Selected Answer: D

shoud be D

upvoted 9 times

⊟ **jackdryan** 2 years, 1 month ago

D is correct

upvoted 2 times

⊟ **36dd0ae** Most Recent ⏲ 1 month, 1 week ago

Selected Answer: D

(D) Log preservation

Preservation should be correct answer as the name implies, we are preserving a log. Log retention is for example my org has a retention policy of 7 years, after which any data with such classification can be overwritten.

upvoted 1 times

⊟ **BigITGuy** 3 months ago

Selected Answer: A

Can't be D. "Log preservation" is not a formal term or standard mechanism. The common term is log retention.

upvoted 1 times

⊟ **MustardHead** 5 months, 3 weeks ago

Selected Answer: D

Question does not regard retention, rather preservation.

upvoted 1 times

⊟ **imather** 6 months ago

Selected Answer: A

A. B and C are not relevant to ensure old log data is not overwritten. According to NIST, log preservation is defined as "Keeping logs that normally would be discarded, because they contain records of activity of particular interest." Log retention is "Archiving logs on a regular basis as part of standard operational activities." D refers to preserving logs specifically because they may have something of interest, whereas A is the regular practice of keeping and storing old logs.

upvoted 1 times

⊟ **nuggetbutts** 7 months, 3 weeks ago

Selected Answer: A

The answer is A. D deals primarily with log file integrity.

upvoted 1 times

⊟ **Bietchasup** 7 months ago

presevation deals with log integrity. Is this not the concern here? if its overwritten you no longer have ingrity. what do you think?

upvoted 1 times

⊟ **somsom** 7 months, 4 weeks ago

answer is D.

upvoted 1 times

⊟ **deeden** 10 months, 4 weeks ago

Selected Answer: A

I would say it should be along the lines of Log retention policy, implementation, and monitoring.

upvoted 1 times

⊟ **MP26** 1 year, 2 months ago

Log retention prevents to logs to be overwritten. If retention time is to short than preservation will not help because it keeps overwritten and not completer. Other advantage. It is easier and cheaper.

A: is my answer

upvoted 1 times

⊟ **john_boogieman** 1 year, 3 months ago

Selected Answer: A

From OSG:

16. Gavin is considering altering his organization's 'log retention' policy to delete logs at the end of each day. What is the most important reason that he should avoid this approach?

A. An incident may not be discovered for several days and valuable evidence could be lost.

upvoted 1 times

⊟ **Kyanka** 1 year, 3 months ago

Selected Answer: A

Think like a manager/policy creator: Answer is A.

upvoted 2 times

⊟ **Hongjun** 1 year, 3 months ago

Selected Answer: D

The organization's policies and procedures should also address the preservation of original logs. Many organizations send copies of network traffic logs to centralized devices, as well as use tools that analyze and interpret network traffic. So D is correct.

upvoted 2 times

⊟ **InclusiveSTEAM** 1 year, 8 months ago

The correct answer is A

The answer that best ensures old log data is not overwritten is log retention, option A.

Log retention policies and procedures specifically preserve and archive logs for compliance and analysis needs, preventing them from being purged or overwritten.

Syslog may provide centralized logging but does not itself retain old logs.

Increasing log file size allows storing more events but does not guarantee retaining old data.

While log preservation is close, log retention is the most precise term for maintaining archives of old log data.

upvoted 5 times

⊟ **LalithW** 1 year, 8 months ago

It says about log overwritten. SO increasing log file size is correct.

upvoted 2 times

⊟ **georgegeorge125487** 1 year, 10 months ago

Selected Answer: A

Only log retention exists in CISSP study guide.

upvoted 6 times

⊟ **MShaaban** 1 year, 10 months ago

I would go with A

upvoted 1 times

Question #91 *Topic 1*

Under the General Data Protection Regulation (GDPR), what is the maximum amount of time allowed for reporting a personal data breach?

A. 24 hours

B. 48 hours

C. 72 hours

D. 96 hours

Suggested Answer: *C*

Community vote distribution

C (100%)

Bach1968 Highly Voted 11 months, 4 weeks ago

Selected Answer: C

Under the General Data Protection Regulation (GDPR), the maximum amount of time allowed for reporting a personal data breach is 72 hours. This means that organizations must notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms.

upvoted 5 times

rdy4u Most Recent 1 year, 8 months ago

Selected Answer: C

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. 2Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

upvoted 2 times

jackdryan 1 year, 1 month ago

C is correct

upvoted 1 times

Humongous1593 1 year, 9 months ago

Selected Answer: C

https://gdpr-info.eu/art-33-gdpr/

Without undue delay, max 72 hours

upvoted 4 times

Cww1 1 year, 9 months ago

correct

upvoted 3 times

Question #92 *Topic 1*

A financial organization that works according to agile principles has developed a new application for their external customer base to request a line of credit. A security analyst has been asked to assess the security risk of the minimum viable product (MVP). Which is the MOST important activity the analyst should assess?

A. The software has been signed off for release by the product owner.

B. The software had been branded according to corporate standards.

C. The software has the correct functionality.

D. The software has been code reviewed.

Suggested Answer: *D*

Community vote distribution

D (68%) C (16%) A (16%)

BigITGuy 2 months, 4 weeks ago

Selected Answer: D

Not C. Correct functionality is necessary but says nothing about whether the functionality is secure.

upvoted 1 times

nuggetbutts 7 months, 3 weeks ago

Selected Answer: C

The answer is C becuase of the keywords "financial institution" - in the Financial sector, functionality is tied directly to security.

upvoted 2 times

nuggetbutts 7 months, 3 weeks ago

Changing my answer after more research - it is indeed D. While functionality is tied to security, code review is paramount for financial applications due to high-risk security/regulatory/privacy impacts.

upvoted 2 times

Ramye 1 year ago

Selected Answer: C

Got to think like an adviser without getting into weeds and providing details solutions.

upvoted 2 times

Demo25 1 year, 11 months ago

Selected Answer: D

D. The software has been code reviewed.

Code review is a process of inspecting code to identify potential security vulnerabilities. It is an important part of the software development lifecycle, and it can help to prevent security breaches.

The other options are not as important as code review.

The software has been signed off for release by the product owner: This is important, but it does not guarantee that the software is secure.
The software has been branded according to corporate standards: This is also important, but it is not as important as security.
The software has the correct functionality: This is important, but it is not as important as security.

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: D

again i forgot to select the answer

upvoted 1 times

Bach1968 1 year, 11 months ago

In assessing the security risk of the minimum viable product (MVP) for a financial organization's new application, the most important activity for the security analyst to assess is option D: The software has been code reviewed.

Code review is a crucial security practice that helps identify and address security vulnerabilities and weaknesses in the software's code. By conducting a thorough code review, the security analyst can identify potential security flaws, coding errors, and vulnerabilities that could be exploited by attackers. This allows for the identification and mitigation of security risks before the software is released to customers, helping to ensure a higher level of security in the application.

upvoted 1 times

HughJassole 2 years ago

C. An MVP is not a finished product, but a test:

"An MVP allows you to prove a concept before committing too much time or budget to full-blown product development. Most agree that an MVP is a product with a minimal number of features needed to engage customers and validate a basic concept for further development. Importantly, it's not final — the idea is that it's something you augment and refine over time."

https://thenewstack.io/building-an-minimum-viable-product-a-founders-guide-to-success/

"Minimum Viable Product is not a finished product or version 1.0. It is the smallest part of the product that clearly demonstrates its main functionality and is available to the public. MVP does not have to work, it can be a prototype of a web application explaining the main idea of a product, for example. MVP's role is to get feedback from the user and learn what he likes about the product and what the things that he does not need are."

https://www.scrumdesk.com/what-is-minimum-viable-product/

upvoted 2 times

oudmaster 2 years, 6 months ago

Option D is the only answer that is related to the security analyst duty.

upvoted 2 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: D

A minimum viable product (MVP) is a version of a product with just enough features to be usable by early customers who can then provide feedback for future product development and updates / upgrades. The question specially asks about THE SECURITY RISK of the MVP. In other words, we already have an MVP, i.e., correct functionality. What we now want is to evaluate the security around this correctly functioning system, not to evaluate if it functions correctly.

upvoted 4 times

somkiatr 2 years, 6 months ago

Agreed.

upvoted 1 times

sphenixfire 2 years, 8 months ago

Selected Answer: D

a security analyst in this case is a pentester. it's not the job to check function, branding and especially not this job to accept a sign off of a product owner. so my vote is D

upvoted 2 times

niti 2 years, 8 months ago

Selected Answer: C

Keywords in the question: " works according to agile principles" "minimum viable product"

so functionality is the main agenda - Ans is "C"

upvoted 1 times

niti 2 years, 8 months ago

Keywords in the question: " works according to agile principles" "minimum viable product"

so functionality is the main agenda - Ans is "C"

upvoted 1 times

franbarpro 2 years, 8 months ago

Selected Answer: D

As a security analyst - You should only care if the code has been reviewed from security standpoint. All the other stuff...... let them deal with it.

upvoted 3 times

Ncoa 2 years, 9 months ago

Selected Answer: C

MVP is being able to demonstrate the functionality of the product to the external customer base to ensure it meets requirements and the appetite to complete development

upvoted 1 times

Ncoa 2 years, 9 months ago

Actually I think D is correct from a security risk perspective. My bad

upvoted 1 times

wyerock 2 years, 9 months ago

Selected Answer: D

A, B, C do not impact security risk

upvoted 2 times

stickerbush1970 2 years, 9 months ago

Selected Answer: A

B, C, and D are covered under A.

upvoted 3 times

Mgz156 2 years, 9 months ago

But as a Security Analyst your first job is to check the code. Answer is D

upvoted 3 times

Question #93 *Topic 1*

An application developer receives a report back from the security team showing their automated tools were able to successfully enter unexpected data into the organization's customer service portal, causing the site to crash. This is an example of which type of testing?

A. Performance

B. Positive

C. Non-functional

D. Negative

Suggested Answer: *D*

Community vote distribution

D (83%) B (17%)

⊟ **dev46** Highly Voted 1 year, 9 months ago

Positive testing determines that your application works as expected. If an error is encountered during positive testing, the test fails.

Negative testing ensures that your application can gracefully handle invalid input or unexpected user behavior. For example, if a user tries to type a letter in a numeric field, the correct behavior in this case would be to display the “Incorrect data type, please enter a number” message. The purpose of negative testing is to detect such situations and prevent applications from crashing. Also, negative testing helps you improve the quality of your application and find its weak points.

The core difference between positive testing and negative testing is that throwing an exception is not an unexpected event in the latter. When you perform negative testing, exceptions are expected – they indicate that the application handles improper user behavior correctly.

upvoted 10 times

⊟ **dev46** 1 year, 9 months ago

SOURCE - https://smartbear.com/learn/automated-testing/negative-testing/

upvoted 1 times

⊟ **dev46** 1 year, 9 months ago

D seems right as we expect website to crash if someone enters unexpected input

upvoted 1 times

⊟ **dev46** 1 year, 9 months ago

However, the below is contradicting to the definition of negative testing

"The purpose of negative testing is to detect such situations and prevent applications from crashing."

upvoted 1 times

⊟ **franbarpro** 1 year, 8 months ago

Which is WHY I think the answer should be "B"

upvoted 1 times

⊟ **niti** 1 year, 8 months ago

" automated tools were able to successfully enter unexpected data" this is not positive testing - why are we going to test the " invalid data " in positive testing?

upvoted 1 times

⊟ **jackdryan** 1 year, 1 month ago

D is correct

upvoted 1 times

⊟ **YesPlease** Most Recent 6 months, 3 weeks ago

Selected Answer: D

Answer is D) Negative Testing

Reason: Negative testing ensures that your application can gracefully handle invalid input or unexpected user behavior. In this case, it fails the negative testing.

For example, if a user tries to type a letter in a numeric field, the correct behavior in this case would be to display the “Incorrect data type, please enter a number” message. The purpose of negative testing is to detect such situations and prevent applications from crashing.

This has nothing to do with Non-functioning testing because Non-functional testing is a type of software testing that verifies non functional aspects of the product, such as performance, stability, and usability....so in essence, both Answer "A" and "C" are the same.

upvoted 1 times

Bach1968 11 months, 4 weeks ago

Selected Answer: D

The example provided, where unexpected data causes the customer service portal to crash, is an example of negative testing.

Negative testing is a testing approach that focuses on validating the system's behavior when exposed to unexpected or invalid inputs or conditions. It aims to identify potential vulnerabilities, weaknesses, and failures by intentionally providing inputs that the system is not designed to handle properly. The objective of negative testing is to uncover potential security vulnerabilities, error handling issues, and system crashes.

In this case, the security team's automated tools were able to enter unexpected data into the customer service portal, causing it to crash. By intentionally providing unexpected data, the security team was able to identify a vulnerability or weakness in the system's ability to handle such inputs.

upvoted 1 times

Delab202 1 year, 6 months ago

Negative Testing is a software testing type used to check the software application for unexpected input data and conditions. Unexpected data or conditions can be anything from wrong data type to strong hacking attack.

upvoted 1 times

Jamati 1 year, 7 months ago

Selected Answer: D

Answer is D.

Negative Testing is when a user enters invalid input to see how the system reacts. Does it crash or it simply pops up a notification informing you that you entered invalid input.

upvoted 2 times

Toyeeb 1 year, 8 months ago

it is D according to the link below

https://www.guru99.com/positive-and-negative-testing.html

upvoted 3 times

Nickname53796 1 year, 8 months ago

Selected Answer: D

Negative test – how the system behaves with unexpected data (should reject the data).

The testing app successfully got the testee to accept data it should not have.

upvoted 2 times

franbarpro 1 year, 8 months ago

Selected Answer: B

Am I the only one going with "B" on this one. I don't understand why it would be "D" sense the site was able to crash.

upvoted 1 times

JAckThePip 1 year, 8 months ago

Anwer id D

"Negative Testing is a software testing type used to check the software application for unexpected input data and conditions. Unexpected data or conditions can be anything from wrong data type to strong hacking attack. The purpose of negative testing is to prevent the software application from crashing due to negative inputs and improve the quality and stability."

https://www.guru99.com/negative-testing.html

upvoted 3 times

franbarpro 1 year, 8 months ago

I meas if the "purpose of negative testing is to prevent the software application from crashing" - then the answer here should be "B" positive testing bcs the test that was conducted caused the site to crash.

upvoted 1 times

Question #94 *Topic 1*

Which of the following is the MOST effective strategy to prevent an attacker from disabling a network?

A. Design networks with the ability to adapt, reconfigure, and fail over.

B. Test business continuity and disaster recovery (DR) plans.

C. Follow security guidelines to prevent unauthorized network access.

D. Implement network segmentation to achieve robustness.

Suggested Answer: *C*

Community vote distribution

A (54%) C (32%) 11%

Dee83 Highly Voted 2 years, 5 months ago

D. Implement network segmentation to achieve robustness.

Network segmentation is a security practice that involves dividing a network into smaller, isolated subnetworks, which can limit the potential damage and spread of an attack. This can prevent an attacker from disabling the entire network, and it can also provide additional security controls such as access controls, firewalls, and intrusion detection/prevention systems (IDS/IPS) to further protect critical network assets.

Designing networks with the ability to adapt, reconfigure, and fail over can also help to maintain network availability in the face of an attack, but network segmentation is considered the most effective way to prevent an attacker from disabling the entire network. Testing business continuity and disaster recovery (DR) plans and following security guidelines to prevent unauthorized network access are important, but they are not directly related to preventing an attacker from disabling the network.

upvoted 16 times

BigITGuy Most Recent 3 months ago

Selected Answer: A

The MOST effective strategy to prevent an attacker from completely disabling a network is to design it with redundancy, failover capabilities, dynamic reconfiguration. Can't be C -- following security guidelines helps prevent unauthorized access, but even authorized users can face network failures if the network is not resilient. Can't be D -- Network segmentation improves security and containment, but by itself does not guarantee that the network will adapt or failover when under attack.

upvoted 1 times

Dtony66 5 months, 3 weeks ago

Selected Answer: D

With a robust network and different paths, the network would not be able to be taken down.

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: A

This approach ensures that the network can maintain its functionality even when under attack. This strategy offers resilience against a wide range of attacks. Examples include:

1. Software-Defined Networking (SDN): SDN controllers enable dynamic network reconfiguration and policy enforcement.
2. Network Function Virtualization (NFV): Virtualizes network services to allow for rapid deployment and scaling.
3. Load Balancers: Distribute traffic across multiple servers to prevent overload and ensure availability.
4. Automated Failover Systems: Tools like Kubernetes for container orchestration support automatic failover for applications.

These solutions collectively enhance network resilience and continuity.

upvoted 4 times

Ramye 1 year, 1 month ago

Based on the key statement - prevent an attacker from disabling a network, the answer is A.

This will ensure access is provided based on who needs it thus making sure preventing access to others to carry on attacks.

upvoted 1 times

Ramye 1 year, 1 month ago

Oops - I meant to say the answer is C.

upvoted 1 times

Dtony66 1 year, 1 month ago

Selected Answer: A

Any network can be hacked

upvoted 2 times

CCNPWILL 1 year, 2 months ago

Selected Answer: A

A. C is just network access only.. you can still point a DOS and disable a. network. no need for network access to disable a network. Answer is A.

upvoted 4 times

Vasyamba1 1 year, 3 months ago

Selected Answer: A

I think the correct answer is A. We are asked about strategy - design networks in a proper way is a strategy. Moreover, C tells us about guidelines to prevent access only, but the question is about disabling network in general.

upvoted 4 times

CCNPWILL 1 year, 2 months ago

I agree with this statement. Answer is indeed A.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: C

C is about best practice. D is a bit technical but best solution.

upvoted 1 times

Kyanka 1 year, 3 months ago

Selected Answer: A

A. I think the key is that it says "prevent an attacker" instead of talking about maintaining availability during an attack. That's why I think it's C instead of A.

upvoted 2 times

gjimenezf 1 year, 5 months ago

Selected Answer: A

A. Design networks with the ability to adapt, reconfigure, and fail over. Even if access controls fails, failover will prevent loss of service

upvoted 1 times

Soleandheel 1 year, 6 months ago

A. Design networks with the ability to adapt, reconfigure, and fail over.

upvoted 1 times

AMANSUNAR 1 year, 7 months ago

Selected Answer: A

Designing networks with adaptability, reconfigurability, and failover mechanisms enhances their resilience and ensures continuity of services even in the face of attacks or disruptions. This approach makes it more difficult for an attacker to disable the network by introducing redundancy and alternative paths.

upvoted 2 times

InclusiveSTEAM 1 year, 8 months ago

The answer is A

The most effective strategy to prevent an attacker from disabling a network is to design networks with adaptability, reconfigurability, and failover capabilities, option A.

Building resiliency into the network architecture provides the greatest protection against total denial of service. The network can recover and adapt.

Testing DR plans, following security guidelines, and segmentation are beneficial but alone don't prevent full denial if the design is still fragile.

While comprehensive security is crucial, a brittle design leaves no options if endpoints are still compromised. Resilient architecture assumes breaches may occur.

upvoted 2 times

aape1 1 year, 8 months ago

Selected Answer: C

C. Because A and B are reactive, not preventive. D is not going to prevent disabling the network assuming the attacker got into a VLAN and performed other attacks, such as VLAN hopping and etc...

upvoted 4 times

aape1 1 year, 8 months ago

Selected Answer: C

C. Because A and B are not reactive, not preventive. D is not going to prevent disabling the network assuming the attacker got into a VLAN and performed other attacks, such as VLAN hopping and etc...

upvoted 1 times

Bach1968 1 year, 11 months ago

Option C, "Follow security guidelines to prevent unauthorized network access," is indeed an important strategy to enhance network security. By following security guidelines and implementing measures such as strong access controls, secure authentication mechanisms, and intrusion detection systems, organizations can prevent unauthorized network access and reduce the risk of network compromise.

However, in the context of preventing an attacker from disabling a network, implementing network segmentation (Option D) is generally considered a more effective strategy. Network segmentation helps isolate different parts of the network, limiting the impact of a potential breach or attack.

While following security guidelines is crucial for overall network security, it may not provide the same level of protection against network disabling as network segmentation. It is important to implement a combination of security measures, including network segmentation, access controls, monitoring, and regular security updates, to safeguard against various threats and ensure the availability and integrity of the network.

always, it is never a one approach to perfection

upvoted 3 times

Question #95 *Topic 1*

What is the FIRST step that should be considered in a Data Loss Prevention (DLP) program?

A. Policy creation

B. Information Rights Management (IRM)

C. Data classification

D. Configuration management (CM)

Suggested Answer: *C*

Community vote distribution

C (53%) A (41%) 6%

⊟ **Peterzhang** Highly Voted 2 years, 9 months ago

The C answer is correct.From CBK:

Discovery and classification: The first stage of DLP is discovery and classification.
Discovery is the process of finding all instances of data, while classification is
the act of categorizing that data based on its sensitivity and value to the organization. While you should have classified your data as part of your information asset
inventory, many DLP tools are capable of applying signature-based logic that
determines the classification of data. In many cases, your existing classification
information can be used to "tune" the DLP to know what you consider sensitive.
Examples of classifications might include "PCI data" (or "cardholder data"),
"Social Security numbers," "PHI," and so on. Comprehensive discovery and
proper classification is critical to the effectiveness of the remaining stages and to
the success of your overall DLP implementation.

upvoted 18 times

⊟ **J_Ko** 2 months, 4 weeks ago

while I do agree with this (and chose C) the confusing thing about the question is the vague statement of A.
Does it mean enterprise wide policies the must be followed when implementing DLP, or the actual policies you configure in the product. Based on the context I kind of guessed C but there could be case for A in the wider "think like a manager" context.

upvoted 1 times

⊟ **sphenixfire** 2 years, 8 months ago

great thanks

upvoted 1 times

⊟ **jackdryan** 2 years, 1 month ago

C is correct

upvoted 1 times

⊟ **Humongous1593** Highly Voted 2 years, 9 months ago

Selected Answer: C

CBK Page 141 as PeterZhang stated word for word.

upvoted 6 times

⊟ **BigITGuy** Most Recent 3 months ago

Selected Answer: C

The first step in a Data Loss Prevention (DLP) program is always to perform data classification.

upvoted 1 times

⊟ **iRyae** 4 months, 2 weeks ago

Selected Answer: C

You need to know what data you're trying to protect (data classification) before you can create policies about how to protect it. Policies are based on the classification levels.

upvoted 2 times

99046af 5 months ago

Selected Answer: C

The first step in any Data Loss Prevention (DLP) program is to perform data classification. Data classification helps the organization understand the sensitivity and value of the data it manages, which is crucial for determining the appropriate level of protection and control needed. By classifying data, you can identify which data is critical, such as personally identifiable information (PII), financial data, or intellectual property, and ensure that it is properly protected and monitored for any potential loss or breach.

upvoted 2 times

99046af 5 months, 2 weeks ago

Selected Answer: C

Discovery/Classificattion - Monitoring - Enforcement ISC 6th Edition

upvoted 1 times

deeden 10 months, 4 weeks ago

Selected Answer: C

Data classification is essential to identify and categorize sensitive data so appropriate DLP policies and controls can be applied effectively. Without understanding what data is sensitive and where it resides, it is challenging to implement effective DLP measures.

upvoted 1 times

Ramye 1 year ago

Selected Answer: A

Policy is the first step. You can't just start classifying data without proper strategy and guidelines. Policy will direct you how the data needs to be classified based on business needs.

upvoted 3 times

Vasyamba1 1 year, 3 months ago

Selected Answer: A

First we need a policy that will tell us how data must be categorized. Data classification is just an existance of structure of classes, without the exact categorization process.

upvoted 3 times

Bach1968 1 year, 11 months ago

Selected Answer: C

C. Data classification.

Data classification involves categorizing and labeling data based on its sensitivity, value, and regulatory requirements. It is a foundational step in a DLP program as it helps organizations understand the types of data they possess, determine their data protection requirements, and prioritize their security efforts accordingly.

By classifying data, organizations can identify which data sets are more sensitive or critical and require stricter protection measures. This allows them to focus their resources on implementing appropriate DLP controls and policies to safeguard the classified data effectively. Data classification also aids in streamlining data handling processes, ensuring proper access controls, and facilitating compliance with relevant data protection regulations.

Once data is classified, organizations can proceed with subsequent steps in their DLP program, such as policy creation (Option A), information rights management (Option B), and configuration management (Option D), based on the specific needs and goals of their data protection strategy.

upvoted 2 times

NageshTiwari 2 years, 2 months ago

C. Data classification.

The first step that should be considered in a Data Loss Prevention (DLP) program is data classification. Data classification involves identifying and categorizing data according to its level of sensitivity, value, and importance. This helps to ensure that appropriate security controls and protections are put in place to safeguard the data and prevent it from being lost or stolen.

Once data has been classified, the organization can then develop policies and procedures to protect the data based on its classification. Information Rights Management (IRM) and Configuration Management (CM) are both important components of a DLP program, but they come after data classification.

In summary, data classification is the foundational step in a DLP program, and it is critical to the success of the program. Without proper data classification, it is difficult to develop effective policies and controls to protect sensitive data from loss or theft.

upvoted 2 times

⊟ **DapengZhang** 2 years, 3 months ago

Selected Answer: B

why it is not B, the 1st thing need to do is identify who shall be the owner of data, then create policy and classify the data.

upvoted 1 times

⊟ **Nickname53796** 2 years, 8 months ago

Selected Answer: A

...first you need a policy. A policy to say watermark this and that, a policy to say no PII on local machines, etc, whatever policy you want. Then this can enforce that policy

upvoted 5 times

⊟ **The_Black_One** 2 years, 9 months ago

The answer should be A - A DLP program seeks to improve information security and protect business information from data breaches. It's not just a tool; it's an approach that combines defined processes, well-informed and trained people, and effective technologies.

upvoted 2 times

⊟ **Jenkins3mol** 1 year, 1 month ago

It is the name of a product.

upvoted 1 times

⊟ **dev46** 2 years, 9 months ago

The question asks about DLP program.

A - policy would include most of the other options

upvoted 2 times

Question #96 *Topic 1*

Which change management role is responsible for the overall success of the project and supporting the change throughout the organization?

A. Change driver

B. Project manager

C. Program sponsor

D. Change implementer

Suggested Answer: *B*

Community vote distribution

C (55%) | B (35%) | 10%

⊟ **sphenixfire** Highly Voted 2 years, 8 months ago

Selected Answer: C

https://www.bmc.com/blogs/change-management-roles/

? Implementor? but never heard of it. project manager probabliy is not present because not all changes are made by a projekt

upvoted 5 times

⊟ **sphenixfire** 2 years, 8 months ago

sorry, I wanted to vote for D

upvoted 2 times

⊟ **Jamati** 2 years, 7 months ago

Seems like D is correct.

upvoted 1 times

⊟ **lsebarry** Most Recent 4 months, 1 week ago

Selected Answer: B

The project manager is primarily responsible for the overall success of a project and supporting the change throughout the organization, ensuring the project objectives are met and stakeholders are satisfied

upvoted 2 times

⊟ **somsom** 8 months ago

C program sponsor is correct

upvoted 1 times

⊟ **klarak** 1 year, 1 month ago

Selected Answer: C

A project sponsor is responsible for the overall success of a project by providing financing and supportive resources, while a project manager oversees a project's day-to-day management by managing tasks, team members, and project progress.

https://monday.com/blog/project-management/project-sponsor/#:~:text=What%20is%20a%20project%20sponsor%20vs%20project%20manager%3F,team%20members%2C%20and%20project%20progress.

upvoted 1 times

⊟ **Vasyamba1** 1 year, 3 months ago

Selected Answer: B

Implementer is not responsible for the whole project. Sponsor is just a sponsor, he is not responsible for the success of the project. Project manager does.

upvoted 1 times

⊟ **homeysl** 1 year, 3 months ago

Selected Answer: C

C are the executives supporting the change throughout the organization

upvoted 2 times

⊟ **YesPlease** 1 year, 6 months ago

Selected Answer: C

Answer C) Program Sponsor

Key phrase in question was "supporting the change throughout the organization"
Project sponsor vs. project manager:
Both the project sponsor and project manager are highly involved in the project and responsible for the outcome and success. The project sponsor is the point of connection between the organization's executive team and the project manager; the project manager is the point of connection between the project sponsor and the project team.
upvoted 1 times

Soleandheel 1 year, 6 months ago
C. Program sponsor. The program sponsor is usually a high-level individual within the organization and has a vested interest in the success of a particular program or project. They are often considered the program owner or the executive sponsor of the project. The program sponsor plays a critical role in providing overall direction, support, and resources to ensure the success of the project. Their role includes providing support, resources, and guidance, as well as influencing the selection of key project personnel like the project manager.
upvoted 2 times

AMANSUNAR 1 year, 7 months ago
Selected Answer: C
The program sponsor is typically a senior leader or executive responsible for ensuring the success of the overall program or project, including supporting the change and its implementation throughout the organization.
upvoted 1 times

Azeeza 1 year, 8 months ago
The change management role responsible for the overall success of the project and supporting the change throughout the organization is:

C. **Program sponsor.**

The program sponsor is a key leadership role in change management. They are typically a senior executive or high-ranking individual within the organization who champions the change initiative. The program sponsor provides strategic direction, secures necessary resources, and ensures that the change aligns with the organization's goals and objectives. They are responsible for the overall success of the project and play a crucial role in supporting and driving the change throughout the organization.
upvoted 2 times

homeysl 1 year, 8 months ago
Selected Answer: C
C. https://asana.com/resources/project-sponsor
upvoted 1 times

Moose01 1 year, 8 months ago
C - the sponsor!
as business owner you sponsor and pay, highering, PM and support, and if anyone slows the project or become an obstacle, you as the sponsor will have to replace her/him/them to meet your timeline and increase the budget if an unexpected unforeseen additional costs come to suffer
upvoted 2 times

[Removed] 1 year, 10 months ago
Selected Answer: C
Chat g p t says program sponsor.
upvoted 1 times

Bach1968 1 year, 11 months ago
Selected Answer: B
While the project manager (Option B) plays a crucial role in managing the project's execution, including planning, organizing, and controlling project activities, the responsibility for the overall success of the project and supporting the change throughout the organization typically falls to the program sponsor (Option C).

The program sponsor holds a broader role, providing strategic guidance and leadership to ensure the successful implementation of the desired change. They have the authority and influence to drive change at an organizational level. The program sponsor acts as a champion for the change, secures necessary resources and support, and aligns the change with the organization's goals and objectives.

the reason the responsibility fall on the PM is that not always a project or a program sponsor understand the full picture, it is the duty of the PM to guide closely the PS and enure that things are implemented. so things change from area to area.
upvoted 2 times

nat0220 2 years, 1 month ago

Project manager is the answer. question is asking about project not a program

upvoted 1 times

CCNPWILL 1 year, 2 months ago

Good Point!

upvoted 1 times

BennyMao 2 years, 1 month ago

Selected Answer: C

Program sponsor is the change management role responsible for the overall success of the project and supporting the change throughout the organization.

A program sponsor is a senior executive who has the authority and responsibility to sponsor a program and ensure that it aligns with the organization's strategic objectives. The program sponsor serves as the primary champion of the program and supports it throughout the organization by providing resources, resolving issues, and communicating the program's benefits to stakeholders.

upvoted 1 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

sausageman 2 years, 4 months ago

Selected Answer: D

The only role that's part of change magement is Change Implementer. Project Manager is not a role under the Change Management.
https://resources.infosecinstitute.com/certification/change-management-cissp/#:~:text=Roles%20and%20responsibilities&text=The%20change%20manager%20is%20the,change%2C%20and%20make%20activity%20reports.

upvoted 2 times

RVoigt 2 years, 3 months ago

Change Implementer is part of ITIL - https://www.greycampus.com/blog/it-service-management/itil-change-management-roles-and-responsibilities

upvoted 1 times

Question #97 *Topic 1*

A company needs to provide shared access of sensitive data on a cloud storage to external business partners. Which of the following identity models is the BEST to blind identity providers (IdP) and relying parties (RP) so that subscriber lists of other parties are not disclosed?

A. Proxied federation

B. Dynamic registration

C. Federation authorities

D. Static registration

Suggested Answer: *C*

Community vote distribution

A (100%)

Cww1 Highly Voted 2 years, 9 months ago

A
A proxied federation model can provide several benefits. Federation proxies can simplify technical integration between the RP and IdP by providing a common interface for integration. Additionally, to the extent a proxy effectively blinds the RP and IdP from each other, it can provide some business confidentiality for organizations that want to guard their subscriber lists from each other.

https://pages.nist.gov/800-63-3/sp800-63c.html#federation

upvoted 19 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

robervalchocolat Most Recent 9 months, 1 week ago

Proxied federation: In this model, an intermediary, known as a federation proxy, acts as a go-between between the IdP and RP. This hides the identity information of the subscribers from both parties, protecting their privacy.
Dynamic registration: This model allows users to register with a federation without having to provide their credentials to individual RPs. However, it does not necessarily hide the subscriber lists from the IdP and RP.
Federation authorities: These are entities that manage and maintain a federation of identity providers and relying parties. While they can provide security and management services, they do not necessarily protect the privacy of subscriber lists.
Static registration: This model requires users to register with each RP individually, which can be cumbersome and does not protect the privacy of subscriber lists.

upvoted 2 times

deeden 10 months, 3 weeks ago

Selected Answer: A

I don't get it. So in using direct federation (without proxy), RP and IdP can access the subscriber list from the server? Is this true, or is it just a badly worded question?

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: A

Answer A) Proxied Federation

https://pages.nist.gov/800-63-4/sp800-63c/federation/#:~:text=A%20proxied%20federation%20model,lists%20from%20each%20other.

upvoted 1 times

BestCommentorNA 1 year, 8 months ago

Selected Answer: A

A is the wAy

upvoted 2 times

Demo25 1 year, 11 months ago

Selected Answer: A

A. Proxied federation.

Proxied federation is a type of federated identity management that allows organizations to share access to resources without revealing the identities of other organizations. In proxied federation, a central identity provider (IdP) acts as a proxy for the other organizations. This means that when an organization wants to access the resources of another organization, it authenticates with the central IdP. The central IdP then authenticates with the other organization on behalf of the first organization. This way, the other organization does not know the identity of the first organization.

upvoted 2 times

⊟ **Bach1968** 1 year, 11 months ago

Selected Answer: A

A. Proxied federation.

Proxied federation is an identity model that allows the sharing of identity information between different parties while maintaining privacy and confidentiality. In this model, a proxy service acts as an intermediary between the IdPs and RPs, ensuring that sensitive subscriber lists are not disclosed to other parties.

With proxied federation, the proxy service handles the authentication and authorization process, acting as a trusted intermediary. It allows the cloud storage provider to verify the identities of external business partners without revealing sensitive information about other subscribers or relying parties. This ensures privacy and confidentiality while enabling shared access to the sensitive data.

upvoted 1 times

⊟ **NJALPHA** 2 years, 3 months ago

In a proxied federation, communication between the IdP and the RP is intermediated in a way that prevents direct communication between the two parties. There are multiple methods to achieve this effect. Common configurations include: A third party that acts as a federation proxy (or broker) • A network of nodes that distributes the communications Where proxies are used, they function as an IdP on one side and an RP on the other. Therefore, all normative requirements that apply to IdPs and RPs SHALL apply to proxies in their respective roles. A proxied federation model can provide several benefits. Federation proxies can simplify technical integration between the RP and IdP by providing a common interface for integration. Additionally, to the extent a proxy effectively blinds the RP and IdP from each other, it can provide some business confidentiality for organizations that want to guard their subscriber lists from each other. Proxies can also mitigate some of the privacy risks -- pg12 -- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63c.pdf

upvoted 1 times

⊟ **Dee83** 2 years, 5 months ago

A. Proxied federation

Proxied federation is a method of identity management that allows identity providers (IdPs) and relying parties (RPs) to communicate through a third-party service, known as a proxy. This allows the IdP and RP to remain anonymous to each other, and it helps to protect the privacy of subscriber lists.

Dynamic registration is a method of identity management that allows new IdPs and RPs to register with the system automatically. While this can be useful for managing a large number of partners, it does not provide the same level of protection for subscriber lists as proxied federation.

Federation authorities and static registration are not related to the question of protecting subscriber lists. Federation authorities are a way of managing and coordinating multiple federations, and static registration is a method of identity management that involves manually registering new IdPs and RPs with the system.

upvoted 1 times

⊟ **rootic** 2 years, 8 months ago

Selected Answer: A

Vote for A.

upvoted 3 times

⊟ **Humongous1593** 2 years, 9 months ago

Selected Answer: A

Cww1 stated, its says verbatim in the NIST doc. Its A

upvoted 4 times

Question #98 *Topic 1*

A security professional needs to find a secure and efficient method of encrypting data on an endpoint. Which solution includes a root key?

A. Bitlocker

B. Trusted Platform Module (TPM)

C. Virtual storage array network (VSAN)

D. Hardware security module (HSM)

Suggested Answer: *B*

Community vote distribution

B (44%) D (30%) A (26%)

⊟ **Arunlab** Highly Voted 👍 2 years, 7 months ago

Solution is Bitlocker and storing location is TPM..

Ans: A

upvoted 12 times

⊟ **cmakiva** 1 year, 8 months ago

Bitlocker is the only encryption method on the list

upvoted 3 times

⊟ **stickerbush1970** Highly Voted 👍 2 years, 9 months ago

Selected Answer: B

A TPM is a specific device to keep it's own keys secure (source of identity)

While an HSM is a general device to secure foreign keys (verify identity)

upvoted 6 times

⊟ **dev46** 2 years, 9 months ago

Yes - B

TPM is in-built chip on motherboard such as iPhone calls it T2 while HSM is external hardware device that can be removed. HSM usage is usually for datacentres while TPM focus on endpoint/ device/ machine.

upvoted 4 times

⊟ **jackdryan** 2 years, 1 month ago

B is correct

upvoted 1 times

⊟ **b0145c1** Most Recent 🕘 1 month, 3 weeks ago

Selected Answer: A

TPM is not an encryption solution!

upvoted 2 times

⊟ **RedMartian** 2 months, 3 weeks ago

Selected Answer: B

Not A. BitLocker is a full disk encryption tool that can use TPM to protect keys, but it does not include a root key itself — it relies on TPM for that.

Not C. VSAN is a virtualized storage infrastructure concept, not a cryptographic or key management solution.

Not D. HSM can manage root keys, but it is typically used in enterprise or server environments, not individual endpoints.

upvoted 2 times

⊟ **Kjee** 2 months, 4 weeks ago

Selected Answer: A

TPM is a hardware component that stores cryptographic keys securely, including the root key used for encryption, but by itself, it is not an encryption solution.

upvoted 1 times

⊟ **amitsir** 3 months, 1 week ago

Selected Answer: A

changing to A, just realised that the keyword is encryption. and bitlocker only provide encryption when TPM is used along with bitlocker it uses root key. but TPM itself is not a encryption method.

upvoted 1 times

amitsir 3 months, 1 week ago

Selected Answer: B

TPM is right. bitlocker can work without TPM as well. however bitlocker + TPM improves security.

upvoted 1 times

Imranbhatti 3 months, 2 weeks ago

Selected Answer: B

The solution that includes a root key is:

B. Trusted Platform Module (TPM).

A Trusted Platform Module (TPM) is a hardware-based security device that provides secure generation and storage of cryptographic keys, including root keys. It is designed to ensure the integrity of the platform and can be used to securely encrypt data on an endpoint.

While BitLocker is a robust encryption solution, it does not inherently include a root key. BitLocker works in conjunction with a Trusted Platform Module (TPM) to provide enhanced security, but the TPM is the component that generates and stores the root key. BitLocker itself is a software feature that encrypts entire volumes and relies on the TPM for secure key management.

In contrast, the TPM is specifically designed to generate, store, and manage cryptographic keys, including root keys, making it the correct answer for a solution that includes a root key.

upvoted 2 times

Edsaasa 3 months, 3 weeks ago

Selected Answer: A

The solution (Bitlocker) includes the use of a root key, which is stored in the TPM

upvoted 1 times

Rider2053 4 months, 1 week ago

Selected Answer: B

A Trusted Platform Module (TPM) is a hardware-based security feature that includes a root key stored in a secure cryptographic processor. TPM is used for encryption, secure boot, and system integrity verification. It helps in securely encrypting data on endpoints by managing encryption keys, such as those used by BitLocker in Windows.

upvoted 2 times

Bau24 4 months, 3 weeks ago

Selected Answer: A

The Bitlocker use Root Key for the encryption and stores Root key in TPM

upvoted 1 times

MustardHead 5 months, 3 weeks ago

Selected Answer: B

While BitLocker can leverage TPM for secure key storage and encryption, it does not include a root key itself. The root key comes from the TPM, not BitLocker.

upvoted 1 times

Socca 5 months, 4 weeks ago

Selected Answer: A

BitLocker is a full disk encryption feature built into Windows that uses a root key to encrypt the data on an endpoint. The root key is typically protected using a Trusted Platform Module (TPM) chip, which provides hardware-based security for the encryption keys, ensuring that they are not easily accessible or tampered with.

upvoted 1 times

RFULL 7 months, 3 weeks ago

Selected Answer: A

Bitlocker is the only encryption solution listed, and it does include a root key. TPM and HSM can store these keys.

upvoted 3 times

deeden 10 months, 3 weeks ago

Selected Answer: B

Comparison:

TPM:

Integrated into endpoint devices.

Secure storage of root keys.

Used for disk encryption (e.g., BitLocker).

Cost-effective for individual devices.

HSM:

External hardware used in server environments.

Provides high-security key management for enterprise applications.

More expensive and complex to implement on individual endpoints.

upvoted 2 times

⊟ **8b48948** 1 year, 2 months ago

HSMs are nothing to do with endpoints.

upvoted 3 times

⊟ **Vasyamba1** 1 year, 3 months ago

Selected Answer: D

OSG - A TPM is an example of a hardware security module (HSM). So, D includes B.

upvoted 2 times

Question #99 *Topic 1*

Which combination of cryptographic algorithms are compliant with Federal Information Processing Standard (FIPS) Publication 140-2 for non-legacy systems?

A. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) > 128 bits Digital Signature: Digital Signature Algorithm (DSA) (>=2048 bits)

B. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) > 128 bits Digital Signature: Rivest-Shamir-Adleman (RSA) (1024 bits)

C. Diffie-hellman (DH) key exchange: DH (<=1024 bits) Symmetric Key: Blowfish Digital Signature: Rivest-Shamir-Adleman (RSA) (>=2048 bits)

D. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) < 128 bits Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) (>=256 bits)

Suggested Answer: *B*

Community vote distribution

A (88%) 13%

⊟ **Jenkins3mol** 7 months, 3 weeks ago

Selected Answer: A

Rsa or dsa shall be over 2048 bits

So, A is correct.

upvoted 1 times

⊟ **pete79** 10 months, 4 weeks ago

B: ...This Standard specifies three choices for the length of the modulus (i.e., nlen): 1024, 2048 and 3072 bits. Federal Government entities shall generate digital signatures using one or more of these choices...

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

upvoted 1 times

⊟ **YesPlease** 1 year ago

Answer A)

DSA lengths 2048 or 3072 are recommended by NIST for lifetime key security.

upvoted 1 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: A

Option A aligns with FIPS 140-2 requirements as it includes the recommended key sizes and algorithms. It uses Diffie-Hellman (DH) key exchange with a key size of at least 2048 bits, Advanced Encryption Standard (AES) with a key size greater than 128 bits for symmetric encryption, and Digital Signature Algorithm (DSA) with a key size of at least 2048 bits for digital signatures.

upvoted 2 times

⊟ **Dee83** 1 year, 11 months ago

A. Diffie-hellman (DH) key exchange: DH (>=2048 bits) Symmetric Key: Advanced Encryption Standard (AES) > 128 bits Digital Signature: Digital Signature Algorithm (DSA) (>=2048 bits)

According to Federal Information Processing Standard (FIPS) Publication 140-2, the combination of algorithms that are compliant for non-legacy systems are:

Diffie-hellman (DH) key exchange: DH (>=2048 bits)
Symmetric Key: Advanced Encryption Standard (AES) > 128 bits
Digital Signature: Digital Signature Algorithm (DSA) (>=2048 bits)

Option A is the only one that matches these requirements for the algorithm used for DH, AES and DSA.

upvoted 2 times

⊟ **jackdryan** 1 year, 7 months ago

A is correct

upvoted 1 times

somkiatr 2 years ago

Selected Answer: A

The correct answer is A not B. FIPS 140-2 allows or approves using key length >= 2048 bit for DSA and RSA .

reference : https://cryptosense.com/blog/which-algorithms-are-fips-140-3-approved

upvoted 4 times

Firedragon 2 years, 1 month ago

Selected Answer: A

A.

https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3488.pdf

[FIPS 186-4] RSA (2048/3072 with all SHA-2 sizes)

[FIPS 186-4] DSA (1024/2048/3072 with all SHA-2 sizes)

upvoted 2 times

rootic 2 years, 2 months ago

Selected Answer: A

Agee with A.

upvoted 1 times

DracoL 2 years, 2 months ago

Selected Answer: A

FIPS140-2 approved Signature Generation

DSA – 2048-bit key length and longer which is A

RSA - RSA – 2048-bit key length and longer, with SHA1, and SHA2 with 256-bit to 512-bit key lengths. B is not correct as it uses only 1024-bit key length which is not approved especially SHA1.

upvoted 2 times

DracoL 2 years, 2 months ago

RSA signature generation – The 256-bit, 512-bit, and 1024-bit key lengths are weak. Longer key lengths are validated for FIPS 140-2.

upvoted 1 times

sphenixfire 2 years, 2 months ago

Selected Answer: A

d is out because of < AES128 (needs to be >=), C because of at least blowfish, and B because of sig-algo < 1024 (at leas 2048 needed)

upvoted 1 times

franbarpro 2 years, 2 months ago

What algorithms are compliant with FIPS 140-2? The following algorithms are compliant with FIPS 140-2:

Symmetric Key Encryption & Decryption

Advanced Encryption Standard (AES)

Triple-DES Encryption Algorithm (TDEA)

Digital Signatures

Digital Signature Standard (DSS), which includes the Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA)

Secure Hash

Secure Hash Standard (SHS), which includes Secure Hash Algorithm (SHA) 1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256

SHA-3 Standard, which includes SHA-3 hash algorithms, SHA-3 extendable output functions (XOF), and SHA-3 derived functions

Message Authentication

Triple-DES Encryption Algorithm (TDEA)

Advanced Encryption Standard (AES)

Hash-Based Message Authentication Code (HMAC)

https://www.trentonsystems.com/blog/fips-140-2-explained#:~:text=If%20a%20cryptographic%20module%20is,features%20outlined%20in%20the%20standard.

upvoted 1 times

stickerbush1970 2 years, 3 months ago

Selected Answer: B

Both AES and RSA are FIPS 140-2 compliant.

upvoted 2 times

Question #100 *Topic 1*

What is the PRIMARY purpose of creating and reporting metrics for a security awareness, training, and education program?

A. Measure the effect of the program on the organization's workforce.

B. Make all stakeholders aware of the program's progress.

C. Facilitate supervision of periodic training events.

D. Comply with legal regulations and document due diligence in security practices.

Suggested Answer: *A*

Community vote distribution

A (73%) D (27%)

Bach1968 Highly Voted 1 year, 11 months ago

Selected Answer: A

A. Measure the effect of the program on the organization's workforce.

Creating and reporting metrics for a security awareness, training, and education program allows organizations to assess the effectiveness and impact of the program on their workforce

By measuring the effect of the program, organizations can determine if their workforce is gaining knowledge, adopting desired behaviors, and applying security practices effectively.

upvoted 5 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

Not D (Comply with legal regulations and document due diligence in security practices) -
While compliance may be a benefit, the primary purpose of metrics is to ensure the program is working effectively, not just to check a compliance box.

upvoted 2 times

deeden 10 months, 3 weeks ago

Selected Answer: A

This is the primary purpose of creating and reporting metrics for a security awareness, training, and education program. By measuring the program's effectiveness, organizations can:

Demonstrate ROI: Justify the program's existence and secure continued funding.
Identify areas for improvement: Pinpoint weaknesses in training content or delivery.
Enhance security culture: Foster a culture of security awareness among employees.
While the other options are important, they are secondary to the overall goal of measuring the program's impact on the workforce.

upvoted 2 times

8b48948 1 year, 2 months ago

I dont see how it is A - how would taking metrics measure the impact the training had already had.

upvoted 1 times

shmoeee 1 year, 7 months ago

It's A, guaranteed

upvoted 2 times

invincible96 2 years, 3 months ago

Selected Answer: A

The main point here is "Primary" which makes option A the right answer.
Option D is not the primary purpose of creating and reporting metrics. While compliance with legal regulations and documenting due diligence are important, the primary purpose of metrics is to measure the effectiveness of the program in changing the behavior of the workforce.

upvoted 2 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

⊟ **RVoigt** 2 years, 3 months ago

Selected Answer: D

Remember its creating and reporting - only D works with creating ...

upvoted 4 times

⊟ **[Removed]** 1 year, 10 months ago

I read it as creating metrics and reporting metrics.

upvoted 1 times

⊟ **meelaan** 2 years, 6 months ago

Selected Answer: A

A sounds good

upvoted 3 times

⊟ **Jamati** 2 years, 7 months ago

A sound correct

upvoted 2 times

⊟ **franbarpro** 2 years, 8 months ago

Yep "A" sounds like a PRIMARY reason

upvoted 2 times

Question #101 *Topic 1*

In a DevOps environment, which of the following actions is MOST necessary to have confidence in the quality of the changes being made?

A. Prepare to take corrective actions quickly.

B. Automate functionality testing.

C. Review logs for any anomalies.

D. Receive approval from the change review board.

Suggested Answer: *D*

Community vote distribution

D (50%) B (48%)

RVoigt Highly Voted 2 years, 3 months ago

Selected Answer: B

CISSP Official Study Guide pg 966 "...organizations using the DevOps model often deploy code several times per day. Some organizations even strive to reach the goal of continuous integration/continuous delivery (CI/CD), where code may roll out dozens or even hundreds of times per day. This requires a high degree of automation, including integrating code repositories, the software configuration management process, and the movement of code between development, testing, and production environments."

upvoted 16 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

Soleandheel 1 year, 6 months ago

Thanks for sharing. You're 100% correct.

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: B

Not D. Change review boards (CRB) are less common in DevOps due to automation and CI/CD pipelines replacing traditional change approval processes.

upvoted 1 times

[Removed] 11 months, 1 week ago

Selected Answer: B

Option D , is indeed a critical step in change mgmt. However, in the context of having confidence in the "quality" of changes being made in a DevOps environment, automated functionality testing (Option B) is typically seen as more directly related. You can then submit your request for change to the CAB knowing that you`ve done the due diligence through testing prior to submittal . Also you may refer to the Official study guide page 966 as RVoigt suggested.

upvoted 2 times

Ramye 1 year, 1 month ago

Selected Answer: B

Change management is critical to vet for changes to go to production, and changes in production does not happen frequently.

On the other hand, in DevOps environments, changes happen frequently which needs thorough testing before they can go to production, so it's not ideal to go to Change Board frequently for these type of changes.

upvoted 1 times

73f8ac3 1 year, 2 months ago

Selected Answer: B

Devops means frenquent changes.

CAB is good - and necessary, but a CAB done too often, sometimes several time a week will not guarantee anything on the quality of the change.

Automated functional tests on the other hand, allows you to be reactive on the change, before and after.

upvoted 1 times

marziparzi 1 year, 3 months ago

Strongly torn between B and D, but I'm leaning towards B because of it being DevOps

upvoted 2 times

homeysl 1 year, 3 months ago

Selected Answer: D

Testing is part of the approval process. CAB won't approve CR if it's not tested.

upvoted 1 times

gjimenezf 1 year, 5 months ago

Selected Answer: B

As CI/CD makes multiples changes is very important to test if functionality is not broken because of a change

upvoted 1 times

Soleandheel 1 year, 6 months ago

B. Automate functionality testing. In DevOps, the emphasis is on automation, continuous integration, and continuous delivery (CI/CD) processes. Automated testing provides immediate feedback to development teams, helping them catch and fix issues early in the development process, reducing the likelihood of introducing defects into the production environment.

upvoted 2 times

thanhlb 1 year, 8 months ago

Selected Answer: B

ACD are more relevant to monitoring and evaluating the changes after they are deployed

upvoted 3 times

homeysl 1 year, 8 months ago

Selected Answer: D

D. Think like a manager.

upvoted 3 times

> **Ramye** 1 year, 1 month ago
>
> Not all thinking like manager is correct / appropriate.
>
> Do what is should be the correct steps or process.
>
> upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: D

In a DevOps environment, receiving approval from the change review board (option D) can indeed be an important step to ensure confidence in the quality of changes being made. The change review board plays a vital role in reviewing and approving changes to be deployed to the production environment.

By obtaining approval from the change review board, organizations can ensure that changes have undergone thorough review and evaluation, including considerations for potential impacts on security, stability, compliance, and overall alignment with the organization's objectives.

While automating functionality testing (option B) is also a crucial aspect of DevOps to validate changes, it is not the only factor in ensuring confidence in the quality of changes. A holistic approach that includes various practices, such as automated testing, change approval, monitoring, and continuous feedback, is typically necessary for achieving a high level of confidence in the quality of changes in a DevOps environment.

Therefore, both options D (receiving approval from the change review board) and B (automating functionality testing) are important considerations, and the specific importance may vary depending on the organization's processes and requirements.

upvoted 4 times

Andy880 2 years, 1 month ago

Selected Answer: D

D.
The Change Review Board (CRB) assists in the assessment and prioritization of changes and approves requested changes...Ensure that all changes adhere to quality requirements (i.e. testing is completed, roll-back plans are in place etc.)

upvoted 4 times

> **Andy880** 2 years, 1 month ago
>
> https://kb.mit.edu/confluence/pages/viewpage.action?pageId=155261648
>
> upvoted 4 times

crazywai1221 2 years, 2 months ago

Selected Answer: D

approval come first

upvoted 2 times

sausageman 2 years, 4 months ago

Answer is B. In DevOps the changes doesn't go through the CAB that's why you need to make sure the quality of the changes are good

upvoted 2 times

Qwertyloopback 2 years, 4 months ago

Selected Answer: B

According to CISSP 9th ed., DevOps and DevSecOps move to frequent code reviews, multiple daily. Although it is not clearly defined in this text, the only practical answer listed would be B. To keep up with multiple code submissions daily the testing needs to be automated to prevent bottlenecking by security and code reviews.

upvoted 2 times

somkiatr 2 years, 6 months ago

Selected Answer: B

A successful DevOps testing strategy is one aimed at building, testing and releasing software faster and more frequently. If you're lucky enough to start out i "greenfield" organization without an established coding culture, it's a good idea to try to create and automate your software delivery pipeline upfront. If you're successful out-of-the-gate in creating a Continuous Delivery DevOps pipeline, your business will be much more competitive since you'll be able to get higher-quality software into the hands of your users and customers faster than your competitors, and you'll be able to react to business demand and change much n rapidly.

reference : https://smartbear.com/blog/devops-testing-strategy-best-practices-tools/#:~:text=A%20successful%20DevOps%20testing%20strategy%20is%20one%20aimed%20at%20building,your%20software%20delivery%20pipeline%20up

upvoted 2 times

somkiatr 2 years, 6 months ago

Why is not D (CAB) ? Please read this --> https://kaimarkaru.medium.com/cab-in-the-age-of-devops-dd6f03b12af8

upvoted 2 times

Question #102 *Topic 1*

What is the MAIN purpose of a security assessment plan?

A. Provide education to employees on security and privacy, to ensure their awareness on policies and procedures.

B. Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.

C. Provide guidance on security requirements, to ensure the identified security risks are properly addressed based on the recommendation.

D. Provide technical information to executives to help them understand information security postures and secure funding.

Suggested Answer: *B*

Community vote distribution

B (89%) 11%

YesPlease 1 year ago

Selected Answer: B

Answer B)

Keyword in question is "plan" and the only sentence that refers to a plan is "The objectives for the control assessments and a detailed roadmap of how to conduct such assessments."

upvoted 3 times

Bach1968 1 year, 5 months ago

Selected Answer: B

The MAIN purpose of a security assessment plan is:

B. Provide the objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.

A security assessment plan outlines the objectives, scope, methodology, and approach for conducting security and privacy control assessments within an organization. Its primary purpose is to provide a clear roadmap and guidance on how to assess and evaluate the effectiveness of security controls in place.

upvoted 2 times

HughJassole 1 year, 6 months ago

B: "The objectives for the control assessments and a detailed roadmap of how to conduct such assessments."
https://csrc.nist.gov/glossary/term/assessment_plan

upvoted 3 times

HughJassole 1 year, 7 months ago

Def B:
https://csrc.nist.gov/glossary/term/assessment_plan

upvoted 4 times

SSimko 11 months ago

Agreed, it is literally the definition.

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: B

Clearly the answer is B here. Before conducting a security assessment, you need to know the objectives of that assessment, and all objectives must be SMART (Specific, Measurable, Attainable/Achievable, Relevant, Time-bound).

upvoted 2 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

Rollizo 2 years, 3 months ago

the key here is "plan": security assessment plan => objectives

upvoted 2 times

dev46 2 years, 3 months ago

B could be right, but D sounds right too

I have been engaged with a few initiatives where executives want to conduct security assessments and see if it's financially viable to kick off the project or not.

upvoted 3 times

franbarpro 2 years, 2 months ago

It cannot be "D" - CEOs pay us to translate technical info into the lengo they understand.

upvoted 2 times

CuteRabbit168 2 years, 3 months ago

Selected Answer: B

Answer is correct

upvoted 3 times

DERCHEF2009 2 years, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

DERCHEF2009 2 years, 3 months ago

Sorry B

upvoted 4 times

Question #103 *Topic 1*

What documentation is produced FIRST when performing an effective physical loss control process?

A. Deterrent controls list

B. Security standards list

C. Asset valuation list

D. Inventory list

Suggested Answer: *C*

Community vote distribution

D (72%) C (28%)

Cww1 Highly Voted 👍 2 years, 3 months ago

I would go D, you need to inventory assets before you can value them.

upvoted 14 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

Dave709 Highly Voted 👍 2 years, 3 months ago

Selected Answer: D

Inventory first

upvoted 10 times

BigITGuy Most Recent 🕘 3 months ago

Selected Answer: D

Can't be C. Asset valuation list is important but is created after you have the inventory.

upvoted 1 times

25cbb5f 8 months, 4 weeks ago

Selected Answer: C

The correct answer is C. Asset valuation list. Here's the reasoning:

Physical Loss Control Process: This process aims to protect an organization's physical assets from various threats like theft, damage, or natural disasters.
Importance of Asset Valuation: Before implementing any protective measures, it's crucial to understand what needs to be protected and the value of those assets. An asset valuation list provides a detailed inventory of assets along with their estimated financial worth.
Why other options come later:
Inventory List (D): While an inventory list is essential, it doesn't include the critical valuation component necessary to prioritize loss control measures.
Security Standards List (B): Standards are developed based on understanding your assets and determining appropriate security controls.
Deterrent Controls List (A): Deterrent controls are designed to discourage potential threats, a step that comes after asset valuation.

upvoted 3 times

e58c193 8 months, 4 weeks ago

Selected Answer: D

You can't value assets that you have no inventory of.

upvoted 1 times

GuardianAngel 10 months, 3 weeks ago

Selected Answer: D

Inventory list.
https://www.cisa.gov/sites/default/files/publications/isc-planning-managing-physical-security-resources-dec-2015-508.pdf Section: 4 Resource Requirements

upvoted 2 times

pete79 10 months, 4 weeks ago

Selected Answer: D

Inventory must exist in first place

upvoted 1 times

⊟ **YesPlease** 1 year ago

Selected Answer: D

Answer D) Inventory List

This is a Chicken-or-the-Egg scenario. Asset Valuation is the first step in the process...but it can not be started without first creating an inventory list of assets and then go through the process of putting a value on it.

https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model

upvoted 1 times

⊟ **Wz21** 1 year, 1 month ago

The key security management practices necessary to assess risk can be broken into six broad steps :

1. Asset identification
2. Risk assessment (Asset Valuation)
3. Policy development
4. Implementation
5. Training and education

upvoted 1 times

⊟ **Wz21** 1 year, 1 month ago

Answer is A. Inventory list (Asset Identification)

upvoted 1 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: C

the documentation produced FIRST when performing an effective physical loss control process is:

C. Asset valuation list.

The asset valuation list is an essential document in the physical loss control process. It involves assessing the value of an organization's assets, including equipment, inventory, facilities, and resources. The asset valuation helps determine the importance and worth of each asset, which in turn assists in prioritizing security measures based on their value and criticality.

By creating an asset valuation list as the first step, organizations can identify high-value assets that require enhanced protection and allocate resources accordingly. This list provides a foundation for implementing appropriate physical security measures and helps guide decision-making in risk management and loss prevention strategies.

upvoted 4 times

⊟ **Ramye** 6 months, 4 weeks ago

Agree.
This valuation is also important to gauge how much it would cost to put the necessary controls. If the cost of controls is higher than what would be protected then why spending more and just accept the risk and move on.

upvoted 1 times

⊟ **Dee83** 1 year, 11 months ago

D. Inventory list
The first step in an effective physical loss control process is to conduct an inventory of the organization's assets. This includes identifying, cataloging, and valuing all physical assets that are important to the organization. The inventory list should include a description of each asset, its location, and its value. This information is used to identify the most critical assets that need to be protected and to prioritize security measures. The inventory list serves as the foundation for the rest of the physical loss control process, providing a clear understanding of the assets that need to be protected and the potential risks that they may face.

upvoted 2 times

⊟ **Delab202** 1 year, 12 months ago

I figured out why most of the answers on this website are wrong.

upvoted 1 times

⊟ **assmaalick** 1 year, 6 months ago

why is that?

upvoted 1 times

⊟ **somkiatr** 2 years ago

Selected Answer: C

I choose C. The effective physical loss control process is knowing the asset value to calculate the loss expectancy (ALE = SLE x ARO and SLE = Asset Value x Exposure Factor)

upvoted 2 times

⊟ **oudmaster** 2 years ago

I believe the key in the question here is word "effective":

(effective physical loss control process).

!

Asset valuation should be the answer. Because this list is not any list, but it is driven from risk analysis process.

upvoted 5 times

⊟ **Jamati** 2 years, 1 month ago

Selected Answer: D

Answer is D. This is all part of ITAM (IT Asses Management).

upvoted 2 times

⊟ **rootic** 2 years, 2 months ago

Selected Answer: D

Agree with D.

upvoted 1 times

⊟ **IXone** 2 years, 2 months ago

Asset Identification, Valuation and Categorization of information systems assets are critical tasks of the process to properly develop and deploy the required security control for the specified IT assets.

Assett Valutation include the value of an asset depends on the sensitivity of data inside the container and their potential impact on CIA, effective keyword I think it's correct C

upvoted 1 times

Question #104 *Topic 1*

Which organizational department is ultimately responsible for information governance related to e-mail and other e-records?

A. Legal

B. Audit

C. Compliance

D. Security

Suggested Answer: *A*

Community vote distribution

A (70%) C (30%)

BigITGuy 3 months ago

Selected Answer: A

Legal has the duty to ensure that records management complies with laws, regulations, and litigation requirements, and e-records are properly retained, archived, and disposed of according to legal obligations.

upvoted 1 times

d7034bf 6 months, 3 weeks ago

Selected Answer: A

Legal is the answer. The dept plays a crucial role in information governance (IG) as it is responsible for ensuring that an organization's data management practices comply with relevant laws and regulations, including data privacy, security, and retention policies, making legal expertise essential for developing and enforcing effective IG strategies.

upvoted 1 times

1460168 11 months ago

Selected Answer: A

Legal is a department, compliance not.

upvoted 2 times

Ramye 1 year, 1 month ago

In theory it my be Legal but in reality this department does not get involve For information governance for email or e-records unless or until there's a litigation situation. In reality it is the compliance team that is responsible for to be compliant in these.

For the sake of CISSP the answer could be Legal as many said but a confirmed answer needed to be sure.

upvoted 2 times

Jenkins3mol 1 year, 1 month ago

None of them is ultimately responsible

How can legal, security, compliance working on 2nd line of defence being held ultimately responsible? Especially legal and compliance.

Who operationally maintains and works on these e-file then who are ultimately accountable.

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: A

OSG p912 - In legal proceedings, each side has a duty to preserve evidence related to the case and, through the discovery process, share information with their adversary in the proceedings. This discovery process applies to both paper records and electronic records, and the electronic discovery (or eDiscovery) process facilitates the processing of electronic information for disclosure.

The Electronic Discovery Reference Model (EDRM) describes a standard process for conducting eDiscovery with nine aspects:

1. Information Governance - Ensures that information is well organized for future eDiscovery efforts.

upvoted 1 times

gjimenezf 1 year, 5 months ago

Selected Answer: A

Information governance helps with legal compliance, operational transparency, and reducing expenditures associated with legal discovery.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: A

Answer A) Legal

While data governance focuses mostly on the technical aspects of data handling, information governance takes a broader approach by incorporating legal, regulatory, and strategic considerations.

https://www.epiqglobal.com/en-us/resource-center/articles/data-governance-vs-information-governance#:~:text=While%20data%20governance%20focuses%20mostly,information%20as%20a%20valuable%20asset.

upvoted 1 times

homeysl 1 year, 8 months ago

Selected Answer: A

They are authorized to do e-discovery and also work on regulatory compliance.

upvoted 1 times

cmakiva 1 year, 8 months ago

Selected Answer: A

I have never worked somewhere with a "compliance" department

upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: A

A. Legal.

The legal department is ultimately responsible for information governance related to e-mail and other electronic records within an organization. This responsibility includes establishing policies, procedures, and guidelines for the proper management, retention, and disposal of electronic records in compliance with applicable laws, regulations, and industry standards. The legal department ensures that the organization maintains legal and regulatory compliance regarding e-records, including e-mail communications. They also handle any legal matters related to e-records, such as e-discovery requests or litigation involving electronic evidence.

upvoted 3 times

Firedragon 2 years, 7 months ago

Selected Answer: A

A.
https://www.ironmountain.com/resources/general-articles/w/who-really-owns-your-information-governance-program
Every IG program needs a Jeter—a senior executive who typically works in the legal, IT, compliance or risk management department.
Player #1: The Legal Eagle. Your legal team's IG role is to determine your firm's ongoing profile based on (among other factors):

upvoted 4 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

rootic 2 years, 8 months ago

Selected Answer: C

Vote for C

upvoted 2 times

rdy4u 2 years, 8 months ago

Selected Answer: C

An organization often requires information governance during a lawsuit or some other consequence of noncompliance. On such occasions, compliance teams must go through potentially millions of pages of documents -- and possibly even more rows of data -- in pursuit of information that has been requested for legal purposes. This process, also called electronic discovery (e-discovery), is daunting even when things are at their most orderly. It can become a nightmare if the organization's information is not well ordered and readily discoverable.

https://www.techtarget.com/searchcio/definition/information-governance

upvoted 4 times

somkiatr 2 years, 6 months ago

I agree with A. A Company implements an information governance (IG) program to improve operational transparency and achieve legal and regulatory compliance. Legal party is ultimate responsible for any types of the information.

upvoted 2 times

Question #105 *Topic 1*

A cloud service provider requires its customer organizations to enable maximum audit logging for its data storage service and to retain the logs for the period of three months. The audit logging gene has extremely high amount of logs. What is the MOST appropriate strategy for the log retention?

A. Keep all logs in an online storage.

B. Keep last week's logs in an online storage and the rest in an offline storage.

C. Keep last week's logs in an online storage and the rest in a near-line storage.

D. Keep all logs in an offline storage.

Suggested Answer: *B*

Community vote distribution

C (60%) B (40%)

dev46 Highly Voted 2 years, 3 months ago

B is right

Near line is ideal if you want to access the data (at least once a month) but for pure retention purpose, off-line is cost-effective option

upvoted 10 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 2 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: C

Offline storage would make older logs difficult and slow to access.

upvoted 1 times

Jenkins3mol 7 months, 3 weeks ago

Selected Answer: B

Nearline for 30 days, coldline for 90 days

https://cloud.google.com/storage/docs/storage-classes

https://cloud.google.com/storage/docs/storage-classes?hl=zh-cn

upvoted 1 times

73f8ac3 8 months, 3 weeks ago

Selected Answer: C

For cloud storage, there are two things to keep in mind :

- Offline storage is cheap, but it can become costly if you need to access it, also for offline, 3 months is short, so there might be penalties there if you access or delete the data before one year
- on the other hand, nearline allows you to retrieve the data with very little or no additional costs when it is in a short period like 3 months.

3 months is an appropriate period for a nearline storage, so C is my choice

upvoted 1 times

pete79 10 months, 4 weeks ago

Selected Answer: B

As it gives access to recent logs while keeping older offline, log availability is not demanded, just preservation is must to follow.

upvoted 1 times

DapengZhang 1 year, 1 month ago

Selected Answer: C

i prefer to C. "last week" is not far away from now, due to business purpose you may need these data frequently, Repeated calls of offline data are instead a cost!

upvoted 1 times

BenjamineSB 1 year, 4 months ago

Selected Answer: C

This option is the most balanced. Logs from the last week (which are the most likely to be immediately accessed for recent incidents or issues) are kept readily available online. The older logs, which might be accessed less frequently but still within a reasonable time frame, are kept in near-line storage, which offers a compromise between accessibility and cost.

upvoted 4 times

⊟ **Mike4649** 1 year, 4 months ago

Agree with C

upvoted 1 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: B

B. Keep last week's logs in an online storage and the rest in an offline storage.

upvoted 1 times

⊟ **HughJassole** 1 year, 6 months ago

D. The question doesn't say anything about needing to access the logs, just to retain. Keep them all in offline. What significance does the past week play? In my experience none.

upvoted 1 times

⊟ **HeadAttacks** 1 year, 11 months ago

This is a strange question. Cost of storage types matters a lot, very hard to say what is most appropriate without more information. Must know the frequency of log reviews as well.

upvoted 3 times

⊟ **meelaan** 2 years ago

Selected Answer: B

B sounds good

upvoted 1 times

Question #106 *Topic 1*

In Federated Identity Management (FIM), which of the following represents the concept of federation?

A. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories or applications

B. Collection of information logically grouped into a single entity

C. Collection of information for common identities in a system

D. Collection of domains that have established trust among themselves

Suggested Answer: *A*

Community vote distribution

D (79%) A (21%)

⊟ **mrgod** Highly Voted 2 years, 3 months ago

Selected Answer: D

The core thing of Federate is Trust among themselves.

upvoted 16 times

⊟ **jackdryan** 1 year, 7 months ago

D is correct

upvoted 1 times

⊟ **BigITGuy** Most Recent 2 months, 4 weeks ago

Selected Answer: D

Not A -- describes identity lifecycle management, not federation.

upvoted 1 times

⊟ **pete79** 10 months, 4 weeks ago

Selected Answer: A

We're talking about already established federation and ask is what defines FIM

upvoted 1 times

⊟ **YesPlease** 1 year ago

Selected Answer: D

Answer D)

Federated identity management is a configuration that can be made between two or more trusted domains to allow consumers of those domains to access applications and services using the same digital identity

https://www.loginradius.com/blog/identity/federated-identity-providers/

upvoted 1 times

⊟ **Socca** 1 year, 2 months ago

Federated identity management, also known as federated SSO, refers to the establishment of a trusted relationship between separate organizations and third parties, such as application vendors or partners, allowing them to share identities and authenticate users across domains.

upvoted 1 times

⊟ **Socca** 1 year, 2 months ago

So D is correct answer

https://www.pingidentity.com/en/resources/blog/post/sso-vs-federated-identity-management.html#:~:text=Federated%20identity%20management%2C%20also%20known,and%20authenticate%20users%20across%20domains.

upvoted 2 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: A

in Federated Identity Management (FIM), the concept of federation involves the collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories, or applications.

A. Collection, maintenance, and deactivation of user objects and attributes in one or more systems, directories, or applications represents the concept of federation in FIM. It involves establishing trust relationships and mechanisms for securely exchanging user identity information across different systems or applications.

upvoted 1 times

HughJassole 1 year, 7 months ago

A appears to be correct since this has to do with Identity, aka users:
Federated identity allows authorized users to access multiple applications and domains using a single set of credentials.

https://www.onelogin.com/learn/federated-identity

upvoted 1 times

Dee83 1 year, 11 months ago

D. Collection of domains that have established trust among themselves represents the concept of federation in Federated Identity Management (FIM).

In FIM, federation is the process of connecting multiple domains or systems together, so that they can share and trust each other's identities. This enables users to access different systems and applications using a single set of credentials, without the need for multiple usernames and passwords. By establishing trust among domains, FIM enables a seamless and secure flow of identity information across multiple systems and organizations, allowing users to access resources they are authorized to access, with out the need to authenticate each time they access a new resource.

upvoted 1 times

Ivanchun 2 years ago

Selected Answer: A

One or more Directory = Federation

upvoted 1 times

oudmaster 2 years ago

Selected Answer: D

CISSP All-In-One Exam Guide 9th Edition:
!
User provisioning refers to the creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes. User provisioning software may include one or more of the following components: change propagation, self-service workflow, consolidated user administration, delegated user administration, and federated change control.
User objects may represent employees, contractors, vendors, partners, customers, or other recipients of a service. Services may include e-mail, access to a database, access to a file server or database, and so on.
!
So option A is a definition of User provisioning.

upvoted 3 times

Firedragon 2 years, 1 month ago

Selected Answer: A

A.
https://www.onelogin.com/learn/federated-identity
Federated Identity Management (FIM) – works on the basis of mutual trust relationships between a Service Provider (SP) such as an application vendor and an external party or Identity Provider (IdP).

upvoted 2 times

Jamati 2 years, 1 month ago

Selected Answer: D

D is correct.
FIM extends beyond a single organization. Multiple organizations can join a federation or group, where they agree to share identity information. Users in each organization can
log on once in their own organization, and their credentials are matched with a federated
Implementing Identity Management system. They can then use this federated identity to access resources in any other organization within the group.
A federation can be composed of multiple organizations sharing resources, or any other group that can agree on a common federated identity management system.
CISSP official study guide 9th edition - page 660

upvoted 2 times

juniorhs86 2 years, 1 month ago

Selected Answer: A

FIM is and can be used between multiple apps and domains

upvoted 2 times

rootic 2 years, 2 months ago

Selected Answer: D

Vote for D.

upvoted 1 times

franbarpro 2 years, 2 months ago

Selected Answer: D

Def. "D" Single Sign-On (SSO) = Trust

upvoted 3 times

Mgz156 2 years, 3 months ago

Answer is A. Please do not confuse with AD Federation with Federated Identity. Federated identity management systems offer single access to a number of applications across various enterprises.

upvoted 4 times

dev46 2 years, 3 months ago

D is right

upvoted 1 times

Question #107 *Topic 1*

Which of the following is an indicator that a company's new user security awareness training module has been effective?

A. There are more secure connections to internal e-mail servers.

B. More incidents of phishing attempts are being reported.

C. Fewer incidents of phishing attempts are being reported.

D. There are more secure connections to the internal database servers.

Suggested Answer: *C*

Community vote distribution

B (72%) C (28%)

Cww1 Highly Voted 2 years, 9 months ago

Its B not C

upvoted 16 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

DERCHEF2009 2 years, 9 months ago

Agree with B

upvoted 1 times

dev46 2 years, 9 months ago

Tricky options B & C - I ended up choosing C, but B is right

The whole idea of awareness training is to change user behaviour. When more incidents are reported, it's a good indicator that users are security aware and taking the right action

upvoted 9 times

cysec_4_lyfe Most Recent 4 months, 1 week ago

Selected Answer: B

You want more engagement and to crowd-source email security. More incidents reported = more chance to remediate from other user's inbox.

upvoted 2 times

Ramye 1 year ago

Selected Answer: B

You have to wonder who/how ExamTopics answering these questions! It appears they didn’t even do simple research for providing answers.

upvoted 2 times

deeden 10 months, 3 weeks ago

I think most answers are purposely incorrect in order to inspire collaboration. :)

upvoted 2 times

nelombg 1 year, 3 months ago

It's a tricky QUESTION, but the answer is B.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: B

Answer B) More...

If users are more aware, then they should be reporting MORE instances of phishing attempts.

upvoted 2 times

Soleandheel 1 year, 6 months ago

C. Fewer incidents of phishing attempts are being reported. For those selecting B, you are mistaken. I understand your logic, you're thinking that employees will report more phishing attemps when they are more away but your approach of looking at it is flawed. When an awareness program is effective, employees will have fewer security incidents. There is a difference between a security event and a security incident. An incident usually means that the phishing event was successful and as such an incident that needs to be contained or mitigated. C. is the correct answer because fewer incidents will be reported because the phishing attempt events will not be successful to become incidents. I hope this makes sense to you. You have to be able to distinguish between a phishing event and a phishing incident. There is a difference between an event and an incident. Not all security events are incidents.

upvoted 4 times

YesPlease 1 year, 6 months ago

I would agree with you if the word "ATTEMPT" was not in the answers provided. Just getting a phishing email is considered an incident, but not a bad one if the attempt failed to get the user to click on the email content and it was reported instead.

upvoted 3 times

homeysl 1 year, 8 months ago

Selected Answer: B

B. This is the goal of phishing awareness program.

upvoted 2 times

Socca 1 year, 8 months ago

B is correct

The objective of awareness training is to change user behavior and if the number of phising incident that have reported is increased means that the awareness program has succeeded

upvoted 1 times

LalithW 1 year, 8 months ago

Here most of the people have misunderstood the word Incident and have voted for C.

According to NIST, an Incident is An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Simply, a security incident is an event that may indicate that an organization's systems or data have been compromised.

So fewer incidents of phishing attempts are being reported means that the awareness training are success.

upvoted 2 times

Soleandheel 1 year, 6 months ago

You are right! Which means the correct answer is C. not B. ....C. Fewer incidents of phishing attempts are being reported. "People have misunderstood the word incident and have voted for B".

upvoted 1 times

georgegeorge125487 1 year, 10 months ago

Selected Answer: B

More aware means being able to identify and report.

upvoted 2 times

akinmoyeroolu 1 year, 10 months ago

C. Fewer incidents of phishing attempts are being reported.

An effective security awareness training module should lead to a decrease in successful phishing attempts, as users become more vigilant and cautious about identifying and reporting phishing attempts.

upvoted 1 times

MShaaban 1 year, 10 months ago

I go with B. After users awareness they are to be more vigilant and report more incidents. Whether those incidents are true or not it is a different story, but the fact they are more suspicious and they would report more incidents.

upvoted 1 times

benllp_sst 1 year, 11 months ago

Selected Answer: C

The incident is the keywords. Fewer incident means successful phishing reduced.

upvoted 1 times

benllp_sst 1 year, 11 months ago

B is correct, mixed up "incident" and "accident"

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: C

C. Fewer incidents of phishing attempts are being reported.

upvoted 1 times

⊟ **ap0ls** 1 year, 3 months ago

Agree with this logic

upvoted 1 times

⊟ **HughJassole** 2 years ago

Sure seems like B. I get these phishing emails at work and click on "report phishing". Although, I now just ignore them since it's obvious to me this is phishing. My employer doesn't care though, but others take the report very seriously and can terminate you if you ignore. So this question actually has both B and C as answers, depending on the situation.

upvoted 1 times

⊟ **dmo_d** 2 years, 1 month ago

C is correct.

It's all about wording.

"fishing attempts" leads us to answer B. But the scenario does not state if these attempts were successful or not.

The word "incident" is the key. An incident indicates that the security event "fishing attempt" already had an negative effect on the organization - the fishing attempt was successful.

This is why a successful awareness campaign should lead to FEWER incidents.

upvoted 3 times

⊟ **dumdada** 2 years ago

You missed it. More are being REPORTED which means users now recognize phishing attempts and report them, which means the training was good. It's B.

upvoted 1 times

⊟ **csco10320953** 2 years, 3 months ago

It would be C ,Since ,it is effective result

upvoted 1 times

Question #108 *Topic 1*

An organization is trying to secure instant messaging (IM) communications through its network perimeter. Which of the following is the MOST significant challenge?

A. IM clients can interoperate between multiple vendors.

B. IM clients can run as executables that do not require installation.

C. IM clients can utilize random port numbers.

D. IM clients can run without administrator privileges.

Suggested Answer: *A*

Community vote distribution

C (80%) A (20%)

⊟ **stickerbush1970** Highly Voted 👍 2 years, 3 months ago

Selected Answer: C

C. IM clients can utilize random port numbers.
Through the perimeter lends me to think they are asking for firewall ports to open

upvoted 10 times

⊟ **dev46** 2 years, 3 months ago

IM clients are capable of the tunnel through a firewall. Most IM clients use well-known ports, but they can easily exploit open firewall ports.

Although the other risk is not in the options file transfer and sending links is the most considerable risk for IM apps. Anyone can send a link or transfer a file with a worm/ virus/ trojan.

Considering available options, C sounds right.

upvoted 1 times

⊟ **jackdryan** 1 year, 7 months ago

C is correct

upvoted 1 times

⊟ **JAckThePip** Highly Voted 👍 2 years, 2 months ago

Answer is C

"IM clients find ways to tunnel through firewalls, creating risk. Most IM services come through well-publicized ports (5190 for AOL Instant Messenger, 1863 for MSN and 5050 for Yahoo), but IM clients also can exploit any open port on the firewall, including those used by other applications (such as Port 80 for Web and HTTP traffic). Some clients also can connect via peer-to-peer connections or establish connections on randomly negotiated ports."

https://www.networkworld.com/article/2323048/top-5-im-security-risks.html

upvoted 5 times

⊟ **BigITGuy** Most Recent 🕘 2 months, 4 weeks ago

Selected Answer: C

Many IM clients are designed to bypass firewalls by using random or dynamic port numbers.

upvoted 1 times

⊟ **murphseal** 8 months, 4 weeks ago

Selected Answer: C

C. IM clients can utilize random port numbers.

Random port numbers can make it difficult for traditional security measures to effectively control and secure IM traffic, as they can bypass standard port-based security policies. This can pose a significant challenge in monitoring and securing IM communications within the network perimeter.

upvoted 1 times

⊟ **YesPlease** 1 year ago

Selected Answer: C

Answer C)

Network perimeter usually refers to firewall

upvoted 1 times

AMANSUNAR 1 year, 1 month ago

Selected Answer: A

Interoperability between IM clients from multiple vendors can pose a challenge because it often involves different protocols and standards. Ensuring security across diverse platforms and protocols can be complex, and vulnerabilities in one vendor's implementation can potentially affect the security of the entire communication system.

upvoted 2 times

MShaaban 1 year, 4 months ago

I go with B. After users awareness they are to be more vigilant and report more incidents. Whether those incidents are true or not it is a different story, but the fact they are more suspicious and they would report more incidents.

upvoted 1 times

MShaaban 1 year, 4 months ago

Commented in the wrong question.

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: A

option A is the most significant challenge in securing instant messaging (IM) communications through the network perimeter.

A. IM clients can interoperate between multiple vendors.

The ability of IM clients to interoperate between multiple vendors poses a significant challenge for securing IM communications. Different IM clients may use different protocols, encryption methods, or security features, making it difficult to enforce consistent security measures across all IM communications. It requires careful configuration, compatibility testing, and ongoing monitoring to ensure that security controls are effective in a heterogeneous IM environment.

upvoted 2 times

jens23 1 year, 6 months ago

This question would be appropriate 10 years ago.

Modern firewall solutions identify applications based on signatures and behavioural analysis, port based security is a pretty outdated concept, but in the context of this question, C is correct. If there was the option of simply switching the network on the phone from Wi-Fi to LTE/5G, I wouldn't hesitate to choose that option, because this would circumvent the entire security perimeter.

upvoted 1 times

Dee83 1 year, 11 months ago

C. IM clients can utilize random port numbers.

The use of random port numbers by IM clients can make it difficult to secure the organization's network perimeter. Because IM clients can use any available port, it can be challenging for network administrators to identify and block IM traffic. This makes it difficult to ensure that all IM traffic is being properly monitored and controlled, increasing the risk that sensitive information could be leaked or that malware could spread through the network. In addition, the use of random port numbers can allow IM clients to bypass firewalls and intrusion detection systems, making it harder to detect and prevent unauthorized access to the network.

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: C

It's easier to secure something that uses known or fixed port numbers.

upvoted 1 times

rootic 2 years, 2 months ago

Selected Answer: C

Definetely C.

upvoted 1 times

SongOTD 2 years, 2 months ago

Selected Answer: C

I think 'network perimeter' is the key words.

upvoted 2 times

Question #109 *Topic 1*

Using the cipher text and resultant cleartext message to derive the monoalphabetic cipher key is an example of which method of cryptanalytic attack?

A. Known-plaintext attack

B. Ciphertext-only attack

C. Frequency analysis

D. Probable-plaintext attack

Suggested Answer: *A*

Community vote distribution

A (64%) B (18%) C (18%)

ygc Highly Voted 2 years, 3 months ago

Answer is A, key word : cryptanalytic

upvoted 7 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

BigITGuy Most Recent 3 months ago

Selected Answer: A

In a known-plaintext attack, the attacker has access to: a piece of ciphertext (the encrypted message) and the corresponding cleartext

upvoted 1 times

imather 5 months, 1 week ago

Selected Answer: A

A. Known-plaintext attack - KPA requires having plaintext and cipher text pairs in order to map out the key. (https://www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks/)

B. Ciphertext-only attack - COA has the cipher text only. This cannot be the answer. (https://www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks/)

C. Frequency analysis - frequency analysis is tempting since it mentions a monoaplphabetic key which is what frequency analysis is strong at breaking. However, as you have both the cipher and plaintext in this scenario, you don't need frequency analysis. (https://www.101computing.net/frequency-analysis/)

D. Probable-plaintext attack - "A probable plaintext attack works by looking at certain bit positions for which a likely value can be predicted." (https://www.cs.columbia.edu/~smb/papers/probtxt.pdf) This attack is not relevant as you have the full plaintext.

upvoted 1 times

GuardianAngel 10 months, 4 weeks ago

known plain text attack is the answer:
https://www.sciencedirect.com/topics/computer-science/plaintext-attack#:~:text=In%20the%20known%20plaintext%20attack,try%20to%20decrypt%20the%20ciphertext.

upvoted 2 times

YesPlease 1 year ago

Selected Answer: B

Answer B) Ciphertext-only attack

The question says "resultant cleartext". this means you did not have the cleartext to start with....so it was a Ciphertext-Only Attack first...and then you used Frequency Analysis on the Plaintext Cipher to figure out the Monoalphabetic Cipher

https://www.101computing.net/frequency-analysis/

https://www.quora.com/What-is-the-fundamental-reason-why-monoalphabetic-cipher-is-vulnerable-to-frequency-analysis-attack#:~:text=The%20fundamental%20reason%20why%20a,style%20or%20type%20of%20publication.

upvoted 3 times

YesPlease 1 year ago

I'm an idiot....the question is asking what cipher was used to figure out the Monoalphabetic Cipher....so it should be FREQUENCY ANALYSIS

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: A

A. Known-plaintext attack

In a known-plaintext attack, the attacker has access to both the cipher text (encrypted message) and the corresponding cleartext (decrypted message). By analyzing the relationship between the two, the attacker attempts to derive the encryption key or discover vulnerabilities in the encryption algorithm.

In this case, using the cipher text and the resultant cleartext message to derive the monoalphabetic cipher key falls under the category of a known-plaintext attack. The attacker can compare the pairs of known cipher text and cleartext to deduce the correspondence between specific characters or patterns, which can lead to the recovery of the encryption key.

upvoted 3 times

meelaan 1 year, 11 months ago

Selected Answer: C

It should be C as it is monoalphabetic

upvoted 2 times

meelaan 2 years ago

Selected Answer: A

A sounds good

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: A

In the known plaintext attack, the attacker has both a copy of the encrypted message along with the plaintext message that was used to generate the ciphertext.

upvoted 3 times

Question #110 *Topic 1*

When developing an organization's information security budget, it is important that the:

A. requested funds are at an equal amount to the expected cost of breaches.

B. expected risk can be managed appropriately with the funds allocated.

C. requested funds are part of a shared funding pool with other areas.

D. expected risk to the organization does not exceed the funds allocated.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bach1968 11 months, 4 weeks ago

Selected Answer: B

B. expected risk can be managed appropriately with the funds allocated.

When developing an organization's information security budget, it is crucial to ensure that the allocated funds align with the expected risk to the organization. This means that the budget should be sufficient to address the identified risks and implement appropriate security measures. By evaluating the potential risks and their potential impact, organizations can determine the necessary funding to effectively manage and mitigate those risks.

upvoted 1 times

Jamati 1 year, 7 months ago

Selected Answer: B

B is correct.

upvoted 1 times

jackdryan 1 year, 1 month ago

B is correct

upvoted 1 times

rdy4u 1 year, 8 months ago

Selected Answer: B

Risk needs to be manageable always.

upvoted 2 times

Question #111 *Topic 1*

A subscription service which provides power, climate control, raised flooring, and telephone wiring but NOT the computer and peripheral equipment is BEST described as a:

A. cold site.

B. warm site.

C. hot site.

D. reciprocal site.

Suggested Answer: *B*

Community vote distribution

A (88%) 12%

[Removed] Highly Voted 7 months, 1 week ago

A: Cold site is the correct answer

Because computer and peripheral equipment's are not icluded.

upvoted 12 times

Nabs1 Highly Voted 2 years, 3 months ago

Selected Answer: A

Answer should be A, cold site.

upvoted 8 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

amitsir Most Recent 3 months, 1 week ago

Selected Answer: A

Its correct Cold site dont have live devices to be operated

upvoted 1 times

Ramye 7 months, 1 week ago

Selected Answer: A

Sites are generally classified based on how prepared they are and the speed with which they can be brought into operation:

cold - facility is prepared

warm - equipment is in place

hot - operational data is loaded

upvoted 2 times

Dtony66 7 months, 4 weeks ago

Selected Answer: A

Why are these questions written this poorly? A has to be the answer.

upvoted 1 times

GuardianAngel 10 months, 3 weeks ago

Here's another definition that supports ANSWER B: WARM SITE

A warm site is a leased or rented facility that is usually partially configured with some equipment, such as HVAC, and foundational infrastructure components, but not all the hardware that would be needed to restore mission-critical business functions.

The raised floors and telephone wiring would be considered "partially configured with some equipment and foundational infrastructure components"

upvoted 1 times

GuardianAngel 10 months, 3 weeks ago

I initially choose cold site, but after reading different sources, the raised floors and telephone wiring would fall under "may have some pre-configured equipment" Personally I would interpret "equipment' as computers only but a cold site only has space and utilities. A raised floor is not a utility and not included in a bare-bones space, it's something that has to be installed and typically would have a cabling system installed with it which goes beyond "space and utilities' for a cold site. It's another one of those "throw in something seemingly minor to trick you" questions.

https://www.snaketray.com/raised-floor-cable-management/

upvoted 4 times

Ramye 7 months, 1 week ago

It's missing foundational infrastructure components - computers, so based on your shared definition/explanation it has to be cold site.

upvoted 1 times

gjimenezf 11 months, 3 weeks ago

Selected Answer: A

Cold, no computers

upvoted 1 times

AMANSUNAR 1 year, 1 month ago

Selected Answer: B

A warm site is a facility that provides essential infrastructure and services, such as power and environmental controls, but does not have the actual computer systems and equipment in place. It allows for a quicker recovery compared to a cold site as it has some infrastructure ready, but organizations need to provide and install their own computing equipment.

upvoted 2 times

Paperboi 1 year, 3 months ago

Selected Answer: B

It's a warm site because it includes telephone wiring which counts as infrastructure. Cold sites only provide power and hvac.

upvoted 2 times

MShaaban 1 year, 4 months ago

I would go with A.

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: B

B. Warm site.

A warm site is a facility that provides essential infrastructure and environmental controls required for a functioning IT environment, such as power, cooling, and networking infrastructure. However, it does not include the actual computer systems or peripheral equipment. In the event of a disaster or disruption, an organization can bring their own computer systems and equipment to the warm site and quickly restore their operations.

upvoted 1 times

Alex71 1 year, 10 months ago

Selected Answer: A

A cold site is a backup data center that is fully equipped with necessary infrastructure, such as power, cooling, and cabling, but it lacks the computing and networking hardware. In the event of a disaster or outage, the organization will need to procure, install, and configure the necessary hardware and software at the cold site, which can take time and lead to significant downtime.

A warm site, on the other hand, is a backup data center that is partially equipped with computing and networking hardware. The hardware and software may not be the same as the primary site, but they will be pre-installed and configured to some extent, allowing for a quicker transition in case of a disaster. A warm site typically has power, cooling, and cabling infrastructure, as well as some level of network connectivity, and it may require additional hardware to be procured and installed before it can become fully operational.

upvoted 2 times

Delab202 1 year, 12 months ago

Selected Answer: A

Cold site
A site without hardware set up in advance. Typically, a cold site will have power, ventilation, and network connectivity, but otherwise, it's an empty space. To recover operations there, you'll need to install hardware, configure the network, install software, and restore backups. A cold site is much slower to restore from than a hot site, but it's no more expensive than the rent.
NO COMPUTER=COLD

upvoted 2 times

somkiatr 2 years ago

Selected Answer: A

How come B ?. It should be A because a warm site will contain servers ready for the installation of production environments but data need to be restored before operating.

upvoted 1 times

sand_d 2 years, 1 month ago

Selected Answer: A

Sybex 9th Edition Page 1411 - Topic: Cold Sites

upvoted 2 times

rootic 2 years, 2 months ago

Selected Answer: A

Definetely A.

upvoted 1 times

Question #112 *Topic 1*

An international trading organization that holds an International Organization for Standardization (ISO) 27001 certification is seeking to outsource their security monitoring to a managed security service provider (MSSP). The trading organization's security officer is tasked with drafting the requirements that need to be included in the outsourcing contract. Which of the following MUST be included in the contract?

A. A detailed overview of all equipment involved in the outsourcing contract

B. The right to perform security compliance tests on the MSSP's equipment

C. The MSSP having an executive manager responsible for information security

D. The right to audit the MSSP's security process

Suggested Answer: *A*

Community vote distribution

D (94%) 6%

stickerbush1970 Highly Voted 2 years, 3 months ago

Selected Answer: D

Would need permission to audit, going with D

upvoted 8 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

giovi Highly Voted 2 years, 3 months ago

Good equipments without good internal policies would result a bad deal. I'd say D

upvoted 6 times

Dtony66 Most Recent 7 months, 4 weeks ago

D. How can you verify what the hardware is if you cannot audit? A makes no sense.

upvoted 2 times

YesPlease 1 year ago

Selected Answer: C

Answer C) The MSSP having an executive manager responsible for information security

ISO 27001 and GDPR require an executive level person to be responsible for Information Security

The 5th clause of ISO 27001 is titled "Management Responsibility". This clause requires organizations to demonstrate leadership and commitment to information security. It also requires organizations to appoint a management representative to oversee the implementation and maintenance of the ISMS.

upvoted 1 times

J_Ko 3 months ago

However, the question does not state that the MSSP has any form of certification. So it would be up to the customer org (which does have ISO27001) to verify how good those MSSP's are (due diligence). I vote for D within those constraints.

upvoted 1 times

PeteyPete 1 year, 5 months ago

D sounds appropriate.

upvoted 1 times

Alex71 1 year, 10 months ago

Selected Answer: D

. The right to audit the MSSP's security process should be included in the outsourcing contract. This allows the organization to verify that the MSSP is meeting the requirements set out in the contract and is providing the level of service that has been agreed upon. The organization should also ensure that the contract includes provisions for reporting on security incidents and breach notifications. While including an overview of equipment and having an executive manager responsible for information security are important considerations, they are not as critical as the right to audit the MSSP's security process.

upvoted 4 times

Gu321 1 year, 10 months ago

gimme that big D

upvoted 1 times

Firedragon 2 years, 1 month ago

Selected Answer: D

D.

There is requirement for MSSP to conduct a security audit but no detailed overview of all equipment.

https://resources.sei.cmu.edu/asset_files/securityimprovementmodule/2003_006_001_14105.pdf

IE3: Identify the third party organization(s) responsible for conducting your latest
security risk evaluation, security audit, and vulnerability assessment. Describe
how often this is done and how it is performed. Include the most recent results
and the date of these results.

upvoted 1 times

rootic 2 years, 2 months ago

Selected Answer: D

Definetely D.

upvoted 1 times

jsnow2258 2 years, 2 months ago

Selected Answer: D

I am also voting for D. It is common that MSSP would not allow access to hardware, etc, but indirect evidence of that via 3rd party auditor, that is common, acceptable and reasonable to ask.

upvoted 4 times

JAckThePip 2 years, 2 months ago

Answer is Correct

First which and how are the servers and then the policies

https://www.csoonline.com/article/2118687/guidelines-for-choosing-to-outsource-security-management.html

upvoted 4 times

Question #113 *Topic 1*

Which of the following is the PRIMARY type of cryptography required to support non-repudiation of a digitally signed document?

A. Hashing

B. Message digest (MD)

C. Symmetric

D. Asymmetric

Suggested Answer: *A*

Community vote distribution

D (70%) A (30%)

Stevooo Highly Voted 2 years, 3 months ago

Selected Answer: D

I would choose Asymmetric. I believe hashing is the same as message digest.

upvoted 14 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

dev46 Highly Voted 2 years, 3 months ago

Selected Answer: D

The question ask about "type of cryptography" - not hashing - that eliminates A & B

You need Asymmetric cryptography for Nonrepudiation

Sender encrypt message (digital signature) with private key and receive decrypt message with sender's public key. This validates integrity and Nonrepudiation.

Note that Symmetric Nonrepduation does not provide Nonrepduation.

upvoted 12 times

franbarpro 2 years, 2 months ago

I agree with the answer "D" bcs of Non-repudiation - but hashing is cryptography. Sometime we could have hashing without "Asymmetric".

upvoted 3 times

SangSang 5 months, 2 weeks ago

Yes but hashing does NOT provide non-repudiation, it's about the INTEGRITY.

upvoted 1 times

BigITGuy Most Recent 3 months ago

Selected Answer: D

Can't be A. Hashing is used to create a digest of the message but does not provide non-repudiation on its own.

upvoted 1 times

Ramye 7 months, 1 week ago

Selected Answer: D

Symmetric encryption uses the same key to both encrypt and decrypt data, while asymmetric encryption uses two different keys for the same purpose. Symmetric encryption is faster and easier to use than asymmetric encryption, but it is less secure.

With asymmetric, one can’t claim that the security with the data/info was compromised.

upvoted 1 times

koolnkuiet2 8 months, 2 weeks ago

Selected Answer: A

first message is hashing > MD, then is sending with the private user's key, first step is hashing

upvoted 1 times

Hermin2023 9 months, 3 weeks ago

Selected Answer: D

Asymmetric, public-private key pairs for communication between parties, supports scability, easykey distribution, an nonrepudiation.

upvoted 1 times

hoho2000 9 months, 3 weeks ago

Selected Answer: D

Question ask for which crypto SUPPORTS NON-Repudiation on an Already created Digital Signature. MD is a output of a HASH. MD only support integrity.

Only using Asym process to open the MD hash by the sender PUBLIC key, it can prove non repudiation.

A digital signature is a block of data produced by hashing the message with a hashing algorithm that produces a message digest based on its content. Encrypting the message digest with the sender's private key produces the digital signature. That digital signature is then appended to the original (unencrypted) message content and sent to the receiver. The receiver must then verify the digital signature by decrypting it with the sender's public key and comparing the resultant plaintext with the message digest of the received message.

upvoted 2 times

maawar83 12 months ago

Answer is B:
digitally signed document is already a process that uses Asymmetric is the message.. you need a digest to add the proof of origin and integrity of the message.

upvoted 1 times

Soleandheel 1 year ago

D. Asymmetric. Asymmetric cryptography uses a public-private key pair where the private key is kept secret by the signer. The signature is created using the private key, and anyone with access to the corresponding public key can verify the signature. This ensures that only the owner of the private key could have created the signature, providing a strong basis for non-repudiation.

upvoted 1 times

Soleandheel 1 year ago

On the other hand, in symmetric cryptography, the same key is used for both encryption and decryption, and if this key were used for digital signatures, it would mean that anyone who has the key could potentially create a valid signature. This would not provide non-repudiation because the sender could deny having signed the document, and there would be no way to prove which party with access to the symmetric key actually created the signature.

upvoted 1 times

shmoeee 1 year ago

Digitally signed document aka certificate. A certificate requires private and public keys (asymmetric). Answer is D

upvoted 1 times

shmoeee 1 year ago

*signature, not certificate

upvoted 1 times

HappyDay030303 1 year, 2 months ago

D. Asymmetric cryptography, also known as public-key cryptography, is the primary type of cryptography required to support non-repudiation of a digitally signed document.

upvoted 1 times

isaac592 1 year, 2 months ago

Selected Answer: D

Three primary types of cryptography: Symmetric, Asymmetric, Hashing.
Digital signatures require both Hashing and Asymmetric cryptography, which narrows down to A or D. Then between A & D, the question becomes which one supports non-repudiation?

I went with D because non-repudiation is the process of proving the integrity.

Digital signature creation to the DOCUMENT is done by hashing with a hashing algorithm. Hashing is a pre-requisite.
Digital signature verification is done through referencing (matching the hashes) using public and private keys - Asymmetric encryption.

upvoted 1 times

Soleandheel 1 year ago

Hashing is a critical component of many cryptographic processes, including digital signatures, as it helps ensure data integrity. However, hashing alone does not provide non-repudiation.

upvoted 1 times

⊟ **homeysl** 1 year, 2 months ago

Selected Answer: D

One of the advantages of Asymmetric over Symmetric.

upvoted 1 times

⊟ **aape1** 1 year, 2 months ago

Selected Answer: A

A. Hashing functions are extremely important to the use of public key cryptography. In particular, to the creation of digital signatures and digital certificates. A hash function is a one-way function that transforms a variable-length input into a unique, fixed-length output. You cannot reverse, therefore, it supports non-repudiation.

upvoted 1 times

⊟ **Paperboi** 1 year, 3 months ago

Selected Answer: D

Hashing and MD are not types of cryptography and only Asymmetrical support non-repudiation. Hashing is also meant for integrity, not non-repudiation.

upvoted 1 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: A

Hashing, specifically message digest algorithms, is the primary type of cryptography required to support non-repudiation of a digitally signed document.

When a document is digitally signed, a hash function is applied to the document to produce a fixed-length value known as a message digest or hash. The message digest serves as a unique representation of the document's content. The signer then encrypts the message digest with their private key to create a digital signature.

Verification of the signature involves recalculating the hash of the received document and comparing it to the decrypted digital signature using the signer's public key. If the recalculated hash matches the decrypted signature, it provides evidence that the document has not been tampered with since the signature was applied.

Hashing ensures data integrity, as even a small change in the document would result in a significantly different hash value. This helps establish non-repudiation, as the signer cannot later deny their involvement since the signature is based on the unique hash value of the document.

upvoted 5 times

⊟ **HughJassole** 1 year, 6 months ago

So this is interesting, the question asks for non-repudiation in digital signatures, and in this case Asymmetric cryptography is correct.

If it asked for audit logs, it seems that the answer would have been message digest, which was my original thought. In Linux we run md5sum to see the hash value which ensures the file has not been touched and therefore non-repudiation and integrity

https://www.tutorialspoint.com/how-does-non-repudiation-help-in-cyber-security#

upvoted 2 times

Question #114 *Topic 1*

What is the MOST effective method to enhance security of a single sign-on (SSO) solution that interfaces with critical systems?

A. Two-factor authentication

B. Reusable tokens for application level authentication

C. High performance encryption algorithms

D. Secure Sockets Layer (SSL) for all communications

Suggested Answer: *A*

Community vote distribution

A (100%)

scoobysnack209 8 months, 1 week ago

The answer is D. SSO does not required additional authentication or verification.

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: A

The MOST effective method to enhance the security of a single sign-on (SSO) solution that interfaces with critical systems is:

A. Two-factor authentication

Two-factor authentication (2FA) adds an additional layer of security to the authentication process by requiring users to provide two forms of identification: something they know (e.g., a password) and something they have (e.g., a physical token or a mobile device). This approach significantly reduces the risk of unauthorized access even if the user's password is compromised.

upvoted 1 times

HughJassole 2 years ago

A. Once you're in sso you can go anywhere without prompts, that's the whole point. So the security is up front at login, MFA is a great way to increase security. Everything should be ssl/tls too.

upvoted 3 times

Ivanchun 2 years, 6 months ago

Selected Answer: A

SSO with Two Factor Authentication is common

upvoted 1 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: A

You may enable SS/TLS, but if an attacker already knows the password then what's the point?

upvoted 1 times

dev46 2 years, 9 months ago

Selected Answer: A

B and C are easily eliminated

A and D both sound right. But A could be right considering the keyword "enhance" - I would assume SSL is already in place for securing data to/ from critical systems. So, validating user authentication with multi-factor sounds right.

upvoted 2 times

franbarpro 2 years, 8 months ago

Also SSL has that heartbleed bug (https://heartbleed.com/) which why SSL is being replaced by TLS. So, Def. "A"

upvoted 1 times

Question #115 Topic 1

Which of the following is MOST appropriate to collect evidence of a zero-day attack?

A. Honeypot

B. Antispam

C. Antivirus

D. Firewall

Suggested Answer: *A*

Community vote distribution

A (100%)

dev46 Highly Voted 1 year, 9 months ago

Selected Answer: A

Honeypot is right

The rest of the options would not collect evidence until the real attack happens. That's what a Zero-day attack means nobody is aware of the attack including the vendor.

upvoted 8 times

jackdryan 1 year, 1 month ago

A is correct

upvoted 1 times

Bach1968 Most Recent 11 months, 4 weeks ago

Selected Answer: A

The MOST appropriate option to collect evidence of a zero-day attack is:

A. Honeypot

A honeypot is a decoy system or network that is designed to attract and trap potential attackers. It is intentionally vulnerable and set up to mimic valuable assets or services to lure attackers into interacting with it. By monitoring the activities within the honeypot, security professionals can gather valuable information and evidence about the zero-day attack.

upvoted 3 times

eatay10 1 year, 6 months ago

A is right. Honeypots give administrators an opportunity to observe attacks and may reveal an attack using a zero-day exploit.

upvoted 1 times

franbarpro 1 year, 8 months ago

Selected Answer: A

A is right... but what if the other options had ML & AI capabilities??

upvoted 2 times

Question #116 *Topic 1*

When assessing web vulnerabilities, how can navigating the dark web add value to a penetration test?

A. Information may be found on hidden vendor patches.

B. The actual origin and tools used for the test can be hidden.

C. Information may be found on related breaches and hacking.

D. Vulnerabilities can be tested without impact on the tested environment.

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **franbarpro** Highly Voted 👍 1 year, 8 months ago

Selected Answer: C

Penetration Tester are good people who know how to do bad things. So, "C" - They don't mind looking for related breaches and hacking on the dark web!

upvoted 6 times

⊟ **jackdryan** 1 year, 1 month ago

C is correct

upvoted 1 times

⊟ **Bach1968** Most Recent 🕒 11 months, 4 weeks ago

Selected Answer: C

When assessing web vulnerabilities, navigating the dark web can add value to a penetration test by:

C. Information may be found on related breaches and hacking.

While the dark web can provide valuable information, it is important to note that accessing and navigating the dark web can be risky and potentially illegal. It should only be done with proper authorization and adherence to legal and ethical guidelines.

upvoted 1 times

⊟ **jsnow2258** 1 year, 8 months ago

Selected Answer: C

The devil is in the details. The question sounds like you would need to find one option from the A-D, which helps pen testing perform at its best.
1) https://www.oreilly.com/library/view/web-penetration-testing/9781783988525/ch02s03.html = this alone would suggest B, but they have to be used in the cloud, or via tor (aka onion network), no indication of that
2) C would help from an information gathering perspective, since that is what pen-tester would look for, a way to get in. And they hope that hasn't been covered.. yet.

upvoted 2 times

⊟ **dev46** 1 year, 9 months ago

Selected Answer: C

C is right

A. Information may be found on hidden vendor patches - why would vendor hide their patches on dark web?

B. The actual origin and tools used for the test can be hidden - doesn't sound right

C. Information may be found on related breaches and hacking - sometime dark web navigation helps to find hidden information or related breach that is usually not available on Internet

D. Vulnerabilities can be tested without impact on the tested environment - navigating dark web doesn't ensure that

upvoted 3 times

Question #117 *Topic 1*

The quality assurance (QA) department is short-staffed and is unable to test all modules before the anticipated release date of an application. What security control is MOST likely to be violated?

A. Change management

B. Separation of environments

C. Program management

D. Mobile code controls

Suggested Answer: *A*

Community vote distribution

A (72%) C (28%)

Roy_Xenon Highly Voted 2 years, 8 months ago

Selected Answer: A

Violated the "Release Control" of Change Management.
Release Control
Once the changes are finalized, they must be approved for release
through the release control procedure. An essential step of the release control process
is to double-check and ensure that any code inserted as a programming aid during the change process (such as debugging code and/or backdoors) is removed before releasing the new software to production. This process also ensures that only approved changes are made to production systems. Release control should also include acceptance testing to ensure that any alterations to end-user work tasks are understood and functional.

upvoted 12 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

Not B. Separation of environments - Unrelated (refers to dev/test/prod isolation, not testing rigor).
Not C. Program management - Too broad (governs overall projects, not specific security checks).
Not D. Mobile code controls - Irrelevant (unless the app is mobile-specific, which isn't stated).

upvoted 1 times

Ramye 1 year ago

Selected Answer: A

This is the most viable answer for the specific keywords “security controls”.

Is program management a security control?

upvoted 2 times

homeysl 1 year, 3 months ago

Selected Answer: A

Release from lower to high environment

upvoted 1 times

Soleandheel 1 year, 6 months ago

A. Change management

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: A

The security control that is most likely to be violated in this scenario is:

A. Change management.

Change management involves implementing processes and controls to ensure that changes to the application, including updates and patches, are properly authorized, tested, and implemented in a controlled manner. It ensures that changes to the application do not introduce security vulnerabilities or compromise its integrity.

upvoted 3 times

HughJassole 2 years ago

A. "The CISSP common body of knowledge asserts that change management systems should manage changes related to the entire life cycle of a system including design, development, testing, evaluation, implementation, distribution, and ongoing maintenance."
https://securitythinkingcap.com/change-management-and-how-it-is-essential-to-your-security/#:~:text=Change%20management%20is%20a%20key,significant%20benefits%20to%20an%20organization.

upvoted 1 times

Alex71 2 years, 4 months ago

Selected Answer: A

The security control that is most likely to be violated in this scenario is "Change management." Change management is a process that is designed to ensure that changes to systems or applications are made in a controlled and authorized manner, minimizing the risk of disruption or compromise. Testing is an important part of the change management process, as it helps to identify and address any security issues that may be introduced as a result of a change. If the QA department is short-staffed and cannot test all modules before the anticipated release date of an application, it is likely that some changes will not be adequately tested, which could result in security issues being introduced into the application.

upvoted 2 times

JohnyDal 2 years, 4 months ago

Selected Answer: C

The new app hasnt been released to production yet. CM only kicks in once app is deployed to prod and we are in ops/maintenance phase

upvoted 3 times

Dee83 2 years, 5 months ago

D. Correct answer

Mobile code controls is most likely to be violated if the quality assurance (QA) department is short-staffed and unable to test all modules before the anticipated release date of an application. Mobile code controls refers to security measures that are put in place to ensure that code from external sources, such as third-party libraries or open-source components, is properly vetted before it is used in an application. Without proper testing, it is possible that malicious code or vulnerabilities could be included in the application, which would compromise its security.

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: A

I agreed with A. Shouldn't be C. What Is Program Management?
Program management refers to managing all processes associated collectively with individual projects, such as looking into the staff, and work-related actions, aligning multiple projects with the company's objectives and reporting on status updates and progress. It also oversees the resource management plan and plans for involved projects regarding strategies and change management.
reference : https://www.simplilearn.com/what-is-program-management-article

The Change Management control can be re-designed to match the release control strategy.
reference : https://cloud.google.com/architecture/devops/devops-process-streamlining-change-approval

upvoted 1 times

Ivanchun 2 years, 6 months ago

Selected Answer: A

to test all modules before the anticipated release date is change management

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: C

C is correct

upvoted 1 times

rootic 2 years, 8 months ago

Selected Answer: C

How can they violate CM if they didn't do all tests? This doesn't make sense.
Vote for C.

upvoted 2 times

dev46 2 years, 9 months ago

Selected Answer: C

A. Change management - can't be this because the solution is not released/ in production yet

B. Separation of environments - it's security control, but the question is about testing

C. Program management - this makes sense, but the question doesn't word well. Not sure if program management has official control but if testing all the modules is agreed upon, and if the product is released, it's clearly a violation of what was agreed for the program scope. I would ask to raise risk and get an endorsement from management if this happens.

D. Mobile code controls - doesn't align with the question

upvoted 2 times

Coolwater 2 years, 8 months ago

Question - "MOST likely to be violated" if they release the software without testing - Ans is A

upvoted 1 times

stickerbush1970 2 years, 9 months ago

I am thinking this does align with C

PM-11 MISSION/BUSINESS PROCESS DEFINITION
Page last updated:

Control Description
The organization:

Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Control Description
The organization:

Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

upvoted 3 times

CuteRabbit168 2 years, 9 months ago

Selected Answer: A

Answer is correct. Program management is not a "security control"

upvoted 2 times

Cww1 2 years, 9 months ago

PM is a control family in nist 800/53

upvoted 2 times

Question #118 *Topic 1*

Which of the following criteria ensures information is protected relative to its importance to the organization?

A. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification

B. The value of the data to the organization's senior management

C. Organizational stakeholders, with classification approved by the management board

D. Legal requirements determined by the organization headquarters' location

Suggested Answer: *A*

Community vote distribution

A (82%) Other

JAckThePip Highly Voted 👍 2 years, 8 months ago

Answer is A

"Information must be classified in terms of legal requirements, value, criticality and sensitivity to any unauthorised disclosure or modification, ideally classified to reflect business activity rather than inhibit or complicate"

https://www.isms.online/iso-27001/annex-a-8-asset-management/

upvoted 10 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 2 times

CuteRabbit168 Highly Voted 👍 2 years, 9 months ago

Selected Answer: A

A data classification identifies the value of the data to the organization and is critical to protect data confidentiality and integrity.

upvoted 7 times

Ramye Most Recent ⏲ 1 year ago

Selected Answer: B

Organization's senior management decides the value of the data and we have to protect those accordingly.

We do not secure and put controls without senior managements' input.

upvoted 1 times

Ramye 1 year ago

On a second thought, I think C is more important than B. Stakeholders (business owners) are the data owners and their input is most important.

upvoted 2 times

georgegeorge125487 1 year, 10 months ago

Selected Answer: C

Information is protected as a result of management decision, not because you identify criteria to classify information.

upvoted 1 times

lifre 5 months, 2 weeks ago

I think C is included in "value" (Answer A).

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: A

A. Legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.

Ensuring that information is protected relative to its importance to the organization involves considering several criteria. Legal requirements, such as data protection laws and industry regulations, provide a baseline for protecting sensitive information.

upvoted 1 times

HughJassole 2 years ago

A. It's all encompassing.

upvoted 1 times

xxxBadManxxx 2 years ago

c is the correct ans

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: A

Just eliminated B,C, and D then chose A.

upvoted 1 times

[Removed] 2 years, 8 months ago

A all day baby!

upvoted 1 times

Cww1 2 years, 9 months ago

agree with A

upvoted 2 times

gooftroop 2 years, 9 months ago

C. Organizational stakeholders, with classification approved by the management board

upvoted 1 times

> **Rollizo** 2 years, 9 months ago
>
> really it is A, because you need first to classify for the stakeholders take the decision
>
> upvoted 2 times
>
> > **Ramye** 1 year, 1 month ago
> >
> > This is exactly what my thinking. Information needs to be protected according to organization’s needs and not just because we want to.
> >
> > upvoted 1 times

Question #119 *Topic 1*

What is the FIRST step when developing an Information Security Continuous Monitoring (ISCM) program?

A. Collect the security-related information required for metrics, assessments, and reporting.

B. Establish an ISCM program determining metrics, status monitoring frequencies, and control assessment frequencies.

C. Define an ISCM strategy based on risk tolerance.

D. Establish an ISCM technical architecture.

Suggested Answer: *C*

Community vote distribution

C (100%)

salimhajji 8 months, 2 weeks ago

page 23 of https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

upvoted 1 times

salimhajji 8 months, 2 weeks ago

Logically, the next step after the development of the Information Security Continuous Monitoring (ISCM) program is Implement an ISCM program which consists of collecting the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data wherever possible.

So the answer must be:A. Collect the security-related information required for metrics, assessments, and reporting.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C) Define an ISCM strategy based on risk tolerance

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

upvoted 2 times

Soleandheel 1 year, 6 months ago

C. Define an ISCM strategy based on risk tolerance. Strategy comes always before establishing a program.

upvoted 3 times

Bach1968 1 year, 11 months ago

Selected Answer: C

C. Define an ISCM strategy based on risk tolerance.

When developing an Information Security Continuous Monitoring (ISCM) program, the first step is to define an ISCM strategy based on the organization's risk tolerance. This involves assessing the organization's risk appetite, understanding its security objectives, and determining the level of risk it is willing to accept.

upvoted 2 times

somkiatr 2 years, 6 months ago

Selected Answer: C

reference : NIST SP 800-137

upvoted 3 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

rajkamal0 2 years, 6 months ago

Selected Answer: C

Information Security Continuous Monitoring Reference

Continuous monitoring can be a ubiquitous term as it means different things to different professions. NIST SP 800-137 sets forth a standard to follow when applying the principle in the risk management framework utilizing the NIST control set. The primary process for implementing ISCM is to:

1 - Define the ISCM strategy

2 - Establish an ISCM program

3 - Implement an ISCM program

4 - Analyze data and report findings

5 - Respond to findings

6 - Review and update the monitoring program and strategy

Factored into this is the use of manual and automated checks to provide continuous updates and feedback to the system as a whole.

upvoted 4 times

Jamati 2 years, 7 months ago

Selected Answer: C

You have to start with strategy

upvoted 2 times

Peterzhang 2 years, 8 months ago

C is correct which from the CISSP Cert guide 2022: According to NIST SP 800-137, ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Organizations should take the following steps to establish, implement, and maintain ISCM:

1. Define an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

2. Establish an ISCM program that includes metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.

upvoted 3 times

IT_Guy23 2 years, 9 months ago

C is correct, the first step would be to define an ISCM strategy based on risk tolerance. B would be the second step.

upvoted 3 times

dev46 2 years, 9 months ago

I chose B but seems C includes B

upvoted 1 times

Question #120 *Topic 1*

An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

A. RAID level 1

B. RAID level 3

C. RAID level 4

D. RAID level 5

Suggested Answer: *D*

Community vote distribution

D (60%) A (40%)

Jamati Highly Voted 2 years, 7 months ago

Selected Answer: D

I think the keyword is BEST. Yes RAID 1 provides fault tolerance and redundancy, but is it BEST?
With RAID 1, fault tolerance is good since more than one disk contains the same data. However, in the case of a write operation, both the disks can get corrupted which will eventually result in a data loss. RAID 5 offers fault tolerance like RAID 1, but instead of using mirroring, it uses parity and checksum where the data is striped and stored evenly across all disks, along with their parity, so the data can be reconstructed at any time.

upvoted 12 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 1 times

somkiatr 2 years, 6 months ago

I agreed with D. In RAID 1, in case of disk error or bad sectors, we don't know which disk is the master disk or when they are not storing identical data.

upvoted 1 times

gjimenezf 1 year, 5 months ago

Raid 5 is better than Raid 1 in cost-effectiviness and performance but not in Redundancy and fault tolerance

upvoted 1 times

fax Highly Voted 2 years, 8 months ago

I go with A
Raid 1 provides redundancy and fault tolerance while Raid 5 provide fault tolerance but not redundancy

upvoted 9 times

Diaperface 2 years, 2 months ago

The answer is RAID 1 but RAID 5 does offer single-drive fault protection. RAID 0 (Stripping) offers no fault tolerance.

upvoted 1 times

EKP Most Recent 1 month ago

Selected Answer: A

Redundancy:
RAID 1, data duplicated on ALL drives in the array.
RAID 5, data is striped across multiple drives.

Fault Tolerance:
RAID 1, a disk failure does not affect performance. Can withstand more than one disk failure.
RAID 5 , a disk failure will impact performance. Susceptible to data loss if multiple disk failure concurrently.

upvoted 1 times

BigITGuy 2 months, 4 weeks ago

Selected Answer: D

Not A. RAID level 1 provides mirroring (full redundancy), but is less space-efficient since it requires 50% of the disk capacity to be used for redundancy.

upvoted 1 times

Treebeard88 8 months, 3 weeks ago

Selected Answer: A

RAID 1 offers superior redundancy because it maintains an exact copy of all data on a second drive. In contrast, RAID 5 uses parity to protect data, which is efficient but slightly less strong in terms of redundancy.

upvoted 2 times

1460168 11 months ago

Selected Answer: A

https://phoenixnap.com/kb/raid-levels-and-types

It is A. The corrupt sector argumentation is not correct -> if a sector is corrupt the mdadm program is going to use the non-faulty sector of the other device. THIS is the reason why we want RAID-1

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: A

RAID1 for FT and redundancy

upvoted 1 times

gjimenezf 1 year, 5 months ago

Selected Answer: A

RAID 1 (Mirroring): Redundancy: 100% (Complete duplication of data on each disk)
RAID 3: Redundancy: 33.33% (Dedicated parity disk can reconstruct data in case of a single disk failure)
RAID 4: Redundancy: 33.33% (Dedicated parity disk can reconstruct data in case of a single disk failure)
RAID 5: Redundancy: 33.33% (Distributed parity across all disks can reconstruct data in case of a single disk failure)

upvoted 6 times

Soleandheel 1 year, 6 months ago

A. RAID level 1.
If you prioritize the highest level of fault tolerance and minimal downtime, RAID 1 is often considered the best choice.

If you need a balance between fault tolerance and performance, and you can accept a brief period of vulnerability during disk rebuilds, RAID 5 might be a suitable choice.

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: D

D. RAID level 5

RAID (Redundant Array of Independent Disks) is a technology that combines multiple physical disks into a single logical unit to improve performance, reliability, or both. Each RAID level offers different features and trade-offs in terms of redundancy, fault tolerance, capacity, and performance.
additional raids,
6, 10 and 50,

upvoted 1 times

HughJassole 2 years ago

RAID5 is the answer:
"RAID 0 lacks data redundancy, ergo, it is not a fault-tolerant array."
"write speeds of RAID 5 suffer due to the redundant creation "
https://www.trentonsystems.com/blog/raid-levels-0-1-5-6-10-raid-types

upvoted 1 times

jbell 2 years, 3 months ago

A
The next-simplest RAID level uses mirroring. This takes all data written to one drive and writes it in parallel to a second drive. This provides the highest redundancy since there is a 1-for-1 copy of all data written.
https://deft.com/blog/the-levels-of-raid/#:~:text=Disaster%20Recovery%20%26%20AWS-,RAID%2D1,copy%20of%20all%20data%20written.

upvoted 2 times

Alex71 2 years, 4 months ago

Selected Answer: D

RAID level 5 provides the best redundancy and fault tolerance out of the given options. It uses distributed parity to achieve data redundancy and is able to sustain a single disk failure without losing data. RAID 1 provides mirroring but only allows for a single disk failure, while RAID 3 and 4 are not commonly used in modern systems.

upvoted 3 times

⊟ **Ivanchun** 2 years, 5 months ago

Selected Answer: D

Best redundancy and faulty tolerance is RAID 5

upvoted 2 times

⊟ **oban** 2 years, 5 months ago

Selected Answer: D

RAID level 5 uses data striping with distributed parity, which means that data is written across multiple disks in a striped pattern and parity information is distributed across all the disks in the array. This allows for a single disk failure without data loss and allows for recovery from multiple disk failures. It also provides good read performance for small-block random I/O and moderate write performance. - source: openai

upvoted 1 times

⊟ **Delab202** 2 years, 6 months ago

RAID level 1 (mirroring) volume layout offers the following: Groups two or more disks as one virtual disk with the capacity of a single disk. Data is replicated on each disk, providing data redundancy. When a disk fails, the virtual disk still works. The data is read from the surviving disk(s)

RAID 3 is a RAID configuration that uses a parity disk to store the information generated by a RAID controller instead of striping it with the data. Because the parity information is on a separate disk, RAID 3 does not perform well when tasked with numerous small data requests.

RAID 4 is a RAID configuration that uses a dedicated parity disk and block-level striping across multiple disks. Because data is striped in RAID 4, the records can be read from any disk. However, since all the writes must go to the dedicated parity disk, this causes a performance bottleneck for all write operations.

RAID 5 is a redundant array of independent disks configuration that uses disk striping with parity. Because data and parity are striped evenly across all of the disks, no single disk is a bottleneck. Striping also allows users to reconstruct data in case of a disk failure.

upvoted 1 times

⊟ **Delab202** 2 years, 6 months ago

The difference between RAID 3 vs RAID 5 can be summarized as follows:

Mirroring, redundancy and fault tolerance are the main components of RAID 3.

RAID 5 cannot boast of this, with fault tolerance storing parity information in one of the drives of the array.

upvoted 1 times

Question #121 *Topic 1*

Compared to a traditional network, which of the following is a security-related benefit that software-defined networking (SDN) provides?

A. Centralized network provisioning

B. Reduced network latency when scaled

C. Centralized network administrative control

D. Reduced hardware footprint and cost

Suggested Answer: *C*

Community vote distribution

C (100%)

dev46 Highly Voted 2 years, 3 months ago

Selected Answer: C

The keyword is "security benefit"

A. Centralized network provisioning - its SDN feature/ capability

B. Reduced network latency when scaled - latency relates to performance

C. Centralized network administrative control - interestingly, this option is a strength and weakness for SDN. Although you can provide defence of depth controls on the SDN controller but compromising the admin account can initiate various types of attacks on SDN. but this option seems right compared to others

D. Reduced hardware footprint and cost - this relates to business cost and deployment

upvoted 11 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

8b48948 Most Recent 8 months, 1 week ago

Could easily be D as this is also correct.

upvoted 1 times

gjimenezf 11 months, 3 weeks ago

Selected Answer: C

security related benefit: Centralized administration

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: C

option C: Centralized network administrative control, is a security-related benefit that software-defined networking (SDN) provides.

upvoted 1 times

rajkamal0 2 years ago

Selected Answer: C

Best answer is C:

Security is also another benefit that enterprises notice with an SDN. This means you can extend your defense capabilities from simply blocking specific attacks to making proactive changes to adjust to new threats. The SDN controller can push global security policy updates out centrally across the network, and a virtualized switch can filter packets at the network edge and redirect suspicious traffic to other security devices for further analysis.

Provisioning is part of administrative control.

upvoted 1 times

franbarpro 2 years, 2 months ago

I mean "C" Centralizing the network admin control will come with a single point of failure, which is not good for security. But I am going with "C" still..... unless someone has a batter explanation.

upvoted 2 times

Jamati 2 years, 1 month ago

Has to be C

upvoted 1 times

Question #122 *Topic 1*

What is the MOST effective response to a hacker who has already gained access to a network and will attempt to pivot to other resources?

A. Warn users of a breach.

B. Reset all passwords.

C. Segment the network.

D. Shut down the network.

Suggested Answer: *C*

Community vote distribution

C (61%) D (26%) 13%

oudmaster Highly Voted 2 years, 6 months ago

I really got laughed when I saw the answer is "segment the network".
Which this solution requires careful design, consideration, and implementation. Which takes time. I don't know how security team can respond to the network by segment it at that time. What kind of network is this?

upvoted 20 times

somkiatr 2 years, 6 months ago

Agreed.

upvoted 1 times

georgegeorge125487 1 year, 10 months ago

Agrred.

upvoted 1 times

dev46 Highly Voted 2 years, 9 months ago

Selected Answer: C

The keyword is "response to hacker"

A. Warn users of a breach - could be internal users or stakeholders, not a direct response to a hacker

B. Reset all passwords - won't help as the attacker has gained access to a network

C. Segment the network - best option as you don't want attackers to break more systems with gained access

D. Shut down the network - can't afford it as it may affect business operations

upvoted 13 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 2 times

CKaraf Most Recent 3 months, 1 week ago

Selected Answer: D

Attacker already has gained access. Too late to segment (requires planning, assessing, testing). Shut down asap

upvoted 1 times

CKaraf 3 months, 3 weeks ago

Selected Answer: D

Segmenting will take too long and the attacker will likely already have moved laterally. Shut down is correct response.

upvoted 1 times

cysec_4_lyfe 4 months, 1 week ago

Selected Answer: D

The most EFFECTIVE response is to shut down the network IMO. Buys time and prevents further damage. Temporarily halts attacker activity, stopping further damage; Provides time for incident response teams to analyze the breach and implement containment measures; Can be disruptive to operations, so it is typically used as an emergency measure.

upvoted 1 times

stack120566 7 months, 2 weeks ago

Given the urgency and potential damage an attacker can cause, the most effective immediate response is D. Shut down the network.

Shutting down the network can prevent the attacker from moving laterally and causing further harm. This action buys time to assess the situation, contain the breach, and implement necessary security measures, including network segmentation, without the attacker causing additional damage.

While network segmentation is crucial for long-term security, shutting down the network is the most immediate and effective way to stop an active attack.

upvoted 2 times

stack120566 7 months, 2 weeks ago

Segmenting the network is not a practical emergecny response. in all but the smallest of IT enfironments, this kind of thing would need extensivie planning and time to execute. in the end will cause service disruptionss and will allow attaker to move latterly. If rushed re-segmenting the network could crash services. . This is the kind of suggestion from a security professional that would prove to everyone else in IT that the securiy profession knows nothing.

upvoted 1 times

angellorv 7 months, 2 weeks ago

Six ways to prevent Lateral Movement:

- Enforce least privilege access
- Implement zero trust
- Require MFA
- Segment networks
- Keep software up to date
- Privileged Access Management (PAM) solution

upvoted 1 times

MP26 1 year, 2 months ago

You need to contain the threath immediately. Segmenting is not done by a day. So shutdown is the answer. And B is not bad to do but, if he has already a domain admin account. He easily can bypass that.

upvoted 1 times

73f8ac3 1 year, 2 months ago

Selected Answer: D

The most effective response is to kill everything. It might not be the best immediate one for business as it also stops the business, but at least it will stop the hacker.

I see lots of people talk about segmenting the network. That's a preventive measure, not a response. Segmenting the network is done at design, and changing the network architecture takes hours (if not well done at all), or weeks (if properly done).

upvoted 3 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C) Segment the network

https://reciprocity.com/resources/https-reciprocity-com-resources-what-is-pci-dss-network-segmentation/

upvoted 1 times

MShaaban 1 year, 10 months ago

Option C sounds correct, but segmenting the network after the hacker is already on it may not be effective. Unless you know which part of the network the hacker has accessed, so that you can disconnect that part and segment the network.

upvoted 3 times

Bach1968 1 year, 11 months ago

Selected Answer: C

The most effective response to a hacker who has already gained access to a network and may attempt to pivot to other resources is to segment the network (option C)

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: B

T think it should be B. According to NIST Cybersecurity Framework.

Identify->Protect->Detect->Response->Recovery

A. Warn users of a breach - This is a response to the threat but it's not effective response.

B. Reset all passwords - This is a good response and should be the first step to response hacker to prevent gaining access or lateral movement to other resources in the network.

If the hacker can gain access into the network that means that some credentials were compromised.

C. Segment the network - This should be done in protect state. You have to re-design and re-configure the network diagram and it may take time.

D. Shut down the network - This is a response but if you shut down the network you can't access the network also.

upvoted 3 times

oudmaster 2 years, 6 months ago

I also agree with B as best option for this scenario.

Because the hacker seems know at least one password. If we force all passwords to be reset, this is an effective and rapid response. But of course not a complete one.

upvoted 2 times

Ivanchun 2 years, 6 months ago

Selected Answer: C

C, segment the network, because hacker attempt to pivot to other resources

upvoted 1 times

sphenixfire 2 years, 7 months ago

Selected Answer: D

I go for d because a respond is asked. You cannot respond by segment the network on the fly. This must be done in advanced.

upvoted 5 times

franbarpro 2 years, 8 months ago

Unplug the network.... but forensic people might not like you for that or what if is a bigger network?. I don't like this question.... am going with "C" but i do believe is a bit too late to VLAN/Segment the network bcs the attacker is already in the network.

upvoted 3 times

Question #123 Topic 1

Which of the following is a common term for log reviews, synthetic transactions, and code reviews?

A. Application development

B. Spiral development functional testing

C. Security control testing

D. DevOps Integrated Product Team (IPT) development

Suggested Answer: *C*

Community vote distribution

C (100%)

dev46 Highly Voted 2 years, 3 months ago

Selected Answer: C

Conduct Security Control Testing
Organizations must manage the security control testing that occurs to ensure that all security controls are tested thoroughly by authorized individuals. The facets of security control testing that organizations must include are vulnerability assessments, penetration testing, log reviews, synthetic transactions, code review and testing, misuse case testing, test coverage analysis, and interface testing.

https://www.pearsonitcertification.com/articles/article.aspx?p=2931575&seqNum=2

upvoted 10 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

maawar83 Most Recent 12 months ago

the Answer should be A: all these testing are more related to applications development and sustaining.
The common term for log reviews, synthetic transactions, and code reviews is "Monitoring." Monitoring involves systematically observing, checking, and analyzing various aspects of a system, application, or codebase to ensure its proper functioning, security, and performance. Each of the activities mentioned falls under the broader umbrella of monitoring

upvoted 2 times

Bach1968 1 year, 5 months ago

Selected Answer: C

The common term for log reviews, synthetic transactions, and code reviews is "security control testing" (option C).

Log reviews involve analyzing system logs to identify any suspicious or anomalous activities that may indicate security incidents or policy violations. Synthetic transactions refer to simulated interactions with an application or system to test its behavior and response. Code reviews involve examining the source code of an application or software to identify security vulnerabilities and ensure compliance with coding standards.

All these activities fall under the broader category of security control testing, which aims to assess the effectiveness of security controls implemented within an organization's systems and applications. By conducting security control testing, organizations can identify weaknesses, vulnerabilities, and compliance gaps in their security measures and take appropriate remedial actions.

upvoted 2 times

Jamati 2 years, 1 month ago

Selected Answer: C

According to Chapter 15 of the Official Study Guide, 9th edition, Security Control Testing is comprised of the following:
Vulnerability assessment
Penetration testing
Log reviews
Synthetic transactions
Code review and testing
Misuse case testing
Test coverage analysis

Interface testing

Breach attack simulations

Compliance checks

upvoted 3 times

⊟ **franbarpro** 2 years, 2 months ago

Selected Answer: C

Yep "C" it is. I thought of Spiral development functional testing first... but that's just an SDLC model used for risk management.

upvoted 1 times

Question #124 *Topic 1*

A database server for a financial application is scheduled for production deployment. Which of the following controls will BEST prevent tampering?

A. Data sanitization

B. Data validation

C. Service accounts removal

D. Logging and monitoring

Suggested Answer: *B*

Community vote distribution

B (67%) C (21%) 13%

⊟ **franbarpro** Highly Voted 👍 2 years, 8 months ago

Selected Answer: B

Input validation is the answer to alot of application attacks/issues. OWASP Top 10.

upvoted 8 times

⊟ **jackdryan** 2 years, 1 month ago

B is correct

upvoted 1 times

⊟ **deeden** Highly Voted 👍 10 months, 3 weeks ago

Selected Answer: D

Scenario: You code is in Dev environment and about to be deployed to Prod. How to ensure your code isn't changed in any way in any way prior to deployment? It has to be some form of FIM tool which could periodically compare the hash and alert for any mismatch (suspected tampering).

upvoted 5 times

⊟ **SangSang** 5 months, 2 weeks ago

Logging and Monitoring is NOT a preventive control

upvoted 2 times

⊟ **b0145c1** Most Recent ⏲ 1 month, 3 weeks ago

Selected Answer: D

Definitely D

upvoted 1 times

⊟ **ServerBrain** 3 months, 2 weeks ago

Selected Answer: C

Key word is 'prevent',

upvoted 1 times

⊟ **Dtony66** 5 months, 3 weeks ago

Selected Answer: C

Service accounts are where the majority of attacks occur from.

upvoted 1 times

⊟ **ElDirec** 11 months, 1 week ago

Selected Answer: D

I think we are trying to avoid tampering with the SERVER, consequently avoiding tampering with the DB. Nowhere in the question it states it will be taking input from a customer. This might be a transaction logging DB, not necesarily one connected to a web server. I think Logging and monitoring is the better answer, as it can help detect and respond to any unauthorized attempts, such as modifying or deleting existing data

upvoted 1 times

⊟ **GuardianAngel** 1 year, 4 months ago

Selected Answer: B

Answer is Data validation: sql injection is possible becuase the data being input from a web form is not validated before it reaches the database by using regular expressions to check for special characters and limiting the number of characters the field (ultimately the parameter(variable)) that is passed to the database to be processed --- AND hopefully, the database is using stored procedures that have parameters to accept the data input instead of a method that is extremely vulnerable like the website using inline sql statements on the form

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C) Service accounts removal

This is the only option that will actually prevent anything from happening. The following do not PREVENT anything.
A. Data sanitization: involves purposely, permanently deleting, or destroying data from a storage device, to ensure it cannot be recovered.
B. Data validation: is the process of checking the accuracy, integrity, and structure of data before it's used in a business operation.
D. Logging and monitoring

upvoted 5 times

Bach1968 1 year, 11 months ago

Selected Answer: B

Data validation (option B).

Data validation involves implementing checks and controls to ensure the integrity and accuracy of data.

upvoted 1 times

HughJassole 2 years ago

C. Remove service accounts. The question states that a DB server is being moved to prod, and they don't want someone to mess with it now that it's in production, so it needs to be locked down.

"Remove all access to your database (except for your own personal domain account). Literally, each and all accounts."
https://softwareengineering.stackexchange.com/questions/369645/preventing-in-database-record-tampering

upvoted 1 times

kptest12 2 years, 8 months ago

Selected Answer: B

https://www.youtube.com/watch?v=ydjDrIZyOIk

upvoted 2 times

Rollizo 2 years, 9 months ago

Input validation (also known as data validation) => this can protects new database deployment

upvoted 1 times

dev46 2 years, 9 months ago

Selected Answer: B

C & D has nothing to do with tampering

A is about sanitization/ clearning

upvoted 4 times

Question #125 *Topic 1*

The Industrial Control System (ICS) Computer Emergency Response Team (CERT) has released an alert regarding ICS-focused malware specifically propagating through Windows-based business networks. Technicians at a local water utility note that their dams, canals, and locks controlled by an internal Supervisory
Control and Data Acquisition (SCADA) system have been malfunctioning. A digital forensics professional is consulted in the Incident Response (IR) and recovery.
Which of the following is the MOST challenging aspect of this investigation?

A. Group policy implementation

B. SCADA network latency

C. Physical access to the system

D. Volatility of data

Suggested Answer: *C*

Community vote distribution

D (52%) C (48%)

⊟ **BigITGuy** 3 months ago

Selected Answer: D

Can't be C. Physical access may sometimes be limited but is generally manageable, especially in local utilities.

upvoted 1 times

⊟ **Tuhaar** 7 months ago

Selected Answer: D

malware lives in RAM (volatile memory). Hence this is the clue to choose option D.

upvoted 2 times

⊟ **KJ44** 7 months, 4 weeks ago

Selected Answer: D

A primary issue in forensics for SCADA systems is data retrieval from volatile memory and network devices. Moreover, legacy systems may not provide long-term logs due to limited memory architectures. OSTI.GOV

upvoted 2 times

⊟ **deeden** 10 months, 3 weeks ago

Selected Answer: D

Volatility of data is the most challenging aspect of this investigation.

In an ICS environment, data is often overwritten or erased quickly, especially in operational systems. This makes it extremely difficult to recover critical evidence and reconstruct the attack timeline. Additionally, the nature of SCADA systems, with real-time control and monitoring, often involves large volumes of data, making the collection and analysis process even more complex.

The other options are challenges, but they are generally more manageable with appropriate tools and techniques.

upvoted 1 times

⊟ **133db51** 1 year, 3 months ago

Electric generation falls under NERC/FERC - its physical access as they have to go to site and then be escorted due to lack of clearances.

upvoted 1 times

⊟ **homeysl** 1 year, 3 months ago

Selected Answer: C

SCADA and OT are typically on a air-gapped networks.

upvoted 1 times

⊟ **hoho2000** 1 year, 3 months ago

Selected Answer: C

Ans C.

It mentions Locks are malfunction. There is no indication the malware is volatile. IF D is the ans than all malware investigations first concern will be volatility.

upvoted 2 times

gjimenezf 1 year, 5 months ago

Selected Answer: C

Scada systems usually are not open to the internet, you need physical access to the office were the SCADA is installed, if the expert don't live in the neighborhood this will be a big challenge.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: D

Answer D) Volatility of data

https://www.osti.gov/servlets/purl/1493135

upvoted 4 times

deeden 10 months, 3 weeks ago

Thank you for providing reference.

upvoted 1 times

Soleandheel 1 year, 6 months ago

A. Configuration item

upvoted 1 times

AMANSUNAR 1 year, 7 months ago

Selected Answer: C

Physical access to the Supervisory Control and Data Acquisition (SCADA) system can be a significant challenge. SCADA systems are critical infrastructure components, and gaining physical access to them may involve logistical and security challenges. Physical access allows an attacker to directly manipulate or compromise the hardware, which can have severe consequences for the operation of the water utility's dams, canals, and locks.

upvoted 1 times

MShaaban 1 year, 10 months ago

I was voting for D but came this question in my head. What would make the SCADA data volatile if logs are stored on external servers. Capturing the logs won't be hard. Physical access though would be harder, which makes C more challenging.

upvoted 3 times

Bach1968 1 year, 11 months ago

Selected Answer: C

n the given scenario, the most challenging aspect of the investigation is likely to be "Physical access to the system" (option C).

Physical access to the SCADA system can be challenging because these systems are often located in critical infrastructure environments and are subject to strict physical security controls. Gaining authorized access to the system requires coordination with the appropriate personnel, adherence to security protocols, and potentially overcoming physical barriers and safeguards.

upvoted 1 times

HughJassole 2 years ago

D. There is no need to access a dam to look at its data; the data is centrally in the SCADA system. The issue with these systems is data volatility.
http://www.people.vcu.edu/~iahmed3/publications/ieee_computer_2012.pdf

upvoted 2 times

gjimenezf 1 year, 5 months ago

but you need to access the SCADA system that usually is installed on premises and without internet access for security

upvoted 1 times

dmo_d 2 years, 1 month ago

Selected Answer: C

C is correct.
The key characteristic of SCADA systems are that they are distributed over a wide area.
Data volatility would come next. But if forensics fails to collect data because the systems are not physically accessible there is no data which causes concerns to volatility.

upvoted 1 times

BennyMao 2 years, 1 month ago

Selected Answer: C

Since the SCADA controls dams, canals, and locks, most likely these devices and related sensors are scattered across wide area, many of which may not be easily accessible.

upvoted 1 times

Dee83 2 years, 5 months ago

D. Volatility of data

The most challenging aspect of this investigation would likely be D. Volatility of data. This is because digital forensics professionals need to collect evidence in a way that preserves the integrity of the data and doesn't alter it. In the case of ICS-focused malware, data can be volatile and can change or be deleted quickly, making it difficult to collect and analyze evidence. Additionally, SCADA systems have their own specific protocols and technologies, which can make data collection and analysis more complex.

upvoted 2 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 2 times

Question #126 *Topic 1*

What term is commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB)?

A. Configuration item

B. Configuration element

C. Ledger item

D. Asset register

Suggested Answer: *A*

Community vote distribution

A (100%)

Cww1 Highly Voted 2 years, 3 months ago

correct.

Within a CMDB, these tracked items are known as configuration items (CIs). As defined by ITIL 4, CIs are "any component that needs to be managed in order to deliver an IT service."

upvoted 6 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

homeysl Most Recent 9 months, 2 weeks ago

Selected Answer: A

ITIL 101

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: A

The term commonly used to describe hardware and software assets that are stored in a configuration management database (CMDB) is "Configuration item" (option A).

A configuration item refers to any component or element of an IT system that needs to be managed and controlled. It can include physical devices, software applications, databases, network components, and other related items. The CMDB is a central repository that stores information about these configuration items, including their attributes, relationships, and configurations.

upvoted 2 times

dev46 2 years, 3 months ago

Selected Answer: A

configuration item type (or CI type) is the data type of the element or configuration item an enterprise wishes to store within the CMDB. At a minimum, all software, hardware, network, and storage CI types are stored and tracked in a CMDB.

- Source (Wiki)

upvoted 3 times

Question #127 *Topic 1*

A company is planning to implement a private cloud infrastructure. Which of the following recommendations will support the move to a cloud infrastructure?

A. Implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices and applications.

B. Implement a virtual local area network (VLAN) for each department and create a separate subnet for each VLAN.

C. Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.

D. Implement a virtual local area network (VLAN) to logically separate the local area network (LAN) from the physical switches.

Suggested Answer: *A*

Community vote distribution

C (54%) A (38%) 8%

YesPlease Highly Voted 1 year, 6 months ago

Selected Answer: C

Answer C) Implement software-defined networking (SDN) to provide the ability for the network infrastructure to be integrated with the control and data planes.

Option A is what SDN can do for you....but that answer doesn't help you move toward it. Whereas Option C helps you connect to your existing local network so that you can then migrate your assets to the cloud.

upvoted 7 times

rdy4u Highly Voted 2 years, 8 months ago

Selected Answer: A

Cloud Network Virtualization: Benefits of SDN over VLAN
- Prefer SDN when available.
-Use SDN capabilities for multiple virtual networks and multiple cloud accounts/segments to increase network isolation.
- Separate accounts and virtual networks dramatically limit blast radius compared to traditional data centers.
- Implement default deny with cloud firewalls.
- Apply cloud firewalls on a per-workload basis as opposed to a per-network basis.
- Always restrict traffic between workloads in the same virtual subnet using a cloud firewall (security group) policy whenever possible.
- Minimize dependency on virtual appliances that restrict elasticity or cause performance bottlenecks.

https://cloudsecurityalliance.org/blog/2021/06/25/cloud-network-virtualization-benefits-of-sdn-over-vlan/

upvoted 5 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

Unlikely to be C. SDN integrating the control and data planes is incorrect because SDN separates (not integrates) the control plane from the data plane for better programmability.

upvoted 1 times

KJ44 7 months, 4 weeks ago

Selected Answer: A

Many of today's services and applications, especially when they involve the cloud, could not function without SDN. SDN allows data to move easily between distributed locations, which is critical for cloud applications. Additionally, SDN supports moving workloads around a network quickly.

upvoted 1 times

Rachy 9 months, 2 weeks ago

Selected Answer: A

A. Management does not understand what a control or data plane is.

upvoted 2 times

homeysl 1 year, 3 months ago

Selected Answer: C

this will help P2V the network

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: A

The recommendation that will support the move to a private cloud infrastructure is:

A. Implement software-defined networking (SDN) to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices, and applications.

upvoted 1 times

Rollingalx 2 years, 3 months ago

I go with C
Implementing SDN to provide the ability to apply high-level policies to shape and reorder network traffic based on users, devices, and applications is a good recommendation for improving network performance and security but it does not necessarily support the move to a private cloud infrastructure as effectively as option C which focuses on the use of SDN to integrate the network infrastructure with the control and data planes in a cloud environment. This provides greater flexibility and control over the network, enabling automated provisioning and orchestration of network resources to support dynamic workloads and elastic scaling, which are key characteristics of a private cloud infrastructure.

upvoted 3 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 2 times

oban 2 years, 5 months ago

A and B are both valid answers

upvoted 1 times

evenkeel 2 years, 5 months ago

If both are valid which one supports migration to the cloud. I would think A.

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: B

Why not B ?
https://www.linode.com/blog/networking/go-private-with-vlans-and-vpcs/

upvoted 1 times

dmo_d 2 years, 1 month ago

One subnet per VLAN doesn't sound benefical.
And why should the company plan the VLANs according to business units?
Both aspects are cons to answer B.

upvoted 3 times

Jamati 2 years, 7 months ago

Selected Answer: A

Answer is A.

upvoted 1 times

sphenixfire 2 years, 7 months ago

The questions has nothing to do with sdn/vlan and vice versa

upvoted 2 times

Question #128 *Topic 1*

Which is MOST important when negotiating an Internet service provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over
Internet Protocol (VoIP) services?

A. Mean time to repair (MTTR)

B. Quality of Service (QoS) between applications

C. Financial penalties in case of disruption

D. Availability of network services

Suggested Answer: *B*

Community vote distribution

D (52%) B (48%)

[Removed] Highly Voted 👍 2 years, 1 month ago

Selected Answer: D

ISP is providing the underlay only. QoS is responsibility of the customer using the internet service.

upvoted 8 times

BigITGuy Most Recent ⏲ 3 months ago

Selected Answer: D

D is correct. Must be answered from the consumer perspective of the VOIP company. This is not about the VOIP company providing service to its customers.

upvoted 1 times

Dtony66 5 months, 3 weeks ago

Selected Answer: B

Without QoS, VOIP will not function properly.

upvoted 1 times

Zapepelele 6 months, 3 weeks ago

Selected Answer: D

Answer is D.

VoIP service is organization's responsibility, therefore, it's responsible for QoS too.

Availability of network is ISP's responsibility, so I want these numbers when negotiating a SLA

upvoted 2 times

KJ44 7 months, 4 weeks ago

Selected Answer: D

Reliability is what you care about with VOIP.

upvoted 1 times

1460168 11 months ago

Selected Answer: D

It can not be b, because of the last words in the setence: "between apps".
QoS between Apps!? Come on...

upvoted 3 times

Jarn 1 year ago

Selected Answer: D

Only one application being provided, so it can't be B

upvoted 1 times

dm808 1 year, 3 months ago

Selected Answer: B

The answer is B.
QOS includes availability

upvoted 1 times

john_boogieman 1 year, 3 months ago

Selected Answer: D

It is the organization that provides the VoIP service, and it will be the one that must guarantee it. The ISP must guarantee the availability of the network and therefore this is the factor to be negotiated in the SLA.

upvoted 1 times

GuardianAngel 1 year, 4 months ago

they only have 1 application VoiceOverIP. There's no other applications to prioritize with QOS. If the network isn't available, there is no phone service since VOIP is completely dependent about the network.

upvoted 2 times

Moose01 1 year, 8 months ago

SLA is what services are purchased and guranteed by the ISP and they are bound to it, they are different level of services package with various SLA and prices, if QOS is dropping below the SLA it is considered an outage.

upvoted 1 times

thanhlb 1 year, 8 months ago

Selected Answer: D

organization solely provides Voice over Internet Protocol (VoIP) services, so only Voip traffic on the wire, do we need QoS than Availability?

upvoted 2 times

ExamTaker1995 1 year, 8 months ago

Selected Answer: D

The MOST important factor when negotiating an Internet Service Provider (ISP) service-level agreement (SLA) by an organization that solely provides Voice over Internet Protocol (VoIP) services would be:

D. Availability of network services

In a business where the sole service is VoIP, network availability is critical. If the network is down, the entire business operation could come to a halt, making availability a primary concern. VoIP is extremely sensitive to network downtime, and therefore, ensuring that the network is available is of utmost importance.

While MTTR, QoS between applications, and financial penalties in case of disruption are also important factors to consider, they are secondary to ensuring that the network services are available for the core business offering of VoIP. This is aligned with best practices for SLAs in critical service delivery as per CISSP certification guidelines.

upvoted 4 times

isaac592 1 year, 8 months ago

We primarily used VoIP as the primary means of voice-communication throughout remote sites. When an entire forward site goes "red" on network connectivity, we would have to exercise the alternate or contingency plans to talk between sites. Cant just call em because the VoIP phones connected to the network dont work.

upvoted 1 times

ljkesmeer 1 year, 8 months ago

Voice is sensitive to QoS, I understand that the network availability is important but the availability of the network doesn't do much if it can't assure the call quality. thus I choose the QOS because that is the only thing that allows me to make sure the service is working properly

upvoted 2 times

homeysl 1 year, 8 months ago

Selected Answer: D

You usually see three or four or five 9s in an SLA but not QoS.

upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: B

Option B, Quality of Service (QoS) between applications, is indeed an important consideration when negotiating an Internet service provider (ISP) service-level agreement (SLA) for an organization that provides Voice over Internet Protocol (VoIP) services.

QoS refers to the ability to prioritize and allocate network resources to ensure the desired level of performance for specific applications or services.

In the case of VoIP, maintaining a consistent and high-quality connection is crucial to ensure clear and uninterrupted voice communications. Negotiating a robust QoS provision in the SLA would help prioritize VoIP traffic and ensure optimal performance.

upvoted 1 times

Kyanka 1 year, 3 months ago

Thanks, ChatGTP!

upvoted 1 times

HughJassole 2 years ago

D, as your ISP is not responsible for your QoS:
https://serverfault.com/questions/800826/is-quality-of-service-my-isps-responsibility

I think QoS is thrown in there to trick you, because VOIP and QoS go together, but an ISP provides the internet service access, so they are about availability, not how your application works.

upvoted 4 times

Moose01 2 years, 1 month ago

Internet do not honor QOS tagging, Best Effort only....
However, ISP can provide some sort of contract guaranteeing the availability of the internet circuit and services (SLA).
SLA is not necessarily available in every parts of the world, not even US or EU, only based on available infrastructure.

upvoted 2 times

Question #129 *Topic 1*

A company hired an external vendor to perform a penetration test of a new payroll system. The company's internal test team had already performed an in-depth application and security test of the system and determined that it met security requirements. However, the external vendor uncovered significant security weaknesses where sensitive personal data was being sent unencrypted to the tax processing systems. What is the MOST likely cause of the security issues?

A. Inadequate performance testing

B. Inadequate application level testing

C. Failure to perform negative testing

D. Failure to perform interface testing

Suggested Answer: *B*

Community vote distribution

D (79%) B (21%)

stickerbush1970 Highly Voted 2 years, 9 months ago

Selected Answer: D

agree with D

upvoted 6 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 1 times

mrgod Highly Voted 2 years, 9 months ago

Selected Answer: D

fail on interface testing

upvoted 5 times

dra3m Most Recent 3 months ago

Selected Answer: D

while lack of apps test is also true, the interface test is more specific to the issue. application test focus on components of apps, sast, dast etc but interfacing part ie API should be the focus here

upvoted 2 times

rsbha 6 months, 3 weeks ago

Selected Answer: B

Its option B , interface testing is between modules of an application ; its system/integration/application testing where u test application/system with external interfaces

upvoted 2 times

1460168 11 months ago

Selected Answer: B

I think it is B:

Because we use the API from the tax processing system, it is literally out of scope. An external and internal IT-Security-Researcher can not, should not and must not test such an API.

But B is something that we can really influence significantly.

upvoted 1 times

8e1c45b 11 months, 1 week ago

Selected Answer: D

agree with D

upvoted 1 times

GuardianAngel 1 year, 4 months ago

PART II -

Looking at the question again, one could assume that application level encryption isn't part of the application testing and would rely on the interface to provide encryption - these questions are so vague. Application-level encryption addresses several main goals:

1)Trust your infrastructure less. Application-level encryption provides data protection on all underlying layers, including all layers of storage and sometimes transit. Defense-in-depth. 2) Add another layer of security if other data-related controls like underlying (disk, transit) encryption 3) The longer sensitive data stays encrypted in its lifecycle, the closer application-level encryption gets to end-to-end encryption and zero trust architecture. The shorter data stays encrypted, the closer it gets to single point-to-point transport encryption or encryption at rest.

https://www.infoq.com/articles/ale-software-architects/

upvoted 1 times

GuardianAngel 1 year, 4 months ago

ANSWER: B. Inadequate application level testing. they try to trick you by distracting you with the other system involved, but the key to answering this question is "being sent UNENCRYPTED". Interface testing would be getting the data from point A to point B (think data leaks) but the application would be responsible for encrypting the data before the data is sent to the interface. Application level testing focuses on evaluating the security measures implemented within the application itself, such as data encryption, access controls, and authentication mechanisms.

upvoted 3 times

gjimenezf 1 year, 5 months ago

Selected Answer: D

https://firewize.com.au/definition/system-interface-test

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: D

Answer D) Failure to perform Interface Test

System Interface Test ("SIT") A system or systems interface (also known as a system integration test) test is an end-to-end functional test of the connection between two or more systems to verify their connection and operation.

upvoted 3 times

Soleandheel 1 year, 6 months ago

This is what Chatgpt says about it and i agree with Chatgpt on this one:

D. Failure to perform interface testing.

In this scenario, it appears that the internal test team focused on the application and security testing of the new payroll system but failed to adequately test the interfaces between the payroll system and the tax processing systems. As a result, they missed the security weakness where sensitive personal data was being sent unencrypted to the tax processing systems. Interface testing is essential to ensure that data flows securely between different systems and components, and it's a common area where vulnerabilities can be overlooked if not properly tested.

upvoted 2 times

ljkesmeer 1 year, 8 months ago

Selected Answer: D

D it is

upvoted 1 times

isaac592 1 year, 8 months ago

Selected Answer: D

"Interface testing is primarily concerned with appropriate functionality being exposed across all the ways users can interact with the application. From a security-oriented vantage point, the goal is to ensure that security is uniformly applied across the various interfaces. This type of testing exercises the various attack vectors an adversary could leverage."

- 11th hour

upvoted 1 times

MShaaban 1 year, 10 months ago

I believe it is D. The unencrypted transmission of Sensitive Data to another system (Tax) is part of Factory Integration Testing (FIT) which in this phase we test the interfacing and integration with external systems. Inadequate application level testing is part of Factory Acceptance Testing (FAT) integration with external systems doesn't happen here.

upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: B

the most likely cause of the security issues is option B: Inadequate application level testing.

The fact that the internal test team had already performed an in-depth application and security test of the system but did not uncover the significant security weaknesses indicates that the testing conducted by the internal team was not thorough enough. It suggests that there were gaps or limitations in the application level testing performed internally, which resulted in the failure to identify the security vulnerabilities related to the unencrypted transmission of sensitive personal data.
who knows what they left also, i would have them review the full test scenario, and re-test the full application.
upvoted 1 times

⊟ **Dee83** 2 years, 5 months ago

B. Inadequate application level testing is the most likely cause of the security issues. The internal test team had already performed an in-depth application and security test of the system, but the external vendor was still able to uncover significant security weaknesses. This suggests that the internal test team did not thoroughly test all aspects of the system, particularly in regards to data encryption and transmission.
upvoted 3 times

⊟ **somkiatr** 2 years, 6 months ago

Selected Answer: B

I select B because the sensitive personal data should be encrypted at rest state. The database should store the encrypted data and be retrieved for sending across interface. If the testers doesn't aware whether the personal data was encrypted or not then they should fail on application level testing.
upvoted 5 times

Question #130 *Topic 1*

An organization wants to define as physical perimeter. What primary device should be used to accomplish this objective if the organization's perimeter MUST cost- efficiently deter casual trespassers?

A. Fences three to four feet high with a turnstile

B. Fences six to seven feet high with a painted gate

C. Fences accompanied by patrolling security guards

D. Fences eight or more feet high with three strands of barbed wire

Suggested Answer: *D*

Community vote distribution

A (67%) D (31%)

mrgod Highly Voted 2 years, 9 months ago

Selected Answer: A

3-4 feet deters casual trespassers.

6-7 feet too high to climb — may block vision.

8 feet with 3 strands of barbed wire will deter determined intruders and is generally considered as the standard height and configuration.

upvoted 17 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

dev46 Highly Voted 2 years, 9 months ago

Selected Answer: D

I know A seems the obvious answer as per OSG, but the keyword is "cost-effective"

A. Fences three to four feet high with a turnstile - did you consider the cost of the turnstile?

B. Fences six to seven feet high with a painted gate - did you consider the cost of a painted gate?

C. Fences accompanied by patrolling security guards - an easy one, they are expensive!

D. Fences eight or more feet high with three strands of barbed wire - this solves the purpose and won't cost compared to A & B

upvoted 9 times

izaman2022 2 years, 8 months ago

Understand your intent here about noticing the additional cost of the turnstile and painted door, but how severely is the turnstile or the painted door going to violate cost effectiveness compared to the additional cost of erecting an eight foot fence with barbed wire (2x the height/material) around the same length physical perimeter?

upvoted 3 times

Humongous1593 2 years, 8 months ago

100% agree with you. I'd go with what the OSG says and if its wrong then thats on ISC for a very poorly worded question/answers.

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

Assumes "casual trespassers".

upvoted 1 times

deeden 10 months, 3 weeks ago

Selected Answer: B

LOL I can't believe nobody selected B.

A. lowest price for fences, however, 4 feet high fence might not much an effective deterrent, for residential yes could be acceptable, but not offices

and buildings — also I have not seen a perimeter fence with a turnstile? how would cars enter? turnstile is good control for piggy-backing on building entrances, not perimeter defenses. Bollards might be a better choice than turnstile but also costly.
C. Good deterrent, but additional cost for a security guard.
D. Best deterrent but has the highest cost, may not be cost effective.
upvoted 2 times

Dtony66 1 year, 1 month ago

Selected Answer: A

This would also depend on linear size of the gate. A massive campus with that is 10000 acres with barbed wire and a taller fence would cost significantly more than one turnstile and a gate half the size. A causal trespasser who sees any fence, by definition would be deterred by an obstacle.
upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: A

Answer A)

Question stated "casual trespassers".
upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: A

For a causal trespasser, 3-4 feet should be enough. Source: https://resources.infosecinstitute.com/certifications/cissp/cissp-perimeter-defenses/

Different heights provide varying degrees of protection

3-4 feet deters casual trespassers.
6-7 feet too high to climb — may block vision.
8 feet with 3 strands of barbed wire will deter determined intruders and is generally considered as the standard height and configuration.
upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: D

the examiner is asking for option D, and we will provide hom with the option.
However i do not agree in full, consider this, trees can be climbed, all you need is a rope and you are in the premises, all i am saying is that this may not be the best solution even with eight feel high,
something to think about
upvoted 2 times

d3ut3r 2 years, 1 month ago

"MUST COST-EFFICIENTLY DETER CASUAL TRESPASSERS"

https://resources.infosecinstitute.com/certification/cissp-perimeter-defenses/#:~:text=Different%20heights%20provide,deters%20casual%20trespassers.
upvoted 1 times

sausageman 2 years, 4 months ago

Unless your trespasser is a midget a 3-4 foot fence wouldn't deter anyone. I'd go with D
upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: D

Turnstile is not cost effective and should be installed in the building.
upvoted 2 times

oudmaster 2 years, 6 months ago

Fences
2-to-3 feet high can be easily crossed and would not be considered a deterrent.
3-to-4 foot fence will deter only casual.
5-to-7 feet high are considered more difficult to climb than a shorter fence.
8 feet high should be used to deter a determined intruder.
upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: A

Agreed, A is the answer

upvoted 1 times

rootic 2 years, 8 months ago

Selected Answer: A

it's A

upvoted 1 times

MG1707 2 years, 8 months ago

Selected Answer: A

...casual deterrent..

upvoted 3 times

kasiya 2 years, 9 months ago

Selected Answer: A

OSG

Various types of fences are effective
against different types of intruders:

✓ ■

Fences 3 to 4 feet high deter casual trespassers.

✓ ■

Fences 6 to 7 feet high are too hard to climb easily and deter most intruders, except determined ones.

✓ ■

Fences 8 or more feet high with strands of barbed or razor wire deter even determined intruders.

upvoted 6 times

ygc 2 years, 9 months ago

security guards, it is not cost-efficintly , the answer should be D

upvoted 5 times

Question #131 *Topic 1*

Which of the following vulnerabilities can be BEST detected using automated analysis?

A. Multi-step process attack vulnerabilities

B. Business logic flaw vulnerabilities

C. Valid cross-site request forgery (CSRF) vulnerabilities

D. Typical source code vulnerabilities

Suggested Answer: *D*

Community vote distribution

D (100%)

InclusiveSTEAM 8 months ago

D is the best answer. Typical source code vulnerabilities are best detected using automated analysis tools like static application security testing (SAST).

A - Multi-step process attacks are complex and span business logic and workflows, difficult for automated tools to detect.

B - Business logic flaws require understanding of application's intended behavior, hard to detect automatically.

C - Valid CSRF tokens can look like false positives, automated tools may not determine legitimacy well.

In contrast, typical code flaws like SQLi, XSS, insecure functions etc. are well detected by SAST which analyzes source code for known vulnerable patterns. Automated analysis excels at finding these typical vulnerabilities that have known signatures in code.

upvoted 2 times

Firedragon 1 year, 7 months ago

Selected Answer: D

D.

https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis

Application scans test websites to detect known software vulnerabilities and incorrect configurations in network or web applications.

upvoted 2 times

jackdryan 1 year, 1 month ago

D is correct

upvoted 1 times

dev46 1 year, 9 months ago

Selected Answer: D

D is correct

upvoted 4 times

CharlesL 1 year, 8 months ago

I know D is correct after clicking the button. :)

upvoted 2 times

Question #132 *Topic 1*

A project manager for a large software firm has acquired a government contract that generates large amounts of Controlled Unclassified Information (CUI). The organization's information security manager had received a request to transfer project-related CUI between systems of differing security classifications. What role provides the authoritative guidance for this transfer?

A. PM

B. Information owner

C. Data Custodian

D. Mission/Business Owner

Suggested Answer: *C*

Community vote distribution

B (67%) C (27%) 6%

dev46 Highly Voted 2 years, 3 months ago

Selected Answer: C

Information/ data owner does the classification and can delegate job for transfer to custodian

upvoted 7 times

a_kto_to Most Recent 1 month, 1 week ago

Selected Answer: B

Answer:

B. Information owner

Explanation:

The information owner is responsible for defining the classification, handling, and dissemination controls for Controlled Unclassified Information (CUI). When transferring CUI between systems of differing security classifications, the information owner provides authoritative guidance on

upvoted 1 times

BigITGuy 2 months, 4 weeks ago

Selected Answer: B

Not C. Data Custodian manages the storage and technical handling of data but follows the information owner's instructions.

upvoted 1 times

e58c193 8 months, 4 weeks ago

Selected Answer: C

B. OSG 9th Edition PG. 207. Data owners often delegate day-day tasks to the custodian.

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: B

Data owner = authority

upvoted 1 times

gjimenezf 11 months, 3 weeks ago

Selected Answer: B

key word is authoritative, that is the data/information owner

upvoted 3 times

Kyanka 9 months, 3 weeks ago

Agreed. In real life, the owner normally has to approve transfer between different classification levels. Not sure what they expect on a test, though.

upvoted 1 times

maawar83 12 months ago

Scope:

Information Owner: Focuses on the strategic management, policies, and decision-making related to specific data assets.

Data Custodian: Primarily concerned with the technical implementation, storage, and security of data assets.

Decision-Making Authority:

Information Owner: Holds decision-making authority regarding data policies, access controls, and overall data strategy.
Data Custodian: Implements decisions made by the information owner and focuses on technical execution.
Accountability:

Information Owner: Ultimately accountable for the governance, quality, and strategic use of the data assets they own.
Data Custodian: Accountable for the secure storage, processing, and technical aspects of data management.
Involvement in Governance:

Information Owner: Actively involved in data governance, policy creation, and ensuring alignment with organizational goals.
Data Custodian: Implements and enforces governance policies but may not be directly involved in setting high-level data strategy.

upvoted 1 times

YesPlease 1 year ago

Selected Answer: B

Answer B) Information Owner

https://blog.idatainc.com/data-governance-roles

upvoted 1 times

homeysl 1 year, 2 months ago

Selected Answer: B

B. OSG 9th Edition. Keyword "authoritative".

upvoted 1 times

MShaaban 1 year, 4 months ago

I go with B. Data custodian doesn't have any authoritative over data, they are just responsible for the day to day activities including data backup etc, after being advised by the Information Owner.

upvoted 2 times

dyndevil 1 year, 5 months ago

Answer:C
Data Owner has ultimate responsibility of the data and hence the classification of the data. Once classification is decided, it is delegated to Data Custodian to carry out the task.

upvoted 1 times

Jacobmy98 1 year, 5 months ago

Selected Answer: B

I think its B due to "authoritative" being used. plus 9th edition Page 204 has insight on data owners being the main personnel to make those decisions.

upvoted 4 times

Bach1968 1 year, 5 months ago

Selected Answer: C

data owner, or data custodian, may seem the correct answer/s

upvoted 1 times

babaseun 1 year, 7 months ago

Selected Answer: B

CISSP 9th Edition, Page 204....

upvoted 3 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

Rollingalx 1 year, 9 months ago

I go with B
The National Institute of Standards and Technology (NIST) Special Publication 800-171, which provides guidance for protecting CUI in nonfederal systems and organizations, states that the "information owner is responsible for identifying and marking CUI and specifying the safeguarding or dissemination controls to be applied to the information."

upvoted 3 times

⊟ **crazywai1221** 1 year, 9 months ago

Selected Answer: C

i voted C, owner only classified data

upvoted 1 times

⊟ **Alex71** 1 year, 10 months ago

Selected Answer: B

The authoritative guidance for the transfer of Controlled Unclassified Information (CUI) between systems of differing security classifications is provided by the Information Owner. The Information Owner is responsible for ensuring that the information is appropriately protected and managed throughout its lifecycle, including during transfer between systems. In this case, the Information Owner should consult with the organization's information security manager and follow any applicable policies, procedures, and guidelines for handling CUI.

upvoted 3 times

Question #133 *Topic 1*

Which of the following determines how traffic should flow based on the status of the infrastructure layer?

A. Control plane

B. Application plane

C. Traffic plane

D. Data plane

Suggested Answer: *D*

Community vote distribution

A (81%) D (19%)

dev46 Highly Voted 2 years, 9 months ago

Selected Answer: A

A. Control plane - controls how data packets are forwarded (such as using a routing table)

B. Application plane - On a network, the Application Plane is the layer that has applications and services that make requests for network functions from the Control Plane and the Data plane.

C. Traffic plane - think it's data plane as it carries traffic

D. Data plane - forwards the packet (a.k.a forwarding plane)

upvoted 10 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

DERCHEF2009 Highly Voted 2 years, 9 months ago

Selected Answer: A

SDN = A

upvoted 6 times

sphenixfire 2 years, 8 months ago

This question has nothing to do with sdn, its simply network architecture

upvoted 4 times

KJ44 Most Recent 7 months, 4 weeks ago

Selected Answer: A

In Software-Defined Networking (SDN), the infrastructure layer and control plane are two distinct layers that work together to manage and configure a network:

Infrastructure layer

Also known as the data plane, this layer is made up of physical and virtual devices like switches, routers, and firewalls. The infrastructure layer forwards network traffic based on instructions from the control plane.

Control plane

Also known as the control layer, this layer contains the centralized SDN controller that manages and configures the network. The control plane communicates with the infrastructure layer using southbound APIs.

The infrastructure layer and control plane work together to provide network administrators with a high level of control and flexibility. The separation of layers allows each plane to focus on its specific tasks, such as the control plane prioritizing efficient routing and decision-making.

SDN uses APIs to enable communication between the layers:

upvoted 1 times

Zapepelele 6 months, 3 weeks ago

It's A. But like sphenixfire said, this question has nothing to do with sdn, its simply network architecture.

upvoted 2 times

stack120566 1 year, 3 months ago

The control plane decides how data is managed, routed, and processed, while the data plane is responsible for the actual moving of data.

upvoted 1 times

GuardianAngel 1 year, 4 months ago

D. Data plane https://www.computernetworkingnotes.com/ccna-study-guide/data-plane-control-plane-and-management-plane.html

The control plane captures and stores all the routing information, but the data plane uses that information to forward the packets based on all the routing tables, protocols and network policies that the control plane captures and maintains. Basically, teh control plane is the map that the data plane uses to drive

upvoted 1 times

GuardianAngel 1 year, 4 months ago

Selected Answer: D

The control plane captures and stores all the routing information, but the data plane uses that information to forward the packets based on all the routing tables, protocols and network policies that the control plane captures and maintains. Basically, teh control plane is the map that the data plane uses to drive

upvoted 1 times

aape1 1 year, 8 months ago

Selected Answer: D

D. The control and data planes do not describe the data itself. Rather, these planes describe how the device handles the data. For example, does the device process a packet itself, or does it forward it to another device?

Control plane is slow and it handles/processes requests. Data plane is fast and it forwards traffic.

A few quick examples;

SSH to a router; Control Plane
Passing SSH traffic through to another device; Data Plane
BGP neighbor relationship; Control Plane
Forwarding BGP traffic; Data Plane
OSPF neighbourships and building the LSDB; Control Plane

The data plane needs to provide a high-speed and low-latency path. To achieve this, a lot of data plane implementation is in hardware.

upvoted 3 times

aape1 1 year, 8 months ago

D. The control and data planes do not describe the data itself. Rather, these planes describe how the device handles the data. For example, does the device process a packet itself, or does it forward it to another device? Control plane is slow and it handles/processes requests. Data plane is fast and it forwards traffic.

A few quick examples;

SSH to a router; Control Plane
Passing SSH traffic through to another device; Data Plane
BGP neighbour relationship; Control Plane
Forwarding BGP traffic; Data Plane
OSPF neighbourships and building the LSDB; Control Plane

The data plane need to provide a high speed and low latency path. To achieve this, a lot of data plane implementation is in hardware.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: A

The control plane is responsible for determining how traffic should flow based on the status of the infrastructure layer. It is responsible for making decisions about the best path for traffic to take through the network, and for setting up and tearing down connections between network devices. The other planes listed (application plane, traffic plane, and data plane) are not directly responsible for determining how traffic should flow based on the status of the infrastructure layer.

upvoted 2 times

georgegeorge125487 1 year, 10 months ago

Selected Answer: A

The control plane makes routing decisions. With SDN routing, decisions are made remotely instead of on each individual router.

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: D

the correct answer is D. Data plane.

The data plane, also known as the forwarding plane, is responsible for handling the actual movement of network traffic. It performs the forwarding and processing of data packets based on the information provided by the control plane. The data plane is implemented in network devices such as routers and switches, and its primary function is to forward packets based on predefined rules or policies.

upvoted 1 times

gregchou 2 years, 3 months ago

Answer D:

Data plane is Forwarding Plane. The so-called Forwarding Plane is to process incoming network packets in the router architecture, and determine which network interface to forward the network packets to next by looking up the routing table.

upvoted 1 times

Alex71 2 years, 4 months ago

Selected Answer: A

The Control plane is responsible for managing the traffic flow based on the status of the infrastructure layer. Specifically, it handles the routing of traffic, manages network topology and configuration, and communicates with other network devices. In the context of the given question, the Control plane would be the most appropriate answer as it is responsible for determining how traffic should flow based on the status of the infrastructure layer.

upvoted 1 times

Dee83 2 years, 5 months ago

A. Control plane determines how traffic should flow based on the status of the infrastructure layer.

upvoted 1 times

Mr_Zaw 2 years, 5 months ago

Ans -= A

Software-Defined Networks (SDNs) SDNs decouple the control
plane from the data plane (or forwarding plane). The control plane
uses protocols to decide where to send traffic, and the data plane
includes rules that decide whether traffic will be forwarded.

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: A

Should be A by definition of SDN Controller Plan.

upvoted 1 times

Firedragon 2 years, 7 months ago

Selected Answer: A

A.

https://www.cloudflare.com/learning/network-layer/what-is-the-control-plane/#:~:text=The%20control%20plane%20is%20the,is%20the%20actual%20forwarding%20process.

What is the control plane? | Control plane vs. data plane

The control plane is the part of a network that controls how data is forwarded, while the data plane is the actual forwarding process.

upvoted 1 times

Question #134 *Topic 1*

When testing password strength, which of the following is the BEST method for brute forcing passwords?

A. Conduct an offline attack on the hashed password information.

B. Use a comprehensive list of words to attempt to guess the password.

C. Use social engineering methods to attempt to obtain the password.

D. Conduct an online password attack until the account being used is locked.

Suggested Answer: *A*

Community vote distribution

A (74%) B (23%)

rootic Highly Voted 2 years, 2 months ago

Selected Answer: A

Comon, guys, using of word list IS NOT A BRUTEFORCE. Brutforce is trying EVERY possible value.
OSG: "A dictionary attack is an attempt to discover passwords by using every possible password in a predefined database or list of common or expected passwords."
It makes B a dictionary attack. And question says "bruteforce".
It's A.

upvoted 13 times

sausageman 1 year, 10 months ago

Dictionary attack is a type of brute-force:
https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/#:~:text=Dictionary%20attack%20definition%3A,used%20by%20businesses%20and%20individuals.%E2%80%9D

upvoted 3 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

NOT B for sure -- Using a list of words is a dictionary attack, not a brute-force attack, and is less thorough.

upvoted 1 times

Hackermayne 10 months, 1 week ago

Its A. testing the hash. In an actual security event, the hacker is going to pull the hash either from some random config file, use mimikatz or something that dumps SAM, or unshadow to merge your /etc/passwd and /etc/shadow and get a hash to crack there. They could also use responder to grab the hash, etc.etc. tons of ways to get the hash and then run every possible wordlist they have at it on their own time, either with a string of GPUs on hashcat or some cloud service that does the same thing x 1000. Trust me its A. Next best answer is B, but not as good as A. You're also not testing the lockout control, you're testing password strength.

upvoted 1 times

GuardianAngel 10 months, 3 weeks ago

Answer D: Conduct an online password attack until the account being used is locked. By testing a real account online until you get in or it locks, you test the security control.
• Dictionary – attacker uses a precompiled list of words, phrases, or compromised passwords (a "dictionary") to attempt to gain access.
• Bruteforce - involve systematically trying every possible combination of characters until the correct one is found
• Rainbow Table - a precomputed table for caching the outputs of a cryptographic hash function, usually for cracking password hashes. Passwords are typically stored not in plain text form, but as hash values. Unlike a brute-force attack, which works by calculating the hash function of every string present with them, calculating their hash value and then compare it with the one in the computer, at every step

upvoted 1 times

Vince_F_Fang 1 year, 1 month ago

Selected Answer: A

Both A and B are violent attacks, but the goal is to test password strength, and using only B to test password strength is too one-sided. When testing password strength, priority should be given to testing cases where the password length is short and the password type is few, before it is the turn to test whether it can be brute force cracked using commonly used words.

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: A

The correct answer is A. Conduct an offline attack on the hashed password information.

Brute-forcing passwords involves systematically trying all possible combinations of characters until the correct password is found. In the case of offline attacks, the attacker has access to the hashed password information and can attempt to crack it using various techniques, such as dictionary attacks or using precomputed tables (rainbow tables). By obtaining the hashed password, the attacker can perform multiple attempts without directly interacting with the target system.

upvoted 1 times

DapengZhang 1 year, 8 months ago

Selected Answer: D

In my mind, A shall be a rainbow attach and B is a dictionary attack. i didnt see good option here and i choose D. This method involves attempting to log in to an account repeatedly with various passwords until the account is locked out.

upvoted 1 times

Dee83 1 year, 11 months ago

A. Conducting an offline attack on the hashed password information is the best method for brute forcing passwords. This method involves obtaining a copy of the hashed password data and using specialized tools to perform a dictionary, rule-based, or pure brute force attack. This method is effective because it allows for a large number of password guesses to be made quickly and without alerting the system being attacked or triggering account lockout mechanisms. It also reduces the risk of detection and IP blocking by the target system. However, it is important to note that offline password cracking is illegal in some jurisdictions and organizations.

upvoted 1 times

Pappykay 1 year, 11 months ago

Selected Answer: A

With enough time, attackers can discover any hashed password using an
offline brute-force attack. However, longer passwords result in sufficiently
longer times, making it infeasible for attackers to crack them.

upvoted 1 times

trojix 1 year, 11 months ago

Selected Answer: A

It is truly blowing my mind that people studying for CISSP are choosing "B". That is a dictionary attack, not bruteforce.

upvoted 2 times

> **dumdada** 1 year, 6 months ago
>
> Rapid7 website says verbatim about dictionnary attack: "A type of brute force attack where an intruder attempts to crack a password-protected security system with a “dictionary list” of common words and phrases used by businesses and individuals."
>
> upvoted 2 times

Mr_Zaw 1 year, 12 months ago

A

There are two modifications that attackers can make to enhance the
effectiveness of a brute-force attack:
Rainbow tables provide precomputed values for cryptographic
hashes. These are commonly used for cracking passwords storedon a system in hashed form.

upvoted 1 times

Delab202 1 year, 12 months ago

A password strength tester gauges how long it might hypothetically take to crack your password by testing the password against a set of known criteria–such as length, randomness, and complexity.

upvoted 1 times

Delab202 1 year, 12 months ago

The main difference between a brute force attack and a rainbow table attack is that there is precomputed data involved with a rainbow table when trying to crack passwords whereas there is no precomputed data when a brute force is to be performed.

B is rainbow table

upvoted 1 times

⊟ **somkiatr** 1 year, 12 months ago

Selected Answer: A

A and B would be correct. The point is online and offline. B doesn't mention about offline so if we perform brute forcing online then the user may be locked.

upvoted 1 times

⊟ **Firedragon** 2 years, 1 month ago

Selected Answer: A

A.

This is an offline brute-force attack. Official study guide P705

upvoted 3 times

⊟ **RVoigt** 1 year, 11 months ago

100% A, if you believe the Official Study Guide P704-705

upvoted 1 times

⊟ **Jamati** 2 years, 1 month ago

Selected Answer: A

So easy. Answer is A

upvoted 1 times

⊟ **Jay_12** 2 years, 1 month ago

Answer is A - b talks about word. If it says something like "combination of words, numbers and characters" then may be B.

upvoted 1 times

Question #135 *Topic 1*

Which of the following is the name of an individual or group that is impacted by a change?

A. Change agent

B. End User

C. Stakeholder

D. Sponsor

Suggested Answer: *B*

Community vote distribution

C (56%) B (44%)

stickerbush1970 Highly Voted 2 years, 3 months ago

Selected Answer: C

A stakeholder is defined as an individual or group that has an interest in any decision or activity of an organization.

upvoted 10 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

dev46 Highly Voted 2 years, 3 months ago

Selected Answer: C

Stakeholder can be user too - it's a good answer

upvoted 9 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: C

Can't be B. End user is a specific type of stakeholder who directly uses the system but does not cover all impacted parties.

upvoted 1 times

CCNPWILL 8 months, 2 weeks ago

End user and stakeholder is correct.. " stake holder is more important than end user so C. ThInK liKE a CiSSp"

upvoted 2 times

gjimenezf 11 months, 3 weeks ago

Selected Answer: C

Typically, we categorize change management stakeholders into three main groups which each have their own part to play in the process: those impacted by the change, those that support the execution of the change, and those who drive the change.

upvoted 1 times

629f731 11 months, 3 weeks ago

Selected Answer: C

"Stakeholders" include all parties interested in a project or change, which can encompass a variety of groups, including end users, sponsors, customers, employees, among others, who may be affected, influenced or have interest in the proposed change. "End users" are a specific subset of "stakeholders" who directly experience the implications of the change in their daily activities or functions.

upvoted 2 times

Soleandheel 1 year ago

C. Stakeholder. The end user is also a stakeholder.

upvoted 1 times

Vince_F_Fang 1 year, 1 month ago

Selected Answer: B

The term 'end user' itself represents the direct stakeholders of the system, and other roles are only indirect influences. Stakeholders and sponsors have many things to do and invest in many projects, so they may not necessarily care about what a single system invested in will become

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

The answer is C. Stakeholder. A stakeholder is any individual or group that has an interest or concern in an organization's activities or decisions, including changes in the area of information security management.

upvoted 2 times

Bach1968 1 year, 5 months ago

Selected Answer: B

In the context of a change, the term "End User" refers to an individual or group that is impacted by the change. End users are the individuals who will directly interact with and use the product or service resulting from the change. They play a crucial role in the success and adoption of the change.

upvoted 3 times

crazywai1221 1 year, 9 months ago

Selected Answer: B

end users are directly impacted by changes, stakeholders are directly impacted

upvoted 2 times

Qwertyloopback 1 year, 10 months ago

Selected Answer: B

I was on the fence between B and C. The word impact stuck out for me. While stakeholders have an interest, they generally are not impacted.

upvoted 5 times

somkiatr 1 year, 12 months ago

Selected Answer: B

Agreed with B. The target group of the change process would be called "End User" The stakeholder contains all parties in the company which may not impacted by the change process.

upvoted 2 times

Ivanchun 2 years ago

Selected Answer: B

B, it same who impact the changes

upvoted 2 times

oudmaster 2 years ago

From business point of view, the answer is stakeholders.

upvoted 2 times

Arunlab 2 years, 1 month ago

Selected Answer: B

The international standard providing guidance on social responsibility, called ISO 26000, defines a stakeholder as an "individual or group that has an interest in any decision or activity of an organization."

Stakeholders may include suppliers, internal staff, members, customers (including shareholders, investors, and consumers), regulators, and local and regional communities. Additionally, stakeholders may include purchasers, clients, owners, and non-governmental organizations (NGOs).

Ans: B

upvoted 3 times

rootic 2 years, 2 months ago

Selected Answer: C

Agree with C

upvoted 2 times

Question #136 *Topic 1*

The European Union (EU) General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Data Owner should therefore consider which of the following requirements?

A. Never to store personal data of EU citizens outside the EU

B. Data masking and encryption of personal data

C. Only to use encryption protocols approved by EU

D. Anonymization of personal data when transmitted to sources outside the EU

Suggested Answer: *B*

Community vote distribution

B (79%) A (21%)

BigITGuy 3 months ago

Selected Answer: B

Can't be A. GDPR does not prohibit storage of personal data outside the EU, but it requires appropriate safeguards if data is transferred internationally. Can't be C. GDPR recommends appropriate encryption, but does not mandate the use of specific EU-approved protocols.
Can't be D/ Anonymization is encouraged but is not strictly required for every transmission; pseudonymization or encryption is often sufficient depending on risk.

upvoted 1 times

RRabbit_111 6 months, 4 weeks ago

Selected Answer: B

A C and D all utilize ABSOLUTES in their answers where B does not and it's asking for the reasonable measure.

upvoted 1 times

8b48948 1 year, 2 months ago

No way its B "think like a manager" - has to be D.

upvoted 1 times

629f731 1 year, 5 months ago

Selected Answer: B

Option A states "Never store personal data of European Union citizens outside the European Union." Although the international transfer of personal data outside the EU is subject to restrictions under the General Data Protection Regulation (GDPR), the law does not strictly prohibit the storage of EU citizens' data outside the region.

Rather than outright prohibiting the storage of data outside the EU, the GDPR states that when personal data is transferred outside the European Union to non-EU countries, appropriate safeguards must be implemented to ensure an adequate level of data protection. These safeguards may include standard contractual clauses, the use of approved certification instruments, or the assessment of the adequacy of the recipient country in terms of data protection.

upvoted 3 times

74gjd_37 1 year, 9 months ago

Selected Answer: B

Data masking and encryption of personal data are some of the measures that can be taken to ensure the security of personal data. However, the GDPR does not require organizations to store personal data of EU citizens only within the EU or use encryption protocols approved by the EU. In contrast, the Russian law of privacy requires companies to store personal data of Russian citizens on servers located within the territory of the Russian Federation. Failure to comply with this requirement may result in fines and other penalties. The GDPR does not impose such a requirement.

upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: B

The correct answer is B. Data masking and encryption of personal data.

The EU General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to ensure the security of personal data. Data masking and encryption are examples of such measures.

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: A

GDPR requires that all EU citizen data be stored within the EU.

upvoted 3 times

Firedragon 2 years, 7 months ago

Does GDPR data need to be stored in EU?

The GDPR requires that all data collected on citizens must be either stored in the EU, so it is subject to European privacy laws, or within a jurisdiction that has similar levels of protection.

upvoted 2 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

sphenixfire 2 years, 7 months ago

Selected Answer: B

Only possible regarding biz

upvoted 3 times

rdy4u 2 years, 8 months ago

Selected Answer: B

A data owner is responsible for the data within their perimeter in terms of its collection, protection and quality.

upvoted 4 times

Question #137 Topic 1

What is the PRIMARY benefit of incident reporting and computer crime investigations?

A. Complying with security policy

B. Repairing the damage and preventing future occurrences

C. Providing evidence to law enforcement

D. Appointing a computer emergency response team

Suggested Answer: *C*

Community vote distribution

B (57%) C (34%) 6%

⊟ **kasiya** Highly Voted 👍 2 years, 9 months ago

Selected Answer: B

benefit! only B

upvoted 12 times

⊟ **jackdryan** 2 years, 1 month ago

C is correct

upvoted 1 times

⊟ **Meowson** 1 year, 11 months ago

Stop giving out meaningless reply without supporting reason.

upvoted 12 times

⊟ **BigITGuy** Most Recent ⏲ 2 months, 4 weeks ago

Selected Answer: B

Not C - Providing evidence to law enforcement may be necessary in some cases, but it's secondary to restoring business operations and preventing future incidents.

upvoted 1 times

⊟ **Rachy** 10 months, 2 weeks ago

Selected Answer: B

All answers should always point to objective of the business. Would your answer benefit the business as a Ceo?

upvoted 1 times

⊟ **pete79** 1 year, 4 months ago

Selected Answer: A

A: Incident reporting can be part of policy, however not every reported incident is required by law enforcers as there might not be an investigation

upvoted 1 times

⊟ **gjimenezf** 1 year, 5 months ago

Selected Answer: B

prevent from happening again is more important than provide evidence otherwise you will provide evidence multiple times and lower the trust in your company

upvoted 1 times

⊟ **Vince_F_Fang** 1 year, 7 months ago

Selected Answer: C

C. Setting aside the company's responsibilities, preventing unnecessary litigation, and investigating can also prevent future incidents from happening again

upvoted 2 times

⊟ **Moose01** 1 year, 8 months ago

A. it is A, an Incident is different then an accident - Incident has no damage where accident has damages... all incidents must be documented per Organization set policies.

upvoted 1 times

⊟ **LalithW** 1 year, 8 months ago

Selected Answer: C

Incident reporting and crime investigation provide evidence to law enforcement. Lessons learned support preventing future occurrences, which has not been mentioned here.

upvoted 1 times

williom 1 year, 9 months ago

I think it's B, thinking like a manager.

- Primary benefit to the organisation, B.

Primary benefit to society, C

upvoted 2 times

74gjd_37 1 year, 9 months ago

Selected Answer: B

The PRIMARY benefit of incident reporting and computer crime investigations is B: "Repairing the damage and preventing future occurrences". Incident reporting helps to identify and analyze security incidents, and computer crime investigations help to determine the cause of the incident and take steps to prevent it from happening again in the future. While complying with security policy, providing evidence to law enforcement, and appointing a computer emergency response team are important, they are not the primary benefit of incident reporting and computer crime investigations.

Providing evidence to law enforcement is an important benefit of incident reporting and computer crime investigations, but it is not the primary benefit because the main focus of incident reporting and computer crime investigations is to repair the damage and prevent future occurrences.

upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: C

the PRIMARY benefit can be considered as C. Providing evidence to law enforcement.

providing evidence to law enforcement is an important benefit of incident reporting and computer crime investigations. While repairing the damage and preventing future occurrences is also a significant benefit, the ability to provide evidence to law enforcement can contribute to the identification, apprehension, and prosecution of individuals involved in computer crimes. It helps in holding perpetrators accountable for their actions and deterring future criminal activity.

upvoted 1 times

HughJassole 2 years ago

I am going with B. An incident report can be anything, like a drive that failed, or a server that crashed, etc. So that needs to be repaired. That's the benefit of an incident report, that the problem will be fixed. Only B addresses repairing a crashed server. Now the confusing part is the crime investigation, but once you figure out how it happened it can be prevented in the future. Complaining to law enforcement is often pointless bc computer crimes are hard to prosecute since they don't have a clear jurisdiction and criminals are hard to catch. So B seems pretty solid, although C is a part of the answer.

upvoted 3 times

jbell 2 years, 1 month ago

Selected Answer: B

From CBK: All incidents should be investigated and remediated to restore the organization's normal operations as quickly as possible and to minimize impacts like lost productivity or revenue. Resuming normal service is the primary goal of incident management.

upvoted 4 times

> **jbell** 2 years, 1 month ago
>
> From NIST SP 800-61 Computer Security Incident Handling Guide:
>
> Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings.
>
> upvoted 1 times

BennyMao 2 years, 1 month ago

Selected Answer: B

By conducting investigations and reporting incidents, organizations can identify the root cause of the incident and take corrective action to prevent it from happening again. Additionally, incident reporting and investigations can help organizations to improve their security posture by identifying vulnerabilities and weaknesses in their security controls.

upvoted 1 times

Dee83 2 years, 5 months ago

C. Correct answer

Providing evidence to law enforcement is the PRIMARY benefit of incident reporting and computer crime investigations.

The primary goal of incident reporting and computer crime investigations is to collect evidence that can be used to identify and prosecute the individuals or organizations responsible for the crime. This may include identifying the methods used to gain unauthorized access, determining the extent of the damage caused, and identifying any sensitive data that may have been compromised.

A. Complying with security policy is also important as it helps organizations to identify and report incidents as part of their compliance requirements and to meet the regulatory requirements.

B. Repairing the damage and preventing future occurrences is a secondary goal. It can help to minimize the damage caused by the incident and prevent it from happening again in the future.

D. Appointing a computer emergency response team (CERT) is an important step in incident response, CERT team can play a key role in identifying and responding to security incidents and to help organizations to recover from the incident.

upvoted 2 times

dumdada 2 years ago

You're just copy/pasting ChatGPT on every question?

upvoted 1 times

Delab202 2 years, 5 months ago

Selected Answer: D

Policies drives what is an incident and reportable.

upvoted 1 times

Delab202 2 years, 5 months ago

option A

upvoted 1 times

somkiatr 2 years, 6 months ago

Selected Answer: C

C is correct.

What is computer forensics?

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

reference: https://www.techtarget.com/searchsecurity/definition/computer-forensics

upvoted 1 times

Question #138 *Topic 1*

Which of the following is the MOST common method of memory protection?

A. Error correction

B. Virtual local area network (VLAN) tagging

C. Segmentation

D. Compartmentalization

Suggested Answer: *C*

Community vote distribution

C (100%)

deeden 10 months, 3 weeks ago

Selected Answer: C

You're right. I had to ask AI just to find this out. Memory segmentation was widely used in older computer architectures, particularly in the 1980s and early 1990s. The Intel x86 architecture, for example, relied on segmentation in both real mode and protected mode. However, as systems evolved, the complexity and limitations of segmentation led to its decline in favor of paging and other memory management techniques. By the late 1990s and early 2000s, most modern operating systems and CPUs had largely moved away from segmentation — Modern systems often rely more on techniques like paging, ASLR (Address Space Layout Randomization) and other mechanisms for memory protection, which offer greater flexibility and efficiency.

upvoted 3 times

8b48948 1 year, 2 months ago

20 yrs in IT, never heard of memory segmentation, closest thing to it is containersation but dont know of any OS flavours you can actually carve up the available RAM.

upvoted 2 times

Soleandheel 1 year, 6 months ago

Memory protection using segmentation is a method of dividing system memory into different segments to control and protect memory access. It is commonly used in x86 architecture systems, where the global descriptor table (GDT) and local descriptor table (LDT) are used to define memory segments and access permissions for different processes or segments of memory.

upvoted 2 times

74gjd_37 1 year, 9 months ago

Selected Answer: C

Segmentation (option C) is still the most common method of memory protection. While error correction (option A) is also a method used to protect memory from errors, it is not as commonly used as segmentation, because it requires expensive hardware (ECC memory and processors that support such memory). Segmentation is widely used in modern operating systems to partition memory into segments and to assign different levels of access permissions to each segment, which helps protect the system from unauthorized access and malicious attacks. Virtual local area network (VLAN) tagging (option B) is a network security technique used to partition a physical network into multiple virtual networks, and compartmentalization (option D) is a technique used to separate different types of data and processes into isolated compartments to reduce the impact of a security breach.

upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: C

The MOST common method of memory protection is segmentation. Segmentation refers to dividing the memory into logical segments or sections, each with its own access rights and permissions. This allows for the isolation and protection of different parts of memory, preventing unauthorized access or modification. Segmentation helps enhance the security and stability of the system by limiting the impact of errors or malicious activities within a specific memory segment.

upvoted 3 times

Jamati 2 years, 7 months ago

Selected Answer: C

Memory protection is a way to control memory access rights on a computer, and is a part of most modern instruction set architectures and operating systems. The x86 architecture has multiple segmentation features, which are helpful for achieving this memory protection. A segment is identified by a reference to a memory location and a segment descriptor may limit access rights, e.g., read only, only from certain rings.

upvoted 3 times

⊟ **jackdryan** 2 years, 1 month ago

C is correct

upvoted 1 times

⊟ **Rollizo** 2 years, 9 months ago

Memory Protection using Segmentation: It is a method of dividing the system memory into different segments. The data structures of x86 architecture of OS like local descriptor table and global descriptor table are used in the protection of memory.

upvoted 4 times

Question #139 *Topic 1*

What testing technique enables the designer to develop mitigation strategies for potential vulnerabilities?

A. Source code review

B. Threat modeling

C. Penetration testing

D. Manual inspections and reviews

Suggested Answer: *B*

Community vote distribution

B (89%) 11%

franbarpro Highly Voted 2 years, 2 months ago

Selected Answer: B

Threat modeling is a proactive method of uncovering threats not usually considered or found through code reviews and other types of audits

- Techtarget

upvoted 7 times

dev46 Highly Voted 2 years, 3 months ago

Selected Answer: B

Threat modeling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified and enumerated, and countermeasures prioritized.

- Source (Wiki)

upvoted 7 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

TheManiac Most Recent 7 months, 1 week ago

Selected Answer: B

potential vulnerabilities = Threat modeling

upvoted 1 times

Vasyamba1 9 months, 1 week ago

Taking my words back. From the OSG about the SAMM Model - Design The process used by the organization to define software requirements and create software. This function includes practices for threat modeling, threat assessment, security requirements, and security architecture. So, B is probably correct.

upvoted 1 times

Vasyamba1 9 months, 1 week ago

Selected Answer: A

As for me, the designer has nothing to do with threat modeling and pentesting.

upvoted 1 times

Vince_F_Fang 1 year, 1 month ago

The keyword is the designer, indicating that it is in the design phase

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

The correct answer is B. Threat modeling is a testing technique that enables the designer to develop mitigation strategies for potential vulnerabilities in software. It involves identifying potential threats and vulnerabilities in a software system and then developing and implementing strategies to mitigate those threats and vulnerabilities. This process can help to ensure that a software system is secure and can help to prevent security breaches and other types of cyber attacks. The other options listed are also testing techniques that can be used to identify potential vulnerabilities in software, but they do not directly enable the designer to develop mitigation strategies for those vulnerabilities.

upvoted 2 times

rootic 2 years, 2 months ago

Selected Answer: A

It's A. Is source code review a testing technique? - Yes

Is it enables the designer to develop mitigation strategies for potential vulnerabilities? - Yes

Threat modeling is testing technique ? - No

Pentest allow to remidiate vulns that was fount and not potential.

Clearly answer is A.

upvoted 1 times

rootic 2 years, 2 months ago

"What testing technique..."

Threat modeling is testing technique ?

upvoted 4 times

Rollizo 2 years, 3 months ago

threat modeling also implements test during the development phase

upvoted 1 times

Question #140 *Topic 1*

Assuming an individual has taken all of the steps to keep their internet connection private, which of the following is the BEST to browse the web privately?

A. Store information about browsing activities on the personal device.

B. Prevent information about browsing activities from being stored on the personal device.

C. Prevent information about browsing activities from being stored in the cloud.

D. Store browsing activities in the cloud.

Suggested Answer: *C*

Community vote distribution

C (54%) B (46%)

projtfer Highly Voted 2 years, 8 months ago

Selected Answer: C

I select C, because if you have stored the browsing/watching/liked history in your local device, it is still private, however if it is in the cloud such as google browse history, it can be turned over to law enforcement authorities unless the user goes and clears the history.

upvoted 12 times

dmo_d Highly Voted 2 years, 1 month ago

Selected Answer: C

It's about privacy aka protection of the users personal data.

The user has control over its own it - so all aspects concerning the users local is not the biggest issue.

But as soon as private data leaves the personal it the user has no control over it. so best thing is to avoid PII getting onto others computers (aka cloud).

upvoted 5 times

a_kto_to Most Recent 1 month, 1 week ago

Selected Answer: B

Because C will not exclude option B, I will start with personal device first, then will think about any cloud. So B.

upvoted 1 times

f168100 3 months, 2 weeks ago

Selected Answer: B

I will go for b

The correct answer is **B. Prevent information about browsing activities from being stored on the personal device.**

Explanation:

- Preventing the storage of browsing activities on the personal device is key to maintaining privacy, as it minimizes the digital footprint that can be accessed by third parties or malicious actors.

- **Option A (store information on the device)** is the opposite of privacy.

- **Option C (prevent cloud storage)** is helpful but not sufficient on its own.

- **Option D (store in the cloud)** introduces additional risks of data breaches and third-party access.

Combining private browsing modes, VPNs, and encrypted communications further enhances privacy.

upvoted 1 times

easyp 5 months ago

Selected Answer: B

While it is important to avoid storing browsing data in the cloud, this is secondary to ensuring no information is stored on the personal device itself. Cloud storage is less of a concern if local traces are eliminated.

upvoted 1 times

angellorv 6 months, 2 weeks ago

Selected Answer: B

Private browsing - it stops your browser from tracking you, it doesn't use cookies. Activity in private browsing mode is also not stored in the browser's history.
https://www.digitaltrends.com/computing/how-to-browse-the-web-privately/

upvoted 1 times

Rachy 10 months, 2 weeks ago

Selected Answer: B

Right answer is B. Read the question again guys

upvoted 1 times

Bietchasup 7 months ago

you never provide any reasoning....

upvoted 2 times

deeden 10 months, 3 weeks ago

Selected Answer: B

B. because steps taken to keep internet connection private, which could mean Firewall, Proxy, VPN, Tor, and all that good stuff.

B. ensures that even if someone gains access to your device, they won't be able to retrieve your browsing history, which enhances privacy. Techniques to achieve this include using private/incognito browsing modes and configuring browser settings to not store history or cookies.

Unless of course you got nsa sniffing on your last hop traffic, then you're toast :)

upvoted 2 times

1460168 11 months ago

Selected Answer: C

C: Because if your data leaves your device to a cloud provider, your data is not private anymore and out of your control, too.

upvoted 3 times

ElDirec 11 months, 1 week ago

Selected Answer: B

This is talking about incognito/private browsing. What does that not do? Store your browsing activities in the local device.

upvoted 1 times

JohnBentass 1 year ago

B.

This option is the most effective in maintaining privacy because it directly addresses the local storage of data, which can include browsing history, cookies, and cache. By preventing this information from being stored, you minimize the risk of it being accessed by unauthorized parties or malware that could compromise your privacy.

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: B

I choose B, because preventing information of being stored locally doesn't automatically mean you store it in the cloud. You may not store it at all.

upvoted 2 times

stack120566 1 year, 3 months ago

The best way to browse the web privately, assuming an individual has taken all necessary steps to secure their internet connection, is to prevent information about browsing activities from being stored on the personal device. By avoiding local storage of browsing history, cookies, and other data, users can minimize the risk of exposure to potential privacy breaches. This approach ensures that sensitive information remains within the confines of the user's device and is not easily accessible to others.

Option B is the correct choice for maintaining privacy while browsing the web. Storing browsing activities on the personal device could potentially lead to data leaks or unauthorized access if the device is compromised. Options C and D involve external storage (in the cloud), which introduces additional security risks. Therefore, preventing local storage is the most effective strategy for maintaining privacy.

upvoted 1 times

Woo7 1 year, 4 months ago

Selected Answer: C

C, they took the steps for the "internet connection", has nothing to do with data storage in the cloud.

upvoted 1 times

pete79 1 year, 4 months ago

Selected Answer: B

Because private device is the only under user's control.

upvoted 2 times

Vince_F_Fang 1 year, 7 months ago

Selected Answer: B

Since it's private browsing, the option to store information is obviously incorrect. I don't think she has the ability to ensure that her browsing activities are stored in the cloud, so I chose B

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: B

The BEST option to browse the web privately is B: "Prevent information about browsing activities from being stored on the personal device". This can be achieved by using private browsing modes or clearing browsing history and cache regularly. Storing browsing activities on the personal device or in the cloud can compromise privacy and potentially expose sensitive information. It is important to note that while browsing privately can help protect privacy to a certain extent, it does not guarantee complete anonymity or protection from all types of online tracking.

Options C and D about storing information in the cloud do not fit the context of browsing the web privately. The cloud is a remote server used for storing and accessing data, and it is not directly related to browsing privacy. Therefore, options B and A are the most relevant to the question.

upvoted 1 times

Question #141 *Topic 1*

A software engineer uses automated tools to review application code and search for application flaws, back doors, or other malicious code. Which of the following is the FIRST Software Development Life Cycle (SDLC) phase where this takes place?

A. Deployment

B. Development

C. Test

D. Design

Suggested Answer: *B*

Community vote distribution

B (79%) 14% 7%

⊟ **franbarpro** Highly Voted 👍 2 years, 2 months ago

Selected Answer: B

I think the answer is "B" and here's why:
Development Stage
The development stage is the part where developers actually write code and build the application according to the earlier design documents and outlined specifications.

This is where Static Application Security Testing or SAST tools come into play.

Product program code is built per the design document specifications. In theory, all of the prior planning and outlined should make the actual development phase relatively straightforward.

Developers will follow any coding guidelines as defined by the organization and utilize different tools such as compilers, debuggers, and interpreters.

I thought of "C" - Testing phase - but the question says Which of the following is the FIRST?
upvoted 6 times

⊟ **gjimenezf** Most Recent ⏲ 11 months, 3 weeks ago

Selected Answer: B

As we pivot from blueprint to build, static code analysis evolves into a daily routine. Within the development phase, it turns into a meticulous overseer, scrutinizing every new line of code for deviations from the set path.
upvoted 1 times

⊟ **Soleandheel** 1 year ago

B. Development .....it starts at the Development stage even though it mostly happens in the testing phase.
upvoted 1 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: B

it is development, you may see it also as testing at the same time
upvoted 1 times

⊟ **HughJassole** 1 year, 6 months ago

C. Test phase:
"Assessments entail the performance of functional testing: unit testing, code quality testing, integration testing, system testing, security testing, performance testing and acceptance testing, as well as nonfunctional testing. If a defect is identified, developers are notified. Validated (actual) defects are resolved, and a new version of the software is produced.

The best method for ensuring that all tests are run regularly and reliably, is to implement automated testing. "

So automated testing is a keyword and security.
https://www.synopsys.com/glossary/what-is-sdlc.html
upvoted 4 times

NJALPHA 1 year, 8 months ago

Answer B:

SDLC 6 stages : 1-Planning & Analysis 2-Design 3- Development 4-Testing 5- Deployment 6- Maintenance so based on the provided scenario will fall in to Development SDLC stage

upvoted 1 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

Rollingalx 1 year, 9 months ago

Selected Answer: C

Correct answer is C. Development is not a phase in SDLC. The SDLC phases are: Requirements analysis/Design/Implementation/Testing/Evolution

upvoted 1 times

explorer3 2 years, 2 months ago

Selected Answer: B

Code review by developers is part of the Development Phase

https://resources.infosecinstitute.com/topic/secure-code-review-practical-approach/#:~:text=In%20the%20SDLC%20(Software%20Development,the%20code%20review%2C%20or%20both.

upvoted 3 times

MG1707 2 years, 2 months ago

Selected Answer: D

the FIRST appearance

upvoted 2 times

MG1707 2 years, 2 months ago

it shall start already in Design phase

upvoted 1 times

franbarpro 2 years, 2 months ago

How are you going to test code that you haven't written?

upvoted 6 times

ccmmaa 2 years, 2 months ago

should be C, test environment for auto code review

upvoted 2 times

Question #142 *Topic 1*

A company developed a web application which is sold as a Software as a Service (SaaS) solution to the customer. The application is hosted by a web server running on a specific operating system (OS) on a virtual machine (VM). During the transition phase of the service, it is determined that the support team will need access to the application logs. Which of the following privileges would be the MOST suitable?

A. Administrative privileges on the hypervisor

B. Administrative privileges on the application folders

C. Administrative privileges on the web server

D. Administrative privileges on the OS

Suggested Answer: *B*

Community vote distribution

B (59%) C (41%)

⊟ **HarkonMoseley** 1 month, 1 week ago

Selected Answer: D

Is not a good pratice store the logs together with the application folder in a web application.
and how to give access to application folder without give access to the Operating System?

upvoted 1 times

⊟ **BigITGuy** 2 months, 4 weeks ago

Selected Answer: B

Not C. Administrative privileges on the web server — Excessive, unless they need to configure or operate the web server itself, which is not mentioned.

upvoted 1 times

⊟ **deeden** 10 months, 3 weeks ago

Selected Answer: B

Agree with B. Admin access to web server allow access to all other application being hosted on that web server. Although there's only one SaaS mentioned, but correct... least privilege principle.

Here's a simplified hierarchical breakdown from the hypervisor to the application folder:

>Hypervisor: Manages virtual machines.
>Operating System: Provides the base environment for applications.
>Web Server: Software application responsible for serving web content.
> Web Server Configuration Files: Store settings for the web server.
> Log Files: Record server activity.
> Application Folders: Contain specific web applications.
> Application Code: Source code for the application.
> Application Data: Configuration files, databases, and other data.
> Application Logs: Specific logs for the application.

upvoted 4 times

⊟ **TheManiac** 1 year, 1 month ago

Selected Answer: B

Least priv is the key here. Dont give access more than they need.
application folders access is what they need.
So, C. Administrative privileges on the web server is wrong. you break least priv here

upvoted 4 times

⊟ **stack120566** 1 year, 3 months ago

Option B is correct . I agree with 629f731.Those of us that have had to scour logs understand that the application does not hold all of the logs. In many cases applications log very little.

upvoted 1 times

⊟ **629f731** 1 year, 5 months ago

Selected Answer: C

Option B involves granting administrative privileges directly to the application folders. While it can provide access to application logs, it also carries additional risks. With access to application folders, changes or modifications can be made to other system files, which could compromise the stability or security of the application if inadvertent or unauthorized modifications are made. Additionally, logs may not be exclusively contained in specific application folders, so limiting privileges to folders only does not guarantee complete access to all necessary logs. For these reasons, option C (administrative privileges on the web server) might be more appropriate as it allows more controlled access to logs without providing direct access to other system components.

upvoted 4 times

Soleandheel 1 year, 6 months ago

B. Administrative privileges on the application folders

upvoted 2 times

Soleandheel 1 year, 6 months ago

least privilege guys. You want to give them access to only what they need to do the Job. No more, no less.

upvoted 3 times

Ukpes 1 year, 7 months ago

B is the right answer. You do not need to have admin privileges to the web server but rather to the app folders. Reason: the principle of least privilege!

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: C

The MOST suitable privilege in this scenario would be C. Administrative privileges on the web server. This would allow the support team to access and analyze the application logs without compromising the security of the hypervisor or the underlying OS. Administrative privileges on the application folders or the OS may be too broad and could potentially allow access to sensitive information beyond just the logs.

upvoted 2 times

Bach1968 1 year, 11 months ago

Selected Answer: B

B. Administrative privileges on the application folders

upvoted 1 times

HughJassole 2 years ago

So we have no idea where the application logs are written to. I am a linux admin and some apps write in their own folders, some write to /var/log, the same place the OS writes to. So I don't think this question provides enough info to answer. A best guess would be B, least privilege, but there is no way to know.

upvoted 2 times

MShaaban 1 year, 10 months ago

I thought the same. Agree with your approach.

upvoted 1 times

DASH_v 2 years, 2 months ago

Selected Answer: C

The most suitable privilege in this scenario would be administrative privileges on the web server.

This is because the web server is responsible for hosting the web application and generating the application logs. By granting administrative privileges on the web server, the support team would be able to access the logs without having complete control over the underlying OS or other applications running on the same VM.

Granting administrative privileges on the hypervisor or the OS would give the support team access to more than just the application logs, which could pose a security risk. Granting administrative privileges on the application folders alone may not provide the support team with enough access to view and analyze the logs.

upvoted 2 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: B

As Humongous1593 has already said. Least privilege rule applies.

upvoted 3 times

⊟ **Coolwater** 2 years, 8 months ago

A,C,D are managed by cloud vendor

upvoted 2 times

⊟ **franbarpro** 2 years, 8 months ago

Give them access to the only resources they need to do their job. No more no less!

upvoted 4 times

⊟ **Humongous1593** 2 years, 8 months ago

Selected Answer: B

Least privilege

upvoted 3 times

Question #143 *Topic 1*

A security practitioner detects an Endpoint attack on the organization's network. What is the MOST reasonable approach to mitigate future Endpoint attacks?

A. Remove all non-essential client-side web services from the network.

B. Harden the client image before deployment.

C. Screen for harmful exploits of client-side services before implementation.

D. Block all client-side web exploits at the perimeter.

Suggested Answer: *C*

Community vote distribution

B (77%) C (23%)

stickerbush1970 Highly Voted 2 years, 9 months ago

I'm leaning more towards B than C.

upvoted 14 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

giovi Highly Voted 2 years, 8 months ago

Selected Answer: B

B makes more sense

upvoted 8 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: B

Hardening reduces the attack surface and helps prevent attackers from easily compromising endpoints. Screening for exploits is useful but does not address endpoint security after deployment.

upvoted 1 times

stack120566 7 months, 1 week ago

The suggested answer , B, only makes sense if the endpoints were to be re-imaged but this step is not mentioned

upvoted 1 times

klarak 1 year, 2 months ago

I can't even figure out what the question has to do with the answers...

upvoted 4 times

sbear123 1 year, 3 months ago

Selected Answer: C

I chose C as all other options are targeting specific cause of attack. Question does not mention the reason of attack.

upvoted 1 times

hoho2000 1 year, 3 months ago

Selected Answer: C

Would go with C. Question is on security and ask REASONABLY, so which option aligns more towards how a security reaction would be? Hardening is part and parcel but will it really stop attacks? Rem TOCTOU concept.

Screening action has more biased towards Security aspect although also susceptible to TOCTOU. Try not to over think between the 2.

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: B

Answer B)

B will make the attack surface footprint smaller.

Both C and D are essentially the same (one looks for and the other blocks...but in both case you have to know exactly what you are looking for and this will not help at all with ZERO DAY exploits).

upvoted 2 times

shmoeee 1 year, 7 months ago

It"s between B and C. I'm going with C because it seems more managerial. Hardening the endpoint seems more technical

upvoted 1 times

shmoeee 1 year, 7 months ago

Also want to note that although the image is hardened, that doesn't mean it is fully protected from all endpoint attacks. At least after screening, you will know all the possible attacks before deployment. These screen attacks can determine necessary endpoint configurations.IMO

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: B

The most reasonable approach to mitigate future Endpoint attacks would be to harden the client image before deployment. This means ensuring that the endpoint devices are properly configured, patched, and updated to reduce vulnerabilities that can be exploited by attackers. This approach would help to prevent future attacks and improve the overall security posture of the organization. The other options listed can also be helpful in improving security, but hardening the client image is the best first step to take in this scenario.

upvoted 4 times

Bach1968 1 year, 11 months ago

Selected Answer: C

screening for harmful exploits of client-side services before implementation (option C) is also an important approach to mitigate future Endpoint attacks.

Screening for harmful exploits involves assessing and evaluating client-side services and their potential vulnerabilities before they are implemented in the network. By conducting security assessments and testing for known vulnerabilities or exploits, organizations can identify and address potential risks and weaknesses in client-side services. This proactive approach helps prevent the introduction of vulnerable software or services that could be targeted by attackers.

Both options B (hardening the client image) and C (screening for harmful exploits) are important steps to enhance the security of endpoints and mitigate the risk of future attacks. These measures should be implemented in combination to establish a robust defense against Endpoint attacks.

upvoted 1 times

dmo_d 2 years, 1 month ago

Selected Answer: C

I was struggeling between B and C.
Because B is general preventive against various misconfiguration and C is a mitigation to specific threads (which may or may not a configuration issue) I choose C.
C also covers common vulnerability scanning and so on.

upvoted 2 times

cryptofetti 2 years, 2 months ago

Why wouldn't hardening the client image be more desired?

Harden the client image before deployment is the most reasonable approach to mitigating future Endpoint attacks. Hardening the client image involves removing or disabling any unnecessary software or services, configuring the system to meet security best practices, and implementing appropriate security controls. By removing or disabling unnecessary software or services, the attack surface of the system is reduced, making it more difficult for attackers to exploit vulnerabilities in the system.

upvoted 3 times

meelaan 2 years, 6 months ago

Selected Answer: B

B looks right

upvoted 1 times

oudmaster 2 years, 6 months ago

Selected Answer: B

My heart tells me B

upvoted 1 times

IXone 2 years, 8 months ago

could be corrected C, restricting compliance and security policies that reduce the attack surface of endpoints

upvoted 1 times

⊟ **franbarpro** 2 years, 8 months ago

Selected Answer: B

B it is

upvoted 2 times

Question #144 *Topic 1*

What are the essential elements of a Risk Assessment Report (RAR)?

A. Executive summary, body of the report, and appendices

B. Executive summary, graph of risks, and process

C. Table of contents, testing criteria, and index

D. Table of contents, chapters, and executive summary

Suggested Answer: *A*

Community vote distribution

A (100%)

⊟ **rdy4u** Highly Voted 1 year, 8 months ago

Selected Answer: A

The essential elements of information in a risk assessment can be described in three sections of the risk assessment report (or whatever vehicle is chosen by organizations to convey the results of the assessment):
(i) an executive summary;
(ii) the main body containing detailed risk assessment results; and
(iii) supporting appendices

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
upvoted 11 times

⊟ **jackdryan** 1 year, 1 month ago

A is correct
upvoted 1 times

⊟ **Bach1968** Most Recent 11 months, 4 weeks ago

Selected Answer: A

he essential elements of a Risk Assessment Report (RAR) typically include:

A. Executive summary: This section provides a high-level overview of the risk assessment, including key findings, identified risks, and recommended actions. It is designed to provide a concise summary for executive stakeholders.

B. Body of the report: This section contains the detailed analysis and findings of the risk assessment. It includes information such as the scope of the assessment, methodology used, risk identification and analysis, control evaluation, and risk treatment recommendations. It provides a comprehensive view of the risks and their potential impact on the organization.

C. Appendices: The appendices contain supporting documentation and additional details that are referenced in the body of the report. This may include technical assessments, data analysis, risk matrices, mitigation plans, or other relevant information. The appendices provide supplemental information to support the findings and recommendations presented in the report.
upvoted 4 times

⊟ **JAckThePip** 1 year, 8 months ago

Answer is correct
https://www.sciencedirect.com/topics/computer-science/risk-assessment-report
upvoted 3 times

Question #145 *Topic 1*

The security operations center (SOC) has received credible intelligence that a threat actor is planning to attack with multiple variants of a destructive virus. After obtaining a sample set of this virus' variants and reverse engineering them to understand how they work, a commonality was found. All variants are coded to write to a specific memory location. It is determined this virus is of no threat to the organization because they had the foresight to enable what feature on all endpoints?

A. Address Space Layout Randomization (ASLR)

B. Trusted Platform Module (TPM)

C. Virtualization

D. Process isolation

Suggested Answer: *A*

Community vote distribution

A (100%)

dev46 Highly Voted 1 year, 9 months ago

Selected Answer: A

The keyword is "feature"

A. Address Space Layout Randomization (ASLR) - feature
B. Trusted Platform Module (TPM) - it's a chip in motherboard, not a feture
C. Virtualization - not a feature
D. Process isolation - not a feature

upvoted 13 times

jackdryan 1 year, 1 month ago

A is correct

upvoted 1 times

74gjd_37 Most Recent 9 months, 1 week ago

Selected Answer: A

The correct answer is A (ASLR).

Process isolation is a security technique that separates individual processes on a system to prevent them from interfering with each other. It is a useful technique for preventing malware or other malicious processes from accessing or modifying data in other processes. However, process isolation alone would not be sufficient to protect against the specific threat posed by the virus variants in this scenario.

The virus variants were coded to write to a specific memory location, which means that they could still potentially write to memory locations within their own isolated process. Therefore, process isolation would not prevent the virus from functioning as intended and carrying out its malicious activities.

upvoted 1 times

Bach1968 11 months, 4 weeks ago

Selected Answer: A

The feature that would have enabled the organization to determine that the virus is of no threat is Address Space Layout Randomization (ASLR).

ASLR is a security technique that randomizes the memory addresses used by a program during its execution. It prevents the predictable allocation of memory addresses, making it harder for attackers to exploit memory-based vulnerabilities or execute code in known memory locations. By enabling ASLR on all endpoints, the organization ensures that the virus variants, which are coded to write to a specific memory location, will not be able to successfully carry out their malicious actions.

upvoted 2 times

Ivanchun 1 year, 6 months ago

Selected Answer: A

Vote A, “All variants are coded to write”

upvoted 1 times

⊟ **Jamati** 1 year, 7 months ago

Selected Answer: A

Answer is A

upvoted 2 times

⊟ **ygc** 1 year, 8 months ago

A is correct, the key words are "a specific memory location".

upvoted 2 times

Question #146 *Topic 1*

The Chief Information Security Officer (CISO) is to establish a single, centralized, and relational repository to hold all information regarding the software and hardware assets. Which of the following s ions would be the BEST option?

A. Information Security Management System (ISMS)

B. Configuration Management Database (CMDB)

C. Security Information and Event Management (SIEM)

D. Information Technology Asset Management (ITAM)

Suggested Answer: *B*

Community vote distribution

B (100%)

stickerbush1970 Highly Voted 2 years, 3 months ago

Selected Answer: B

The CMDB tracks IT assets from a service and operational perspective, while ITAM focuses on IT assets from a financial and cost perspective.

upvoted 11 times

somkiatr 1 year, 12 months ago

THe CMDB can keep and show the "relationship" between CI while the ITAM won't.

upvoted 3 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

lifre Most Recent 5 months, 2 weeks ago

Selected Answer: B

First I though it was ITAM. But the question is not just about recording the assets but all information regarding the assets.

upvoted 1 times

klarak 8 months, 1 week ago

Selected Answer: B

The key term here is RELATIONAL. The ITAM isn't normally relational, it's static.https://www.flexera.com/flexera-one/glossary/itam-versus-cmdb

upvoted 1 times

Soleandheel 1 year ago

B. Configuration Management Database (CMDB)

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

The BEST option for establishing a single, centralized, and relational repository to hold all information regarding the software and hardware assets would be a Configuration Management Database (CMDB). A CMDB is a database that stores information about all hardware and software assets in an organization. It provides a central source of information for asset management, including configuration details, relationships between assets, and the status of those assets. This makes it an ideal solution for the CISO's requirement.

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: B

The BEST option for establishing a single, centralized, and relational repository to hold all information regarding software and hardware assets would be a Configuration Management Database (CMDB).

A CMDB is a centralized database that stores information about all assets and configuration items within an organization's IT infrastructure. It provides a comprehensive view of the relationships between different assets, including software and hardware components. A CMDB is commonly used for configuration management and helps organizations maintain accurate and up-to-date records of their assets, their configurations, and their relationships.

upvoted 1 times

DeepCyber 1 year, 6 months ago

Selected Answer: B

Difference between CMDB and ITAM: thttps://www.device42.com/blog/2022/11/02/itam-vs-cmdb-what-are-the-differences/#:~:text=Therefore%2C%20ITAM%20products%20provide%20an,IT%20environment%20and%20its%20relationships.

upvoted 1 times

somkiatr 1 year, 12 months ago

Selected Answer: B

What is the difference between Asset Management and CMDB?

Read hear -> https://www.alloysoftware.com/resources/what-is-cmdb/

upvoted 1 times

> **somkiatr** 1 year, 12 months ago
>
> THe CMDB can keep and show the "relationship" between CI while the ITAM won't.
>
> Reference : https://help.servicedeskplus.com/cmdb/defining_relationships.html
>
> upvoted 1 times

oudmaster 2 years ago

Is there any ITAM solution in the world does not use relational database?

upvoted 1 times

franbarpro 2 years, 2 months ago

A configuration management database (CMDB) is a file -- usually, in the form of a standardized database -- that contains all relevant information about the hardware and software components used in an organization's IT (information technology) services and the relationships between those components. A CMDB provides an organized view of configuration data and a means of examining that data from any desired perspective

upvoted 1 times

dev46 2 years, 3 months ago

Selected Answer: B

CMDB is right

upvoted 2 times

kasiya 2 years, 3 months ago

Selected Answer: B

relational repository !

upvoted 4 times

Cww1 2 years, 3 months ago

D: ITAM

upvoted 2 times

> **Cww1** 2 years, 3 months ago
>
> changing to B ;)
>
> upvoted 3 times

Question #147 *Topic 1*

What type of investigation applies when malicious behavior is suspected between two organizations?

A. Regulatory

B. Operational

C. Civil

D. Criminal

Suggested Answer: *C*

Community vote distribution

C (60%) D (30%) 10%

djedwards 3 weeks, 2 days ago

Selected Answer: D

When malicious behavior is suspected between two organizations, a criminal investigation is the most applicable type of investigation. This type of investigation is typically initiated by law enforcement and focuses on potential criminal offenses like fraud, theft of trade secrets, or cyberattacks.

upvoted 1 times

CKaraf 3 months, 3 weeks ago

Selected Answer: D

A criminal investigation is appropriate when there is suspicion of illegal activities, such as hacking, data breaches, theft of intellectual property, or other cyber crimes. These investigations are conducted by law enforcement agencies or other authorized entities to determine if a crime has occurred and to gather evidence for potential prosecution. If malicious behavior is confirmed, it can lead to legal action against the offending party.

upvoted 1 times

cysec_4_lyfe 4 months ago

Selected Answer: D

Malicious behavior is illegal so I would say criminal. I think civil would be more inline with negligence or gross negligence leading to an attack carried out by someone else.

upvoted 2 times

Tuhaar 6 months, 2 weeks ago

Selected Answer: C

Civil - I referenced multiple sources include AI and the common word that caught my attention was 'suspected' (NOT PROVEN).

upvoted 1 times

Zapepelele 6 months, 3 weeks ago

Selected Answer: C

It depends:
Civil: If the malicious behavior is something like breach of contract or intellectual property disputes.
Criminal: if the malicious behavior is something like hacking, fraud, etc -explicit illegal-.

In the absence of specific details, a civil investigation is a general approach to addressing disputes between 2 organizations.

upvoted 1 times

angellorv 6 months, 3 weeks ago

Selected Answer: C

Civil: used to prepare evidence necessary to present a case in civil court resolving a dispute between two parties.
Official Study Guide 10th ed - Investigation and Ethics

upvoted 1 times

Tuhaar 7 months ago

Selected Answer: D

When malicious behavior is suspected between two organizations, such as hacking, theft of intellectual property, or cyberattacks, the situation often involves actions that violate laws. These actions are typically investigated under criminal law, focusing on identifying and prosecuting the responsible parties for illegal activities.

Examples of criminal behavior include unauthorized access, data breaches, or denial-of-service (DoS) attacks, which are addressed by legal frameworks like the Computer Fraud and Abuse Act (CFAA) in the U.S.

upvoted 1 times

Mrawrrr 7 months, 3 weeks ago

Selected Answer: D

Criminal investigations are conducted when there is suspicion of illegal activities, such as hacking, fraud, or other malicious behaviors that violate laws.

upvoted 1 times

Skittle4710 1 year ago

Selected Answer: D

D: Criminal

When there is suspicion of malicious behavior, such as hacking, fraud, or other illegal activities between organizations, a criminal investigation is warranted. This type of investigation aims to uncover and prosecute violations of the law.

upvoted 3 times

629f731 1 year, 5 months ago

Selected Answer: B

In the context of malicious behavior, operations research focuses more on the internal practices and processes of the organizations involved to identify flaws or weaknesses that may have allowed such behavior.

upvoted 1 times

Sedap 1 year, 7 months ago

Selected Answer: D

A "malicious behavior" is not a disagreement, it is a crime.

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: C

When malicious behavior is suspected between two organizations, the type of investigation that applies is typically a civil investigation.

A civil investigation focuses on legal issues and disputes between parties, including breaches of contract, intellectual property infringement, or other non-criminal offenses. In the context of malicious behavior between organizations, a civil investigation may involve gathering evidence, conducting interviews, and pursuing legal action to resolve the dispute and seek damages or other remedies.

upvoted 2 times

Toa 2 years, 7 months ago

Answer Civil

A civil trial is a type of court case involving two individual citizens who disagree on an issue that relates to their rights as citizens. For example, if one person sues another for damages caused by a domestic accident, the case will likely be conducted as a civil trial. Civil investigators are responsible for gathering the evidence essential to such a trial.

https://www.pinow.com/investigations/civil-investigations

upvoted 2 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

dev46 2 years, 9 months ago

Selected Answer: C

Civil is correct

upvoted 4 times

Question #148 *Topic 1*

Which of the following techniques evaluates the secure design principles of network or software architectures?

A. Risk modeling

B. Waterfall method

C. Threat modeling

D. Fuzzing

Suggested Answer: *C*

Community vote distribution

C (100%)

dev46 Highly Voted 👍 2 years, 3 months ago

Selected Answer: C

Threat Modeling approaches on below is the foundation of secure design

1) Focus on assets
2) Focus on attackers
3) Focus on software/ application

upvoted 9 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

Meowson 1 year, 5 months ago

Your reply is totally useless and not helping, stop trolling around.

upvoted 6 times

zilm0diafpinc Most Recent ⏲ 11 months, 3 weeks ago

C. design is the keywoard

upvoted 1 times

Vince_F_Fang 1 year, 1 month ago

Risk modeling includes threat modeling and vulnerability modeling. This question evaluates security design principles and does not yet involve specific software and network architecture. There is no need to evaluate vulnerability, so only threat modeling is needed. Unfortunately, I initially saw that software and network architecture chose risk modeling, but now I have compiled the interpretation according to the correct answer□□

upvoted 3 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

The technique that evaluates the secure design principles of network or software architectures is C (Threat modeling).

Threat modeling is a process used to identify potential threats and vulnerabilities in software, network, or system architectures. It involves identifying potential attackers, their capabilities, and the types of attacks they may carry out. Threat modeling considers the system's design and implementation to identify weaknesses and potential vulnerabilities before they can be exploited.

Risk modeling (A) is a broader process that includes identifying potential risks to an organization, assessing their likelihood and impact, and developing strategies to mitigate or manage those risks.

upvoted 2 times

J_Ko 3 months ago

thanks, my brain does strange things sometimes, my thought process was the use of threat modelling to guide/influence the designs. That left me with no answer so my guess was C. Now I know why :)

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: C

The technique that evaluates the secure design principles of network or software architectures is threat modeling.

Threat modeling is a structured approach used to identify, assess, and mitigate potential threats and vulnerabilities in a system or application. It involves analyzing the system's components, data flows, and potential attack vectors to identify potential threats and their potential impact. By evaluating the secure design principles of network or software architectures, organizations can identify and address security weaknesses early in the development lifecycle.

Therefore, the correct answer is C. Threat modeling.
upvoted 1 times

Question #149 Topic 1

Which element of software supply chain management has the GREATEST security risk to organizations?

A. Unsupported libraries are often used.

B. Applications with multiple contributors are difficult to evaluate.

C. Vulnerabilities are difficult to detect.

D. New software development skills are hard to acquire.

Suggested Answer: *A*

Community vote distribution

A (63%) B (26%) 11%

EKP 1 month ago

Selected Answer: C

A primary concern in software supply chain management is the potential for malicious actors to compromise software at any stage, from development to deployment, introducing vulnerabilities, malware, or other malicious code.

upvoted 1 times

BigITGuy 2 months, 4 weeks ago

Selected Answer: A

Not B. Though it's true that multiple contributors make evaluation more complex, this is a management challenge, not the top security risk.

upvoted 1 times

dm808 9 months ago

Selected Answer: B

Considering the fairly recent SolarWinds hack.. I would have to go with B

upvoted 2 times

Vasyamba1 9 months, 1 week ago

Selected Answer: C

From OSG - When evaluating organizational risk, consider external factors that can affect the organization, especially related to company stability and resource availability. The supply chain can be a threat vector, where materials, software, hardware, or data is being obtained from a supposedly trusted source but the supply chain behind that source could have been compromised and the asset poisoned or modified.

upvoted 2 times

Soleandheel 1 year ago

A. Unsupported libraries refer to software libraries or components that are no longer actively maintained or updated by their developers. These libraries may have become outdated or obsolete, making them vulnerable to security vulnerabilities and issues that could be exploited by attackers. Unsupported libraries are a concern in software development and supply chain security because they pose a risk to the security and stability of the applications and systems that depend on them. Organizations should actively monitor and update their software components, including libraries, to mitigate these risks and ensure the security of their software supply chain.

upvoted 3 times

shmoeee 1 year, 1 month ago

OSG 9th edition. pg 99 , "This could happen if your supplier reuses components (like libraries) developed elsewhere..."

Tough one, but I'm going with...A

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: A

The correct answer is A: "Unsupported libraries are often used". The use of unsupported libraries in software development can pose a significant security risk to organizations. Unsupported libraries may have vulnerabilities that are not patched or addressed by the developer, which can be exploited by attackers. Additionally, unsupported libraries may not receive timely updates or support, which can leave them vulnerable to exploits. It is, therefore, essential for organizations to manage their use of libraries carefully and ensure that they are using supported and up-to-date libraries in their software development processes to minimize security risks.

upvoted 3 times

benllp_sst 1 year, 4 months ago

Selected Answer: C

I think Option C is better than option A because software supply chain included a lot of open source software or components and which is difficult to detect vulnerabilities.

upvoted 1 times

Bach1968 1 year, 5 months ago

Selected Answer: A

option A (Unsupported libraries are often used) can also pose a significant security risk in software supply chain management.

When organizations use unsupported or outdated libraries in their software development process, they may expose themselves to known vulnerabilities that have not been patched or addressed by the library developers. These vulnerabilities can be exploited by attackers to gain unauthorized access, compromise the system, or steal sensitive data. Unsupported libraries may not receive regular security updates, leaving them more susceptible to attacks.

Therefore, option A is indeed a valid consideration and can contribute to the security risks associated with software supply chain management.

upvoted 1 times

xxxBadManxxx 1 year, 6 months ago

A: In software supply chain management, the element that poses the greatest security risk to organizations is often considered to be the third-party components and dependencies used in software development. Third-party components include libraries, frameworks, modules, or plugins that are integrated into an organization's.

upvoted 1 times

nat0220 1 year, 7 months ago

B MULTIPLE VENDORS

upvoted 1 times

dmo_d 1 year, 7 months ago

Selected Answer: A

A and B both are reasonable risks.

B can cause high risks in many cases.

But A cause high risks in every case - unmaintained/unsupported libraries are a huge problem because often there are impossible to replace and there are no fixes even for known vulnerabilities.

upvoted 4 times

The1BelowAll 1 year, 8 months ago

Selected Answer: A

Unsupported libraries can contain vulnerabilities

upvoted 2 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

RVoigt 1 year, 10 months ago

Selected Answer: B

Official Study Guide pg 35 - "Understand supply chain risk management (SCRM) concepts. SCRM is a means to ensure that all the vendors or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners. SCRM includes evaluating risks associated with hardware, software, and services; performing third-party assessment and monitoring; establishing minimum security requirements; and enforcing service-level requirements."

upvoted 1 times

JohnyDal 1 year, 10 months ago

Selected Answer: A

unsupported libraries pose the biggest risk

upvoted 3 times

trojix 1 year, 11 months ago

Selected Answer: B

Applications with multiple contributors are difficult to evaluate. Software supply chain management refers to the process of controlling the flow of software components and dependencies throughout the software development lifecycle.

upvoted 1 times

oban 1 year, 11 months ago

Selected Answer: B

B. Applications with multiple contributors are difficult to evaluate.

Applications with multiple contributors, such as open-source software, are popular among organizations because they can be a cost-effective way to acquire software capabilities. However, these applications also present a significant security risk to organizations. Due to their open-source nature, it's hard to ensure that all contributors have the necessary security skills and that the application is free of vulnerabilities. Additionally, it can be difficult for an organization to understand the provenance of the code and track updates, which could create the risk of introducing new vulnerabilities or malware into the organization. - openai

upvoted 2 times

Question #150 *Topic 1*

Which of the following should be done at a disaster site before any item is removed, repaired, or replaced?

A. Communicate with the press following the communications plan

B. Dispatch personnel to the disaster recovery (DR) site

C. Take photos of the damage

D. Notify all of the Board of Directors

Suggested Answer: *D*

Community vote distribution

C (50%) D (33%) B (17%)

trojix Highly Voted 2 years, 5 months ago

Selected Answer: C

From a CISSP perspective, it is important to document the state of the disaster site before any item is removed, repaired, or replaced. This documentation, in the form of photographs, can be used as evidence in the event of an investigation or lawsuit.

upvoted 12 times

Delab202 Highly Voted 2 years, 5 months ago

Selected Answer: C

Notify all of the Board of Directors=How?
Do you know all the board members? Are they available for your notification?

Take photos, use your communication channel to send it up

upvoted 8 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: C

Not D - Notifying the Board is important for governance, but it is not an immediate step before handling physical assets at the disaster site.

upvoted 1 times

adc9365 10 months ago

D correct. You do the CISSP exam from the point of view of a CISO not a forensic analyst. Directors is your first action

upvoted 1 times

TheManiac 1 year, 1 month ago

Selected Answer: D

Guys yes, photos must be taken. But if the disaster is an outage, what are you gonna do with them? And you are not a technician. You are a manager.
You first inform the Board of Directors

upvoted 2 times

8b48948 1 year, 2 months ago

C - preserve evidence

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: B

Human life and safety are on the first place! If the disaster site is the site where disaster occured and the disaster recovery site is the spare site, we need to dispatch personnel to the safe place first.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: D

What's the use of the picture if the outage is from the service provider's end?

upvoted 1 times

GuardianAngel 1 year, 4 months ago

Answer: Send someone to the site. In studying with one of the udemy courses, I came across this outline of typical Diaster Recovery plan activation steps. I had selected 'take pictures, but now rethinking this questions based on new knowledge, the answer is send someone to the site.

DR plan activation Steps:
1. Declaration of disaster
2. Activation of the DR team
3. Internal communications (ongoing from here on out)
4. Protection of human safety (e.g., evacuation)
5. Damage assessment
6. Execution of appropriate system-specific DRPs (each system and network should have its own DRP)
7. Recovery of mission-critical business processes/functions
8. Recovery of all other business processes/functions

upvoted 1 times

629f731 1 year, 5 months ago

Selected Answer: D

The answer as technicians is obvious "C", remember, we must think like a Manager, The manager would first notify the board of directors of the disaster. D is the answer

upvoted 2 times

DapengZhang 1 year, 7 months ago

Selected Answer: B

The sequence shall be,
B>C>D>A
send someone into site and cross check if the damage severity whether fulfill the criteria of disaster. if positive, the record the proof and notify top management, then align with press via PR channels.

upvoted 1 times

[Removed] 1 year, 4 months ago

There are 2 sites mentioned: disaster and disaster recovery

upvoted 1 times

homeysl 1 year, 8 months ago

Selected Answer: C

C. Take evidence. Also BOD are just after the stocks.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: C

From the point of view of a Certified Information Systems Security Professional (CISSP), the best answer would be C: "Take photos of the damage". This is because photographic documentation is important for maintaining the integrity of the disaster site, as well as for insurance and legal purposes. It is also important to document the damage before any remediation work is done, as this can help to support any insurance claims or legal actions that may be necessary. As a CISSP, it is important to follow best practices for disaster recovery and to ensure that all necessary documentation is collected and preserved.

upvoted 3 times

georgegeorge125487 1 year, 10 months ago

Selected Answer: B

Secure the site material.

upvoted 1 times

MShaaban 1 year, 10 months ago

I would say C. What are you going to notify the board of directors with. You need to know what the damage is so that you have something to say to them.

upvoted 1 times

Bach1968 1 year, 11 months ago

Selected Answer: D

this situation raise a valid point. In some cases, it may be necessary to notify the Board of Directors or senior management immediately after a disaster occurs, especially if the impact is significant and has the potential to affect the organization's operations, reputation, or financials. The decision of whether to notify the Board of Directors at the disaster site before any item is removed, repaired, or replaced would depend on the specific circumstances and the organization's incident response protocols. It's important to have clear communication channels and predefined roles and responsibilities in place to ensure effective decision-making and timely reporting to key stakeholders during a disaster.

taking photo and documenting, is also very important prior of any action on ground

upvoted 2 times

⊟ **lferolm** 2 years, 2 months ago

Selected Answer: B

It is not clear at all. D makes no sense, the recovery cannot be stop in case a BOD member is not located. C, pictures of a software? of the memory of a computer or files? the only that can have some logic is B.

upvoted 2 times

Question #151 *Topic 1*

When designing a new Voice over Internet Protocol (VoIP) network, an organization's top concern is preventing unauthorized users accessing the VoIP network.
Which of the following will BEST help secure the VoIP network?

A. 802.11g

B. Web application firewall (WAF)

C. Transport Layer Security (TLS)

D. 802.1x

Suggested Answer: *C*

Community vote distribution

D (57%) C (43%)

Bhuraw Highly Voted 👍 2 years, 8 months ago

Selected Answer: D

Where does Examtopics get their answers from?

upvoted 16 times

6dc1fe1 2 weeks, 3 days ago

They are using an algorithm that picks the most voted choice, whether the choice is correct or wrong!

upvoted 1 times

MShaaban 1 year, 10 months ago

Hahaha, I was thinking the same 😂. Agree D is the answer.

upvoted 4 times

Jamati 2 years, 7 months ago

I never look at their answers, I just go straight to the discussion.

upvoted 5 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 2 times

Qwertyloopback Highly Voted 👍 2 years, 4 months ago

Selected Answer: C

I am going with C on this one. Here is my reasoning from research:

The CISSP 9ed mentions 802.1x but as a vulnerability, not as a protection. It basically states that due to the nature of voip devices, it is easy to spoof Mac addresses and get past layered defenses. It also mentions TLS and SRTP as protection mechanisms.

Cisco has an article that I found helpful. (Link below) It does not mention 802.1x at all but does go into to TLS and SRTP.

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/tips-ip-phone-security.html#~configure-and-protect-systems

Given that SRTP is not an option. TLS seems to be the best answer in this case.

upvoted 9 times

BigITGuy Most Recent 🕘 3 months ago

Selected Answer: D

802.1X is a network access control protocol that provides port-based authentication, making it the BEST choice for preventing unauthorized users from accessing the VoIP network.

upvoted 1 times

d7034bf 6 months, 2 weeks ago

Selected Answer: D

802.1x is the standard for authenticating devices on a VOIP network before access (this is with a RADIUS server, I think). Since VOIP data encryption is not mentioned which is SRTP, the only answer is D.

upvoted 1 times

KJ44 7 months, 4 weeks ago

Selected Answer: D

802.1x authenticates the users before allowing access. TLS and other protocols will secure the call while in progress. The questions asks how to prevent unauthorized users, so the answer is 802.1x

upvoted 1 times

Treebeard88 8 months, 2 weeks ago

Selected Answer: C

802.1X is a network authentication and access control mechanism, while TLS is a protocol that protects data transfers between a client and a web server

upvoted 3 times

8b48948 1 year, 2 months ago

Has to be C - 802.1x is port authentication.

upvoted 1 times

dm808 1 year, 3 months ago

Selected Answer: D

I think the VOIP detail is irrelevant. TLS will provide privacy between sessions.
The question is asking about preventing unauthorized access to the network.. so it has to be D

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: D

Question is asking about preventing access.

upvoted 1 times

splash2357 1 year, 5 months ago

Going with D.

TLS protect man-in-the-middle attackers who is already in range within the VOIP network from eavesdropping connections. It provide no authentication nor authorization that prevent unauthorized users getting in the network. With TLS, attackers in range may still connect their devices to the VOIP network and make connections (just that they can't eavesdrop others).

upvoted 2 times

YesPlease 1 year, 6 months ago

Answer C) Transport Layer Security (TLS)

I really hate these ambiguous questions. Essentially, 802.11g and 802.1x are the same...they provide a protocol to authenticate network traffic...just one happens to be direct and state it is for wireless.

If two options are the same, then it must mean that they are not the right choice and it is must be TLS. (At least one would think)

upvoted 1 times

> **splash2357** 1 year, 5 months ago
>
> No, 802.11g is a standard for Wi-Fi (a legacy one though)
> https://www.intel.com/content/www/us/en/support/articles/000005725/wireless/legacy-intel-wireless-products.html
>
> upvoted 2 times

isaac592 1 year, 8 months ago

Selected Answer: C

Similar to @qwertyloopback, went with C because SRTP was not an option but you can encrypt VoIP SIP traffic with TLS.

upvoted 1 times

homeysl 1 year, 8 months ago

Selected Answer: C

I did not see SRTP, so it must be TLS.

upvoted 2 times

74gjd_37 1 year, 9 months ago

Selected Answer: D

https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/concept/802-1x-pnac-voip-understanding-mx-series.html

When you use Voice over IP (VoIP), you can connect IP telephones to the router and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. Starting with Junos OS Release 14.2, 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone.

You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In multiple-supplicant mode, the 802.1X process allows multiple supplicants to connect to the interface.

The BEST option to secure the VoIP network is option D, 802.1x. This is a standard for port-based network access control that provides authentication and authorization to devices trying to connect to the network. By implementing 802.1x, only authorized devices can connect to the VoIP network, preventing unauthorized access.

upvoted 2 times

BoZT 1 year, 10 months ago

Selected Answer: C

Bard says TLS is a cryptographic protocol that encrypts data in transit between two endpoints. This means that even if an unauthorized user is able to intercept the data, they will not be able to read it. TLS is the most widely used encryption protocol for VoIP traffic, and it is considered to be very secure.

The other options are not as secure as TLS.

802.11g is a wireless networking standard that does not provide any encryption by default.
A WAF is a firewall that is designed to protect web applications from attacks. It can be used to block malicious traffic, but it does not encrypt data.
802.1x is a network access control protocol that can be used to authenticate users before they are allowed to access the network. However, it does not encrypt data in transit.
In conclusion, TLS is the best way to secure a VoIP network from unauthorized access.

upvoted 5 times

Bach1968 1 year, 11 months ago

Selected Answer: D

The BEST option to help secure a Voice over Internet Protocol (VoIP) network and prevent unauthorized access is option D, 802.1x.

802.1x is a network access control protocol that provides authentication and authorization for devices attempting to connect to a network. It allows for user-based authentication and provides a secure method to control access to the VoIP network. By implementing 802.1x, only authorized users or devices with valid credentials will be granted access to the network, while unauthorized users will be prevented from connecting.

upvoted 1 times

HughJassole 2 years ago

C. "Call encryption uses Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP). These VoIP protocols work together to establish high-grade security in every call."
"For the greatest interoperability, SIP isn’t encrypted."
https://www.nextiva.com/blog/voip-security.html

upvoted 2 times

Question #152 *Topic 1*

A user's credential for an application is stored in a relational database. Which control protects the confidentiality of the credential while it is stored?

A. Use a salted cryptographic hash of the password.

B. Validate passwords using a stored procedure.

C. Allow only the application to have access to the password field in order to verify user authentication.

D. Encrypt the entire database and embed an encryption key in the application.

Suggested Answer: *D*

Community vote distribution

A (64%) D (32%) 4%

izaman2022 Highly Voted 2 years, 8 months ago

Selected Answer: A

Its absurd that D is listed as the correct answer, when the second part of the answer says "embed an encryption key in the application."

upvoted 8 times

Az900500 11 months, 3 weeks ago

Very absurd and even surprise that's the selected answer by Examtopic

upvoted 1 times

JAckThePip Highly Voted 2 years, 8 months ago

Answer is A

"Hashes cannot be used to discover the contents of the original message, or any of its other characteristics, but can be used to determine whether the message has changed. In this way, hashes provide confidentiality, but not integrity."

https://www.sciencedirect.com/topics/computer-science/hash-function

upvoted 6 times

dmo_d 2 years, 1 month ago

Determine wether a message has changed is the goal of integrity.

This is why hashing provides integrity only.

P.S.: Even scientists make mistakes ;-)

upvoted 1 times

angellorv Most Recent 6 months, 2 weeks ago

Selected Answer: A

ANS A is correct.

Storing passwords in plain text is NOT a secure solution - this is my understanding of ANS B and C.

ANS A: Hashing is a one way function - practically impossible to reverse. A good cryptographic hash function has lesser number of Collisions. Additionally, adding salt, pepper, and a number of iterations will result in a method to store passwords more securely than a simple hash. Hashing with salt, pepper, and several iterations to the passwords provides a better solution.

ANS D: Encrypting the password and then storing it, IS NOT the best solution (encryption functions are reversible).

When taking the CISSP exam, one has to keep in mind laws such as GDPR, therefore for this question I would keep in mind the rules of the CNIL (French National Commission on Informatics and Liberty) - it recommends that any password be transformed by a non-reversible cryptographic function.

upvoted 2 times

KJ44 7 months, 4 weeks ago

Selected Answer: D

All answers but D are in regards to passwords, NOT credentials. Plus, encrypting a database to ensure confidentiality makes sense. I pick D.

upvoted 1 times

nerdo9 9 months, 3 weeks ago

Selected Answer: D

I also selected 'A' while practicing, but that satisfies integrity. The key word is confidentiality, the correct answer is D.

upvoted 1 times

ServerBrain 3 months, 2 weeks ago

confidentiality of the credential, NOT database..

upvoted 1 times

Dtony66 1 year, 1 month ago

Selected Answer: A

A is the answer. Are these really correct answers from the CISSP exam? Why would you embed an encryption key in the application?

upvoted 1 times

eboehm 1 year, 2 months ago

Selected Answer: A

its disturbing the amount of people persuing a security certification and think D is the correct answer. Would you really embed aka hard code the encryption key inside of the application software? You might as well hard code the password too!

upvoted 4 times

splash2357 1 year, 5 months ago

Selected Answer: A

Going with A.
Hashed password are not reversible (or extremely hard to reverse it) back to the original form (strong hashing algorithms).
Encryption do provide extra layer of protection, however, ciphertexts can be reverted back to their original form with a decryption key. Just in case both the key and the DB records are leaked, the DB records in cleartext would be leaked. Example of such incident includes the Adobe breach at 2013:
https://www.csoonline.com/article/540070/network-security-adobe-confirms-stolen-passwords-were-encrypted-not-hashed.html

upvoted 1 times

Rifandy 1 year, 5 months ago

How come given answer D, what if size of the DB is large then need to encrypt entirely?

upvoted 1 times

629f731 1 year, 5 months ago

Selected Answer: A

A is correct because option "D" proposes to encrypt the entire database and embed an encryption key in the application. While this measure provides a level of protection, it is not best suited to protect the confidentiality of specific user credentials in the database. Using a single encryption key for the entire database and embedding it in your application can compromise security if that key is compromised or accessed.

upvoted 1 times

homeysl 1 year, 8 months ago

Selected Answer: D

D. It says relational DB. You encrypt the table or DB.

upvoted 1 times

MShaaban 1 year, 10 months ago

I see people saying hash is for integrity which is correct. But at the same time it's a one way process like you can't extract the password from the hash.
I see A and D are valid. I wonder if the exam would have such similar answers. I would be doomed

upvoted 4 times

Bach1968 1 year, 11 months ago

Selected Answer: D

Option D, encrypting the entire database and embedding an encryption key in the application, can indeed be an effective control to protect the confidentiality of the credential while stored.

By encrypting the entire database, including the stored credentials, unauthorized access to the database would not reveal the plaintext passwords. The encryption key, which is embedded in the application, is required to decrypt the database and access the stored credentials. This provides an additional layer of protection against unauthorized access to the sensitive information.

Encrypting the database ensures that even if an attacker gains access to the stored data, they would not be able to read the credentials without the encryption key. It adds an extra level of security beyond just hashing and salting the passwords.

Therefore, option D, encrypting the entire database and embedding an encryption key in the application, is a valid control to protect the confidentiality of the credential while stored in a relational database.

upvoted 3 times

HughJassole 2 years ago

D sounds wrong but A is hashing, which provides integrity only:

"Integrity ensures that data is maintained and that no unauthorized changes have been made to the data. One example of this is signature hashing, such as an MD5 or SHA256 checksum."

D talks about encryption, which is confidentiality.

upvoted 1 times

dmo_d 2 years, 1 month ago

Selected Answer: D

D is the right one.

Credentials comprises of user id AND authentication token (password).
This is why answer A is wrong as it covers only the password part.

Second the question was what provides confidentiality to the credentials.
Hashing does not provide confidentiality but it provides integrity only.

upvoted 4 times

DeepCyber 2 years ago

agreed! They are taking about credential and not only password. Also, They are looking for protection while password is stored in the database. Salt helps to ensure attacker can't crack but we also need to protect hashed password to ensure It never reaches in the hand of attacker. Answer should be D.

upvoted 2 times

Tygrond87 2 years, 1 month ago

Selected Answer: B

Option C is the correct answer because it addresses the access control aspect of the question. By allowing only the application to have access to the password field in order to verify user authentication, it ensures that only authorized entities can access the credential. Access controls are a critical security control to prevent unauthorized access to sensitive information.

upvoted 1 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

Cg007 2 years, 2 months ago

A

What is password salting? Password salting is a technique to protect passwords stored in databases by adding a string of 32 or more characters and then hashing them. Salting prevents hackers who breach an enterprise environment from reverse-engineering passwords and stealing them from the database.

upvoted 1 times

Question #153 *Topic 1*

Which of the following frameworks provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD)?

A. Common Vulnerabilities and Exposures (CVE)

B. Center for Internet Security (CIS)

C. Common Vulnerability Scoring System (CVSS)

D. Open Web Application Security Project (OWASP)

Suggested Answer: *C*

Community vote distribution

C (88%) 12%

⊟ **Vino22** Highly Voted 2 years, 2 months ago

A is correct

https://cve.mitre.org/about/cve_and_nvd_relationship.html

upvoted 11 times

⊟ **JohnBentass** 6 months, 3 weeks ago

Question says metrics. Hence answer should be C

upvoted 1 times

⊟ **TheManiac** Most Recent 7 months, 1 week ago

Selected Answer: C

CVSS is the correct answer.
what about CVE? It gives you characteristics but not the metrics. Score on CVSS is the metric for example

upvoted 2 times

⊟ **ExamTaker1995** 1 year, 2 months ago

Selected Answer: C

CVSS is the framework for creating the metrics that determine CVEs. key word here is metrics

upvoted 1 times

⊟ **Bach1968** 1 year, 5 months ago

Selected Answer: C

The framework that provides vulnerability metrics and characteristics to support the National Vulnerability Database (NVD) is the Common Vulnerability Scoring System (CVSS).

CVSS is a standardized framework for assessing and rating the severity of vulnerabilities. It provides a set of metrics and scores that help to quantify the impact and exploitability of vulnerabilities. These scores are used by the NVD to provide consistent and objective information about vulnerabilities in various software and systems.

Therefore, option C, Common Vulnerability Scoring System (CVSS), is the correct answer.

upvoted 2 times

⊟ **HughJassole** 1 year, 6 months ago

C. "The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the
characteristics and impacts of IT vulnerabilities. The National Vulnerability Database (NVD) provides specific CVSS scores for publicly known vulnerabilities."
https://www.govinfo.gov/content/pkg/GOVPUB-C13-19c8184048f013016412405161920394/pdf/GOVPUB-C13-19c8184048f013016412405161920394.pdf

upvoted 1 times

⊟ **NJALPHA** 1 year, 8 months ago

C-The Common Vulnerability Scoring System (aka CVSS Scores) provides a numerical (0-10) representation of the severity of an information security vulnerability. CVSS scores are commonly used by infosec teams as part of a vulnerability management program to provide a point of comparison between vulnerabilities, and to prioritize remediation of vulnerabilities.

A CVSS score is composed of three sets of metrics (Base, Temporal, Environmental), each of which have an underlying scoring component.

upvoted 1 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

init2winit 1 year, 11 months ago

Selected Answer: C

CVSS - Keyword here is Metrics

upvoted 2 times

somkiatr 1 year, 12 months ago

Selected Answer: C

Reference : https://www.balbix.com/insights/whats-the-difference-between-cve-and-cvss/

upvoted 1 times

rajkamal0 2 years ago

Selected Answer: C

C is the best answer.

https://ieeexplore.ieee.org/abstract/document/8594738

upvoted 1 times

oudmaster 2 years ago

Selected Answer: C

Given answer is correct:

!

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities:

https://nvd.nist.gov/

upvoted 1 times

sphenixfire 2 years, 1 month ago

Selected Answer: C

Metrics and character = cvss

https://nvd.nist.gov/vuln/vulnerability-detail-pages

upvoted 3 times

Jamati 2 years, 1 month ago

Selected Answer: A

CVE is a list of publicly disclosed cybersecurity vulnerabilities and exposures that is free to search, use, and incorporate into products and services. NVD, a U.S. government repository, is the CVE List augmented with additional analysis, a database, and a fine-grained search engine. The NVD is synchronized with CVE such that any updates to CVE appear immediately on the NVD.

https://nvd.nist.gov/general/FAQ-Sections/General-FAQs

upvoted 2 times

explorer3 2 years, 2 months ago

Selected Answer: C

C is Correct

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental

https://nvd.nist.gov/vuln-metrics/cvss

upvoted 3 times

Jamati 2 years, 1 month ago

CVSS is a scoring system, it does not provide the characteristics and attributes of the vulnerability.

upvoted 1 times

Toyeeb 2 years, 2 months ago

i agree with Vino, it is A

upvoted 2 times

⊟ **JAckThePip** 2 years, 2 months ago

Answer is correct

"A CVSS score is composed of three sets of metrics (Base, Temporal, Environmental), each of which have an underlying scoring component."

https://www.balbix.com/insights/understanding-cvss-scores/

upvoted 4 times

⊟ **franbarpro** 2 years, 2 months ago

The answer is "A" - based on the qeustion. CVSS is just a CVE scoring system.

upvoted 4 times

Question #154 *Topic 1*

A security architect is reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes. The current design has all of the application infrastructure located within one co-location data center. Which security principle is the architect currently assessing?

A. Disaster recovery (DR)

B. Availability

C. Redundancy

D. Business continuity (BC)

Suggested Answer: *B*

Community vote distribution

B (87%) 13%

Nickname53796 Highly Voted 2 years, 2 months ago

Selected Answer: B

Tricky bastards. Reviewing the BC...which is availability

upvoted 19 times

Mann0302 2 years, 1 month ago

The only reason why I hate CISSP!

upvoted 5 times

Jay_12 Highly Voted 2 years, 1 month ago

B - Key word security principle (CIA).

upvoted 13 times

629f731 11 months, 3 weeks ago

You are rigth!

upvoted 1 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

36dd0ae Most Recent 1 month, 1 week ago

Selected Answer: D

Went with D and agree why the answer is B.

English is not my first language, will need to reread each question at least 3 times before attempting to answer

upvoted 1 times

f168100 3 months, 2 weeks ago

Selected Answer: A

With some help of chatgpt

Even though *availability* is part of the broader *business continuity* effort, *disaster recovery (DR)* is the correct security principle being assessed here because the question focuses on the recovery of the application within the specific *RPO* (15 minutes). Therefore, the best answer remains *A. Disaster recovery (DR)*.

upvoted 1 times

RevZig67 5 months, 3 weeks ago

Selected Answer: A

The architect is primarily assessing disaster recovery (DR), as the Recovery Point Objective (RPO) is a critical metric used in disaster recovery planning to ensure that data loss is minimized and recovery can be achieved within an acceptable timeframe.

upvoted 3 times

homeysl 1 year, 2 months ago

Selected Answer: B

Availability is the answer.

upvoted 1 times

royalibex 1 year, 3 months ago

Someone's getting paid just to be a pro trickster. Another reason why this test is weird.

upvoted 4 times

Tygrond87 1 year, 7 months ago

Selected Answer: A

The security principle that the security architect is currently assessing is "disaster recovery (DR)."

Disaster recovery is the process of restoring an organization's critical systems, applications, and data in the event of a disaster or disruptive event. The Recovery Point Objective (RPO) is the maximum amount of data loss that is acceptable to the organization. In this case, the RPO is 15 minutes, which means that the organization cannot afford to lose more than 15 minutes' worth of data in the event of a disaster.

The current design of having all of the application infrastructure located within one co-location data center does not provide adequate disaster recovery capability. If a disaster were to occur at that location, the entire infrastructure could be lost, resulting in data loss and application unavailability. The security architect is therefore assessing the adequacy of the disaster recovery plan for the application.

upvoted 3 times

kandegama 1 year, 8 months ago

Selected Answer: A

planning to have RPO - 15 min for application DR
only have one co location primary data center
correct answer is the consultant currently evaluation of disaster recovery site for their application

upvoted 1 times

bynd 2 years, 1 month ago

Selected Answer: B

There is only one security principle as option: Availability

upvoted 4 times

izaman2022 2 years, 2 months ago

I chose C but I can see why B is the correct answer. The keyword is security principle. Availability is a security principle (C I A) and would include redundancy. A and D are not security principles

upvoted 5 times

sandeepghadge 2 years, 2 months ago

"reviewing plans for an application with a Recovery Point Objective (RPO) of 15 minutes." does this indicated DR ?

upvoted 1 times

JAckThePip 2 years, 2 months ago

Answer is correct
https://www.securitymetrics.com/blog/what-is-a-business-continuity-plan

upvoted 1 times

Question #155 *Topic 1*

Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?

A. System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements

B. Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements

C. Data stewardship roles, data handling and storage standards, data lifecycle requirements

D. System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

Suggested Answer: *A*

Community vote distribution

C (76%) A (24%)

⊟ **sandeepghadge** Highly Voted 2 years, 8 months ago

"classifying information " isnt its Data owner(steward) job ?

upvoted 9 times

⊟ **jackdryan** 2 years, 1 month ago

C is correct

upvoted 2 times

⊟ **franbarpro** Highly Voted 2 years, 8 months ago

Selected Answer: C

From Google: Data stewardship is the collection of practices that ensure an organization's data is accessible, usable, safe, and trusted.

upvoted 6 times

⊟ **BigITGuy** Most Recent 3 months ago

Selected Answer: C

A, B, and D mention important factors but focus more on systems or roles not directly related to data classification for risk, legal, and compliance purposes.

upvoted 1 times

⊟ **Scheds** 7 months ago

Selected Answer: C

One technique I learnt is if there are two answers that kinda look similar, choose the one that engulfs/contains the other as its element.

upvoted 2 times

⊟ **TheManiac** 1 year, 1 month ago

Selected Answer: C

classifying information = classifying data. Other options do not talk about data, but A and C. A starts with system owner roles. System owner or Data steward. Which one is more important on this issue? Data steward. So, it is C

upvoted 3 times

⊟ **splash2357** 1 year, 5 months ago

Selected Answer: C

Since the question doesn't specify the assets are:

- related to software development (e.g. source code repositories)
- storage only
- on the cloud

I'm going with C

upvoted 1 times

⊟ **Soleandheel** 1 year, 6 months ago

Guys the correct answer is C. Data Stewart..... A. could have been the best answer if it said Data owner as opposed to system owner.

upvoted 2 times

⊟ **Moose01** 1 year, 8 months ago

Life Cycle! Categorize the Data, Classify (active data, or data at rest, retention period) all these is covered in the question itself. Data Owner is responsible to identifying and categorizing, legal team is will decide how to retain the data, data at rest must be secured (encrypted).

the answer is "A" - See below Oban has good explanation

upvoted 1 times

oban 2 years, 5 months ago

Selected Answer: A

A. System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements are important factors that must be considered when classifying information and supporting assets for risk management, legal discovery, and compliance.

In order to effectively manage the risks associated with sensitive information, it is important to understand who is responsible for that information, how it is supposed to be handled, and where and how it is stored. This includes understanding the roles and responsibilities of system owners, who are responsible for the security and operation of the systems that hold the data, as well as the standards for data handling and storage and the requirements for secure development lifecycle (SDLC) . This can help organizations to ensure that they are following best practices for protecting sensitive information and meeting regulatory requirements.

B,C and D options also include some important factors that need to be considered but A option covers most of the important points for classifying information and assets for risk management, legal discovery and compliance. - openai

upvoted 4 times

Delab202 2 years, 5 months ago

Selected Answer: C

Data steward

A person responsible for data management from a business and stakeholder perspective; may or may not also be a custodian or owner. Data stewards ensure that data quality meets business needs, that data is supported by sufficient metadata to make it easy to use, and that it meets all regulatory requirements. They also work with stakeholders to create and monitor data acquisition and dissemination procedures.

upvoted 4 times

somkiatr 2 years, 5 months ago

Selected Answer: C

C is better than A.

Reference : https://www.techtarget.com/searchdatamanagement/definition/data-stewardship

upvoted 3 times

boyin 2 years, 6 months ago

Selected Answer: A

The question is asking for "classifying information and supporting assets"

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: C

Definitely C

upvoted 3 times

kuberk 2 years, 8 months ago

Selected Answer: A

It is not specifically for data, hence A makes more sense

upvoted 3 times

DracoL 2 years, 8 months ago

Selected Answer: C

It is data lifecycle not secure development lifecycle. This is really a give away why it is NOT A.

upvoted 6 times

Hava_2013 2 years, 7 months ago

secure development is for the Due Diligence part

upvoted 1 times

MG1707 2 years, 8 months ago

Selected Answer: C

data stewards are first to be asked...

upvoted 2 times

Question #156 *Topic 1*

The Chief Information Security Officer (CISO) of a small organization is making a case for building a security operations center (SOC). While debating between an in-house, fully outsourced, or a hybrid capability, which of the following would be the MAIN consideration, regardless of the model?

A. Headcount and capacity

B. Scope and service catalog

C. Skill set and training

D. Tools and technologies

Suggested Answer: *B*

Community vote distribution

B (59%) C (41%)

dumdada Highly Voted 1 year, 6 months ago

You can't be looking at the SKILLS and TRAINING if you don't even know the SCOPE !! The scope drives what skills/training your SOC analysts will need !

upvoted 5 times

BoZT Highly Voted 1 year, 3 months ago

Selected Answer: B

The scope and service catalog of a SOC defines the specific security services that the SOC will provide. This includes threat monitoring, incident response, vulnerability management, and other security-related activities. The scope and service catalog will also determine the required headcount, skills, and tools and technologies.

Regardless of whether the SOC is in-house, fully outsourced, or a hybrid, the scope and service catalog will be the main consideration. This is because the scope and service catalog will determine the overall cost of the SOC, as well as the level of security that the SOC can provide.

upvoted 5 times

dra3m Most Recent 3 months ago

Selected Answer: C

Scope can be defined regardless of model, the only concerns is around skillset and training, will the inhouse competent enough?, and how competent is the 3rd party soc if 100% outsourced (regardless of who is doing what -scope)

upvoted 1 times

JohnBentass 6 months, 3 weeks ago

C. Skill set and training.

This consideration is crucial regardless of the chosen model because the effectiveness of a SOC heavily depends on the skills and expertise of its personnel. Whether the SOC is managed in-house, outsourced, or a combination of both, having a team with the appropriate cybersecurity skills and continuous training is essential to effectively monitor, detect, analyze, and respond to cybersecurity incidents.

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: C

You need an effective & functioning SOC.

upvoted 2 times

maawar83 1 year ago

MAIN Consideration Regardless of the Model: Answer is D

Rule of Elimination:

- SCOPE and SEVICE Catalog is already defined (Small company in the question)
- Skil set and Training, Regardless of the model means it is not the focus (just ruled out by itself)
- Headcount & Capacity (Ruled out as there is not decision made).
- Tools & Technology seems to stands out more

upvoted 1 times

maawar83 1 year ago

Just to ADD,, if it is in-house or outsourced the 1 that matches both requirements is tools & technology.

upvoted 1 times

[Removed] 1 year ago

Selected Answer: B

I think it's B.
When outsourcing completely, issues related to skill sets and training are the concerns of the outsourcing partner, and cannot be considered as issues for our own company.

upvoted 4 times

Moose01 1 year, 2 months ago

which of the following would be the MAIN consideration?
The CISO and the management team must scope the service that they are interested in and right after they will be thinking about the HR resources and skills.

upvoted 2 times

HughJassole 1 year, 6 months ago

B seems to make sense but I researched and the SOC appears to have a pretty defined set of responsibilities, so I don't think there is much of a scope and service catalog.
https://www.ibm.com/topics/security-operations-center

Therefore C is the answer.

upvoted 3 times

dmo_d 1 year, 7 months ago

Selected Answer: B

It is not C because "regardless of the model" means all aspects regarding the decision between in-house, hybrid or outsourced are NOT asked for.

Therefore B and D remains. But D is not a main consideration for establishing a SOC.

upvoted 2 times

crazywai1221 1 year, 8 months ago

Selected Answer: C

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

After go through NIST800-61r2, I think skill set and training are the main consideration regarding the SOC model.

It metioned team model selection factors:
The need for 24/7 Availability
Full-Time vs Part-Time Team Members
Employee morale
Cost
Staff Expertise

When considering outsourcing, organizations should keep these issues in mind:
Current and Future Quality of Work
Division of Responsibilities
Sensitive Information Revealed to the Contractor
Lack of Organization-Specific Knowledge
Lack of Correlation
Handling Incidents at Multiple Locations
Maintaining Incident Response Skills In-House

A successful SOC requires a team of skilled and experienced security professionals who can monitor and analyze security events, identify potential threats and vulnerabilities, and respond quickly and effectively to security incidents.

upvoted 3 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

Alex71 1 year, 10 months ago

Selected Answer: C

C. Skill set and training would be the MAIN consideration when debating between an in-house, fully outsourced, or a hybrid security operations center (SOC) capability. The effectiveness of a SOC is highly dependent on the skills and experience of the analysts who staff it, regardless of the model used. The organization needs to consider whether it has the internal resources and expertise to build and operate an in-house SOC, or if it would be more efficient and cost-effective to outsource the function to a managed security service provider (MSSP). A hybrid model may also be considered, where some SOC functions are handled in-house and others are outsourced. Regardless of the model chosen, the organization should prioritize hiring or training skilled analysts to staff the SOC.

upvoted 2 times

Jamati 2 years, 1 month ago

Selected Answer: B

B - Once we've determined the goals of the SOC and what it's being created to accomplish, we can then look at the required head count and capacity.

upvoted 3 times

ygc 2 years, 3 months ago

B, absolutely

upvoted 3 times

Question #157 *Topic 1*

An organization would like to ensure that all new users have a predefined departmental access template applied upon creation. The organization would also like additional access for users to be granted on a per-project basis. What type of user access administration is BEST suited to meet the organization's needs?

A. Decentralized

B. Hybrid

C. Centralized

D. Federated

Suggested Answer: *D*

Community vote distribution

B (72%) | D (17%) | 10%

RVoigt **Highly Voted** 1 year, 10 months ago

Selected Answer: B

CISSP Official Student Guide pg 169 "Hybrid: In a hybrid approach, centralized control is exercised for some information and decentralized control is allowed for other information. One typical arrangement is that central administration is responsible for the broadest and most basic access, and the creators/owners of files control the types of access or users' abilities for the files under their control. For example, when a new employee is hired into a department, a central administrator might provide the employee with access permissions based on the functional element they are assigned to, the job classification and the specific task they were hired to work on. The employee might have readonly access to an organization-wide SharePoint document library and to project status report files but read-and-write privileges to his department's weekly activities report. Also, if the employee leaves a project, the project manager can easily close that employee's access to that file."

upvoted 8 times

Oppenheimer **Highly Voted** 2 years, 2 months ago

Selected Answer: B

Agree with B it is a hybrid of RBAC and ABAC

upvoted 7 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 2 times

BigITGuy **Most Recent** 2 months, 4 weeks ago

Selected Answer: B

A hybrid model combines centralized control for standard access (e.g., departmental templates) and decentralized flexibility for project-specific access, making it the best fit here.

upvoted 2 times

Dtony66 7 months, 4 weeks ago

Selected Answer: B

How could it be D when Federated refers to inter organizational?

upvoted 1 times

Vasyamba1 9 months, 1 week ago

Selected Answer: C

I go with C. OSG - Centralized access control implies that a single entity within a system performs all authorization verification.

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: C

Why B? Hybrid is both on-prem and cloud. I didn't see anything about cloud in the question.

upvoted 2 times

maawar83 1 year ago

B It Is!

upvoted 1 times

GPrep 1 year ago

I believe the answer is C. Hybrid and Federated refer to the back end solution for IAM, including SSO, etc. See page 688 of the official study guide "Hybrid Environment". According to pg 659, there are two options for Identity Management, Centralized and Decentralized. Therefore, I choose C.

upvoted 2 times

BoZT 1 year, 3 months ago

Selected Answer: B

Combination of RBAC and ABAC, ABAC can be per project basis.

upvoted 1 times

Dee83 1 year, 11 months ago

B. Hybrid user access administration is BEST suited to meet the organization's needs.

Hybrid user access administration is a combination of both centralized and decentralized access administration. It allows for a predefined departmental access template to be applied to new users upon creation, which is a centralized approach. And also allows for additional access to be granted on a per-project basis, which is a decentralized approach. This allows for a balance between centralized control and flexibility for departments and project teams to manage their own access needs.

upvoted 2 times

Ncoa 2 years, 2 months ago

Selected Answer: B

Agree with B it is a hybrid of RBAC and ABAC

upvoted 3 times

Cww1 2 years, 3 months ago

agree with B

https://www.serverbrain.org/infrastructure-design-2003/identifying-the-hybrid-administration-model.html

upvoted 1 times

mrgod 2 years, 3 months ago

Selected Answer: B

The question is talking about inside organization, so this is nothing to do with Federate..I think hybrid is a better choice.

upvoted 3 times

stickerbush1970 2 years, 3 months ago

I would go with A

upvoted 1 times

Stevooo 2 years, 3 months ago

Selected Answer: D

Can someone justify this answer please

upvoted 5 times

kurtvon 2 years, 1 month ago

Only: Because the test said so... (This question is a bad question)

upvoted 1 times

Question #158 *Topic 1*

Which of the following is a secure design principle for a new product?

A. Restrict the use of modularization.

B. Do not rely on previously used code.

C. Build in appropriate levels of fault tolerance.

D. Utilize obfuscation whenever possible.

Suggested Answer: *C*

Community vote distribution

C (67%) D (20%) 13%

projtfer Highly Voted 2 years, 2 months ago

Selected Answer: C

Fault tolerance is (C) is correct because it covers the availability aspect. Obfuscation is not a design principle and the rest of them don't make sense!

upvoted 7 times

BDSec Highly Voted 2 years, 3 months ago

C, obfuscation is not a recommended design principle

upvoted 7 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: C

Fault tolerance is a core secure design principle, ensuring that the system continues to operate securely and reliably even in the event of failures, errors, or unexpected conditions. Obfuscation can be used as a minor security enhancement, but it is not a core secure design principle. It is more of an obscurity tactic than a security control.

upvoted 1 times

eboehm 8 months, 3 weeks ago

Selected Answer: C

At first I was going with D because I thought fault tolerance was about systems design and adding more complents. However, in software it just means that the application is designed to "fail graciously" . That is the application will continue to work despite an error

upvoted 3 times

Moose01 1 year, 2 months ago

Selected Answer: D

obfuscation ! having built fault tolerance system does not help the weaknesses within the Software code, and obfuscation means to make the SW code hard to understand if compromised, meaning more secure more work for the hackers.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

The correct answer is C. Build in appropriate levels of fault tolerance. Building in fault tolerance is a secure design principle because it helps ensure that a product can continue to function even if a component fails or is compromised. This is an important aspect of security, as it helps prevent attackers from exploiting vulnerabilities in the product to gain unauthorized access or cause other types of harm. Restricting the use of modularization, not relying on previously used code, and utilizing obfuscation whenever possible can also be important security measures, but they are not necessarily secure design principles in and of themselves.

upvoted 1 times

RVoigt 1 year, 10 months ago

Selected Answer: D

CISSP Official Student Guide 6th ed, page 253 - "Secure coding techniques: Use of proper cryptographic algorithms, static and dynamic code analysis and obfuscation techniques in the deployment of code may reduce the risk of some of the common forms of compromise noted above (...vulnerabilities)."

upvoted 1 times

RVoigt 1 year, 10 months ago

I have to change to BDSec's point - CISSP Official Study Guide pg 343 - Fault tolerance is the ability of a system to suffer a fault but continue to operate. Fault tolerance is achieved by adding redundant components such as additional disks within a redundant array of independent disks (RAID) (a.k.a. redundant array of independent disks (RAID)(a.k.a. redundant array of inexpensive disks (RAID)) array, or additional servers within a failover clustered configuration. Fault tolerance is an essential element of security design. It is also considered part of avoiding single points of failure and the implementation of redundancy. For more details on fault tolerance, redundant servers, RAID, and failover solutions, see Chapter 18, "Disaster Recovery Planning."

upvoted 1 times

Dee83 1 year, 11 months ago

C. Build in appropriate levels of fault tolerance.

Fault tolerance refers to the ability of a system to continue functioning properly in the event of the failure of one or more of its components. By building in appropriate levels of fault tolerance, the system can continue to operate even in the event of a failure, reducing the risk of data loss and downtime. This can help to ensure the continuity of operations and the availability of the system, which are important for security and reliability.

On the other hand, the other options given may not be considered as secure design principle, as Restricting the use of modularization can make it harder to maintain and update the system, not relying on previously used code can make it harder to ensure compatibility and stability, and Utilizing obfuscation whenever possible can make it harder to debug and troubleshoot the system.

upvoted 3 times

Mr_Zaw 1 year, 11 months ago

C.

I will go with C. Below is the phrase from Official Study Guide,

While security through obscurity is typically not considered a valid security measure, it may still have value in some cases.

Hence D is not an answer. Every application need to have exception handling (kind of fault tolerance). Improper handling of errors can introduce a variety of security problems.

upvoted 2 times

somkiatr 1 year, 12 months ago

Selected Answer: B

I will choose B. The previous source code would outdated or exposed to vulnerability like zero days. I don't choose D because one of the design principle is "keep it simple and open". I don't choose C because one of the design principle is "Fail securely".

upvoted 2 times

somkiatr 1 year, 12 months ago

Reference : https://cybersophia.net/articles/how-to/10-design-principles-for-secure-system-development/

upvoted 1 times

Hava_2013 2 years, 1 month ago

why not B?

upvoted 1 times

oudmaster 2 years ago

because it is totally fine to use libraries (reusable code) in software development as long as they are secure.

upvoted 2 times

Jamati 2 years, 1 month ago

Selected Answer: D

I think D.

Code is often obfuscated to protect intellectual property or trade secrets, and to prevent an attacker from reverse engineering a proprietary software prograr
or all of a program's code is one obfuscation method. The main advantages of obfuscation are Secrecy, Efficiency (some obfuscation techniques, like unused
the effect of shrinking the program and making it less resource intensive to run) and Security (obfuscation is a built-in security method, sometimes referred t
self-protection. It is well-suited for protecting applications that run in an untrusted environment and that contain sensitive information). One of the main disa
obfuscation is it is also by malware writers to evade antivirus programs.
https://www.techtarget.com/searchsecurity/definition/obfuscation#:~:text=Obfuscation%20means%20to%20make%20something,code%20is%20one%20obfu

upvoted 1 times

JAckThePip 2 years, 2 months ago

On the base of Principle of Avoiding Security by Obscurity the obfuscation can be used

upvoted 1 times

⊟ **stickerbush1970** 2 years, 3 months ago

I would go with D on this.

upvoted 1 times

Question #159 *Topic 1*

What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?

A. Standardize specifications between software security products.

B. Achieve organizational compliance with international standards.

C. Improve vulnerability assessment capabilities.

D. Save security costs for the organization.

Suggested Answer: *A*

Community vote distribution

C (50%) A (47%)

⊟ **JAckThePip** Highly Voted 2 years, 8 months ago

Answer is c

"The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization,"

https://en.wikipedia.org/wiki/Security_Content_Automation_Protocol

upvoted 13 times

⊟ **cysec_4_lyfe** Most Recent 2 months, 3 weeks ago

Selected Answer: A

The primary benefit of SCAP is its ability to standardize specifications across security tools and systems, enabling interoperability and consistent communication of security data. This standardization forms the foundation for automated vulnerability assessments, compliance checks, and cost savings, but the core value lies in creating a unified framework for security automation.

upvoted 2 times

⊟ **BigITGuy** 3 months ago

Selected Answer: C

The keyword is PRIMARY. Security Content Automation Protocol (SCAP) enhances vulnerability assessment by automating the identification, measurement, and management of security flaws. It streamlines processes like configuration verification and compliance checks, ensuring efficient and accurate evaluations.

upvoted 1 times

⊟ **easyp** 4 months, 4 weeks ago

Selected Answer: A

The primary benefit of relying on Security Content Automation Protocol (SCAP) is A. Standardize specifications between software security products.

SCAP provides a standardized way to express security checklists, vulnerability information, and other security-related data.

This standardization allows different security tools to interoperate and share information more effectively. While SCAP can contribute to the other options (compliance, vulnerability assessment, and cost savings), its core purpose and primary benefit is standardization.

Sources and related content

upvoted 2 times

⊟ **easyp** 5 months ago

Selected Answer: A

The correct answer is A. Standardize specifications between software security products.

Explanation:

The Security Content Automation Protocol (SCAP) is a suite of open specifications used to standardize the format and exchange of security-related information between tools and systems. It enables consistent, automated management of security configurations, vulnerability assessments, and compliance evaluations across multiple software products.

upvoted 1 times

⊟ **J_Ko** 3 months ago

the way I read it, is that standardization is what it does, but it enables consistent, automated, etc; which I interpret as the benefit.

upvoted 1 times

RevZig67 5 months, 3 weeks ago

Selected Answer: B

The primary benefit of SCAP is to help organizations achieve and maintain compliance with international standards and regulations by automating processes related to vulnerability management and compliance checking.

upvoted 1 times

Tuhaar 6 months, 2 weeks ago

Selected Answer: C

from: https://www.tenable.com/sc-report-templates/scap-audit-report;
The Security Content Automation Protocol (SCAP) is a standardized method for expressing security checks in the areas of automated vulnerability management, measurement and policy compliance. Organizations can leverage SCAP-validated tools and SCAP-expressed checklists to more efficiently discover and close security gaps before those gaps can be exploited.

upvoted 1 times

KJ44 7 months, 4 weeks ago

Selected Answer: C

Here are some things SCAP can do:
Automate vulnerability assessments: SCAP can scan and identify weaknesses in software, operating systems, and configurations.
Measure and score vulnerabilities: SCAP combines the Common Vulnerability Scoring System (CVSS), CVE, and CPE to measure and score software flaw vulnerabilities.
Standardize and compare data: SCAP makes it easier to standardize and compare data.
Automate manual processes: SCAP allows federal agencies to automate many manual processes.

upvoted 1 times

JohnBentass 1 year ago

Answer is A
SCAP provides a collection of standardized, interoperable specifications for automating vulnerability management, policy compliance, and security measurement. This standardization ensures that different security tools and products can work together seamlessly, improving the overall efficiency and effectiveness of an organization's security posture

upvoted 1 times

JohnBentass 1 year ago

C. Improve vulnerability assessment capabilities.

SCAP provides a standardized framework that helps organizations automate the process of vulnerability management. This includes identifying, assessing, and mitigating vulnerabilities in systems. By using SCAP, organizations can effectively enhance their security posture by ensuring that vulnerabilities are promptly and accurately identified and addressed

upvoted 1 times

CCNPWILL 1 year, 2 months ago

primary would be to make an improvement, not standardize. Answer is C.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: C

Easy one for those in vulnerability management

upvoted 1 times

hoho2000 1 year, 3 months ago

Selected Answer: C

Read carefully, A states Standardize specifications. SCAP uses specific standards to check vulnerability.
SCAP is a method for using specific standards to help organizations automate vulnerability management and policy compliance evaluation. SCAP comprises numerous open security standards, as well as applications which use these standards to check systems for vulnerabilities and misconfigurations.

upvoted 1 times

Kyanka 1 year, 3 months ago

Selected Answer: C

SCAP scanner is a vulnerability scanner. That's its primary purpose.

upvoted 1 times

629f731 1 year, 5 months ago

Selected Answer: A

A. The security community depends on a common set of standards to provide a common language for describing and evaluating vulnerabilities. NIST provides the community with
the Security Content Automation Protocol (SCAP) to meet this need. SCAP provides this common framework for discussion and also facilitates the automation of interactions between different security systems. Source: Pag 731. CISSP® Certified Information
Systems Security Professional
Official Study Guide. Ninth Edition

upvoted 2 times

YesPlease 1 year, 6 months ago

Selected Answer: A

Answer A)

SCAP was to create standards by NIST.

https://heimdalsecurity.com/blog/security-content-automation-protocol-scap/#:~:text=Security%20Content%20Automation%20Protocol%20(SCAP)%20is%20a%20security%2Dcentric,extra%20security%20padding%2C%20if%20nec

upvoted 1 times

Mulema 1 year, 7 months ago

The correct answer here is C
From
https://bard.google.com/chat/4d841d0c62a0d8d7, we read the following:
The Security Content Automation Protocol (SCAP) is a suite of open standards that are used for automating vulnerability management, security configuration verification, and patch compliance activities. SCAP provides a common framework for exchanging information about security vulnerabilities, configurations, and patches, which makes it possible to automate a wide range of security tasks.

More information about SCAP at https://scap.nist.gov/: https://scap.nist.gov/.

upvoted 1 times

Question #160 *Topic 1*

What are the three key benefits that application developers should derive from the northbound application programming interface (API) of software defined networking (SDN)?

A. Network syntax, abstraction of network flow, and abstraction of network protocols

B. Network syntax, abstraction of network commands, and abstraction of network protocols

C. Familiar syntax, abstraction of network topology, and definition of network protocols

D. Familiar syntax, abstraction of network topology, and abstraction of network protocols

Suggested Answer: *A*

Community vote distribution

D (67%) A (17%) C (17%)

somkiatr Highly Voted 1 year, 12 months ago

Selected Answer: D

The following key benefits of SDN to application developers are :

-Familiar syntax provided by common APIs.

-Abstraction of network topology, network flow, and network protocols because the control plane and infrastructure plane will handle those issues.

upvoted 7 times

Soleandheel Highly Voted 1 year ago

D. The three key benefits that application developers should derive from the northbound API of software-defined networking (SDN) are as follows:

1. It converts to a syntax that is more familiar to developers.
2. It provides abstraction of the network topology and network layer.
3. It provides abstraction of the network protocols themselves.

Therefore, the correct answer is indeed option D: Familiar syntax, abstraction of network topology, and abstraction of network protocols.

upvoted 6 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: D

NOT A and B. Mention "network syntax" which is not a formal benefit in SDN API terminology.

NOT C. Talks about the "definition of network protocols," but developers using the northbound API are not defining protocols; they are using abstracted versions provided by the controller.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

"C"

See Software Defined Networks A Comprehensive Approach (Second Edition), 2017

https://www.sciencedirect.com/book/9780128045558/software-defined-networks

4.1.3 Network Automation and Virtualization

...

There are three key benefits that the application developer should derive from the northbound API: (1) it converts to a syntax that is more familiar to developers (e.g., REST or JSON are more convenient syntaxes than are TLVs); (2) it provides abstraction of the network topology and network layer allowing the application programmer to deal with the network as a whole rather than individual nodes; and (3) it provides abstraction of the network protocols themselves, hiding the application developer from the details of OpenFlow or BGP.

...

upvoted 2 times

Soleandheel 1 year ago

You meant D. right. C is wrong. D is correct.

upvoted 3 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: A

A is correct.

upvoted 1 times

babaseun 1 year, 8 months ago

Selected Answer: A

Northbound APIs present an abstraction of network functions with a programmable interface for applications to consume the network services and configure the network dynamically. They allow the applications to dictate the behaviour of the network.

upvoted 1 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 2 times

sphenixfire 2 years, 1 month ago

Selected Answer: D

Familiar sytax to developer not network syntax. Abstraction of topology, so d

upvoted 3 times

Rollizo 2 years, 3 months ago

A is right:

http://www.ijesrt.com/issues%20pdf%20file/Archive-2016/October-2016/61.pdf

Forwarding decisions are flow-based, instead of destination-based. A flow in the context of SDN, is a sequence of packets between a source and a destination. All packets of a flow receive identical service policies at the forwarding devices. The abstraction in this flow...

upvoted 2 times

Cww1 2 years, 3 months ago

correct

https://www.researchgate.net/publication/330306237_The_Northbound_APIs_of_Software_Defined_Networks

upvoted 1 times

Question #161 *Topic 1*

Which of the following is a unique feature of attribute-based access control (ABAC)?

A. A user is granted access to a system at a particular time of day.

B. A user is granted access to a system based on username and password.

C. A user is granted access to a system based on group affinity.

D. A user is granted access to a system with biometric authentication.

Suggested Answer: *A*

Community vote distribution

A (93%) 7%

⊟ **JAckThePip** Highly Voted 2 years, 2 months ago

Answer correct is C

"An example of ABAC would be allowing only users who are type=employees and have department=HR to access the HR/Payroll system and only during busi within the same timezone as the company."

https://blog.identityautomation.com/rbac-vs-abac-access-control-models-iam-explained#:~:text=Defining%20Attribute%2DBased%20Access%20Control&text=An%20example%20of%20ABAC%20would,same%20timezone%20as%20the%2

upvoted 7 times

⊟ **jackdryan** 1 year, 7 months ago

A is correct

upvoted 1 times

⊟ **explorer3** Highly Voted 2 years, 2 months ago

Selected Answer: A

A seems right - Time and location are some examples of attributes

https://en.wikipedia.org/wiki/Attribute-based_access_control#Attributes

upvoted 6 times

⊟ **TheManiac** Most Recent 7 months, 1 week ago

Selected Answer: A

it doesnt event need an explanation :)

upvoted 1 times

⊟ **74gjd_37** 1 year, 3 months ago

Selected Answer: A

https://en.wikipedia.org/wiki/Attribute-based_access_control#Attributes

Attributes can be about anything and anyone. They tend to fall into 4 different categories:

1. Subject attributes: attributes that describe the user attempting the access e.g. age, clearance, department, role, job title
2. Action attributes: attributes that describe the action being attempted e.g. read, delete, view, approve
3. Object attributes: attributes that describe the object (or resource) being accessed e.g. the object type (medical record, bank account), the department, the classification or sensitivity, the location
4. Contextual (environment) attributes: attributes that deal with time, location or dynamic aspects of the access control scenario.

The unique feature of attribute-based access control (ABAC) is that a user is granted access to a system based on attributes or characteristics associated with the user, such as job title, security clearance level, location, time of day, and many others. Therefore, the correct answer is A.

upvoted 1 times

⊟ **georgegeorge125487** 1 year, 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

⊟ **Treymb6** 1 year, 11 months ago

Selected Answer: A

Should be A. Key word is "unique". Group affinity is something RBAC can do as well, but time of day access can only be done by ABAC.

upvoted 3 times

cissp16 1 year, 11 months ago

Selected answer: A

ABAC is a flexible and dynamic access control model that grants access to a system based on attributes associated with the user, resource, action, and environment. Group affinity is one such attribute that defines the user's membership in a particular group and is used to determine their access privileges within the system.

In contrast, traditional access control models such as role-based access control (RBAC) and discretionary access control (DAC) primarily use static roles and permissions to control access. Time of day, username and password, and biometric authentication are also used in access control, but they are not unique features of ABAC.

upvoted 2 times

Mr_Zaw 1 year, 11 months ago

Selected Answer: A

With ABAC, an organisation's access policies enforce access decisions based on the attributes of the subject, resource, action, and environment involved in an access event.

The environment is the broader context of each access request. All environmental attributes speak to contextual factors like the time and location of an access attempt, the subject's device, communication protocol, and encryption strength. Contextual information can also include risk signals that the organisation has established, such as authentication strength and the subject's normal behaviour patterns.

upvoted 2 times

sphenixfire 2 years, 1 month ago

Selected Answer: A

groupaffinity also possible in rbac, but not time. A

upvoted 3 times

kuberk 2 years, 2 months ago

Selected Answer: C

It should be C, the group affinity like which department the user is created is aligned with the attribute-based access control. A is for Just-in-time access control, but not attribute-based access control

upvoted 1 times

franbarpro 2 years, 2 months ago

So let's defined "affinity" = the relationship existing between things or persons that are naturally or involuntarily drawn together.
That to me sounds like ABAC.

upvoted 4 times

Question #162 *Topic 1*

Which of the following is the BEST approach to implement multiple servers on a virtual system?

A. Implement one primary function per virtual server and apply individual security configuration for each virtual server.

B. Implement multiple functions within the same virtual server and apply individual security configurations to each function.

C. Implement one primary function per virtual server and apply high security configuration on the host operating system.

D. Implement multiple functions per virtual server and apply the same security configuration for each virtual server.

Suggested Answer: *D*

Community vote distribution

A (80%) D (20%)

Rollizo Highly Voted 1 year, 9 months ago

It is A. This sentence is from standard as PCI DSS:

"2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)"

upvoted 9 times

Rollizo 1 year, 9 months ago

the keyword is "one primary function", the email or antimalware could be a secondary function

upvoted 1 times

jackdryan 1 year, 1 month ago

A is correct

upvoted 1 times

jon1991 Highly Voted 1 year, 9 months ago

Selected Answer: A

The answer should be - A -

upvoted 6 times

cysec_4_lyfe Most Recent 2 months, 3 weeks ago

Selected Answer: A

A. - as others have stated repeatedly regarding 2.2.1 PCI DSS standards.

upvoted 1 times

BigITGuy 2 months, 4 weeks ago

Selected Answer: A

D is suboptimal. Applying the same security configuration for all VMs ignores the fact that different functions have different security needs.

upvoted 1 times

74gjd_37 9 months, 1 week ago

Selected Answer: A

The BEST approach to implement multiple servers on a virtual system is A.

Requirement 2.2.1 of the PCI DSS states that organizations must implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server. This requirement helps to reduce the risk of unauthorized access or data leakage between different functions.

Moreover, Requirement 2.2.2 of the PCI DSS states that organizations must ensure that security configurations are not applied to other servers in a manner that would negatively impact the security of the cardholder data environment. This requirement emphasizes the importance of applying individual security configurations to each virtual server to ensure that the security of each server is not compromised.

upvoted 4 times

Dee83 1 year, 5 months ago

A. Implement one primary function per virtual server and apply individual security configuration for each virtual server.

This approach allows for more granular control of security and reduces the attack surface. Each virtual server can be configured with a unique security configuration that is tailored to its specific function, which minimizes the risk of a compromise affecting multiple servers or functions. Additionally, if one virtual server is compromised, the attacker would have access to only the resources and data on that specific virtual server, which limits the overall impact.

Implementing multiple functions within the same virtual server, and apply the same security configuration for each virtual server, may lead to a scenario where a vulnerability in one service can be used to compromise the security of other services or the whole system, and it would be harder to identify and isolate the breach.

upvoted 1 times

bynd 1 year, 7 months ago

Selected Answer: D

The answer is D. The first benefit of VMs is consolidation. That's why the answer should be the easiest and more secure option. On the other hand, If you configure different security configurations on each virtual server, it might not work when you deploy. It's recommended to keep the same configuration.

upvoted 2 times

Firedragon 1 year, 7 months ago

Selected Answer: D

D.

It doesn't say this is for PCI. Multiple functions per VM is the standard configuration and multiple VMs, which provides high availability.

upvoted 2 times

fax 1 year, 8 months ago

It should be A

upvoted 1 times

Peterzhang 1 year, 9 months ago

To think about this question in real-life, the AV or Anti-malware product in agentless or lite agent modes all be implemented by the central management with one unified policy&tasks or profiles and distributed to the clients/servers based upon hypervisor like MS Hyper-V or VMware ESXi,so still vote to D.

upvoted 3 times

stickerbush1970 1 year, 9 months ago

Selected Answer: A

A is correct

upvoted 4 times

DERCHEF2009 1 year, 9 months ago

Selected Answer: A

Highest security

upvoted 4 times

Question #163 *Topic 1*

Which of the following is the MOST common cause of system or security failures?

A. Lack of physical security controls

B. Lack of change control

C. Lack of logging and monitoring

D. Lack of system documentation

Suggested Answer: *B*

Community vote distribution

B (88%) 13%

⊟ **74gjd_37** Highly Voted 👍 1 year, 3 months ago

Selected Answer: B

ISC2 identifies lack of change control as a common cause of security failures in its Common Body of Knowledge (CBK). It includes a section on Security Operations, which covers topics such as change management, configuration management, and incident management. Within this section, lack of change control is identified as a common cause of security failures. Additionally, many other sources in the field of information security also identify lack of change control as a common issue that can lead to security incidents.

upvoted 6 times

⊟ **xxxBadManxxx** Most Recent 🕘 11 months, 1 week ago

Selected Answer: C

C. Lack of logging and monitoring / you have to check the logs and monitor.

upvoted 1 times

⊟ **maawar83** 12 months ago

I m leaning more towards C: System and Security "Failures" ---- unrecoverable

The lack of logging and monitoring in a system poses significant security risks, including limited visibility into activities, delayed incident detection, challenges in incident investigation, non-compliance with regulations, and difficulties in forensic analysis. It also hampers threat hunting efforts, monitoring user activities, ensuring accountability, receiving timely alerts for anomalies, and detecting security baseline deviations. To mitigate these risks, organizations should implement robust logging, monitoring, and incident response practices.

upvoted 2 times

⊟ **Koko4Kosh** 10 months, 1 week ago

How can a lack of logging cause a system failure? If logging was on debug I could see it filling up the file system but otherwise, this makes no sense as the answer.

upvoted 2 times

⊟ **meelaan** 1 year, 11 months ago

Selected Answer: B

its B for sure

upvoted 2 times

⊟ **jackdryan** 1 year, 7 months ago

B is correct

upvoted 1 times

⊟ **rdy4u** 2 years, 2 months ago

Selected Answer: B

Lack of a good change control process, and the solid implementation of it, will cause internal problems like that, and can also result in data breaches.

https://totalsecurityadvisor.blr.com/cybersecurity/why-cybersecurity-and-change-control-go-together-like-peanut-butter-and-jelly/

upvoted 2 times

Question #164 *Topic 1*

The Chief Information Officer (CIO) has decided that as part of business modernization efforts the organization will move towards a cloud architecture. All business-critical data will be migrated to either internal or external cloud services within the next two years. The CIO has a PRIMARY obligation to work with personnel in which role in order to ensure proper protection of data during and after the cloud migration?

A. Chief Security Officer (CSO)

B. Information owner

C. Chief Information Security Officer (CISO)

D. General Counsel

Suggested Answer: *C*

Community vote distribution

B (57%) C (43%)

izaman2022 Highly Voted 2 years, 8 months ago

I think in the context of the CISSP, the CISO generally reports to the CIO. So in this case, the CIO primarily needs to work with the CISO. The next logical step is that the CISO would work with the information owners to properly protect the data

upvoted 5 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 3 times

BigITGuy Most Recent 3 months ago

Selected Answer: B

"during and after" ... Tricky question. C is a trap. The CISO is responsible for implementing security controls and advising on best practices, but the information owner decides what protection is required. The information owner is the role primarily responsible for defining the classification, sensitivity, and security requirements for business-critical data.

upvoted 1 times

easyp 4 months, 4 weeks ago

Selected Answer: C

All the AI said C

The CIO's primary obligation in ensuring data protection during and after a cloud migration is to work with the C. Chief Information Security Officer (CISO). While collaboration with other roles is important, the CISO is specifically responsible for developing and implementing the security strategy and controls necessary to protect the organization's data, regardless of where it resides (on-premises or in the cloud). They are the key individual for addressing the security implications of the cloud migration.

upvoted 1 times

TheManiac 1 year, 1 month ago

Selected Answer: B

I'd say B. It says primary obligation, not about hierarchy or sth. You can do this move without the CISO. Can you do it without the information owner? You are moving the information to cloud. owners are responsible with these information. You are obliged to do with this personnel. Sorry, dear ciso.

upvoted 4 times

Vasyamba1 1 year, 3 months ago

Selected Answer: B

CIO will not get other title, he will remain CIO.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: B

B for Data Owner

upvoted 1 times

gjimenezf 1 year, 5 months ago

Selected Answer: C

CIO is a top management, he will not be working with lots of Information owners of lower levels in the company, he works closely with CISO

upvoted 2 times

CoolCat22 1 year, 6 months ago

Selected Answer: B

B since it says proper protection of data.

upvoted 1 times

Soleandheel 1 year, 6 months ago

C. Chief Information Security Officer (CISO)

upvoted 1 times

HughJassole 2 years ago

C. The question asks for protection of data

"The CISO's responsibilities include developing, implementing, and enforcing security policies to protect critical data. "

https://www.cisco.com/c/en/us/products/security/what-is-ciso.html

upvoted 2 times

Treebeard88 8 months, 1 week ago

Although many CISOs report to the CIO, that organizational structure is now considered to be a conflict of interest. More and more Fortune 500 companies have made the CISO coequal with the CIO. In these companies the CISO may report to the chief technology officer (CTO), the chief security officer (CSO), the chief risk officer (CRO), or even the chief operating officer (COO) or chief executive officer (CEO).

CISO reporting to CIO is now likely seen as a conflict of interest. The owner of the data still has a responsibility to ensure proper protection of the data that they own.

upvoted 1 times

oudmaster 2 years, 6 months ago

Information Owner (or Data Owner) they own the data and usually the CIO report to them.

While CISO reports to CIO.

!

In my opinion, for the CIO to ensure the proper protection for the data, he should understand what is the protection requirement from the data owner first.

upvoted 3 times

Jamati 2 years, 7 months ago

Selected Answer: C

CIO works with the CISO

upvoted 1 times

Vino22 2 years, 8 months ago

i would go for B since it says proper protection of data.

upvoted 2 times

franbarpro 2 years, 8 months ago

Information owner don't protect data.... they create and work with the data.

upvoted 2 times

Vasyamba1 1 year, 3 months ago

Information owner is responsible to define controls and ensure data is protected properly.

upvoted 4 times

Question #165 *Topic 1*

A developer is creating an application that requires secure logging of all user activity. What is the BEST permission the developer should assign to the log file to ensure requirements are met?

A. Execute

B. Read

C. Write

D. Append

Suggested Answer: *C*

Community vote distribution

D (53%) C (47%)

Rollizo Highly Voted 2 years, 9 months ago

I think that it is D:

Append Data allows or denies making changes to the end of the file but not changing, deleting, or overwriting existing data (applies to files only).

You are no interested in the application delete previous logs.

upvoted 14 times

jackdryan 2 years, 1 month ago

D is correct

upvoted 1 times

BigITGuy Most Recent 3 months ago

Selected Answer: D

The append permission allows the application to add new log entries to the log file without the ability to modify or delete existing entries.

upvoted 1 times

Treebeard88 8 months, 1 week ago

Selected Answer: D

D

Append-only ledger tables allow only INSERT operations on your tables, which ensure that privileged users such as database administrators can't alter data through traditional Data Manipulation Language operations.

upvoted 1 times

Treebeard88 8 months, 1 week ago

Selected Answer: D

D

How to Prevent

Developers should implement some or all the following controls, depending on the risk of the application:

Ensure all login, access control, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts and held for enough time to allow delayed forensic analysis.

Ensure that logs are generated in a format that log management solutions can easily consume.

Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring systems.

Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.

upvoted 1 times

deeden 10 months, 3 weeks ago

Selected Answer: C

Yes, there is a file permission that allows users to append to a file, which is write permission (w). Write permission allows users to modify or change the contents of a file, including using the redirect or append operators (>) or (>>) in the shell to change the file's contents. Without write permission, users are not allowed to change the file's contents.
https://www.redhat.com/sysadmin/linux-file-permissions-explained#:~:text=duplicate%20of%20it.-,Write%20(w),file's%20contents%20are%20not%20permitted.

upvoted 1 times

⊟ **1460168** 11 months ago

Selected Answer: D

It is D, because O_APPEND is a permission. Whenever you open a file, you can set the permission to O_APPEND and the application can not delete the file, APPEND only.

On OS you have permissions for O_APPEND via SELinux or NTFS ACL on Windows with APPEND only.

What you want is, that nobody can delete the logs.

upvoted 1 times

⊟ **Jarn** 1 year ago

Selected Answer: C

Answer is C, there is no "Append" permission.

upvoted 1 times

⊟ **Zapepelele** 6 months, 3 weeks ago

I disagree because I use it every week. Append isn't a standalone permission like +r, +w, +x .. it's more like a file attribute. But chattr +a (Append) is a real thing.

upvoted 1 times

⊟ **CCNPWILL** 1 year ago

Selected Answer: C

read write execute.. these are PERMISSIONS. append isnt a permission.. read write execute 3x.. 777.. right? what is the number for append? Answer is C.

upvoted 1 times

⊟ **klarak** 1 year, 2 months ago

Selected Answer: D

I'm not sure if this question is accurate but I think what they're getting at is D because best practice is to set your log files to Append rather than overwrite previous entries in their log files. The first 3 are irrelevant.

upvoted 1 times

⊟ **klarak** 1 year, 2 months ago

Other commenters have me convinced this should be write

upvoted 1 times

⊟ **homeysl** 1 year, 3 months ago

Selected Answer: C

It needs to write file

upvoted 1 times

⊟ **GuardianAngel** 1 year, 4 months ago

The following are the common types of rights that can be assigned to log files:

Read: This permission allows users or processes to view the contents of the log file. Reading from log files is essential for monitoring system activity, troubleshooting issues, and analyzing historical data.

Write: This permission allows users or processes to modify or append to the contents of the log file. Writing to log files is necessary for recording new events, updating log entries, or adding additional information.

Execute: In some cases, log files may have execute permissions, allowing them to be executed as scripts or programs. However, this is less common for log files and is typically reserved for executable files.

upvoted 1 times

⊟ **GPrep** 1 year, 5 months ago

Selected Answer: C

C - I've found no evidence that "append" is actually a file system permissions option. Write would be the right option here. The ability to delete/modify data is included in that, however, if Append isn't a valid option, write is the only option left. If anyone has direct evidence of append being a permission option, I'd like to learn, please share it. Windows has the "create folder / append data" option, though my testing doesn't show it does what I would assume it can do.

upvoted 4 times

Soleandheel 1 year, 6 months ago

D. Append

To ensure secure logging of all user activity, the developer should assign the "Append" permission to the log file. This permission allows new log entries to be added to the existing log file without overwriting or deleting the previous entries, ensuring that a complete record of user activity is maintained. It prevents users from modifying or deleting log entries, which is essential for maintaining the integrity of the log file for security and auditing purposes.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: D

There is the append permission in Windows and in many cloud storage types, see https://en.wikipedia.org/wiki/Append-only

upvoted 2 times

Yokota 1 year, 11 months ago

Selected Answer: C

This permission allows writing or modifying the contents of the file, making it essential for the application to log user activity securely.

upvoted 1 times

HughJassole 2 years ago

I am a Linux admin and there is no "append" in Linux. The developer doesn't assign permissions; sysadmins do. The app would need write permission but for everyone else it should be probably no access or just read.

upvoted 4 times

Alex71 2 years, 4 months ago

Selected Answer: D

The BEST permission the developer should assign to the log file to ensure secure logging of all user activity is the "Append" permission.

The "Append" permission allows new data to be added to the end of a file without overwriting or modifying any existing data in the file. This is important for secure logging of user activity because it ensures that the log file cannot be tampered with or modified by anyone, including the application itself.

If the log file had the "Write" permission, then it would be possible for someone or something to modify or overwrite existing log data, which could compromise the integrity and security of the log file.

The "Read" permission is not relevant for this use case since it only allows someone to view the contents of the file. The "Execute" permission is also not relevant since it only applies to executable files, which the log file is not.

Therefore, the "Append" permission is the BEST permission to ensure secure logging of all user activity.

upvoted 3 times

Question #166 *Topic 1*

When performing an investigation with the potential for legal action, what should be the analyst's FIRST consideration?

A. Data decryption

B. Chain-of-custody

C. Authorization to collect

D. Court admissibility

Suggested Answer: *B*

Community vote distribution

B (67%) C (21%) 12%

projtfer Highly Voted 2 years, 8 months ago

Selected Answer: B

The given answer is correct, because the question states "When performing an investigation " - it means the investigation process has already been started implying that you have been authorized to collect any pertinent info, therefore CoC is the right answer!

upvoted 20 times

klarak 1 year, 2 months ago

Agree.

upvoted 1 times

0211e3f 8 months, 1 week ago

Although I agree chain-of-custody is critically important, if you are not authorized to collect the data, via banner, consent, or a search warrant, then nothing else matters because none of it will be able to be used in court.

upvoted 2 times

franbarpro Highly Voted 2 years, 8 months ago

Selected Answer: B

When performing an investigation = B. Chain-of-custody

upvoted 8 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

muhha Most Recent 4 months, 1 week ago

Selected Answer: C

The analyst's first consideration when performing an investigation with the potential for legal action is authorization to collect. Authorization to collect is the process of obtaining the necessary permissions and approvals to collect the evidence from the relevant sources, such as the owners, custodians, or authorities. Authorization to collect is essential to ensure the legality, validity, and admissibility of the evidence, as well as to protect the rights and privacy of the parties involved. Authorization to collect can also prevent any legal or ethical issues that may arise from unauthorized or improper collection of evidence.

The other options are not the first considerations when performing an investigation with the potential for legal action, as they either come after the collection of evidence, or do not relate to the legal aspect.

upvoted 1 times

RevZig67 5 months, 3 weeks ago

Selected Answer: C

The first consideration in an investigation with potential legal action is ensuring that the analyst has the proper authorization to collect the evidence. Without this authorization, any collected evidence may be inadmissible and could jeopardize the entire investigation.

upvoted 1 times

imather 5 months, 4 weeks ago

Selected Answer: D

D. Court admissibility. Since there is the potential for legal action, evidence and procedures must be performed with the three basic requirements for admissible evidence which are:

Relevant - makes a fact more or less probable

Material - related to case
Competent - legally defensible

DoJ also adds being authentic and withstanding scrutiny of collection and preservation as additional factors.

A. Data decryption is not relevant
B. Establishing and preserving chain of custody is part of ensuring the competency of evidence
C. Ensuring the proper authorization to collect also is part of the competency of evidence.

Since B and C are included in D, the answer is D.

upvoted 1 times

deeden 10 months, 3 weeks ago

Selected Answer: C

Without proper authorization, any evidence collected could be inadmissible in court, rendering the investigation fruitless.
This includes:

Legal warrants or subpoenas: If required by jurisdiction.
Company policies and procedures: Outlining data handling and investigation protocols.
Consent from relevant parties: If necessary, obtaining permission to access data.

upvoted 1 times

CCNPWILL 1 year, 2 months ago

Selected Answer: B

B is correct.

upvoted 1 times

homeysl 1 year, 3 months ago

Selected Answer: D

Court admissibility. If you don't have that, you'll lose your case.

upvoted 1 times

[Removed] 1 year, 6 months ago

Selected Answer: B

I think it's B.
The existence of opinions stating D is likely due to the investigation and documentation of the possibility of legal measures. If legal measures are not taken, D seems meaningless, and what is the criteria for acceptability in the courtroom in the first place?

upvoted 1 times

mikelartetawabon 1 year, 7 months ago

Selected Answer: D

What ever investigation or evidence you collect, the first thing is to ensure its admissible in court. Court admissibility encompasses Chain-of-Custody and Authorization to collect. Its basic. I will choose D. What ever you do, ensure court admissibility first

upvoted 1 times

mikelartetawabon 1 year, 7 months ago

Court Admissibility. That should be the first. If you

upvoted 1 times

williom 1 year, 8 months ago

The question of "Authorization to collect" (Option C) versus "Chain-of-custody" (Option B) is a nuanced one. Both are critically important in a legal investigation. However, the sequence in which they matter is the distinction.

Before an analyst can even worry about maintaining a proper chain-of-custody, they first need to ensure they have the proper legal and/or organizational authority to collect the evidence in the first place. Collecting evidence without proper authorization can render the evidence inadmissible in court or potentially lead to legal consequences for the analyst or their organization.

Once the evidence is legally and properly collected, the chain-of-custody becomes paramount. It ensures that the evidence has been handled, stored, and transferred in a way that maintains its integrity and authenticity.

In essence, without proper authorization to collect, the chain-of-custody is moot because the evidence shouldn't have been collected in the first place. That's why "Authorization to collect" is the FIRST consideration in the context of the question.

upvoted 3 times

74gjd_37 1 year, 9 months ago

Selected Answer: B

The importance of chain-of-custody in investigations is defined in various legal and regulatory frameworks. For example, in the United States, the Federal Rules of Evidence and the Daubert standard require that evidence presented in court be relevant, reliable, and obtained through proper procedures. The chain-of-custody is critical in establishing the reliability and authenticity of evidence. Additionally, the International Organization for Standardization (ISO) provides guidelines for the management of digital evidence, including the importance of maintaining the chain-of-custody. Finally, in the context of the CISSP certification, the importance of chain-of-custody is discussed in the Information Security Governance and Risk Management domain.

upvoted 1 times

HughJassole 2 years ago

B. Chain-of-custody. Without it the evidence is probably not admissible in court. "authorization to collect" has nothing to do with collecting evidence, it's about picking up documents.

upvoted 1 times

oudmaster 2 years, 6 months ago

The question says First Consideration.
Then, I will keep option D for later stage. Because I can later decide what is admissible and what is not.
both Options B and C make sense to me. But C seems should be considered first.
What if you maintain the chain-of-custody, but the evidence collected was illegal?

upvoted 2 times

dmo_d 2 years, 1 month ago

C comes before an investigation starts.
In this scenario the investigation was already started, so the authorization was granted.
There is no dedicated need for "data collection" within the investigation process.

upvoted 1 times

dmo_d 2 years, 1 month ago

dedicated need for "data collection" authorization

upvoted 1 times

Ivanchun 2 years, 6 months ago

Selected Answer: B

I think is B, Chain-of-custody is the whole process included

upvoted 2 times

Firedragon 2 years, 7 months ago

Selected Answer: C

C.
The first step of Investigation Process is Gathering Evidence which includes.
First, voluntarily surrender
Second, a subpoena
Third, the plain view doctrine
fourth, a search warrant
OSG P919

upvoted 1 times

Question #167 *Topic 1*

Building blocks for software-defined networks (SDN) require which of the following?

A. The SDN is composed entirely of client-server pairs.

B. Random-access memory (RAM) is used in preference to virtual memory.

C. The SDN is mostly composed of virtual machines (VM).

D. Virtual memory is used in preference to random-access memory (RAM).

Suggested Answer: *C*

Community vote distribution

C (60%) D (27%) 13%

⊟ **BigITGuy** 3 months ago

Selected Answer: C

Software-Defined Networks (SDN) typically rely on 1. virtualization for network components. 2.Separation of the control plane and the data plane. 3. Virtual machines (VMs) or containers to host network functions like routers, switches, firewalls, and controllers.

upvoted 1 times

⊟ **cysec_4_lyfe** 4 months ago

Selected Answer: C

This is from AI: The correct answer is none of the provided options accurately describe the building blocks of Software-Defined Networks (SDN). Let me clarify what the building blocks of SDN are based on the provided search results.
I made it pick one anyways and it chose C haha.

upvoted 1 times

⊟ **deeden** 10 months, 3 weeks ago

Selected Answer: C

This is incorrect.

While virtualization can be used in an SDN environment, it's not a core building block. SDN is primarily about separating the control plane from the data plane.

SDN building blocks typically include:

- SDN Controller: Centralized intelligence for managing network traffic.
- Network Devices: Switches, routers, and other hardware that forward traffic based on controller instructions.
- Northbound Interface: API for applications to interact with the SDN controller.
- Southbound Interface: Protocol for communication between the controller and network devices.

These components work together to create a flexible and programmable network.

None of the options are entirely accurate.

upvoted 2 times

⊟ **CCNPWILL** 1 year ago

Selected Answer: C

Bad question and answer is just as bad. I would go with C.

cisco-hosted or on-prem setups are going to be setup using VMs. Answer is C...

upvoted 3 times

⊟ **eboehm** 1 year, 2 months ago

Selected Answer: A

SDN uses virtualization, but is not MOSTLY composed of VMs. SDN is modelled as a set of client-server relationships with the SDN controller at its core.
https://safe.menlosecurity.com/doc/docview/viewer/docNC2DBDD5FD5C050a8f26ba6bbb1be40d084fa0902dd66838758e41d2675edfd35731a53f565ce

upvoted 1 times

eboehm 1 year, 2 months ago

wanted to add that Network virtualization is different than SDN virtualization. You CAN configure an SDN to set up virtual machines and server clusters, but the core of an SDN is still physical devices.

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: C

OSG - Virtualization extends beyond just servers and networking. Software-defined everything

(SDx) refers to a trend of replacing hardware with software using virtualization.

upvoted 1 times

Dee83 2 years, 5 months ago

C. The SDN is mostly composed of virtual machines (VM)

A Software-defined Network (SDN) is a network architecture that uses software to abstract the underlying physical network infrastructure and provide programmability, flexibility, and control over the network resources.

In order to build a SDN, it is necessary to have the network infrastructure composed mostly of virtual machines (VMs) or virtual network functions (VNFs) that are running on top of a physical infrastructure, these VMs or VNFs are the building blocks for the SDN. These virtualized components can be easily moved, scaled, and managed, providing the flexibility and programmability required for a SDN.

upvoted 3 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

Firedragon 2 years, 7 months ago

Selected Answer: D

D.

C. The SDN is mostly composed of virtual machines (VM). - This is wrong statement. SDN has 3 layers and VM is not one of them.

a) an infrastructure layer

b) a control layer and

c) an application layer.

SDN technology combined with virtual machines and virtualization of networks provides efficiencies to service providers as well.

https://www.ibm.com/cloud/blog/software-defined-networking

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: A

With SDN, it's mostly the Orchestrator / controller that's virtualized. Everything else is hardware.

upvoted 1 times

rdy4u 2 years, 8 months ago

Selected Answer: C

SDN technology combined with virtual machines and virtualization of networks provides efficiencies to service providers as well. With these resources, they can provide distinct network separation and control to customers.

https://www.ibm.com/cloud/blog/software-defined-networking

upvoted 2 times

sec_007 2 years, 8 months ago

The benefits of DCO may include reduced operational costs, more efficient use of infrastructure, and access to more server, storage or computing capacity on demand. The risks include lack of control over security and disaster recovery, lack of flexibility, problems with SLA fulfillment and vendor lock-in.

upvoted 1 times

projtfer 2 years, 8 months ago

Selected Answer: C

Given answer is the best, not a good question (agree with GregP). vManage – Management Dashboard.

vEdge – The edge router at branches.

vBond – The Orchestrator.

vSmart – The Controller.

Most of them are VMs.

upvoted 4 times

⊟ **GregP** 2 years, 8 months ago

its a rubbish question, but I'd say the given answer is the best.

upvoted 2 times

⊟ **Rollizo** 2 years, 9 months ago

Selected Answer: D

I think that it is D: SDN prefer to use virtual memory to use RAM memory because this guarantees flexibility to the applications.

upvoted 3 times

⊟ **Rollizo** 2 years, 9 months ago

C seems no be right, because you have VM for the controller and other elements but you have a lot of switch and routers and they are physical appliances.

upvoted 1 times

Question #168 *Topic 1*

What is the MINIMUM standard for testing a disaster recovery plan (DRP)?

A. Quarterly or more frequently depending upon the advice of the information security manager

B. As often as necessary depending upon the stability of the environment and business requirements

C. Annually or less frequently depending upon audit department requirements

D. Semi-annually and in alignment with a fiscal half-year business cycle

Suggested Answer: *D*

Community vote distribution

B (49%) D (29%) C (20%)

SF_NERD Highly Voted 2 years, 3 months ago

Selected Answer: D

The tricky GOTCHA point here to notice is the "or less frequently" part of C. Regulation requires NO MORE THAN 12 months (1 year) so C can't be correct. D is the BEST (and most annoying CISSP style) answer

upvoted 16 times

Petergriffith 2 years, 1 month ago

In the Book, the following is written:"The plan must be tested periodically to determine whether the plan to restore is actually
operational, and personnel should be trained to take the actions required. Although
dependent on the industry and regulatory requirements, testing should be performed no
less than annually"

upvoted 3 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

74gjd_37 Highly Voted 1 year, 3 months ago

Selected Answer: B

According to the CISSP Common Body of Knowledge (CBK), there is no specific minimum frequency stipulated for testing a disaster recovery plan (DRP). However, it is recommended that DRPs should be tested regularly to ensure that they are effective and up-to-date. The frequency of testing should be based on the organization's business requirements, the stability of the environment, and the advice of the information security manager.

There are several industry standards and regulations that provide guidance on DRP testing frequency. For example, the National Institute of Standards and Technology (NIST) recommends that DRPs should be tested at least annually. The Payment Card Industry Data Security Standard (PCI DSS) requires annual testing of DRPs as well. However, these are only recommendations and actual testing frequency may vary depending on the organization's needs and risk appetite.

Therefore, the answer is "B".

upvoted 12 times

BigITGuy Most Recent 3 months ago

Selected Answer: B

The minimum standard for testing a Disaster Recovery Plan (DRP) is not based on a fixed period but rather on 1. criticality of the business, 2. stability of the IT environment, 3. business requirements and regulatory obligations.

upvoted 1 times

Jarn 6 months, 3 weeks ago

Selected Answer: C

ISC^2 is looking for Annually, regardless of what a "good" policy may be.

upvoted 1 times

klarak 8 months, 1 week ago

Selected Answer: B

Everything in CISSP land goes back to risk tolerance and risk management. So everything is relative to risk and there is no static minimum or maximum answer for a question like this.

upvoted 2 times

homeysl 9 months, 2 weeks ago

Selected Answer: B

Business requirements

upvoted 1 times

hoho2000 9 months, 3 weeks ago

Selected Answer: D

Looking at the question, the main crux is asking, the MINIMUM based on the below.
C is out at per the word "or less" than per annum as this is against CISSP recoomendation.
The rest are all higher than D, so choose the minimum frequency answer along with the best answer.

upvoted 1 times

gjimenezf 11 months, 2 weeks ago

Selected Answer: B

Business requirements

upvoted 1 times

homeysl 1 year, 2 months ago

Selected Answer: B

Depends on your environment

upvoted 2 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: B

DRP tests are driving by changes (IT or business).

upvoted 3 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: A

DRP tests are driving by changes.

upvoted 1 times

dyndevil 1 year, 5 months ago

Correct answer B:
Audit requirements and fiscal alignment don't drive DR testing. Business requirements do (as long as it meets at least once a year). In many aspects of CISSP (Risk, BCP, DR etc etc), business requirements drive the decisions.

upvoted 2 times

HughJassole 1 year, 6 months ago

I am thinking B.
"While there is no one standard for how often you should test your DRP and BCP, you should generally conduct functional disaster recovery testing at least once per year."
https://www.eccouncil.org/cybersecurity-exchange/disaster-recovery/test-disaster-recovery-plan/#:~:text=While%20there%20is%20no%20one,at%20least%20once%20per%20year.

C says annually or less frequently, but that "less frequently" is wrong.

upvoted 1 times

xxxBadManxxx 1 year, 6 months ago

B is correct you do DRP whenever is required. not sure why folks answering C &D :)

upvoted 1 times

xxxBadManxxx 1 year, 6 months ago

B: As often as necessary depending upon the stability of the environment and business requirements

upvoted 1 times

DASH_v 1 year, 8 months ago

Selected Answer: B

NIST SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems:

"The frequency of testing should be determined by the criticality and volatility of the system, and the DR plan should be updated as necessary to reflect changes in the system and its environment."

DRI International Professional Practices for Business Continuity Management:

"The frequency of testing should be determined by the criticality of the process, the complexity of the recovery, and the frequency of change to the process or supporting technology. The frequency of testing should be sufficient to ensure that the plan remains effective and relevant in addressing potential disasters."

upvoted 4 times

init2winit 1 year, 11 months ago

Selected Answer: B

DRP Testing should follow a policy that meets the business requirement.

upvoted 3 times

Question #169 *Topic 1*

Which security audit standard provides the BEST way for an organization to understand a vendor's Information Systems (IS) in relation to confidentiality, integrity, and availability?

A. Service Organization Control (SOC) 2

B. Statement on Standards for Attestation Engagements (SSAE) 18

C. Statement on Auditing Standards (SAS) 70

D. Service Organization Control (SOC) 1

Suggested Answer: *D*

Community vote distribution

A (68%) B (32%)

[Removed] Highly Voted 👍 2 years, 3 months ago

Selected Answer: A

Soc 2 for sure

upvoted 8 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

Rollizo Highly Voted 👍 2 years, 3 months ago

Selected Answer: A

SOC1 it is only financial... it is SOC2

upvoted 5 times

BigITGuy Most Recent 🕘 3 months ago

Selected Answer: A

A SOC 2 report specifically evaluates a vendor's information systems against the Trust Services Criteria, which include CIA.

upvoted 1 times

Jarn 6 months, 3 weeks ago

Selected Answer: B

SSAE 18 is the standard, which is what the question is looking for.

upvoted 2 times

klarak 8 months, 1 week ago

SSAE 18 seems to be the answer here: https://reciprocity.com/resources/what-is-a-ssae-18-audit/

upvoted 1 times

eboehm 8 months, 3 weeks ago

ugh I really dont like questions like this. Technically based on the wording the true answer is that it would be SSAE 18 as this defines how the SOC reports are generated. But the question is would a CEO/manager give a shit what standard was being using or would they just want the SOC 2 report

upvoted 1 times

eboehm 8 months, 3 weeks ago

Even though the officially correct answer is SSAE 18. The organization is concernted with the controls so ima go with SOC 2. SSAE 18 applies to all 3 reports. That would be the CEO answer. You would be in a world of hurt if a ceo for the audit standard to achieve confidentiality, integrity, and availability and you were like well actually the standard is defining 3 reports

upvoted 1 times

dm808 9 months ago

Selected Answer: B

The question is asking about an auditing standard

SSAE 18 is a standard. SOC 1 an 2 are reports..

and SOC reports are defined in the SSAE 18

upvoted 1 times

YesPlease 1 year ago

Selected Answer: A

Answer A) Service Organization Control (SOC) 2

The other three refer to financial standards. https://ssae-16.com/soc-1/#:~:text=The%20SOC1%20Report%20is%20what,of%20May%201%2C%202017).

upvoted 1 times

7f7b53c 1 year, 1 month ago

B. Soc is not a standard

upvoted 1 times

Dann108 1 year, 4 months ago

Selected Answer: A

SOC 2 is a voluntary compliance standard for service organizations,

upvoted 1 times

MShaaban 1 year, 4 months ago

It is A.

upvoted 1 times

HughJassole 1 year, 6 months ago

Answer is B, the question clearly states "standard". The SSAE 18 is a standard that is used to generate the SOC2 report.
"The Statement on Standards for Attestation Engagements 18, or SSAE 18, is a standard that auditors can use to review the controls of technology vendors and other service providers so that businesses using those vendors can be confident that the vendors' controls-particularly those related to cybersecurity"
https://reciprocity.com/understanding-ssae-18-requirements/

upvoted 1 times

RVoigt 1 year, 10 months ago

Selected Answer: A

CISSP Official Study Guide pg 729 - "SOC 2 Engagements Assess the organization's controls that affect the security (confidentiality, integrity, and availability) and privacy of information stored in a system. SOC 2 audit results are confidential and are normally only shared outside the organization under an NDA."

upvoted 3 times

ST811 1 year, 11 months ago

Why A? SOC2 should be confidential

upvoted 1 times

somkiatr 1 year, 12 months ago

Selected Answer: B

B (SSAE) would be correct.
Reference : https://www.advancedbusinesssolutions.com/whats-a-soc-compliant-service-provider/

upvoted 3 times

Ivanchun 2 years ago

Selected Answer: A

Select A, SOC 1 is about the financial report?

upvoted 1 times

Petergriffith 2 years, 1 month ago

Definitely A... SOC 2 provides, CIA + Privacy + Process Integrity + Security (Data Loss etc.)

upvoted 1 times

Question #170 *Topic 1*

An application team is running tests to ensure that user entry fields will not accept invalid input of any length. What type of negative testing is this an example of?

A. Allowed number of characters

B. Population of required fields

C. Reasonable data

D. Session testing

Suggested Answer: *B*

Community vote distribution

A (46%) C (41%) 13%

74gjd_37 Highly Voted 1 year, 9 months ago

Selected Answer: A

Although both "Allowed number of characters" and "Reasonable data" are important concepts in input validation testing, they are not the same thing.

"Allowed number of characters" testing focuses specifically on ensuring that user input does not exceed the maximum allowed length of a field. This is important because input that exceeds the maximum allowed length can potentially cause buffer overflow vulnerabilities or other security issues.

On the other hand, "Reasonable data" testing focuses on ensuring that the input data is reasonable and meets the expected criteria. This can include testing for data types, formats, and content. For example, if a field is expecting a numeric value, "Reasonable data" testing would ensure that only numeric values are accepted.

In the case of the scenario described, the application team is specifically testing the maximum length of input fields, which falls under "Allowed number of characters" testing. Therefore, it is more accurate to describe this testing as "Allowed number of characters" rather than "Reasonable data".

upvoted 9 times

bassfunk Most Recent 3 weeks, 2 days ago

Selected Answer: C

The answer is C. The key phrase here is "will not accept invalid input of ANY length." The question specifically says that length doesn't matter. This is not a test of max number of characters. Its a test of reasonable data.

upvoted 1 times

shiiitboi 2 months ago

Selected Answer: C

It says "will not accept invalid input of any length' meaning regardless of length. This nullifies Length being the main test,. The main test here is reasonable data, regardless of its length.

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: A

Keyword is "length". Can't be C. Reasonable data checks if the input is realistic (e.g., an age field does not accept 500).

upvoted 1 times

deeden 10 months, 3 weeks ago

Selected Answer: C

Reasonable data is the most accurate answer. This type of negative testing involves inputting data that is technically correct but logically incorrect or out of range. By testing with invalid input lengths, the application team is ensuring that the system can handle unexpected data and prevent potential vulnerabilities like buffer overflows.

upvoted 2 times

Seikolipa 5 months, 2 weeks ago

The answer is not Reasonable Data because reasonable data means not allowing users to put their birth year as 1664, or something unreasonable. A reasonable birthyear would be within the last 100 years. This question is specifically asking about input length, therefore the answer is A. Allowed number of characters.

upvoted 2 times

klarak 1 year, 2 months ago

Selected Answer: C

The answer is C: Reasonable data – https://smartbear.com/learn/automated-testing/negative-testing/ "Some applications and web pages include fields that have a reasonable limit, for example, entering 200 or a negative number as the value for the "Your age:" field is not allowed. To check the application's behavior, create a negative test that enters invalid data into the specified field."

upvoted 1 times

gjimenezf 1 year, 5 months ago

Selected Answer: A

Negative tests:

Invalid Input:, Exceeding Input Limits, Empty or Null Input, Special Characters, Injection Attacks, Boundary Value Testing, Concurrency Testing, Unexpected Configurations, Invalid Authentication, Negative Workflow Testing, Resource Exhaustion, Network Failures, Time Zone and Date Issues

upvoted 1 times

YesPlease 1 year, 6 months ago

Selected Answer: C

Answer C) Reasonable Data

https://smartbear.com/learn/automated-testing/negative-testing/#:~:text=Reasonable%20data%20%E2%80%93%20Some%20applications%20and,data%20into%20the%20specified%20field.

upvoted 1 times

cyber_master 1 year, 9 months ago

Selected Answer: A

Allowed number of Characters addresses length of input

upvoted 3 times

MShaaban 1 year, 10 months ago

I would say C.

upvoted 1 times

Dee83 2 years, 5 months ago

A. Allowed number of characters

This type of negative testing is an example of testing for the allowed number of characters. This test is to ensure that user entry fields will not accept invalid input of any length. This test is used to check the validation of the input fields and to ensure that the application is not vulnerable to buffer overflow attacks.

upvoted 4 times

babaseun 2 years, 2 months ago

will not accept input of any length is "A" but will not accept invalid input of any length is "C"

upvoted 1 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

827 2 years, 5 months ago

Selected Answer: C

Reasonable data – Some applications and web pages include fields that have a reasonable limit, for example, entering 200 or a negative number as the value for the "Your age:" field is not allowed. To check the application's behavior, create a negative test that enters invalid data into the specified field.

https://smartbear.com/learn/automated-testing/negative-testing/

upvoted 1 times

somkiatr 2 years, 5 months ago

Selected Answer: C

"Will not accept invalid input of any length". This means the application will check for invalid input value regardless of the input length.

upvoted 3 times

zelda923 2 years, 6 months ago

Selected Answer: C

The question states that developers are testing the application against "invalid inputs of any length". This means that the application must only accept "valid inputs" = "reasonable data" and reject all invalid inputs irrespective of their length. This excludes testing the population of required fields, and the maximum number of characters for each field.

upvoted 2 times

rajkamal0 2 years, 6 months ago

Selected Answer: A

Negative testing using more characters with a limitation of allowed number of characters.

upvoted 1 times

Cccccccc123 2 years, 7 months ago

Selected Answer: C

It says 'of any length'. Hence C.

upvoted 1 times

Nickolos 2 years, 7 months ago

Selected Answer: C

https://smartbear.com/learn/automated-testing/negative-testing/

This resource best addresses this and in the most direct way.

Based on this and the question, the answer should be C, reasonable data

upvoted 1 times

Question #171 *Topic 1*

An organization is considering partnering with a third-party supplier of cloud services. The organization will only be providing the data and the third-party supplier will be providing the security controls. Which of the following BEST describes this service offering?

A. Platform as a Service (PaaS)

B. Anything as a Service (XaaS)

C. Infrastructure as a Service (IaaS)

D. Software as a Service (SaaS)

Suggested Answer: *A*

Community vote distribution

D (53%) A (47%)

IT_Guy23 Highly Voted 2 years, 3 months ago

Selected Answer: A

How come all the comments are always so wrong?? If you look it up, in a PAAS, application and data are user managed, while the provider manages the rest. In a SAAS, the user provides nothing. I'm just stunned at these CISSP comments all around.

upvoted 22 times

splash2357 11 months, 1 week ago

Examples of PaaS are Google AppEngine, Heroku, AWS lambda, AWS Elastic Beanstalk where you need to bring your own codes.

Most of them require you provide your code to the platform and it will help you to run it.
The PaaS provider will manage the server and the "executable used to run the code" (sorry for bad english, i dun know the exact term, maybe "runtime"?). You are responsible for the security of the application though.

For example, you can upload a python web application (e.g. flask/django) to Google AppEngine/Heroku, you won't need to manage the server (e.g. server hardening, apply server update patches). But you do need to manage the security of your python web app :)

upvoted 4 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

dumdada 1 year, 6 months ago

When you use a SaaS platform like Youtube or Gmail, you provide the Data, the vendor provides EVERYTHING else ...

upvoted 3 times

Toyeeb 2 years, 2 months ago

In saas, the user provides data. take gmail for example, your mails are your data while the gmail platform is the service you are using.

upvoted 8 times

Joe_Cheng Highly Voted 2 years, 3 months ago

Selected Answer: D

https://www.ispsystem.com/news/xaas

You will know it when you see the photo

upvoted 11 times

Vulcan6x9 1 year ago

the comment on that webpage made me reconsider my thoughts on giving the CISSP exam

upvoted 2 times

SF_NERD 2 years, 3 months ago

This link is the MOST helpful!

upvoted 2 times

BigITGuy Most Recent 3 months ago

Selected Answer: D

In a SaaS model, the third-party supplier provides both the application and its security controls. The organization only provides the data and consumes the service. The supplier is responsible for managing: Infrastructure, Platform, Application, Security controls (e.g., authentication, encryption, patching).

upvoted 1 times

iRyae 4 months, 1 week ago

Selected Answer: D

The organization is providing the data, which is a key aspect of using a software application. The third-party supplier is providing the security controls and the application itself. This means the organization is using a complete application, which is the definition of SaaS.

upvoted 1 times

Rider2053 4 months, 2 weeks ago

Selected Answer: C

C. Infrastructure as a Service (IaaS) – The cloud provider offers the infrastructure and security controls, while the organization is responsible for providing and managing the data.

upvoted 2 times

KakekGuru 5 months, 1 week ago

Selected Answer: A

OSG 10, FIGURE 16.1 Cloud shared responsibility model

In SaaS, data and application responsibility are shared. In PaaS, customer manages data and application. In IaaS, customer manages application, data, runtime, OS.

So, I guess the answer could be A. PaaS.

But I think they purposely made this a very tricky question, because no clear information regarding PaaS (vendor provides the platform), or SaaS (vendor provides the application).

upvoted 1 times

RevZig67 5 months, 3 weeks ago

Selected Answer: C

In this case, where the third-party supplier is providing security controls for the infrastructure and the organization is providing the data, the best description is IaaS.

upvoted 1 times

aznbat21 7 months, 3 weeks ago

Selected Answer: D

D is correct. Take a course about cloud and you will know.

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: A

PaaS = customer provides code/data and vendor runs it in their cloud

upvoted 1 times

GuardianAngel 10 months, 3 weeks ago

SaaS can be something like quicken where they supply the software and security controls, the user with the software subscription just puts their bank account data in quicken using the application to manage it.

upvoted 1 times

shmoeee 1 year, 1 month ago

A is correct:

https://res.cloudinary.com/practicaldev/image/fetch/s--9smmBPKg--/c_limit%2Cf_auto%2Cfl_progressive%2Cq_auto%2Cw_800/https://dev-to-uploads.s3.amazonaws.com/uploads/articles/jkfnnrt8lw0ijnf8hlk1.png

upvoted 1 times

shmoeee 1 year, 1 month ago

A is correct:

- https://res.cloudinary.com/practicaldev/image/fetch/s--9smmBPKg--/c_limit%2Cf_auto%2Cfl_progressive%2Cq_auto%2Cw_800/https://dev-to-uploads.s3.amazonaws.com/uploads/articles/jkfnnrt8lw0ijnf8hlk1.png

upvoted 1 times

HappyDay030303 1 year, 1 month ago

D: 58%, A: 42%

Amazing how many cissp questions on here are so evenly split

upvoted 2 times

homeysl 1 year, 2 months ago

Selected Answer: D

D. Data of the customer = Saas

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: A

It is not a PaaS offering because in a PaaS offering, the third-party supplier would provide a platform for the organization to build, test, and deploy their own applications. In this scenario, the organization is only providing data and is not responsible for building, testing, or deploying any applications. The third-party supplier is also responsible for providing the security controls, which is a component of the software service that the organization will be using. Therefore, it is a SaaS offering rather than a PaaS offering.

upvoted 1 times

irritans 5 months, 1 week ago

So why did you select answer A? Correct your selection.

upvoted 1 times

[Removed] 1 year, 3 months ago

D. Software as a Service (SaaS)

upvoted 1 times

BoyBastos 1 year, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

Question #172 *Topic 1*

Which of the following factors should be considered characteristics of Attribute Based Access Control (ABAC) in terms of the attributes used?

A. Mandatory Access Control (MAC) and Discretionary Access Control (DAC)

B. Discretionary Access Control (DAC) and Access Control List (ACL)

C. Role Based Access Control (RBAC) and Mandatory Access Control (MAC)

D. Role Based Access Control (RBAC) and Access Control List (ACL)

Suggested Answer: *D*

Community vote distribution

D (90%) 10%

⊟ **RVoigt** Highly Voted 2 years, 4 months ago

Selected Answer: D

CISSP Official Study Guide pg 686 - "ABAC models use policies that include multiple attributes for rules. Attributes can be almost any characteristic of users, the network, and devices on the network. For example, user attributes can include group membership, the department where they work, and devices they use such as desktop PCs or mobile devices. The network can be the local internal network, a wireless network, an intranet, or a wide area network (WAN). Devices can include firewalls, proxy servers, web servers, database servers, and more."

upvoted 7 times

⊟ **BigITGuy** Most Recent 3 months ago

Selected Answer: D

ABAC uses a set of attributes to make access decisions. While ABAC is distinct from RBAC and ACL, it can incorporate characteristics from both RBAC, which contributes to the idea of using roles as an attribute. In ABAC, roles are just one of many possible attributes. ACL contributes the concept of explicit permissions, but in ABAC, permissions are granted based on matching attributes rather than just listing users or roles directly.

upvoted 1 times

⊟ **cysec_4_lyfe** 4 months ago

Selected Answer: C

I picked C from the start.

From Perplexity - While none of the options perfectly describe ABAC, C is the best choice because ABAC can incorporate elements of both RBAC and MAC, depending on how attributes are defined and policies are enforced:

RBAC: ABAC can use roles as one of many attributes for decision-making.

MAC: ABAC can enforce strict access rules based on attributes like security classifications.

ABAC is a more flexible and dynamic model than RBAC or MAC, but since these models can be implemented using attributes, C is the closest match for the CISSP exam.

upvoted 2 times

⊟ **Passmi** 4 months, 1 week ago

Selected Answer: C

Deepseek-Role-Based Access Control (RBAC): ABAC extends RBAC by using roles as one of the attributes in its decision-making process.

Mandatory Access Control (MAC): ABAC incorporates policy-driven access decisions, similar to MAC, where access is determined by a central authority based on predefined rules and labels.

While D mentions RBAC (which is relevant to ABAC), the inclusion of ACLs makes it incorrect. Therefore, C is the best choice for the CISSP exam

upvoted 2 times

⊟ **Tuhaar** 6 months, 2 weeks ago

Selected Answer: C

ACL is a network function and does not take any criteria other than Layer 3 (IP address and port number). ABAC is a combination of RBAC + Policy (say time of the day - MAC strongly adheres to this). Hence C is the option

upvoted 2 times

Tuhaar 7 months ago

Selected Answer: C

Answer is C as per: The CISSP Official Study Guide, Domain 5 (Identity and Access Management), describes ABAC as a dynamic access control model that evaluates multiple attributes, integrating principles from RBAC and MAC, but exceeding their capabilities with granular, policy-driven access control. Additionally, NIST SP 800-162 provides guidance on ABAC.

upvoted 3 times

klarak 1 year, 2 months ago

How can RBAC be an answer? I thought combining RBAC with ABAC makes it a hybrid environment? How is RBAC part of ABAC, that makes no sense?

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: D

The correct answer is D. Role Based Access Control (RBAC) and Access Control List (ACL) are the attributes used in Attribute Based Access Control (ABAC). RBAC defines access based on a user's job function within an organization and ACL defines access based on a user's identity.

upvoted 1 times

georgegeorge125487 1 year, 10 months ago

Selected Answer: D

ABAC is an improvments over RuBAC which is based on merging roles with ACL. 1 role = several sevral actions i.e. rules.

upvoted 1 times

Tygrond87 2 years, 1 month ago

Selected Answer: C

Abac can be based on your group RBAC or your label MAC

upvoted 2 times

> **jackdryan** 2 years, 1 month ago
>
> D is correct
>
> upvoted 2 times

iwannapass 2 years, 4 months ago

Selected Answer: D

I think this might be a typo. I'm going with Rule-Based Access Control and ACL. My reasoning is backed by the sybex book 9th edition, page 686. Topic on ADAC. ADAC is an advanced form of Rule-Based Access Control . Correct me if i am wrong.

upvoted 3 times

Question #173 *Topic 1*

Which of the following is the MOST significant key management problem due to the number of keys created?

A. Exponential growth when using symmetric keys

B. Exponential growth when using asymmetric keys

C. Storage of the keys require increased security

D. Keys are more difficult to provision and revoke

Suggested Answer: *C*

Community vote distribution

A (63%) | B (24%) | 13%

kasiya Highly Voted 👍 2 years, 3 months ago

Selected Answer: A

due to the number of keys created!

upvoted 12 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

RVoigt Highly Voted 👍 1 year, 10 months ago

Selected Answer: A

for Asymmetric key = no*2 so if we have 10 subjects we need 20keys.

for Symmetric key =10*(10-1)/2=45keys

upvoted 6 times

BigITGuy Most Recent 🕒 3 months ago

Selected Answer: A

The most significant key management problem with symmetric encryption is the exponential growth of the number of keys required as more users or entities are added.

upvoted 1 times

cysec_4_lyfe 4 months ago

Selected Answer: A

Symmetric for n users, the total number of keys required is n(n-1) divided by 2.

Asymmetric would be 1 public and 1 private key for each.

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: A

N*(N-1)/2

upvoted 3 times

gjimenezf 11 months, 2 weeks ago

Selected Answer: B

B. Exponential growth when using asymmetric keys

The MOST significant key management problem due to the number of keys created is typically associated with the use of asymmetric keys. In asymmetric cryptography (also known as public-key cryptography), each entity typically has a pair of keys: a public key and a private key. As the number of entities (such as users or systems) increases, the number of key pairs grows exponentially.

Option B, "Exponential growth when using asymmetric keys," addresses this challenge accurately. The growth is exponential because, for every new entity, a new key pair must be generated, resulting in a quadratic increase in the number of keys to manage.

While managing symmetric keys (Option A) also poses challenges, the growth is typically linear, not exponential, as each entity requires only one key.

Options C and D touch on other aspects of key management but are not as directly related to the exponential growth issue associated with the number of keys created

upvoted 1 times

[Removed] 1 year ago

Selected Answer: A

I think it's either A or C.

The number of generated keys seems to be the cause...
Considering this statement, I believe A is the correct answer.

Whether the number of keys is small or large, it is necessary to maintain security in the storage of secret keys. Is it acceptable not to enhance security if the number of keys is small? I don't think so

upvoted 1 times

homeysl 1 year, 2 months ago

Selected Answer: A

(N * (N-1)) / 2.

upvoted 1 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

win610 1 year, 5 months ago

Selected Answer: A

A is correct

upvoted 1 times

Moose01 1 year, 7 months ago

C is the correct answer.
no matter symmetric or asymmetric or even your VPN keys, or your routing protocol peering keys.... they all have to be safe guarded, even from internal users and IT guys, you dont wants your router to peer with a masquerade as partner knowing your keys.

upvoted 3 times

A1nthem 1 year, 8 months ago

Selected Answer: C

Obviously,A is not correct compared to B.
protecting/Storage of key is smore concern.

upvoted 1 times

Dee83 1 year, 11 months ago

D. Keys are more difficult to provision and revoke

The number of keys created can create a significant key management problem. As the number of keys increases, it becomes more difficult to manage and maintain them. One of the most significant problems is that keys are more difficult to provision and revoke. This is because as the number of keys increases, it becomes harder to keep track of which keys are associated with which users, systems, or services. This can make it harder to ensure that the right keys are being used by the right people and that keys are being used for the right purposes. Additionally, revoking a key can be challenging as it requires identifying all the locations where that key is being used and updating them accordingly.
While the other options mention that key management can be an issue but they are not the most significant key management problem as the exponential growth when using symmetric or asymmetric keys can be handled

upvoted 1 times

trojix 1 year, 11 months ago

Selected Answer: B

Read "somkiatr's" comments, he hit in on the head.

upvoted 2 times

somkiatr 1 year, 11 months ago

Selected Answer: B

Supposing we have 10 persons. For asymmetric key, each person have to store 1 own private key for decrypting receiving data and 9 public keys of others persons for encrypting sending data. The total available storing keys of 10 persons are 10x10 = 100 (exponential). While in case of symmetric key, every of two persons will share a common key then the total keys stored are (10x9)/2=45

upvoted 5 times

⊟ **Securitypampam** 1 year, 7 months ago

Regarding the asymmetric key, only the public keys are stored in a central location , which are just 10.

upvoted 2 times

⊟ **Delab202** 1 year, 12 months ago

for Asymmetric key= no*2 so if we have 10 subjects we need 20keys.

for symmetric key=10*(10-1)/2=45keys

upvoted 3 times

⊟ **RVoigt** 1 year, 10 months ago

The formulas from Delab202 are correct

Asymmetric is 2N or 2*10 = 20

Symmetric is (N*(N-1))/2 or (10*(10-1))/2 = 45

upvoted 1 times

⊟ **rajkamal0** 2 years ago

Selected Answer: C

C is correct

upvoted 1 times

Question #174 *Topic 1*

Systems Security Professional (CISSP) with identity and access management (IAM) responsibilities is asked by the Chief Information Security Officer (CISO) to perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit. The CISSP has never performed this before. According to the (ISC)
Code of Professional Ethics, which of the following should the CISSP do?

A. Inform the CISO that they are unable to perform the task because they should render only those services for which they are fully competent and qualified

B. Since they are CISSP certified, they have enough knowledge to assist with the request, but will need assistance in order to complete it in a timely manner

C. Review the CISSP guidelines for performing a vulnerability assessment before proceeding to complete it

D. Review the PCI requirements before performing the vulnerability assessment

Suggested Answer: *A*

Community vote distribution

A (85%) D (15%)

crazywai1221 Highly Voted 1 year, 8 months ago

Selected Answer: A

For exam, A. For real work environment, D.

Your boss ask you to do it, do it please

upvoted 19 times

shmoeee 1 year, 1 month ago

AGREEED!

upvoted 3 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 2 times

gjimenezf Most Recent 11 months, 2 weeks ago

Selected Answer: A

According to the (ISC) Code of Professional Ethics, CISSP professionals are obligated to provide services only in areas where they are competent and qualified. If a CISSP has never performed a vulnerability assessment on a web application and is unsure of their capabilities, the ethical course of action is to inform the CISO that they are unable to perform the task and may need to seek assistance or additional training.

Option A aligns with the principle of integrity and responsibility outlined in the (ISC) Code of Professional Ethics. It emphasizes the importance of honesty and competence in providing services. Seeking assistance or training in areas where competence is lacking is a responsible and ethical approach.

upvoted 3 times

74gjd_37 1 year, 3 months ago

Selected Answer: A

The CISSP cannot perform a vulnerability assessment on a web application to pass a Payment Card Industry (PCI) audit if they are not fully competent and qualified because it goes against the (ISC) Code of Professional Ethics. The code requires that a CISSP should render only those services for which they are fully competent and qualified. Performing a task that the CISSP is not fully competent and qualified to do can result in inadequate or incorrect assessment and recommendations, which can lead to security vulnerabilities and non-compliance with regulations such as PCI DSS. It is essential to ensure that the person performing the vulnerability assessment has the necessary knowledge, skills, and experience to carry out a comprehensive and accurate assessment.

upvoted 3 times

shash33 1 year, 11 months ago

Selected Answer: A

Separation of Duties plus act honestly !

upvoted 1 times

init2winit 1 year, 11 months ago

Selected Answer: D

Not sure why the answer would be A, anyone that has worked with PCI-DSS knows its a self regulated standard. There is no accreditation on the part of the assessor

https://www.pcidssguide.com/how-to-successfully-pass-a-pci-compliance-scan/

upvoted 1 times

Ivanchun 2 years ago

Selected Answer: A

A, no experience should not take the task

upvoted 1 times

Cccccccc123 2 years, 1 month ago

Selected Answer: D

First step would be to investigate whether they are actually not qualified and competent if you ask me. With A you are already assuming this. D for me.

upvoted 3 times

> **evenkeel** 1 year, 11 months ago
>
> Agreed. Due Diligence.
>
> upvoted 1 times

Rollizo 2 years, 3 months ago

Selected Answer: A

A is right, it is a canon of ISC2

upvoted 4 times

Question #175 *Topic 1*

While performing a security review for a new product, an information security professional discovers that the organization's product development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers. Which of the following recommendations should be made to the product development team?

A. Customer identifiers should be a variant of the user's government-issued ID number.

B. Customer identifiers should be a cryptographic hash of the user's government-issued ID number.

C. Customer identifiers that do not resemble the user's government-issued ID number should be used.

D. Customer identifiers should be a variant of the user's name, for example, "jdoe" or "john.doe."

Suggested Answer: *B*

Community vote distribution

C (84%) D (16%)

izaman2022 Highly Voted 2 years, 2 months ago

Selected Answer: C

C sounds like it is defining/leading towards tokenization. Take the government identifier and turn into a token. Ideally the token won't resemble the original sensitive gov id but could be used as a unique derived customer identifier

upvoted 7 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

Joe_Cheng Highly Voted 2 years, 3 months ago

Selected Answer: C

I don't think it is needed to use government ID for Customer identifiers.

upvoted 5 times

TheManiac Most Recent 7 months, 1 week ago

Selected Answer: C

I know you are between B and C. but the answer is C. WHY?

Bcoz it is another department and you are the CISSP. You cannot tell them what to do. There might be easier ways for them to use govt ID numbers in different ways or use something else.

Also, when you say "B", it means you agree C so that you take a step ahead to give them this idea on B. C comes first and leads to B.

C is the answer.

upvoted 2 times

splash2357 11 months, 1 week ago

I choose C.

Even hash is meant to be irreversible, storing hash still store the actual ID in some form.

Hash may be cracked to reveal the actual data. This is especially the case when weak hash are used. And of course cracking strong hashing algorithm like BCrypt is very hard, but theoretically it can still be performed. It may also be easier to create a rainbow table/perform a bruteforce attack, given the ID format/length is fixed and publicly known.

C just said that a ID that doesn't resembles the actual government ID was used, which sounds better.

upvoted 1 times

YesPlease 1 year ago

Selected Answer: C

Answer C)

You may need to put the customer identifier on paperwork....and writing out a HASH won't be reasonable.

upvoted 2 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

Option D suggests using a variant of the user's name as the customer identifier, for example, "jdoe" or "john.doe." While this may seem like a reasonable alternative, it is not recommended because it is still possible for an attacker to use the customer identifier to guess the user's actual name or other personal information.

Using customer identifiers that do not resemble the user's government-issued ID number is a better approach because it makes it more difficult for attackers to guess or obtain the user's personal information.

upvoted 1 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: C

Do not use PII, unless you absolutly need it.

upvoted 1 times

Dee83 1 year, 11 months ago

C. Customer identifiers that do not resemble the user's government-issued ID number should be used.

Using government-issued ID numbers as customer identifiers could put customers' personal information at risk, as these numbers can be used for identity theft. Additionally, it may violate regulations such as the General Data Protection Regulation (GDPR) and other privacy laws.
To mitigate this risk, the information security professional should recommend that the product development team use a different type of customer identifier that does not resemble the user's government-issued ID number. This could include a randomly generated alphanumeric string or a combination of letters and numbers, it could also be a unique identifier that is generated by the system and is not related to the user's personal information.

upvoted 1 times

RVoigt 1 year, 11 months ago

CISSP Official Study Guide 6th edition - 'Hashing functions are algorithms which, when applied to plain text, produce a representation of that plain text. This message digest can be used to verify the integrity of the original plaintext (or a copy of it) by reapplying the hash function to it.'

Hash the government ID and you obfuscate what the original number was.

upvoted 1 times

RVoigt 1 year, 11 months ago

hit submit instead of convert to vote - answer - IS - B!

upvoted 1 times

rajkamal0 2 years ago

Selected Answer: C

Carefully reading option C - I am interpreting as "Use non government user ID instead"
C is correct.

upvoted 1 times

oudmaster 2 years ago

Option C is the general definition of de-identification techniques.
And I feel it is right, because you can use any technique you want for example; anonymization, masking, tokenization, hashing, encryption, etc.

upvoted 1 times

Nickname53796 2 years, 2 months ago

Selected Answer: D

I don't care if I am right or not; it would be wrong to collect gov IDs for such a trivial thing.

upvoted 4 times

franbarpro 2 years, 2 months ago

Good luck on the CISSP with that....

upvoted 6 times

Rollizo 2 years, 3 months ago

Selected Answer: C

"development team is proposing to collect government-issued identification (ID) numbers from customers to use as unique customer identifiers", it this is the unique usage, it would be right to use another identifier

upvoted 3 times

Cww1 2 years, 3 months ago

B makes sense because it would hide the gov identifier, but i think im leaning C?

upvoted 3 times

Question #176 *Topic 1*

The development team has been tasked with collecting data from biometric devices. The application will support a variety of collection data streams. During the testing phase, the team utilizes data from an old production database in a secure testing environment. What principle has the team taken into consideration?

A. Biometric data cannot be changed.

B. The biometric devices are unknown.

C. Biometric data must be protected from disclosure.

D. Separate biometric data streams require increased security.

Suggested Answer: *A*

Community vote distribution

C (82%) A (18%)

Li_Rong_Han Highly Voted 2 years, 3 months ago

The question says: "the team utilizes data from an old production database in a secure testing environment." If you are going to use REAL data from a production database in a testing/staging environment, you should consider the confidentiality of those data. C. Biometric data must be protected from disclosure.

upvoted 11 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: C

Not A. Biometric data cannot be changed. This is true, but it is a fact about biometric data itself, not the principle reflected by securing the testing environment.

upvoted 1 times

pete79 10 months, 4 weeks ago

Selected Answer: A

They were tasked to collect biometric data, but they ended reuse existing DB, hence it implies that biometric data cannot be changed, therefore old DB is good as it contains valid data.

upvoted 2 times

Socca 1 year, 2 months ago

A is correct

Biomitric data can't be changed. Biomitric data can be stored for 10 years by government for relative use

upvoted 3 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

The principle taken into consideration by the team from the point of view of a CISSP is:

C. Biometric data must be protected from disclosure.

By utilizing data from an old production database in a secure testing environment, the team is ensuring that the biometric data is kept confidential and not disclosed to unauthorized individuals or parties. This is an important aspect of biometric data security, as such data is highly sensitive and can be used for identity theft or other malicious purposes if it falls into the wrong hands.

upvoted 1 times

Nicola_2_Reg 1 year, 3 months ago

Biometric datas are setup to be true all the time of your life... Therefore even if from an old production, the information remains correct/exact. Non disclosure preveals !

upvoted 1 times

⊟ **HughJassole** 1 year, 6 months ago

A and C are both correct:

"You can change passwords, but you can't change your biometric details. If your biometric data is stolen or lost, it could be permanently compromised."

"if biometric data is exposed, the risk of identity theft and fraud rises."
https://www.avast.com/c-what-is-biometric-data#:~:text=A%20biometric%20is%20only%20as,t%20change%20your%20biometric%20details.

The question asks for the principle used when the team utilized a secure environment. Seems like they are guiding towards C.

upvoted 3 times

⊟ **pete79** 1 year, 7 months ago

Selected Answer: A

They wrongly assumed that Biometric data cannot be change, hence ended up using prod DB.

upvoted 2 times

⊟ **Rollingalx** 1 year, 9 months ago

I go with C
Option A is not applicable in this scenario as it refers to the immutability of biometric data, which means that once biometric data is collected, it cannot be changed.

upvoted 1 times

⊟ **sausageman** 1 year, 10 months ago

A seems correct. C doesn't make any sense in this context

upvoted 3 times

⊟ **oudmaster** 2 years ago

Selected Answer: C

May I know whom decide the correct answers of these questions?
Is it based on the passing rate of CISSP exam?

upvoted 4 times

⊟ **omarb79** 1 year, 8 months ago

Are these questions from this website are coming the real CISSP exam ?

upvoted 2 times

⊟ **sphenixfire** 2 years ago

Selected Answer: C

"Any information about an individual maintained by an agency, including
(1) any information that can be used to distinguish or trace an individual's
identity, such as name, social security number, date and place of birth,
mother's maiden name, or biometric records; and
(2) any other information that is linked or linkable to an individual, such
as medical, educational, financial, and employment information. ...The key is that organizations have a responsibility to protect PII. This includes PII related
to employees and customers. Many laws require organizations to notify individuals if a data
breach results in a compromise of PII." CISSP 9th ed. off. study guide

upvoted 2 times

⊟ **IXone** 2 years, 2 months ago

I think the answer a is correct

upvoted 3 times

⊟ **projtfer** 2 years, 2 months ago

Selected Answer: C

It does not ask what is the purpose of collecting biometric data, there for A is wrong. C is right because the question is about why the biometric data is tested in a secure old prod environment.

upvoted 3 times

⊟ **Cww1** 2 years, 3 months ago

hate the question, i think its A though

upvoted 2 times

⊟ **stickerbush1970** 2 years, 3 months ago reread the question, C doesn't even make sense in this aspect.

upvoted 2 times

⊟ **DERCHEF2009** 2 years, 3 months ago

Selected Answer: C

I think its C

upvoted 4 times

⊟ **DERCHEF2009** 2 years, 3 months ago

Jea its A

upvoted 2 times

Question #177 *Topic 1*

Information security practitioners are in the midst of implementing a new firewall. Which of the following failure methods would BEST prioritize security in the event of failure?

A. Failover

B. Fail-Closed

C. Fail-Safe

D. Fail-Open

Suggested Answer: *B*

Community vote distribution

B (78%) C (22%)

sphenixfire Highly Voted 2 years ago

Selected Answer: B

cissp ninth edititon, Page 315-316

upvoted 5 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: B

Not Fail-Safe. Often misunderstood, but in security context, it typically refers to safety for people, not data confidentiality or integrity.

upvoted 1 times

Vasyamba1 9 months, 1 week ago

Selected Answer: C

A failsecure system will default to a secure state in the event of a failure, blocking all access. A fail-open system will fail in an open state, granting all access. The choice is dependent on whether security or availability is more important after a failure.

upvoted 1 times

Vasyamba1 9 months, 1 week ago

Sorry, B, not C.

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: B

aka Fail-Secure

upvoted 1 times

Soleandheel 1 year ago

The failure method that would BEST prioritize security in the event of failure is:

B. Fail-Closed

A "fail-closed" approach means that in the event of a failure, such as a firewall malfunction or outage, the default behavior is to block all traffic or deny access. This prioritizes security by ensuring that, in the absence of normal operation, the firewall will still enforce a security posture that restricts access and protects the network from potential threats.

upvoted 2 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

he best failure method to prioritize security in the event of failure is B: "Fail-Closed". This means that in the event of a firewall failure, the firewall will deny all network traffic by default, ensuring that no unauthorized traffic is allowed through. This ensures that even if the firewall fails, the network is protected from potentially harmful traffic. Method A, Failover, is a process of automatically switching to a backup system in the event of a failure. While failover can be useful way to ensure business continuity and minimize downtime, it may not necessarily prioritize security in the event of a firewall failure. Failover can be useful to ensure that network traffic continues to flow, but it does not necessarily guarantee that the traffic is secure. In some cases, the failover system may not be as secure as the primary system, which could result in unauthorized traffic being allowed through the firewall. Therefore, Fail-Closed is considered the best method to prioritize security in the event of a firewall failure as it ensures that no unauthorized traffic is allowed through, even if the firewall fails.

upvoted 2 times

dumdada 1 year, 6 months ago

Fail-safe means that a device will not endanger lives or property when it fails. Fail-secure, also called fail-closed, means that access or data will not fall into the wrong hands in a security failure.

upvoted 2 times

Delab202 1 year, 12 months ago

Selected Answer: C

Different systems use different terminology, so pay attention to context. When a system affects human safety, “fail-safe” means protecting people at the expense of other assets. When it only affects data, “fail-safe” means protecting confidentiality and integrity at the expense of availability.

upvoted 3 times

> **jackdryan** 1 year, 7 months ago
>
> B is correct
>
> upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: B

The fail-secure (fail-closed) failure state puts the system into a high level of security (and possibly even disables it entirely) until an administrator can diagnose the problem and restore

the system to normal operation. The fail-open (fail-safe) state allows users to bypass failed security controls, erring on the side of permissiveness.

upvoted 4 times

> **oudmaster** 2 years ago
>
> The fail-safe can be divided into fail-open and fail-closed depend on the system design and implementation.
>
> Fail-safe is the condition, while fail-open and fail-closed is the result.
>
> upvoted 2 times

sec_007 2 years, 2 months ago

Selected Answer: B

Fail Closed - common in situations where security concerns override the need for access.

https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2020/05/20/fail_closed_failop-ZYAt.html

upvoted 3 times

Question #178 *Topic 1*

Which of the following services can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities?

A. Multi-factor authentication (MFA)

B. Directory

C. User database

D. Single sign-on (SSO)

Suggested Answer: *B*

Community vote distribution

B (71%) D (24%) 6%

projtfer Highly Voted 👍 2 years, 2 months ago

Selected Answer: B

Directory is the source, SSO is a process. Directory can be an AD container or GC domain controller that holds the directory structure and hence can be an authoritative source!

upvoted 11 times

> **jackdryan** 1 year, 7 months ago
>
> B is correct
>
> upvoted 1 times

DERCHEF2009 Highly Voted 👍 2 years, 3 months ago

authoritative source of user identities = directory

upvoted 7 times

d740f62 Most Recent 3 weeks, 5 days ago

Selected Answer: B

Active "Directory" / Azure Active "Directory"

upvoted 1 times

BigITGuy 2 months, 4 weeks ago

Selected Answer: B

SSO is a service provided by IDaaS but relies on a directory for user identities.

upvoted 1 times

Soleandheel 1 year ago

ChatGPT

ChatGPT

The service that can be deployed via a cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities is:

B. Directory

A directory service, such as Active Directory or LDAP (Lightweight Directory Access Protocol), can be used as the authoritative source of user identities and integrated with IDaaS solutions, whether hosted in the cloud or on-premises. This allows for centralized identity management and authentication across various applications and services.

upvoted 1 times

> **Soleandheel** 1 year ago
>
> I know many Chatgpt answers are flawed but this one is correct based on my research. Active Directory integrates with IDaaS which can be a centralized source for Identity management and authentication.
>
> upvoted 2 times

DapengZhang 1 year, 1 month ago

Selected Answer: C

why it is not a user database as data source?

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

According to the CISSP (Certified Information Systems Security Professional) perspective, the service that can be deployed via cloud service or on-premises to integrate with Identity as a Service (IDaaS) as the authoritative source of user identities is the Directory (option B). Directory services are used to store and manage user identity and access information, and can be integrated with IDaaS platforms to provide a centralized and consistent source of user identity information. Multi-factor authentication (MFA), user databases, and single sign-on (SSO) can also be deployed with IDaaS, but they do not typically serve as the authoritative source of user identities.

upvoted 1 times

RVoigt 1 year, 11 months ago

Selected Answer: D

From CISSP Official Student Guide 6th Edition - SSO is where 'a user only has to sign in to a single authorization provider and they are then grated access to all resources they have privileges for...' Then there is a diagram where the request is from SSO to an d IAM system.

What is 'Directory' anyway - it doesnt say 'Active Directory'...

upvoted 3 times

RVoigt 1 year, 9 months ago

Also from the CISSP Official Study Guide pg 662 "Identity as a service, or identity and access as a service (IDaaS), is a third-party service that provides identity and access management. IDaaS effectively provides SSO for the cloud and is especially useful when internal clients access cloud-based software as a service (SaaS) applications. Google implements this with its motto of "One Google Account for everything Google." Users log into their Google account once, and it provides them access to multiple Google cloud-based applications without requiring users to log in again."

upvoted 1 times

rajkamal0 2 years ago

Selected Answer: B

Reading the question carefully - "Source of user identity"

B is the best answer.

upvoted 3 times

Rollizo 2 years, 3 months ago

Selected Answer: D

It is D sure

upvoted 1 times

brb77 2 years, 3 months ago

D; cloud based IAM uses federated IAM which is a form of SSO

upvoted 2 times

BDSec 2 years, 3 months ago

B is right

upvoted 2 times

Cww1 2 years, 3 months ago

agree with D

upvoted 1 times

gooftroop 2 years, 3 months ago

D. Single sign-on (SSO)

upvoted 1 times

Question #179 *Topic 1*

Which of the following statements is TRUE about Secure Shell (SSH)?

A. SSH supports port forwarding, which can be used to protect less secured protocols.

B. SSH does not protect against man-in-the-middle (MITM) attacks.

C. SSH is easy to deploy because it requires a Web browser only.

D. SSH can be used with almost any application because it is concerned with maintaining a circuit.

Suggested Answer: *A*

Community vote distribution

A (100%)

Rollizo Highly Voted 2 years, 3 months ago

Selected Answer: A

Port forwarding via SSH (SSH tunneling) creates a secure connection between a local computer and a remote machine through which services can be relayed. Because the connection is encrypted, SSH tunneling is useful for transmitting information that uses an unencrypted protocol, such as IMAP, VNC, or IRC

upvoted 6 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

Soleandheel Most Recent 1 year ago

A. SSH supports port forwarding, which can be used to protect less secured protocols. Also known as SSH tunneling. SSH is used on less secure protocols like FTP to make them secure (SFTP) etc.

upvoted 1 times

homeysl 1 year, 2 months ago

Selected Answer: A

SFTP is an example

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: A

Based on the CISSP (Certified Information Systems Security Professional) perspective, the correct statement about Secure Shell (SSH) is:

A. SSH supports port forwarding, which can be used to protect less secured protocols.

SSH is a protocol used for secure remote access, file transfers and management of network devices. SSH supports port forwarding, also known as SSH tunnelling, which can provide a secure channel to transfer less secured protocols such as Telnet and FTP. SSH protects against man-in-the-middle (MITM) attacks by encrypting the communication between the two devices. It is not easy to deploy because it requires installing and configuring SSH client and server software. Finally, SSH is not concerned with maintaining a circuit, rather it is concerned with providing a secure and encrypted channel for communication.

upvoted 2 times

MShaaban 1 year, 4 months ago

Answer is A

upvoted 1 times

somkiatr 1 year, 11 months ago

Selected Answer: A

read hear !

https://www.ftpgetter.com/ftp-ssh-tunnel.php

upvoted 1 times

sphenixfire 2 years ago

Selected Answer: A

correct. also used for pivoting in pentest/attacking

upvoted 1 times

Question #180 *Topic 1*

What is considered a compensating control for not having electrical surge protectors installed?

A. Having dual lines to network service providers built to the site

B. Having a hot disaster recovery (DR) environment for the site

C. Having network equipment in active-active clusters at the site

D. Having backup diesel generators installed to the site

Suggested Answer: *B*

Community vote distribution

B (61%) D (35%) 4%

Bhuraw Highly Voted 2 years, 8 months ago

very very unreal scenario. They haven't money for Surge protectors but want DR capabilities

upvoted 20 times

J_Ko 3 months ago

agree... someone did a really odd risk analysis and cost-benefit calculation on this one.... by reduction of wrong answers you're left with with B.

upvoted 1 times

cysec_4_lyfe 4 months ago

Agree with everyone. Wut?

upvoted 1 times

klarak 1 year, 2 months ago

Exactly. Dumb question. Still, won't keep it off the exam...

upvoted 1 times

Mann0302 2 years, 6 months ago

Exactly, the question doesn't even make sense smh.

upvoted 5 times

Humongous1593 Highly Voted 2 years, 8 months ago

Selected Answer: B

Key here is "the site". If surge hits and nothing is protecting the hardware the entire site could be down and PSU fried. DR site would be elsewhere and be unaffected.

upvoted 8 times

36dd0ae Most Recent 1 month, 1 week ago

Selected Answer: B

Electrical surge is gyrations in power supply leading to equipment failure, so not sure how having backup diesel generators will be a compensating control.

Only reason I see why D is the answer is it is the least expensive alternative to a hot disaster recovery site which is why this would be the answer but still does not resonate well as it gyrations in power cause a site failure not just equipment failure, hasta-la-vista what is the business to do?

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: B

A compensating control is a control that reduces risk when the primary control (in this case, surge protectors) is not in place. Since surge protectors help protect equipment from power surges or electrical events, the closest compensating control is having a hot DR site

upvoted 1 times

Tuhaar 6 months, 2 weeks ago

Selected Answer: B

sorry guys option B after rethinking this. Generator does not help with surges, it restores power. In case there is a surge and the servers are toast, there is no business continuity at which time the DR comes handy. Though expensive than a generator from a compensating control DR makes sense

upvoted 1 times

Tuhaar 6 months, 2 weeks ago

Selected Answer: D

A hot disaster recovery (DR) site is designed to take over operations in the event of a major failure or disaster, ensuring business continuity. However, it doesn't specifically address the issue of electrical surges at the primary site. Electrical surge protectors are meant to protect equipment from voltage spikes that can cause immediate damage or degrade the performance of electronic components over time12.

Backup diesel generators, on the other hand, can provide a continuous power supply during electrical disturbances, including surges, thereby directly mitigating the risk associated with not having surge protectors

upvoted 2 times

Tuhaar 7 months ago

Selected Answer: D

The CISSP Official Study Guide, Domain 7 (Security Operations), discusses compensating controls as alternative measures designed to mitigate risks when primary controls are absent. Backup power solutions, like diesel generators, are commonly cited as compensating controls for electrical power risks, including surges and outages.

upvoted 2 times

stack120566 7 months ago

Selected Answer: D

The answers would make a little more sense if it were worded you do not have a backup generator what would be a compensating control. or you do not have UPS what would be a compensating control.

upvoted 2 times

stack120566 7 months ago

Selected Answer: D

You walk up to the director of IT and say we do not ahve surge protection, but dont worry we have an hot site avialable. You are looking for a job becuse you are too stupid to requisition surrge protectors .

upvoted 2 times

CCNPWILL 1 year ago

Selected Answer: D

HOT site is better than having diesel generators? i mean thats not a realistic implementation of this. Having backup ANY kind of generators would be suffice generally and is a more realistic answer to such scenario.

I have to go against the grain. D

upvoted 2 times

Zapepelele 6 months, 3 weeks ago

A big electrical surge without protection can cause damaged to electrical infrastructure... so, it doesn't matter if you have 1 Diesel generator or fifty, you will be down anyway.

upvoted 2 times

eboehm 1 year, 2 months ago

Selected Answer: C

interesting that literally every question here seems wrong. The question isnt about loss of power. Does literally no one know what a surge protector does? Surge protector is not a control protecting the entire building. Therefore a DR hot site and a backup generator is overkill. A generator would be a compensating control for UPS but not a surge protector.

Surge protectors are controls that protect a piece of equipment. Therefore a valid compensating control would be having redundancy for that system. AKA active/active clusters ---> network equipment can apply to servers as well

upvoted 1 times

Vasyamba1 1 year, 3 months ago

Selected Answer: D

I don't think B is a correct answer.
Imagine you are a manager, you come to the director of the company and he said "Look, we don't have surge protectors. What are we going to do when a surge happens?" You say "No worries, we will just move to another buillding!" :)

upvoted 2 times

629f731 1 year, 5 months ago

Selected Answer: D

If we think as a Manager, and the main problem is power failures, a "compensatory control" that is, not the best solution but something that helps when the best option which is a DR site is not viable, is having "backup diesel generators ". I go with D

upvoted 2 times

maawar83 1 year, 5 months ago

Agree the question does not make a lot of sense.. but thinking for cost effective and considering that no surge protectors... it is very expensive to have hot disaster recovery DR...
looking at C. active-active to clusters... can ensure data protection and integrity and availability considering that clusters are connected to different power sources..

I think C. can be a good answer as well.

upvoted 1 times

Soleandheel 1 year, 6 months ago

In the event of electrical surges that could potentially damage systems, a hot DR environment provides redundancy by replicating critical systems and data in a separate location. This ensures that essential services can quickly fail over to the DR environment, minimizing downtime and data loss.

upvoted 1 times

Soleandheel 1 year, 6 months ago

B. Having a hot disaster recovery (DR) environment for the site

upvoted 1 times

Zonas 1 year, 7 months ago

D is correct

upvoted 1 times

homeysl 1 year, 8 months ago

Selected Answer: B

Other answers don't make sense with the given scenario

upvoted 1 times

Question #181 *Topic 1*

What is the FIRST step in risk management?

A. Identify the factors that have potential to impact business.

B. Establish the scope and actions required.

C. Identify existing controls in the environment.

D. Establish the expectations of stakeholder involvement.

Suggested Answer: *C*

Community vote distribution

A (90%) 7%

kasiya Highly Voted 2 years, 9 months ago

Selected Answer: A

risk identification

upvoted 8 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

sec_007 Highly Voted 2 years, 8 months ago

Selected Answer: A

A is correct.

Five steps of risk management:

1. Identify the Risk
2. Analyze the Risk
3. Evaluate or Rank the Risk
4. Treat the Risk
5. Monitor and Review the Risk

The initial step in the risk management process is to identify the risks that the business is exposed to in its operating environment.

https://www.360factors.com/blog/five-steps-of-risk-management-process/

upvoted 6 times

8e1c45b Most Recent 10 months, 3 weeks ago

Selected Answer: B

B. Establish the scope and actions required.

upvoted 2 times

klarak 1 year, 2 months ago

Selected Answer: A

A is correct

upvoted 1 times

629f731 1 year, 5 months ago

Selected Answer: A

FIRST BIA is Identify the Risk

upvoted 1 times

Nicola_2_Reg 1 year, 9 months ago

Selected Answer: A

The FIRST step isn't even written...

"Risk management is the process of identifying, examining, measuring, mitigating, or transferring risk".

upvoted 3 times

PeteyPete 1 year, 11 months ago

Selected Answer: C

How can you identify the risk without first looking at the controls that are in place?

upvoted 1 times

pete79 2 years, 1 month ago

Selected Answer: C

Because there might be some in place already, so first- identify them.

upvoted 1 times

sausageman 2 years, 3 months ago

Selected Answer: A

A is the correct. In the book it says:

"Risk management is composed of two primary elements: risk assessment and risk response.

Risk assessment or risk analysis is the examination of an environment for risks, evaluating each threat event as to its likelihood of occurring and the severity of the damage it would cause if it did occur, and assessing the cost of various countermeasures for each risk. This results in a sorted criticality prioritization of risks. From there, risk response takes over."

upvoted 2 times

Dee83 2 years, 5 months ago

A. Identify the factors that have potential to impact business.

The first step in risk management is to identify the factors that have the potential to impact the business. This includes identifying the risks and threats that the organization may face, such as natural disasters, cyber-attacks, and human errors. This step is also known as risk identification, it's important as it helps to understand the organization's risk profile and where to focus the risk management efforts. By identifying the factors that have potential to impact the business, it allows the organization to prioritize the risks that need to be addressed and to allocate resources accordingly.

upvoted 2 times

DJOEK 2 years, 5 months ago

Selected Answer: A

ChatGPT says it is A, and so does my gut instinct

upvoted 4 times

oudmaster 2 years, 6 months ago

Option A is related to Business Impact Analysis (BIA), and this is part of Risk Assessment which is a next stage.

I vote for B, because Risk Management is a program, and first thing we have to do is to identify what are we going to do, whom involved, strategy etc.

upvoted 3 times

Peduk70 2 years, 8 months ago

The first step in risk management is to identify critical assets that require protection.

A is not correct because risk identification comes after critical assets have been identified and prioritised.

C could be the correct answer if identifying existing controls includes digital assets identification, but the answer was poorly worded.

upvoted 4 times

Rollizo 2 years, 9 months ago

Selected Answer: A

it is A because risk management only try to identify factors that can affect to the company. Scope no make sense because it is for DRP or BCP (where can be included a risk management)

upvoted 2 times

Question #182 *Topic 1*

Which of the following is the PRIMARY goal of logical access controls?

A. Restrict access to an information asset.

B. Ensure availability of an information asset.

C. Restrict physical access to an information asset.

D. Ensure integrity of an information asset.

Suggested Answer: *A*

Community vote distribution

A (77%) D (23%)

⊟ **RVoigt** Highly Voted 👍 1 year, 10 months ago

Selected Answer: A

CISSP Official Study Guide pg 639 - "
Information An organization's information includes all of its data. Data is stored in simple files on servers, computers, and smaller devices. It can also be stored in databases within a server farm. Logical access controls attempt to prevent unauthorized access to the information. "

upvoted 6 times

⊟ **jackdryan** 1 year, 7 months ago

A is correct

upvoted 1 times

⊟ **CCNPWILL** Most Recent ⏲ 6 months, 3 weeks ago

Selected Answer: A

Logical access control to restrict access... not to ensure availability or restrict physical control or ensure integrity.

implementing logical access control exactly that. Access. Answer is A

upvoted 1 times

⊟ **HughJassole** 1 year, 6 months ago

Access controls don't only restrict, they also allow. Why do I care if the wrong person has access to my data? So they don't steal or change it on me. So I think it is D, I want access controls so someone doesn't go in there are mess with my critical files. That is accomplished by A, but the goal is not to restrict, but to make sure my data is safe, which is accomplished by restricting.

upvoted 4 times

⊟ **shash33** 1 year, 11 months ago

Selected Answer: D

Think like a manager, why we restrict access? to ensure CIA !

upvoted 3 times

⊟ **DJOEK** 1 year, 11 months ago

Selected Answer: A

Logical is not physical so its not C. also integrity and availability are not the PRIMARY goals so its not B and D.

upvoted 2 times

⊟ **Peterzhang** 2 years, 2 months ago

Selected Answer: A

Seems A is correct: https://www.cybersecurity-automation.com/what-is-logical-access-control-in-computer-security/#:~:text=Logical%20access%20control%20composes%20policies%2C%20procedures%2C%20and%20other,to%20restrict%20access%20to%20compu
What is Logical Access Control?
Logical access control composes policies, procedures, and other activities that are part of the managerial control of an organization. It restricts the use of in
individuals, groups, or organizations.

Moreover, it is a subset of security that deals with the processes used to restrict access to computer files and databases. This process includes authenticati

Logical access control uses logical security measures to protect computer systems, data, applications, and services from unauthorized access.

upvoted 2 times

jaysparky 2 years, 2 months ago

A is correct. The primary goal is to restrict access. The access is to logical and physical systems.

upvoted 2 times

Cww1 2 years, 3 months ago

Given answer is correct

upvoted 2 times

stickerbush1970 2 years, 3 months ago

I'm thinking this should be C.

upvoted 2 times

Ivanchun 2 years ago

Same as you, but think about the access not only physical

upvoted 1 times

Question #183 *Topic 1*

Which of the following is a covert channel type?

A. Pipe

B. Memory

C. Storage

D. Monitoring

Suggested Answer: *D*

Community vote distribution

C (90%) 10%

[Removed] Highly Voted 2 years, 3 months ago

Storage channels are used by attackers to encode the information getting transferred and then decode it later. In TCP/IP stacks, some fields are left vacant or unused. Attackers utilize these unused fields as storage channels.

upvoted 14 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

[Removed] Highly Voted 2 years, 3 months ago

Storage. C

upvoted 8 times

sbear123 Most Recent 9 months, 1 week ago

Selected Answer: C

Covert Channel types: Timing or Storage

upvoted 3 times

Soleandheel 1 year ago

In the context of computer security, covert channels typically refer to timing and storage covert channels. So, the correct answer is:

C. Storage

upvoted 2 times

isaac592 1 year, 2 months ago

Selected Answer: C

Two types of covert channels: covert storage and covert timing.

• A covert storage channel is used when one process writes data to a hard drive and another process reads it. In a covert storage attack, a higher-level subject writes data to a storage area and a lower subject reads it. In a covert storage channel, security risks arise due to the storage location.

• A covert timing channel is used when a process transmits data to another process. Covert timing channels convey information by modifying the timing of a system resource in some measurable way.

upvoted 4 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

According to the official study guide, there are only two types of covert channels: timing and storage. Since the question is about a covert channel TYPE, the only valid response is "storage" (C). All other options are not a covert channel types and thus are incorrect. While a pipe can be used as a communication mechanism between processes, it is not a covert channel type in the context of computer security. Therefore, the only valid response to this question is "storage" (C), as it is the only option that represents a covert channel type.

upvoted 2 times

BoZT 1 year, 3 months ago

Selected Answer: C

A covert channel is a way for unauthorized information to be transferred between two entities that are not supposed to be able to communicate with each other. There are two main types of covert channels: storage channels and timing channels.

Storage channels use shared storage space, such as a hard drive, to transfer information. For example, an attacker could create a hidden file on the hard drive and then modify the file to encode the information they want to transfer.

Timing channels use the timing of system events to transfer information. For example, an attacker could measure the time it takes for a system to perform a certain task and then use that information to transfer data.

upvoted 1 times

HughJassole 1 year, 6 months ago

It is C, as storage, timing-based, and behavior are the three types of covert channels:

https://medium.com/insa-tc/covert-channels-in-computer-networks-26a33fd911b2

upvoted 1 times

NJALPHA 1 year, 8 months ago

will go with C

Storage-based covert channels. This involves hiding data in some unexpected portion of the message

Timing-based covert channels. Time is a parameter, it was used in morse code, so why not use it in packet based networks to create a covert channel

upvoted 2 times

Rollingalx 1 year, 10 months ago

A.Pipe

A pipe is a type of covert channel that can be used to transfer information between two processes in a way that is not easily detectable by system administrators or security personnel. Covert channels are communication channels that are not intended to be used for information transfer, but can still be used to transfer information due to weaknesses or limitations in the system security mechanisms. Pipes are a common type of covert channel that can be used to transfer information between two processes on the same system by writing to and reading from a shared pipe file.

upvoted 5 times

Dee83 1 year, 11 months ago

B. Memory

A covert channel is a type of communication channel that allows two processes to communicate in a way that is not intended or visible to an observer. Memory is one example of a covert channel, as two processes can share information by writing to and reading from shared memory, without the observer being aware of it. Other examples of covert channels include timing channels, where two processes communicate by modulating the time of certain events, and storage channels, where they communicate by writing and reading data to and from shared storage devices.

upvoted 2 times

DJOEK 1 year, 11 months ago

Selected Answer: D

This is simply a knowledge question from the official study guide 9th edition

upvoted 1 times

cobbs 2 years ago

Selected Answer: C

Storage - https://study.com/academy/lesson/covert-communication-channels-definition-issues-tunneling.html

upvoted 1 times

abb77 2 years, 2 months ago

Selected Answer: C

storage and timing

upvoted 3 times

rdy4u 2 years, 2 months ago

Selected Answer: C

The existence of a covert storage channel in a communications channel may release information which can be of significant use to attackers.

https://owasp.org/www-community/vulnerabilities/Covert_storage_channel

upvoted 2 times

jsnow2258 2 years, 2 months ago

Selected Answer: D

D because all the other ones follow strict rules for manipulating data. Creating a covert channel using monitoring must be very smart. I never actually heard about it before, but now that I know about it, sounds very tricky and smart.

upvoted 2 times

Oppenheimer 2 years, 2 months ago

Selected Answer: C

storage and timing

upvoted 4 times

Question #184 *Topic 1*

A software developer wishes to write code that will execute safely and only as intended. Which of the following programming language types is MOST likely to achieve this goal?

A. Weakly typed

B. Dynamically typed

C. Strongly typed

D. Statically typed

Suggested Answer: *B*

Community vote distribution

C (100%)

Rollizo Highly Voted 👍 2 years, 3 months ago

Selected Answer: C

Statically-typed programming languages do type checking (i.e., the process of verifying and enforcing the constraints of types on values) at compile-time, whereas dynamically-typed languages do type checks at runtime.

Weakly-typed languages make conversions between unrelated types implicitly; whereas, strongly-typed languages don't allow implicit conversions between unrelated types.

upvoted 9 times

pingundas 2 years, 2 months ago

The question says "execute" which is = runtime, so dynamically could be right. (PS: amazed at how many answers defaults answers do make sense)

upvoted 1 times

pingundas 2 years, 2 months ago

I meant do not make sense

upvoted 1 times

Rollizo 2 years, 3 months ago

conversions between unrelated types can produce unexpected behaviour

upvoted 1 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

DJOEK Highly Voted 👍 1 year, 11 months ago

Selected Answer: C

According to CISSP, the most likely programming language type to achieve the goal of executing safely and only as intended is a strongly typed language. Strongly typed languages require explicit declarations of variables and enforce strict rules for how variables can be used, making it more difficult for developers to make errors that could compromise the security of the code. In contrast, weakly typed languages have more flexible rules for variable declarations and use, making it easier for developers to make mistakes that could compromise the security of the code. Dynamically typed languages are similar to weakly typed languages in that they do not require explicit declarations of variables, but they also allow variables to change type during execution, which can increase the risk of security vulnerabilities. Statically typed languages are similar to strongly typed languages in that they require explicit declarations of variables and enforce strict rules for how variables can be used, but they also perform type checking at compile time rather than runtime, which can help to identify and fix potential security issues before the code is deployed.

upvoted 7 times

Duncan314 Most Recent 🕘 5 months, 1 week ago

Selected Answer: D

Statically typed languages help catch type errors at compile time, reducing the likelihood of runtime errors and enhancing the overall safety of the code.

upvoted 1 times

Soleandheel 1 year ago

C. Strongly typed

Strongly typed programming languages enforce strict type checking and do not allow implicit type conversion, which can help prevent unintended behavior and make the code more robust and safe.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

The concept of strongly typed programming languages as a means to achieve safe and intended code execution is a fundamental concept in computer science and software development, and it is widely accepted and taught in various resources, including official study guides and CBKs for the CISSP certification.

upvoted 1 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

Firedragon 2 years, 1 month ago

Selected Answer: C

C.
https://www.techtarget.com/whatis/definition/strongly-typed

upvoted 2 times

ataaf 2 years, 2 months ago

Dynamic type
checking checks the values stored in a program's variables as it is running to ensure data
matches the expected type. Languages that implement these features are known as typesafe, and they support important security goals related to integrity of data

upvoted 2 times

BDSec 2 years, 3 months ago

Strongly

upvoted 1 times

Yanjun 2 years, 3 months ago

Selected Answer: C

should be strongly

upvoted 3 times

Nickolos 2 years, 3 months ago

Why is that?

upvoted 1 times

Question #185 *Topic 1*

Which of the following roles is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications?

A. Data Custodian

B. Data Reviewer

C. Data User

D. Data Owner

Suggested Answer: *D*

Community vote distribution

A (69%) D (31%)

Peduk70 Highly Voted 2 years, 2 months ago

D is correct.

Data Owners are responsible for protecting data and implementing policies that define the appropriate use of the data.

Data Custodians are responsible for the safe custody, transport, and storage of the data

upvoted 17 times

CuteRabbit168 Highly Voted 2 years, 3 months ago

Selected Answer: A

Data custodians are established to ensure that important datasets are developed, maintained, and are accessible within their defined specifications.

upvoted 13 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

Can't be D. Data Owner is responsible for defining the data's classification, policies, and requirements, but does not perform the day-to-day development and maintenance tasks.

upvoted 2 times

klarak 8 months, 1 week ago

Selected Answer: D

Answer is D as the owner is ultimately responsible for ensuring these details. It's not A because the Data Custodian is mostly just responsible for data at rest, if you think about it.

upvoted 3 times

Vasyamba1 9 months, 1 week ago

Selected Answer: A

Think it's Data Custodian as specifications are already defined by the Owner.

upvoted 2 times

xxxBadManxxx 9 months, 2 weeks ago

Selected Answer: D

The correct answer is D. Data Owner. The Data Owner is responsible for ensuring that important datasets are developed, maintained, and accessible within their defined specifications. They have ownership and control over the data, making decisions regarding its management, security, and access.

upvoted 1 times

GPrep 11 months, 3 weeks ago

Selected Answer: A

Tough question but I'm going with A (after much deliberation). The key (for me) is the word responsible, not accountable...think RACI (Responsible, Accountable, Consult, Inform). The data owner is ultimately accountable for everything, though the data custodian is responsible (delegated responsibility by the data owner) for ensuring the day-to-day is running as expected.

upvoted 4 times

GPrep 1 year ago

Initially, I thought D, however, after additional review, I'm going with A. The key words here are "responsible" (as opposed to accountable) and "within their defined specifications". The Data Owner is "accountable" AND defines the specs whereas the Data Custodian is "responsible" and works within specs which have already been defined.

https://blog.satoricyber.com/the-datamasters-data-owners-vs-data-stewards-vs-data-custodians/

upvoted 1 times

Soleandheel 1 year ago

D. Data Owner

The Data Owner is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications.

upvoted 2 times

Soleandheel 1 year ago

Even though the Data Custodians focus on the safeguard and custody of data, they don't develop the datasets. This is the primiary responsibility of the data owner. As such, the correct answer here is definitely D. Data Owner.

upvoted 1 times

Nicola_2_Reg 1 year, 3 months ago

Data Owner : Top level/Primary responsibility for data, Define level of classification, Define controls for levels of classification
Data custodian : Ensure compliance with data policy and data ownership guidelines

The question specify who ensure the compliance with specification therefore it should be "data custodian".

upvoted 2 times

Rollingalx 1 year, 10 months ago

A is correct

upvoted 1 times

Dee83 1 year, 11 months ago

A. Data Custodian

A data custodian is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications. The data custodian is responsible for the physical care and protection of data, including ensuring that data is backed up, stored securely, and that access controls are in place to protect the data. Additionally, data custodians are also responsible for monitoring access to the data, and for ensuring that the data is accurate, complete, and accessible in accordance with the organization's policies and procedures.

While the Data Owner is responsible for the overall management of a specific set of data, including determining who can access it, and for what purpose. The Data Reviewer is responsible for reviewing the data to ensure that it is accurate,

upvoted 1 times

Destcert 1 year, 2 months ago

Data owner is accountable for data while Data custodian is responsible for technical development and maintenance of data. As the question ask responsible for maintaining I too think it's data custodian role .

upvoted 2 times

somkiatr 1 year, 11 months ago

Selected Answer: D

Agreed with D. A Data Custodian is responsible for implementing and maintaining security controls for a given data set in order to meet the requirements specified by the Data Owner in the Data Governance Framework.
Reference : https://blog.idatainc.com/data-governance-roles

upvoted 2 times

DJOEK 1 year, 11 months ago

Selected Answer: D

The Data Owner is responsible for ensuring that important datasets are developed, maintained, and are accessible within their defined specifications. Data Owners have the authority to make decisions about how their data is used and managed, and they are responsible for ensuring that the data is used appropriately and in accordance with relevant laws and regulations. Data Owners are also responsible for ensuring that their data is protected from unauthorized access or disclosure, and for developing and implementing policies and procedures for managing and protecting the data.

The Data Custodian is responsible for maintaining and protecting the data, but they are not responsible for ensuring that the datasets are developed and are accessible within their defined specifications. That responsibility would typically fall to the Data Owner or possibly the Data Reviewer. The Data User is responsible for accessing and using the data, but they are not typically responsible for its development or maintenance.

upvoted 5 times

Rollizo 2 years, 3 months ago

Selected Answer: A

custodian. Data owner only establish to the beginning the data governance rules

upvoted 2 times

Yanjun 2 years, 3 months ago

Selected Answer: A

data custodian

upvoted 6 times

Question #186 *Topic 1*

What is static analysis intended to do when analyzing an executable file?

A. Search the documents and files associated with the executable file.

B. Analyze the position of the file in the file system and the executable file's libraries.

C. Collect evidence of the executable file's usage, including dates of creation and last use.

D. Disassemble the file to gather information about the executable file's function.

Suggested Answer: *B*

Community vote distribution

D (72%) B (28%)

⊟ **RVoigt** Highly Voted 1 year, 10 months ago

Selected Answer: D

There are multiple places in the CISSP Official Study Guide where static analysis is discussed/defined, but pg 1114 sums it up - "Static analysis performs assessment of the code itself, analyzing the sequence of instructions for security flaws."

upvoted 5 times

⊟ **jackdryan** 1 year, 7 months ago

D is correct

upvoted 1 times

⊟ **BigITGuy** Most Recent 2 months, 4 weeks ago

Selected Answer: D

Not B. Analyzing the file's position and its libraries might help identify dependencies but won't provide the actual behavior.

upvoted 1 times

⊟ **Soleandheel** 1 year ago

D. Disassemble the file to gather information about the executable file's function.

Static analysis involves examining the code and structure of an executable file without actually executing it. This process can help uncover potential security vulnerabilities, malware, or other issues by disassembling the file and examining its code and behavior without running it.

upvoted 2 times

⊟ **74gjd_37** 1 year, 3 months ago

Selected Answer: D

Static analysis is a technique used to examine an executable file without executing it. The goal is to understand how the file functions and what it does by analyzing its code and structure. Disassembling the file is a common static analysis technique that involves converting the executable code into assembly code to allow for easier analysis of the file's functions and operations. Therefore, option D is the correct answer.

upvoted 3 times

⊟ **somkiatr** 1 year, 11 months ago

Selected Answer: B

B is static analysis. D is static code analysis.

1. Static analysis: This is the process of analyzing a binary without executing it. It is easiest to perform and allows you to extract the metadata associated with the suspect binary. Static analysis might not reveal all the required information, but it can sometimes provide interesting information that helps in determining where to focus your subsequent analysis efforts. Static Analysis, covers the tools and techniques to extract useful information from the malware binary using static analysis.

2. Dynamic analysis (Behavioral Analysis):

3. Code analysis: Static code analysis involves disassembling the suspect binary and looking at the code to understand the program's behavior, whereas Dynamic code analysis involves debugging the suspect binary in a controlled manner to understand its functionality. Code analysis requires an understanding of the programming language and operating system concepts.

4. Memory analysis (Memory forensics):

https://subscription.packtpub.com/book/networking-&-servers/9781788392501/1/ch01lvl1sec13/4-types-of-malware-analysis

upvoted 3 times

⊟ **DJOEK** 1 year, 11 months ago

Selected Answer: D

Static analysis is intended to disassemble the file and gather information about the executable file's function. It involves analyzing the code of the file without actually executing it, in order to identify potential vulnerabilities or security risks. This can include analyzing the code to identify the functions it performs, the variables it uses, and the algorithms it employs, as well as searching for known vulnerabilities or malicious code. Static analysis is an important tool for ensuring the security and reliability of software, as it allows developers to identify and fix potential issues before the software is released.

upvoted 1 times

⊟ **sphenixfire** 2 years, 1 month ago

Selected Answer: D

D for sure

upvoted 1 times

⊟ **Firedragon** 2 years, 1 month ago

Selected Answer: B

B.

Static Analysis is the automated analysis of source code without executing the application. And here's examples on how to analyze binary files in Linux, it's all about libraries.

https://opensource.com/article/20/4/linux-binary-analysis

upvoted 2 times

⊟ **OROR** 2 years, 2 months ago

D is the right answer

upvoted 3 times

⊟ **krassko** 2 years, 3 months ago

Selected Answer: D

https://infosecwriteups.com/malware-analysis-101-basic-static-analysis-db59119bc00a

upvoted 3 times

> ⊟ **SSimko** 11 months, 1 week ago
>
> Your source never uses the word "disassemble" and actually confirms that B is correct with the information below.
>
> "Static analysis consists of examining the executable file without viewing the actual instructions. It is used to confirm, at least get an idea whether the file being inspected is malicious or not. We do this by figuring out the functions and libraries that are being called by the executable."
>
> upvoted 1 times

⊟ **DERCHEF2009** 2 years, 3 months ago

Selected Answer: D

Static analysis consists of examining the executable file without viewing the actual instructions. It is used to confirm, at least get an idea whether the file being inspected is malicious or not. We do this by figuring out the functions and libraries that are being called by the executable.

upvoted 2 times

Question #187 *Topic 1*

A network security engineer needs to ensure that a security solution analyzes traffic for protocol manipulation and various sorts of common attacks. In addition, all
Uniform Resource Locator (URL) traffic must be inspected and users prevented from browsing inappropriate websites. Which of the following solutions should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis?

A. Application-Level Proxy

B. Intrusion detection system (IDS)

C. Host-based Firewall

D. Circuit-Level Proxy

Suggested Answer: *A*

Community vote distribution

A (82%) C (18%)

gjimenezf 11 months, 2 weeks ago

Selected Answer: A

Both application proxies and circuit-level proxies can potentially detect protocol manipulation, but they operate at different levels of the network stack and have different approaches.Application proxy works at the application layer and circuit level proxy at the session layer
Application proxies are more suited for detecting protocol manipulation at the application layer, where they have visibility into the specifics of application-layer protocols. Circuit-level proxies, on the other hand, may be more focused on identifying anomalies or manipulation at the transport layer, based on patterns or behaviors that deviate from standard TCP behavior.

upvoted 2 times

Soleandheel 1 year ago

A. Application-Level Proxy

An application-level proxy (also known as an application firewall or application gateway) can inspect traffic at the application layer and enforce policies based on application-specific rules. This allows administrators to analyze traffic, block inappropriate websites, and log user activity for further analysis. It provides granular control over the traffic and is well-suited for these requirements.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: A

From a CISSP perspective, the solution that should be implemented to enable administrators the capability to analyze traffic, blacklist external sites, and log user traffic for later analysis is an Application-Level Proxy.

An Application-Level Proxy operates at the application layer of the OSI model, allowing for deep inspection of network traffic. It can analyze traffic for protocol manipulation and various sorts of common attacks, while also allowing administrators to blacklist external sites and log user traffic for later analysis.

Intrusion detection systems (IDS) are designed to detect and alert on malicious activity on the network, but they do not offer the same level of traffic analysis or control as an Application-Level Proxy. Host-based firewalls are designed to protect individual hosts from network attacks, but they do not offer the same level of network-wide control as a proxy. Circuit-level proxies do not offer the same level of traffic analysis or control as an Application-Level Proxy.

upvoted 2 times

Marzie 1 year, 9 months ago

Selected Answer: C

Host-based Firewall seems like a good fit here given that is calling out user behavior's e.g. blocking websites

upvoted 2 times

DJOEK 1 year, 11 months ago

Selected Answer: A

We are talking about a webfilter here like ZScaler.

upvoted 2 times

⊟ **jackdryan** 1 year, 7 months ago

A is correct

upvoted 1 times

⊟ **Jamati** 2 years, 1 month ago

Selected Answer: A

Answer is A. Confused me at 1st coz I thought it would be running on the actual application, but it's just a proxy server operating at the application layer of the OSI model.

upvoted 2 times

⊟ **rdy4u** 2 years, 2 months ago

Selected Answer: A

Application proxies provide one of the most secure types of access you can have in a security gateway. An application proxy sits between the protected network and the network you want to be protected from. Every time an application makes a request, the application intercepts the request to the destination system.

upvoted 2 times

Question #188 Topic 1

What is the PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses?

A. ICS often run on UNIX operating systems.

B. ICS often do not have availability requirements.

C. ICS are often sensitive to unexpected traffic.

D. ICS are often isolated and difficult to access.

Suggested Answer: *C*

Community vote distribution

C (80%) D (20%)

⊟ **Boats** Highly Voted 2 years, 2 months ago

Selected Answer: C

The very fact of testing/scanning ICS devices could cause them problems. Also, they are not always hard to get to so D does not apply all the time.

upvoted 6 times

⊟ **jackdryan** 1 year, 7 months ago

C is correct

upvoted 1 times

⊟ **BigITGuy** Most Recent 2 months, 4 weeks ago

Selected Answer: C

Often highly sensitive to unexpected or abnormal network traffic.

upvoted 1 times

⊟ **TheManiac** 7 months, 1 week ago

Selected Answer: C

D is a common fact

C is a weakness

upvoted 1 times

⊟ **Soleandheel** 1 year ago

The PRIMARY consideration when testing industrial control systems (ICS) for security weaknesses is:

C. ICS are often sensitive to unexpected traffic.

Industrial control systems are designed to manage and control critical infrastructure and industrial processes. They are highly sensitive to unexpected or unauthorized traffic because any disruptions or unauthorized access can have serious consequences, including physical damage or safety risks. Therefore, security testing of ICS should prioritize ensuring that unexpected traffic or unauthorized access is detected and mitigated to protect the integrity and availability of these systems.

upvoted 2 times

⊟ **74gjd_37** 1 year, 3 months ago

Selected Answer: C

The primary consideration when testing industrial control systems (ICS) for security weaknesses, from a CISSP perspective, is that ICS are often sensitive to unexpected traffic. Therefore, option C is the correct answer. ICS are often designed to function within a specific set of parameters and can be easily disrupted by unexpected network traffic or activity. As such, it is critical to test and analyze ICS security measures to identify and address potential vulnerabilities before they can be exploited by malicious actors.

upvoted 1 times

⊟ **DJOEK** 1 year, 11 months ago

Selected Answer: C

The primary consideration when testing industrial control systems (ICS) for security weaknesses is that ICS are often sensitive to unexpected traffic. Industrial control systems are used to control and monitor critical infrastructure and industrial processes, and disruptions to their operation can have serious consequences. Therefore, it is important to carefully consider the potential impact of any security testing on the operation of the ICS and to ensure that the testing does not disrupt or compromise the system.

upvoted 2 times

Firedragon 2 years, 1 month ago

Selected Answer: C

C.

https://www.cisa.gov › recommended_practices

Some ICS protocol implementations are vulnerable to packets that are malformed or contain illegal or otherwise unexpected field values.

upvoted 4 times

Jamati 2 years, 1 month ago

Selected Answer: C

C is the best answer. ICS systems can sometimes be internet facing so D is wrong.

upvoted 3 times

dumdada 1 year, 6 months ago

ICS systems facing the Internet? Recipe for a disaster ...

upvoted 2 times

rdy4u 2 years, 2 months ago

" ICS are often isolated and difficult to access" is not a weakness

upvoted 1 times

daniecsn14 2 years, 2 months ago

Selected Answer: C

C is the correct

upvoted 3 times

brb77 2 years, 3 months ago

question asks in the context of sec testing for sec weaknesses. in this context I'd go with C

upvoted 3 times

Nickolos 2 years, 3 months ago

Selected Answer: D

Physical location/access are usually the primary concerns with ICS, SCADA systems

upvoted 1 times

Nickolos 2 years, 1 month ago

I was wrong. Security weakness is c. D is not a security weakness.

upvoted 3 times

stickerbush1970 2 years, 3 months ago

Selected Answer: D

Agree with D

upvoted 2 times

Stevooo 2 years, 3 months ago

Selected Answer: D

Physical location/access are usually the primary concerns with ICS, SCADA systems

upvoted 2 times

Question #189 *Topic 1*

The security team plans on using automated account reconciliation in the corporate user access review process. Which of the following must be implemented for the BEST results with fewest errors when running the audit?

A. Frequent audits

B. Segregation of Duties (SoD)

C. Removal of service accounts from review

D. Clear provisioning policies

Suggested Answer: *D*

Community vote distribution

D (100%)

Soleandheel 1 year ago

D. Clear provisioning policies

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: D

Clear provisioning policies would ensure that user access is accurately defined and documented, making it easier for the security team to regularly review employee user access and spot any discrepancies or unauthorized access. Segregation of duties and frequent audits are also important, but they are not as directly related to the effectiveness of automated account reconciliation. Removing service accounts from review may actually increase the risk of errors or unauthorized access.

upvoted 3 times

DJOEK 1 year, 11 months ago

Selected Answer: D

The security team's plan to use automated account reconciliation in the corporate user access review process is likely to be most effective and have the fewest errors if they implement clear provisioning policies. This is because clear provisioning policies outline the specific roles, responsibilities, and procedures for granting, modifying, and revoking user access to systems and resources. By clearly defining these policies, the security team can ensure that the automated account reconciliation process is accurately and consistently applied to all user accounts. This will help to reduce the risk of errors and ensure that the audit process is thorough and effective.

upvoted 3 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

jsnow2258 2 years, 2 months ago

Selected Answer: D

Agree, clear provisioning processes guarantees or at least increases chances for an automatic reconciliation to work as expected.

upvoted 4 times

Question #190 *Topic 1*

In the common criteria, which of the following is a formal document that expresses an implementation-independent set of security requirements?

A. Organizational Security Policy

B. Security Target (ST)

C. Protection Profile (PP)

D. Target of Evaluation (TOE)

Suggested Answer: *C*

Community vote distribution

C (90%) 10%

⊟ **DeepCyber** Highly Voted 👍 1 year, 6 months ago

Selected Answer: C

The Common Criteria process is based on two key elements: protection profiles and security targets. Protection profiles (PPs) specify for a product that is to be evaluated (the TOE) the security requirements and protections, which are considered the security desires, or the "I want," from a customer. Security targets (STs) specify the claims of security from the vendor that are built into a TOE. STs are considered the implemented security measures, or the "I will provide," from the vendor.

upvoted 7 times

⊟ **Soleandheel** Most Recent ⊙ 1 year ago

A formal document that expresses an implementation-independent set of security requirements is called:

C. Protection Profile (PP)

A Protection Profile (PP) defines security requirements for a specific type of product or system without specifying how those requirements should be implemented. It serves as a baseline set of security requirements that can be used to evaluate and compare products or systems.

upvoted 1 times

⊟ **74gjd_37** 1 year, 3 months ago

Selected Answer: C

A Protection Profile (PP) is a vendor-neutral document that defines a set of security requirements common to a specific class of IT products or systems. PPs provide a baseline to evaluate security features or functions of any IT product or system within that class. PPs specify a set of security objectives, threats and countermeasures, whereas a Security Target (ST) is specific to an implementation of an IT product or system and includes implementation-specific details.

upvoted 2 times

⊟ **Tygrond87** 1 year, 7 months ago

Selected Answer: B

A Protection Profile (PP) is a document that specifies security requirements for a particular class of information technology products or systems, and can be used as the basis for product or system evaluations.

In contrast, a Security Target (ST) is a formal document that expresses a set of security requirements for a specific product or system, and is implementation-dependent.

Therefore, the correct answer to the question is B, Security Target (ST).

upvoted 1 times

⊟ **jackdryan** 1 year, 7 months ago

C is correct

upvoted 1 times

⊟ **Pappykay** 1 year, 11 months ago

Selected Answer: C

Protection profiles (PPs) specify for a product that is to be evaluated (the
TOE) the security requirements and protections, which are considered the security desires

or the “I want” from a customer. Security targets (STs) specify the claims of security from
the vendor that are built into a TOE

upvoted 3 times

DJOEK 1 year, 11 months ago

Selected Answer: C

The Security Target (ST) is a formal document that expresses an implementation-independent set of security requirements in the common criteria. It specifies the security functionality and assurance requirements of a Target of Evaluation (TOE), which is the product or system being evaluated. The ST is used as a reference for evaluating the security capabilities of the TOE and ensuring that it meets the specified security requirements. It is one of the key components of the common criteria evaluation process, along with the Protection Profile (PP) and the Evaluation Assurance Level (EAL). The PP is a document that specifies the security functional and assurance requirements for a particular class of TOEs, while the EAL is a measure of the depth and rigor of the security evaluation conducted on the TOE.

upvoted 2 times

dumdada 1 year, 6 months ago

"The Security Target (ST) is a formal document that expresses an implementation-DEPENDENT", not INDEPENDENT.

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 1 times

rdy4u 2 years, 2 months ago

Selected Answer: C

A Protection Profile (PP) is an implementation-independent set of security requirements for a class of Targets of Evaluation (TOEs) that meet specific consumer needs

https://www.cisa.gov/uscert/bsi/articles/best-practices/requirements-engineering/the-common-criteria

upvoted 3 times

explorer3 2 years, 2 months ago

Selected Answer: C

C is correct, as PP is implementation independent and ST is product specific

upvoted 1 times

franbarpro 2 years, 2 months ago

protection profile (pp) is defined as: A minimal, baseline set of requirements targeted at mitigating well defined and described threats. The term Protection Profile refers to NSA/NIAP requirements for a technology and does not imply or require the use of Common Criteria as the process for evaluating a product.

upvoted 1 times

gautamzone 2 years, 2 months ago

Selected Answer: B

Shouldn't it be B based on this link?

https://en.wikipedia.org/wiki/Common_Criteria

Reference Text: Security Target (ST) – the document that identifies the security properties of the target of evaluation

upvoted 1 times

brb77 2 years, 3 months ago

C is correct

upvoted 2 times

Cww1 2 years, 3 months ago

C is correct

upvoted 2 times

gooftroop 2 years, 3 months ago

D. Target of Evaluation (TOE)

upvoted 1 times

DERCHEF2009 2 years, 3 months ago

Wrong its C

upvoted 2 times

Question #191 *Topic 1*

Which of the following is an example of a vulnerability of full-disk encryption (FDE)?

A. Data on the device cannot be restored from backup.

B. Data on the device cannot be backed up.

C. Data in transit has been compromised when the user has authenticated to the device.

D. Data at rest has been compromised when the user has authenticated to the device.

Suggested Answer: *D*

Community vote distribution

D (75%) C (25%)

⊟ **BigITGuy** 2 months, 4 weeks ago

Selected Answer: D

NOT C. FDE only protects data at rest, not data in transit. Data in transit requires network-level encryption, such as TLS.

upvoted 1 times

⊟ **629f731** 11 months, 3 weeks ago

Selected Answer: D

This scenario can occur if an attacker gains unauthorized access to the device while it's in use (authenticated state) and the FDE gets temporarily deactivated. If the attacker can exploit this situation, they might access or tamper with data that is supposed to be protected by FDE.

upvoted 3 times

⊟ **Soleandheel** 1 year ago

D. Data at rest has been compromised when the user has authenticated to the device.

Full-disk encryption typically protects data when the device is powered off or at rest. However, if an attacker gains access to the device while it's running and the user has authenticated to the device (e.g., logged in), the data may be vulnerable. This is because FDE generally decrypts the data when the user is authenticated and using the device, making it susceptible to compromise if the device is compromised while in use.

upvoted 4 times

⊟ **RVoigt** 1 year, 10 months ago

Selected Answer: D

CISSP OSG pgs 410-411 talk about FDE. One section includes "If most or all of the storage media of a device can be encrypted, this is usually a worthwhile feature to enable. However, encryption isn't a guarantee of protection for data, especially if the device is stolen while unlocked or if the system itself has a known backdoor attack vulnerability."

upvoted 2 times

⊟ **jackdryan** 1 year, 7 months ago

D is correct

upvoted 1 times

⊟ **georgegeorge125487** 1 year, 4 months ago

D is correct

upvoted 1 times

⊟ **init2winit** 1 year, 11 months ago

Selected Answer: D

FDE is Data at Rest, Weakness is if the user has the credentials to authenticate to the Device

upvoted 4 times

⊟ **DJOEK** 1 year, 11 months ago

Selected Answer: D

Option C, "Data in transit has been compromised when the user has authenticated to the device," is not a vulnerability of FDE. FDE is designed to protect data at rest and has no impact on data in transit. Data in transit is typically protected using other security measures such as encryption or secure communication protocols.

Option D, "Data at rest has been compromised when the user has authenticated to the device," is a potential vulnerability of FDE. If a user has authenticated to a device with FDE enabled, it is possible that an attacker could gain access to the data if the user's authentication credentials are compromised or if there is a weakness in the FDE implementation. It is important to ensure that FDE is properly configured and implemented to minimize this risk.

upvoted 1 times

⊟ **oudmaster** 2 years ago

Selected Answer: D

Given answer seems correct.

Because the FDE is not responsible to protect data in transit anyway.

But it is responsible to protect data at rest. Now, once a user login the machine (decrypt the disk), all data will be accessible, and if a hacker compromised the machine remotely, he can read the data clearly.

upvoted 1 times

⊟ **oudmaster** 2 years ago

with FDE, any data in transit is compromised whether the user is authenticated or not. So, I believe option C is irrelevant answer.

upvoted 1 times

⊟ **Jamati** 2 years, 1 month ago

Selected Answer: C

Answer is C. One of the vulnerabilities of FDE is that it does not protect data in transit. The 5 limitations of FDE are as follows:

1. FDE Doesn’t Protect Data in Transit
2. FDE Can Slow Down Processes
3. FDE Is Only as Strong as Its Password
4. FDE Doesn’t Apply When Files Are in Use as they have to be decrypted 1st before being handed over to the processor.
5. FDE Is Only Effective If Applied Consistently

https://www.cigent.com/resources/5-limitations-of-full-disk-encryption-1464

upvoted 4 times

⊟ **rdy4u** 2 years, 2 months ago

Selected Answer: D

Just as full disk encryption doesn't encrypt data in transit, it doesn't protect files currently in use, either. When an authorized user opens an FDE-encrypted file, they decrypt it, and it encrypts again once they log out. That means this data could be vulnerable while users are working with it.

https://www.cigent.com/resources/5-limitations-of-full-disk-encryption-1464

upvoted 2 times

⊟ **Jamati** 2 years, 1 month ago

D applies to data at rest, which is well secured by FDE. Only data in-transit and data in-process are at risk.

upvoted 1 times

⊟ **Cww1** 2 years, 3 months ago

correct

upvoted 3 times

Question #192 *Topic 1*

What is the FIRST step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks?

A. Implement network access control lists (ACL).

B. Implement an intrusion prevention system (IPS).

C. Implement a web application firewall (WAF).

D. Implement egress filtering at the organization's network boundary.

Suggested Answer: *D*

Community vote distribution

A (74%) D (21%) 6%

⊟ **RVoigt** Highly Voted 👍 1 year, 10 months ago

Selected Answer: A

CISSP Official Study Guide pg 824 "
Active Response Active responses can modify the environment using several different methods. Typical responses include modifying firewall ACLs to block traffic based on ports, protocols, and source addresses, and even disabling all communications over specific cable segments. For example, if an IDS detects a SYN flood attack from a single IP address, the IDS can change the ACL to block all traffic from this IP address. Similarly, if the IDS detects a ping flood attack from multiple IP addresses, it can change the ACL to block all ICMP traffic."

upvoted 8 times

⊟ **BigITGuy** Most Recent ⏲ 2 months, 4 weeks ago

Selected Answer: D

NOT D. Implement egress filtering while egress filtering helps prevent outgoing malicious traffic, the first step in limiting exposure to ICMP-based attacks is usually to control incoming ICMP traffic with ACLs.

upvoted 1 times

⊟ **YesPlease** 1 year ago

Selected Answer: A

Answer A)

Although I found interesting articles about egress filtering and ICMP attacks, the fact still remains that network ACLs can both do Ingress and Egress filtering at the network boundary.

Here is the interesting article:
https://www.ietf.org/rfc/rfc5927.html#section-4:~:text=As%20with

upvoted 3 times

⊟ **ramingt** 1 year, 1 month ago

Selected Answer: D

https://www.giac.org/paper/gsec/705/egress-filtering-keeping-internet-safe-systems/101588
Best Practices and Considerations in Egress Filtering (cmu.edu)
it looks like D for me

upvoted 2 times

⊟ **74gjd_37** 1 year, 3 months ago

Selected Answer: A

Implementing egress filtering at the organization's network boundary refers to the practice of controlling outgoing traffic from an organization's network to the Internet. While egress filtering can help prevent some types of attacks, such as data theft and malware propagation, it may not necessarily reduce exposure to ICMP-based attacks.

ICMP-based attacks typically involve sending ICMP packets to a victim's IP address or network, causing it to become overwhelmed with requests and making it unavailable for legitimate users. The primary way to mitigate these types of attacks is by restricting or blocking certain types of ICMP traffic using network access control lists (ACL).

Therefore, implementing egress filtering at the organization's network boundary alone might not be as effective in preventing ICMP-based attacks compared with implementing network ACLs that can specifically block unwanted/unnecessary ICMP traffic based on their characteristics such as source/destination IP address or port numbers.

upvoted 4 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: A

A is correct

upvoted 1 times

v1223 1 year, 7 months ago

Ambiguous. Depends on which type of attack. Smurf attack would be A - ACL. ICMP covert channels would be D - egress blocks.

upvoted 2 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

FlimFlam 1 year, 9 months ago

It's got to be D.
The question says 'first step' in reducing the risk. Blacklisting an IP that is sending your bad traffic is a response, not a first step. The egress filtering is preventative and stop the formation of a covert ICMP channel.

upvoted 1 times

Tygrond87 1 year, 7 months ago

you do not blacklist an IP you make an ACL to block all inbound ICMP traffic. your First action would be to asume the burgler is already inside and try to catch him at the door ? No your first action is to lock the door with an ACL

upvoted 4 times

dumdada 1 year, 6 months ago

You can filter all ICMP traffic to be dropped as well. ACL is not required necessarily

upvoted 1 times

Dee83 1 year, 11 months ago

D. Implement egress filtering at the organization's network boundary.

The first step in reducing the exposure of a network to Internet Control Message Protocol (ICMP) based attacks is to implement egress filtering at the organization's network boundary. Egress filtering is the process of monitoring and controlling outbound traffic from the organization's network. It can be used to block or limit the types of traffic that can leave the network, such as ICMP traffic. By implementing egress filtering, the organization can prevent malicious ICMP traffic from leaving the network and reaching its intended target.

upvoted 1 times

somkiatr 1 year, 11 months ago

Selected Answer: D

I will go with D.
We should filter egress traffic to respond ICMP message from WAN while keep the ICMP message enabled or responding from LAN.
reference : https://blog.paessler.com/disabling-icmp-and-snmp-wont-increase-security-but-will-impact-network-monitoring

upvoted 2 times

DJOEK 1 year, 11 months ago

Selected Answer: D

The first step in reducing the exposure of a network to ICMP based attacks according to CISSP is to implement egress filtering at the organization's network boundary. This involves setting up rules that determine which types of traffic are allowed to leave the network and which are not. Egress filtering can help to prevent attackers from using ICMP to exfiltrate data from the network or to launch other types of attacks. Other measures, such as implementing network access control lists (ACLs) and an intrusion prevention system (IPS), may also be effective in mitigating the risk of ICMP based attacks, but implementing egress filtering at the network boundary is typically the first step in this process.

upvoted 1 times

mccoy 1 year, 12 months ago

D. Implement egress filtering at the organization's network boundary.
Egress filtering involves checking outgoing traffic from a network to ensure that it conforms to the organization's security policies. This can help to reduce the exposure of the network to Internet Control Message Protocol (ICMP) based attacks by blocking or limiting the types of ICMP messages that are allowed to leave the network. This can help to prevent attackers from using ICMP messages to probe the network for vulnerabilities or to carry out other types of attacks. Egress filtering should be implemented at the organization's network boundary, such as at a firewall or router, to ensure that all outgoing traffic is checked.

upvoted 1 times

⊟ **oudmaster** 2 years ago

Selected Answer: D

Common ingress filters and egress filters can be used to block spoofed packets that often relate to malware, botnets, and other unwanted activities. Egress filtering prevents any unauthorized or malicious traffic to leave the internal network. Information flowing from the internal network to the internet is monitored and controlled. TCP/IP packets that are being sent out of the internal network are examined through a router, firewall, or a similar edge device.

!

Example: Payment Card Industry Data Security Standard (PCI DSS) requires egress filtering from any server in the cardholder environment.

upvoted 1 times

⊟ **stickerbush1970** 2 years, 1 month ago

I am going to disagree with A. An ICMP attack is more than likely coming from the outside of the network, an ACL would do nothing to stop this from happening. An ACL is used to control access to this file or that server, and attacker is not going to be on the ACL.

upvoted 1 times

⊟ **sphenixfire** 2 years, 1 month ago

Selected Answer: B

Icmp can be needed and is not only to be covert by ping. Tvere are also reroute issues by icmp. Recognice attacks by ips, because they are known.

upvoted 2 times

⊟ **bynd** 2 years, 1 month ago

Selected Answer: D

You can prevent Ping Attacks by:

Configuring your firewall to block ICMP pings from entering your network at the perimeter.

Adding filters to tell your router to detect and drop malformed data packets or those coming from suspicious sources.

- Looking for spoofed packets that do not originate from within your network, also known as egress filtering.

Installing network monitoring software to alert for traffic patterns that are not ordinary.

Scanning your network for open ports on a regular basis that is outside of your baseline.

upvoted 1 times

⊟ **Jamati** 2 years, 1 month ago

Selected Answer: A

A is correct

upvoted 2 times

Question #193 *Topic 1*

A large organization's human resources and security teams are planning on implementing technology to eliminate manual user access reviews and improve compliance. Which of the following options is MOST likely to resolve the issues associated with user access?

A. Implement a Privileged Access Management (PAM) system.

B. Implement a role-based access control (RBAC) system.

C. Implement identity and access management (IAM) platform.

D. Implement a single sign-on (SSO) platform.

Suggested Answer: *C*

Community vote distribution

C (92%) 8%

⊟ **DJOEK** Highly Voted 👍 1 year, 11 months ago

Selected Answer: C

C. Implement identity and access management (IAM) platform.

An identity and access management (IAM) platform is designed to centralize and automate the management of user access to systems and resources. This can help eliminate manual user access reviews and improve compliance by automating the process of granting, modifying, and revoking user access based on defined policies and rules. It can also provide visibility into user access and activity, making it easier to identify and address any potential compliance issues.

upvoted 6 times

⊟ **jackdryan** 1 year, 7 months ago

C is correct

upvoted 1 times

⊟ **TheManiac** Most Recent ⏲ 7 months, 1 week ago

Selected Answer: B

Implement a role-based access control (RBAC) system should be the answer

upvoted 1 times

⊟ **Soleandheel** 1 year ago

C. Implement identity and access management (IAM) platform.

upvoted 1 times

⊟ **74gjd_37** 1 year, 3 months ago

Selected Answer: C

An IAM platform provides a comprehensive solution for the lifecycle of identities within an organization, ranging from account creation to deletion while ensuring compliance with organizational policies and industry regulations such as HIPAA or GDPR. The IAM platform also streamlines User Access Reviews by automating them which reduces human errors in performing manual reviews thus enhancing security and compliance posture of organizations.

upvoted 3 times

⊟ **rdy4u** 2 years, 2 months ago

Selected Answer: C

This article will explain what user access reviews are, why they are important for the cybersecurity and compliance of your company and how the right IAM solution can help you automate the access review process.

https://www.tenfold-security.com/en/user-access-review/

upvoted 4 times

⊟ **Rollizo** 2 years, 3 months ago

Selected Answer: C

While IAM identifies each user and allows them access to an array of applications and services, PAM manages access and user’s actions on highly sensitive systems that are often limited to those with administrative privileges.

https://www.citrix.com/blogs/2022/01/10/iam-vs-pam-how-are-they-different/

upvoted 3 times

Question #194 *Topic 1*

A cloud service accepts Security Assertion Markup Language (SAML) assertions from users to exchange authentication and authorization data between security domains. However, an attacker was able to spoof a registered account on the network and query the SAML provider. What is the MOST common attack leveraged against this flaw?

A. Attacker leverages SAML assertion to register an account on the security domain.

B. Attacker forges requests to authenticate as a different user.

C. Attacker exchanges authentication and authorization data between security domains.

D. Attacker conducts denial-of-service (DoS) against the security domain by authenticating as the same user repeatedly.

Suggested Answer: *B*

Community vote distribution

B (100%)

Soleandheel 1 year ago

B. Attacker forges requests to authenticate as a different user.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

By spoofing a registered account and querying the SAML provider, the attacker can forge requests to authenticate as a different user and potentially gain unauthorized access to sensitive data or systems.

upvoted 2 times

DJOEK 1 year, 11 months ago

Selected Answer: B

The MOST common attack leveraged against this flaw would be the attacker forging requests to authenticate as a different user (option B). This type of attack is known as a SAML spoofing attack, where the attacker is able to impersonate a legitimate user by sending a forged SAML assertion to the cloud service. This can allow the attacker to gain unauthorized access to resources within the security domain.

upvoted 2 times

> **jackdryan** 1 year, 7 months ago
>
> B is correct
>
> upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: B

This is a silver ticket attack.

upvoted 2 times

> **sausageman** 1 year, 10 months ago
>
> Silver ticket is for Kerberos not for SAML
>
> upvoted 2 times

rdy4u 2 years, 2 months ago

Selected Answer: B

There is privilege escalation issues through SAML response tampering.

https://www.mcafee.com/blogs/enterprise/pentesters-can-take-advantage-weakness-saml/

upvoted 2 times

Question #195 *Topic 1*

An organization is implementing security review as part of system development. Which of the following is the BEST technique to follow?

A. Perform incremental assessments.

B. Engage a third-party auditing firm.

C. Review security architecture.

D. Conduct penetration testing.

Suggested Answer: *A*

Community vote distribution

A (53%) C (30%) B (17%)

⊟ **DJOEK** Highly Voted 👍 2 years, 5 months ago

Selected Answer: A

Option A allows the organization to review and assess the security of the system as it is being developed, rather than waiting until the system is fully developed. This can help identify and address any security vulnerabilities or weaknesses early on in the development process.

Option B, engaging a third-party auditing firm, can also be a useful technique in certain situations, but it is not necessarily the best option in all cases, especially if the organization is already performing its own security review as part of system development.

Option C, reviewing security architecture, is a high-level activity that should be done before system development begins, rather than during the development process.

Option D, conducting penetration testing, is a useful technique for evaluating the security of a fully developed system, but it is not necessarily the best option for reviewing security during system development.

upvoted 18 times

⊟ **jackdryan** 2 years, 1 month ago

A is correct

upvoted 2 times

⊟ **BigITGuy** Most Recent ⏲ 3 months ago

Selected Answer: A

Performing security reviews at multiple stages of development, not just at the end. Catching and correcting issues early when they are cheaper and easier to fix.

upvoted 1 times

⊟ **ayadmawla** 5 months, 1 week ago

Selected Answer: A

An incremental assessment is a security assessment that focuses on specific areas of concern, rather than performing a full assessment. This allows companies to: Prioritize resources, Increase productivity, Increase compliance, and Reevaluate countermeasures.
How does an incremental assessment work?
An incremental assessment focuses on specific areas of concern, such as new equipment or policies
It allows companies to quickly reassess specific areas
It can help companies identify areas that need the most resources
What are the benefits of an incremental assessment?
Incremental assessments can help companies increase productivity and compliance
They can help companies quickly reassess specific areas
They can help companies identify areas that need the most resources

upvoted 1 times

⊟ **[Removed]** 10 months, 3 weeks ago

Selected Answer: A

B, D when the end of development. C in design phase. So Option A is right

upvoted 1 times

⊟ **homeysl** 1 year, 3 months ago

Selected Answer: C

Going with C on this one

upvoted 1 times

⊟ **gjimenezf** 1 year, 5 months ago

Selected Answer: C

Review of the security design for the application is the best way

upvoted 1 times

⊟ **Soleandheel** 1 year, 6 months ago

C. Review security architecture. This involves examining the security measures and protocols in place to ensure that they align with the real requirements and evaluate whether policies and procedures match these requirements.

upvoted 1 times

⊟ **CoolCat22** 1 year, 7 months ago

Selected Answer: C

C. Review security architecture.

Reviewing security architecture is considered the BEST technique when implementing security reviews as part of system development. This involves assessing the design and implementation of security controls within the system to ensure they align with best practices and meet security requirements. A thorough security architecture review helps identify potential vulnerabilities, weaknesses, or design flaws early in the development process, enabling their mitigation before the system is deployed.

upvoted 1 times

⊟ **74gjd_37** 1 year, 9 months ago

Selected Answer: C

Reviewing security architecture should not be a one-time event. It should be an ongoing process throughout the development process to ensure that any changes made to the system do not introduce new vulnerabilities or weaknesses.

Moreover, as part of an Agile methodology such as DevOps or SecDevOps, designing and incorporating security into software development is always checked during each iteration by performing code reviews or testing which includes securing code pipeline and version control strategies. By keeping this approach, anyone can identify design flaws at appropriate stages of SDLC which would save business time and cost much more efficiently.

upvoted 1 times

⊟ **Demo25** 1 year, 10 months ago

Selected Answer: C

The best technique for an organization implementing security review as part of system development is to review the security architecture. This involves assessing the overall design and structure of the system to ensure that security measures and principles are integrated from the ground up. Reviewing security architecture is a proactive approach that helps identify vulnerabilities and weaknesses early in the development process, making it an essential step in building a secure system. While the other options (performing incremental assessments, engaging a third-party auditing firm, and conducting penetration testing) can be valuable components of a security review, they are typically performed in conjunction with, or after, a thorough security architecture review.

upvoted 1 times

⊟ **NJALPHA** 2 years, 2 months ago

Answer A

Incremental Assessments allow an organization to only assess what's needed without performing a full assessment. This means the company can focus only on the things that concern them, such as new equipment, new policies, or simply reevaluating the countermeasures that were found to be deficient during the previous full assessment to ensure that the previous problems have been fixed or even new questions that did not exist in the previous assessment. This allows for a targeted reassessment to be completed quickly, without wasting time on things that are unlikely to change, like security policies

Validation Assessments allow site managers to perform an initial self-assessment before a third party or your own internal team arrives to conduct a full assessment

upvoted 2 times

⊟ **JohnyDal** 2 years, 4 months ago

Selected Answer: B

Auditing by an unbiased 3rd party provides best option

upvoted 2 times

⊟ **Rollingalx** 2 years, 4 months ago

I vote for C. Key word here is development, during development process.

So while all of the options listed can be valuable techniques for security review, reviewing the security architecture is the most important step to follow. This will ensure that the system is designed with security in mind and that any potential vulnerabilities are identified and addressed before the system is deployed. Incremental assessments, engaging a third-party auditing firm, and conducting penetration testing can all be useful in identifying and mitigating vulnerabilities in an already-deployed system, but they should not be the primary focus during the development process.

upvoted 2 times

Darealis 2 years, 5 months ago

Selected Answer: C

C. Review security architecture.

While all of the options listed can be valuable techniques for security review, reviewing the security architecture is the most important step to follow. This will ensure that the system is designed with security in mind and that any potential vulnerabilities are identified and addressed before the system is deployed. Incremental assessments, engaging a third-party auditing firm, and conducting penetration testing can all be useful in identifying and mitigating vulnerabilities in an already-deployed system, but they should not be the primary focus during the development process.

upvoted 2 times

Darealis 2 years, 5 months ago

Selected Answer: C

C. Review security architecture.

While all of the options listed can be valuable techniques for security review, reviewing the security architecture is the most important step to follow. This will ensure that the system is designed with security in mind and that any potential vulnerabilities are identified and addressed before the system is deployed. Incremental assessments, engaging a third-party auditing firm, and conducting penetration testing can all be useful in identifying and mitigating vulnerabilities in an already-deployed system, but they should not be the primary focus during the development process.

upvoted 2 times

oudmaster 2 years, 6 months ago

Selected Answer: B

I vote for B.

upvoted 2 times

meelaan 2 years, 6 months ago

Selected Answer: B

Options B looks good

upvoted 1 times

Question #196 *Topic 1*

What Hypertext Transfer Protocol (HTTP) response header can be used to disable the execution of inline JavaScript and the execution of eval()-type functions?

A. X-XSS-Protection

B. Content-Security-Policy

C. X-Frame-Options

D. Strict-Transport-Security

Suggested Answer: *C*

Community vote distribution

B (100%)

Soleandheel 1 year ago

B. Content-Security-Policy

The Content-Security-Policy header allows you to define a policy for controlling what types of content can be executed or loaded on a web page, including JavaScript. By specifying the appropriate directives in the Content-Security-Policy header, you can enhance the security of your web application by preventing certain types of code execution, such as inline JavaScript. This helps mitigate the risk of cross-site scripting (XSS) attacks.

upvoted 2 times

sanj10 1 year, 4 months ago

Answer is B

Web developers and administrators can set the X-Frame-Options header to help protect their web applications from being embedded in malicious or unauthorized frames. By preventing unauthorized framing, this header reduces the risk of clickjacking attacks and enhances the security of web applications. It's important to note that X-Frame-Options is now being replaced by the more modern Content-Security-Policy (CSP) frame-ancestors directive, which offers more fine-grained control over framing options and other security-related settings.

upvoted 4 times

Dee83 1 year, 11 months ago

B. Content-Security-Policy

The Content-Security-Policy (CSP) HTTP response header is used to control and restrict the types of resources that a web page can load and execute, such as scripts, images, and other media.

upvoted 1 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 1 times

Darealis 1 year, 11 months ago

Selected Answer: B

B. Content-Security-Policy

The Content-Security-Policy (CSP) HTTP response header can be used to disable the execution of inline JavaScript and the execution of eval()-type functions. This header allows website administrators to define which sources of content are allowed to be loaded on a page, such as scripts, images, and stylesheets. By disabling inline JavaScript and eval(), the CSP header can help prevent cross-site scripting (XSS) attacks.

Other HTTP headers that can be used for security are:

X-XSS-Protection, which can be used to enable the browser's built-in XSS protection.
X-Frame-Options, which can be used to prevent a page from being rendered within an iframe on another site.
Strict-Transport-Security, which can be used to enforce the use of HTTPS on a website.

upvoted 3 times

DJOEK 1 year, 11 months ago

Selected Answer: B

The correct answer is B, Content-Security-Policy. The Content-Security-Policy HTTP response header is used to specify policies for the browser to follow when executing content, such as JavaScript and eval()-type functions. It can be used to disable the execution of inline JavaScript and the execution of eval()-type functions. The other options listed are also HTTP response headers, but they are used for different purposes. X-XSS-Protection is used to enable the browser's built-in XSS protection, X-Frame-Options is used to prevent clickjacking attacks, and Strict-Transport-Security is used to enforce the use of secure connections (HTTPS) on a website.

upvoted 1 times

Mann0302 2 years ago

Selected Answer: B

Use a content security policy (CSP) that attempts to rigidly enforce same-origin restrictions for most browser-side active technologies (integrated into browsers and referenced
by HTML header values).

9th Edition page 374

upvoted 1 times

DracoL 2 years, 2 months ago

Selected Answer: B

https://glebbahmutov.com/blog/disable-inline-javascript-for-security/

as explained is content security policy

upvoted 1 times

[Removed] 2 years, 2 months ago

Refer to example 5 here:
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

upvoted 1 times

franbarpro 2 years, 2 months ago

Content-Security-Policy is the name of a HTTP response header that modern browsers use to enhance the security of the document (or web page). The Content-Security-Policy header allows you to restrict how resources such as JavaScript, CSS, or pretty much anything that the browser loads.

upvoted 3 times

Rollizo 2 years, 3 months ago

Selected Answer: B

The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites.

upvoted 2 times

Rollizo 2 years, 2 months ago

Strict-Transport-Security Force to use https
X-xss-protection is not more used

upvoted 1 times

Mgz156 2 years, 3 months ago

Selected Answer: B

Answer is B .
The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. These protections are largely unnecessary in modern browsers when sites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline').
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

upvoted 2 times

Cww1 2 years, 3 months ago

B.

The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. With a few exceptions, policies mostly involve specifying server origins and script endpoints. This helps guard against cross-site scripting attacks (Cross-site_scripting).

upvoted 4 times

DERCHEF2009 2 years, 3 months ago

correct

upvoted 1 times

Question #197 *Topic 1*

A security professional was tasked with rebuilding a company's wireless infrastructure. Which of the following are the MOST important factors to consider while making a decision on which wireless spectrum to deploy?

A. Facility size, intermodulation, and direct satellite service

B. Performance, geographic location, and radio signal interference

C. Existing client devices, manufacturer reputation, and electrical interference

D. Hybrid frequency band, service set identifier (SSID), and interpolation

Suggested Answer: *B*

Community vote distribution

B (67%) C (33%)

BigITGuy 2 months, 4 weeks ago

Selected Answer: B

Not C. While existing client devices matter, manufacturer reputation is less important than ensuring the spectrum selection fits technical and regulatory needs.

upvoted 1 times

1460168 11 months ago

Selected Answer: B

Can not be C. Manufacturer reputation isn't something a Security Professionell should consider. We want facts, so we go with B.

upvoted 1 times

maawar83 1 year, 5 months ago

I would consider C: taking into consideration the existing clients devices, and electrical interference.

upvoted 1 times

thanhlb 1 year, 8 months ago

Selected Answer: B

Performance refers to the speed, capacity, and latency of the wireless network. Geographic location refers to the physical environment and the regulatory framework of the wireless network. Different countries or regions may have different rules and standards for using the spectrum, such as licensing requirements, power limits, or channel allocations. The physical environment, such as terrain, buildings, or weather, may also affect the propagation and attenuation of the wireless signal.
Radio signal interference refers to the noise or distortion caused by other devices or sources that use the same or adjacent frequencies. Interference can degrade the performance and security of the wireless network by causing errors, delays, or loss of data.

C. Existing client devices may limit the compatibility and performance of the wireless network, but they can be upgraded or replaced if needed. Manufacturer reputation may affect the quality and support of the wireless equipment, but not the spectrum itself.

upvoted 4 times

xxxBadManxxx 1 year, 8 months ago

Selected Answer: C

For security Existing client devices & manufacturer reputation important
and electrical interference because i have seen some genius folks installed AP in the Kitchen.

upvoted 1 times

74gjd_37 1 year, 9 months ago

Selected Answer: B

Compatibility with existing client devices is important, but not the only factor to consider when choosing a wireless spectrum. Other factors such as security, signal quality, and interference must also be considered. Sometimes, a more secure or performant spectrum may require upgrading or replacing existing client devices. Terrain, building materials, and interferers can impact radio signal propagation, making geographic location an important factor too. Considering all of these factors help select the best performing wireless spectrum for optimal operation of wireless devices at the specific location.

upvoted 1 times

Tygrond87 2 years, 1 month ago

Selected Answer: C

good luck with your new high preformance geography based 5ghz install when all your warehouse scanners only support 2.4

upvoted 3 times

jackdryan 2 years, 1 month ago

B is correct

upvoted 1 times

Darealis 2 years, 5 months ago

Selected Answer: B

B. Performance, geographic location, and radio signal interference

When making a decision on which wireless spectrum to deploy, the most important factors to consider are performance, geographic location, and radio signal interference.

Performance: The wireless spectrum should be able to provide the required bandwidth and throughput for the organization's needs.
Geographic location: The wireless spectrum should be able to cover the entire area of the facility, including any remote or outdoor locations.
Radio signal interference: The wireless spectrum should not be prone to interference from other wireless devices, such as Bluetooth or microwaves.
Other factors that are important to consider are the existing client devices, the reputation of the wireless equipment manufacturer, and the potential for electrical interference, but they are not as crucial as the factors above.

upvoted 4 times

DJOEK 2 years, 5 months ago

Selected Answer: B

The most important factors to consider while making a decision on which wireless spectrum to deploy are: performance, geographic location, and radio signal interference (option B).

Performance refers to the speed and range of the wireless network. The chosen wireless spectrum should be able to support the required performance for the organization's needs.

Geographic location is important because different regions may have different regulations and standards for wireless spectrum usage. The chosen spectrum should comply with these regulations and standards.

Radio signal interference can affect the performance of the wireless network. The chosen spectrum should have minimal interference from other devices or sources to ensure optimal performance.

upvoted 2 times

ringoru 2 years, 6 months ago

Selected Answer: C

Its C. The question is talking about an existing location. You cant change the Geo-graphical location of the site. Electrical interference is accurate. Example: Its not recommended to install a wireless access point near a microwave due to the electrical interference it will cause.

upvoted 4 times

J_Ko 2 months, 4 weeks ago

Electromagnetic waves are radio signal interference. Electrical interference has to do with electrical circuits, like power lines or network cables and is less of an issue than radio signal interference when related to wireless (and yes eventually wireless tech uses a cable somewhere :D)

upvoted 1 times

J_Ko 2 months, 4 weeks ago

and also, it asks to "rebuild" the infrastructure. Wireless tech also includes point to point or satellites so geo location is important even if something is already there.

upvoted 1 times

Jamati 2 years, 7 months ago

Selected Answer: B

I think B is the best answer

upvoted 4 times

Peterzhang 2 years, 8 months ago

In terms of https://www.iotacommunications.com/blog/what-is-wireless-spectrum/ and the answer is correct as following:

What is “spectrum management”?

To understand the meaning of spectrum management, you first have to know a little more about the EM spectrum. Even though the spectrum is not tangible, it can be compared to real estate:

The spectrum is a fixed, finite resource. Only a certain range of radio frequencies exist, and once a “slice” of the spectrum has been allocated, its use by others is limited.
Location matters. As noted above, the performance characteristics of each part of the spectrum vary, making some parts more valuable, or in-demand, than others. For example, the 500 to 1000 megahertz range is very valuable because it offers sufficient speed and can transmit meaningful amounts of data; signals in this range also propagate (travel) well. Telecom operators, in particular, prefer what’s called the UHF spectrum—600, 700, and 800 MHz—for its propagation characteristics because it means they need fewer cell phone towers to use it, making the cost of building their networks cheaper. Verizon paid $9.4B for its slice of 700 MHz spectrum.
upvoted 2 times

Question #198 *Topic 1*

A software development company has a short timeline in which to deliver a software product. The software development team decides to use open-source software libraries to reduce the development time. What concept should software developers consider when using open-source software libraries?

A. Open source libraries contain known vulnerabilities, and adversaries regularly exploit those vulnerabilities in the wild.

B. Open source libraries can be used by everyone, and there is a common understanding that the vulnerabilities in these libraries will not be exploited.

C. Open source libraries contain unknown vulnerabilities, so they should not be used.

D. Open source libraries are constantly updated, making it unlikely that a vulnerability exists for an adversary to exploit.

Suggested Answer: *A*

Community vote distribution

A (84%) D (16%)

74gjd_37 Highly Voted 1 year, 9 months ago

Selected Answer: A

Option B is incorrect because the common understanding that vulnerabilities in open-source libraries will not be exploited is not true.
Option C is incorrect because while unknown vulnerabilities in open-source libraries are possible, it does not mean they should not be used.
Option D is incorrect because although many open-source libraries are constantly updated and maintained by a large community of contributors, it does not mean they are free from vulnerabilities

upvoted 5 times

BigITGuy Most Recent 2 months, 4 weeks ago

Selected Answer: A

Can't be D. While some open-source projects are actively maintained, not all are, and the existence of vulnerabilities is common.

upvoted 1 times

shaitand 8 months, 1 week ago

Selected Answer: D

D. All software has vulnerabilities but an open source solution with equivalent popularity will have fewer UNPATCHED known vulnerabilities and because vulnerabilities are patched more frequently, typically upon discovery.

upvoted 1 times

eboehm 1 year, 2 months ago

Selected Answer: D

So weird how many people think the answer is A. Just because a libary is open-source it doesnt make it automatically have known vulnerabilities. The answer is 100% D. If a library is open then its under public scrutiny far more. Therefore, when a vulnerability is detected, a fix is found quite fast.

For example just look at the SSL vulnerability.

upvoted 2 times

Maximillian 10 months, 2 weeks ago

I mean you need to think like a CISO or a least an IT security manager. Will you tell the developers that "Please use open source software without concerns as issues will be fast"? How will you explain log4j issue then

upvoted 3 times

shaitand 8 months, 1 week ago

That isn't thinking like a CISO unless you mean that CISOs are stuck in an 80's mindset where obscurity provides security. There are issues like log4j in both closed and open systems, they get found and patched more quickly with the more eyes see and review the source.

upvoted 1 times

georgegeorge125487 1 year, 10 months ago

Selected Answer: A

A is correct

upvoted 1 times

RVoigt 2 years, 5 months ago

Selected Answer: A

From the CISSP Official Study Guide - "Many of these libraries are available as open source projects, whereas others may be commercially sold or maintained internally by a company. Over the years, the use of shared libraries has resulted in many security issues...

To protect against similar vulnerabilities, developers should be aware of the origins of their shared code and keep abreast of any security vulnerabilities that might be discovered in libraries that they use. This doesn't mean that shared libraries are inherently bad. In fact, it's difficult to imagine a world where shared libraries aren't widely used. It simply calls for vigilance and attention from software developers and cybersecurity professionals."

upvoted 4 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

DJOEK 2 years, 5 months ago

Selected Answer: A

A. Open source libraries contain known vulnerabilities, and adversaries regularly exploit those vulnerabilities in the wild.

While it is true that open source libraries can be updated regularly, this does not guarantee that vulnerabilities will not exist or that they will not be exploited. In fact, the use of open source libraries can potentially increase the risk of vulnerabilities because they are widely used and known to many people, including adversaries. This means that if a vulnerability is discovered in an open source library, it may be more likely to be exploited compared to a proprietary library that is not widely known. Additionally, it is not uncommon for open source libraries to contain known vulnerabilities, as these libraries are often developed by a community of volunteers who may not have the resources or time to thoroughly test and secure the code. Therefore, it is important for software developers to consider the potential risks of using open source libraries, including the possibility of known vulnerabilities, when making decisions about which libraries to use.

upvoted 3 times

Ivanchun 2 years, 6 months ago

Selected Answer: A

A, developer known the vulnerabilities before use the open source library

upvoted 1 times

sphenixfire 2 years, 6 months ago

Selected Answer: D

?!? Guys?!

Only d is correct. If vulnerbinities are recogniced, they are fixed. All poeple can look for them. Review is done much more frequently. Unknown vulnerabilities exist in every software. And there is no consense fir nit attacking anything.

upvoted 2 times

Serliop378 2 years, 1 month ago

Some librairies and projects have a very low community and time commitment(busy devs) to find the bugs, vulnerabilities and to fix them accordingly.

upvoted 1 times

shaitand 8 months, 1 week ago

True but also true of closed software which generally has few development resources committed if isn't a popular money maker or has a locked in market. As indicated in the study material for the CISSP, vulnerabilities in open source code are typically found and patched more quickly than closed.

A is false because any KNOWN vulnerabilities in open source software are generally patched when discovered.

upvoted 1 times

rdy4u 2 years, 8 months ago

Selected Answer: A

Open source vulnerabilities are basically security risks in open source software. These are weak or vulnerable code that allows attackers to conduct malicious attacks or perform unintended actions that are not authorized.

https://www.cypressdatadefense.com/blog/open-source-security-risk/

upvoted 2 times

kptest12 2 years, 8 months ago

Selected Answer: A

Answer is right e.g log4j

upvoted 2 times

JAckThePip 2 years, 8 months ago

IN my opinion the correct Answer is B

"Sometimes it’s noted that a vulnerability that exists but is unknown can’t be exploited, so the system “practically secure.” In theory this is true, but the problem is that once someone finds the vulnerability, the finder may just exploit the vulnerability instead of helping to fix it. Having unknown vulnerabilities doesn’t really make the vulnerabilities go away; it simply means that the vulnerabilities are a time bomb, with no way to know when they’ll be exploited. Fundamentally, the problem of someone exploiting a vulnerability they discover is a problem for both open and closed source systems."

https://dwheeler.com/secure-programs/Secure-Programs-HOWTO/open-source-security.html

https://www.darkreading.com/application-security/flaws-found-in-some-open-source-projects-exploited-more-often

upvoted 1 times

Question #199

Topic 1

A security engineer is assigned to work with the patch and vulnerability management group. The deployment of a new patch has been approved and needs to be applied. The research is complete, and the security engineer has provided recommendations. Where should the patch be applied FIRST?

A. Lower environment

B. Desktop environment

C. Server environment

D. Production environment

Suggested Answer: *A*

Community vote distribution

A (80%) D (20%)

Soleandheel 1 year ago

A. Lower environment. The lower environment is known for development and testing. The patch should be applied first in a lower environment or a test lab environment. This is to thoroughly evaluate the patch before being applied to the production environment, as there is a chance that it will have issues.

upvoted 3 times

74gjd_37 1 year, 3 months ago

Selected Answer: A

The term "lower environment" refers to the development and testing stages of an application or system. In SDLC, it is the environment where developers and testers work on creating, modifying, and testing software applications before deploying them into a production environment.

From a CISSP perspective, lower environments are testing and development environments that replicate the configurations of production systems as closely as possible. By applying the patch to a lower environment first, the security engineer can evaluate its performance and ensure that it doesn't negatively impact any critical system functionality or cause conflicts with existing applications. This approach also allows them to identify and fix any issues before deploying the patch into a production environment where live users may be affected.

upvoted 2 times

SaintDaSinner 1 year, 10 months ago

D: It should be the Production environment, since the new patch has been researched and approved with recommendations...

upvoted 2 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: A

The patch should be applied FIRST in the lower environment. This is because the lower environment is typically used for testing and staging, and any issues or problems with the patch can be identified and addressed before it is deployed in more critical environments such as the production environment. It is important to test patches and updates in a controlled environment before deploying them to the live production systems to ensure that they do not cause any disruptions or issues. This is especially important when working with vulnerability and patch management, as it is important to ensure that vulnerabilities are properly patched and that the patch does not cause any additional problems.

upvoted 2 times

Jamati 2 years, 1 month ago

Selected Answer: A

Lower environments are complete replicas of production and are designed to test new releases before installing them in production. They're only accessible internally and not to external consumers.

The idea is simple, you build out a smaller scale model of your production solution. A percentage of your user base is provisioned on this system and they use it for day-to-day operations. In every way, the “lower environment” solution should be treated like production. Meaning, it is connected into your production network and uses the same security measures applied in production, Integrates with LDAP, uses the corporate antivirus, etc. etc. It should be subjected to the same change control policies or a special subset of those policies. The main difference is that the lower environment is where new software versions, feature sets, configurations, etc. pop up after they are researched and vetted in the lab.

upvoted 2 times

sec_007 2 years, 2 months ago

Selected Answer: D

D

It is not clear what method they are using for patch approval. Normally - as per the best practice - patch is approved when the patch is already tested on non-production systems and there are no regressions/side effects. If this process is followed, then this should be immediately deployed to production to reduce the risk uncovered due to absence of patch.

See: https://www.manageengine.com/patch-management/help/test-approve-patches.html

upvoted 2 times

Humongous1593 2 years, 2 months ago

Selected Answer: A

Given answer is correct. Lower environment is non-production. The rest of the answers are production equipment.

upvoted 2 times

stickerbush1970 2 years, 3 months ago

lower = development environment.

upvoted 2 times

Coolwater 2 years, 2 months ago

YOu are wrong .

https://www.infoq.com/presentations/skyscanner-production-environments/#:~:text=First%2C%20I%20just,such%20as%20databases.

upvoted 1 times

Coolwater 2 years, 2 months ago

what i mean to say is that = Lower=non production environment , just like the parallel site

upvoted 1 times

Question #200 *Topic 1*

What BEST describes the confidentiality, integrity, availability triad?

A. A vulnerability assessment to see how well the organization's data is protected

B. The three-step approach to determine the risk level of an organization

C. The implementation of security systems to protect the organization's data

D. A tool used to assist in understanding how to protect the organization's data

Suggested Answer: *C*

Community vote distribution

C (52%) D (44%) 4%

stickerbush1970 Highly Voted 2 years, 9 months ago

Selected Answer: C

CIA is all about Data and access to it. I don't have a good reason for C, however I would go C by elimination of the others, B doesn't have the word data in the answer, CIA is not an vulnerability assessment, and CIA isn't a tool.

upvoted 10 times

jackdryan 2 years, 1 month ago

C is correct

upvoted 1 times

inmymind84 Highly Voted 2 years, 9 months ago

Selected Answer: D

Why it isnt D?

upvoted 9 times

maawar83 1 year, 6 months ago

it is not a tool

upvoted 2 times

eboehm 1 year, 2 months ago

yes it is. It is used to assist you in figuring out how to implement controls based on those 3 principles

upvoted 1 times

bibibi Most Recent 3 months ago

Selected Answer: D

The CIA Triad is "a tool used to assist in understanding how to protect the organization's data."

It serves as a conceptual framework that helps organizations define security policies and implement appropriate safeguards. While the triad guides security decisions, the actual implementation of security systems (firewalls, encryption, backups, etc.) falls under security controls and strategies derived from the CIA principles.

upvoted 2 times

mattygster 3 months ago

Selected Answer: D

wouldnt it be d?

upvoted 2 times

Hangulmal 3 months, 2 weeks ago

Selected Answer: D

Reason for my choice:
The CIA triad serves as a guiding principle for security professionals to design and assess security measures.

I dont think it is C because, the implementation of security systems is a result of applying the CIA triad but implementing security systems does not define it.

upvoted 3 times

angellorv 6 months ago

Selected Answer: C

CISSP Official Study Guide (page 4-5)

The CIA triad is a security concept and is perceived as the primary goal and objective of a security infrastructure. It defines the basic parameters needed for a secure environment. Security controls are evaluated on how well they address these three core information security tenets.

upvoted 1 times

RRabbit_111 6 months, 4 weeks ago

Selected Answer: D

The CIA Triad guides security implementations, but it is not the implementation itself. It is a model or tool for planning and analysis.

upvoted 4 times

KJ44 7 months, 3 weeks ago

Selected Answer: D

it is there to assist in our understanding.

upvoted 2 times

deeden 10 months, 3 weeks ago

Selected Answer: A

I vote A just because.. the CIA triad is a conceptual framework for understanding information security objectives, rather than a specific methodology or tool.

A vulnerability assessment is a process to identify weaknesses in an organization's systems and networks.

upvoted 1 times

1460168 11 months ago

Selected Answer: D

The C-I-A triad is a framework to help us understand how to proceed, for example when securing data. It is therefore irrelevant whether the word 'tool' is to be understood here as software, it is rather to be understood as an assistant.

upvoted 1 times

50e940e 1 year ago

Selected Answer: D

security systems did not mean program or framework. We may not develop systems to protect our data

upvoted 2 times

CCNPWILL 1 year, 1 month ago

C is the best option given the wording. deleted the other A and B based on just being way off.

upvoted 1 times

eboehm 1 year, 2 months ago

Selected Answer: D

Haha soooo many people on here have zero understanding of the word "tool" A tool is ANYTHING that would assist you with the implementation. This could be training, google, a manual, a model, a concept, a standard, CISSP certification, the list goes on.

Hillarious how many think the CIA triad, an intangible construct that is only in our heads, is somehow an implementation of security controls

upvoted 2 times

gjimenezf 1 year, 5 months ago

Selected Answer: C

Data security

upvoted 1 times

SpaceMonkey1 1 year, 7 months ago

Selected Answer: D

Option C could be interpreted as implying that the confidentiality, integrity, and availability (CIA) triad refers to the implementation of security systems to protect an organization's data. While security systems are indeed employed to uphold these principles, the CIA triad itself is not a specific implementation or system but rather a foundational concept guiding security strategies.

The CIA triad outlines three primary objectives essential to information security—ensuring data confidentiality, maintaining data integrity, and guaranteeing data availability. It's a principle or guideline used to shape the design, selection, and implementation of security measures and systems within an organization to protect its data and resources. Therefore, while security systems are implemented to align with the CIA triad, the triad itself represents the overarching principles rather than the specific tools or systems used for protection.

upvoted 4 times

74gjd_37 1 year, 9 months ago

Selected Answer: C

Among the given options, C best describes the CIA triad from a CISSP perspective as it highlights the implementation of security systems to safeguard and protect an organization's data.

upvoted 2 times

Nicola_2_Reg 1 year, 9 months ago

Selected Answer: D

The wording is not appropriate enough... I mean, D would be more accurate.
CIA triad does not implement, it is a concept (moreless a immaterial tool to help CISOs).

upvoted 3 times

Question #201 *Topic 1*

Why is it important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision?

A. To provide each manager with precise direction on selecting an appropriate recovery alternative

B. To demonstrate to the board of directors that senior management is committed to continuity recovery efforts

C. To provide a formal declaration from senior management as required by internal audit to demonstrate sound business practices

D. To demonstrate to the regulatory bodies that the company takes business continuity seriously

Suggested Answer: *D*

Community vote distribution

A (100%)

krassko Highly Voted 2 years, 3 months ago

Selected Answer: A

A for me as well. Knowing MTD (time you have in case of failure) you can consider what tech, systems, procedures etc you can introduce to the company

upvoted 9 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 2 times

CCNPWILL Most Recent 7 months ago

A is the best answer compared to the other. Its actually taking actions and its the best answer to this question.

upvoted 1 times

homeysl 1 year, 2 months ago

Selected Answer: A

It will determine whether to go with a hot or warm or cold recovery site.

upvoted 2 times

74gjd_37 1 year, 3 months ago

Selected Answer: A

While demonstrating commitment to continuity recovery efforts, sound business practices, and compliance with regulatory bodies are also important, they are not directly related to the communication of MTD decisions.

upvoted 1 times

MShaaban 1 year, 4 months ago

It is A. MTD is the threshold when the business after it is doomed. There is no point to show anyone that senior management take business seriously, the most important is that there are sufficient alternatives to make business going in case of a disaster so the business is not lost.

upvoted 1 times

KCLung 1 year, 6 months ago

Why it select the answer A?? It does not make sense. The manager has the right to determine the selection of the recovery alternative???? Please tell me which company manager has such this right. Is it the manager = senior management??

upvoted 1 times

HughJassole 1 year, 6 months ago

It seems that D is the best match, as it is the only one referencing business continuity:
https://www.agilityrecovery.com/business-continuity-management-glossary

upvoted 2 times

Dee83 1 year, 11 months ago

A. To provide each manager with precise direction on selecting an appropriate recovery alternative.

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: A

The correct answer is A. It is important that senior management clearly communicates the formal Maximum Tolerable Downtime (MTD) decision to provide each manager with precise direction on selecting an appropriate recovery alternative. This ensures that everyone in the organization is aware of the expected downtime and can plan accordingly to minimize the impact on the business. It is also important to demonstrate to regulatory bodies that the company takes business continuity seriously, but that is not the primary reason for communicating the MTD decision.

upvoted 1 times

oudmaster 2 years ago

BTW, option D will lead to increase business reputation if the organization get complied with regulation (e.g. ISO standards). But I am not sure if D is the answer.

upvoted 2 times

pingundas 2 years, 2 months ago

I do not think the managers will have independent DR toolsets. D should right (PS: amazed at how many answers default answers do not make sense)

upvoted 1 times

sphenixfire 2 years ago

For ecery system, a recovery dr plan is needed that fits into corp bcm. There, yes, they need to have.

upvoted 1 times

byolar 2 years, 2 months ago

A looks more appropriate as that is the essence of disaster recovery metrics in the first place.

upvoted 1 times

Cww1 2 years, 3 months ago

im going A

upvoted 3 times

Question #202 *Topic 1*

A Simple Power Analysis (SPA) attack against a device directly observes which of the following?

A. Magnetism

B. Generation

C. Consumption

D. Static discharge

Suggested Answer: *B*

Community vote distribution

C (100%)

Stevooo Highly Voted 👍 2 years, 3 months ago

Selected Answer: C

Simple power analysis is a method of side-channel attack that examines a chip's current consumption over a period of time

upvoted 10 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

YesPlease Most Recent ⏲ 1 year ago

Selected Answer: C

Answer C)

https://en.wikipedia.org/wiki/Power_analysis#:~:text=Variations%20in%20power%20consumption%20occur%20as%20the%20device%20performs%20differen

upvoted 2 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

In a Simple Power Analysis (SPA) attack, an attacker measures the power consumption of a device while it's performing cryptographic operations to obtain sensitive information such as encryption keys. The attacker directly observes the power consumption levels of the device to extract this data.

The key in the question is the word "directly". While key generation may be observed, it is not observed as directly as power consumption

upvoted 2 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

Dee83 1 year, 11 months ago

A Simple Power Analysis (SPA) attack against a device directly observes the consumption of power. (Option C)

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: C

A Simple Power Analysis (SPA) attack directly observes consumption. SPA is a type of side-channel attack that involves analyzing the power consumption of a device to extract sensitive information, such as encryption keys. By measuring the power consumption of a device as it performs various operations, an attacker can deduce the data being processed by the device and potentially gain access to sensitive information.

upvoted 1 times

Ncoa 2 years, 2 months ago

Selected Answer: C

Consumption

upvoted 2 times

Yanjun 2 years, 3 months ago

Selected Answer: C

consumption

upvoted 4 times

Nickolos 2 years, 3 months ago

Selected Answer: C

Power analysis observes consumption, so c

upvoted 4 times

matt1976 2 years, 3 months ago

C - Consumption.

https://en.wikipedia.org/wiki/Power_analysis

upvoted 4 times

Question #203 *Topic 1*

Which of the following MUST the administrator of a security information and event management (SIEM) system ensure?

A. All sources are synchronized with a common time reference.

B. All sources are reporting in the exact same Extensible Markup Language (XML) format.

C. Data sources do not contain information infringing upon privacy regulations.

D. Each source uses the same Internet Protocol (IP) address for reporting.

Suggested Answer: *A*

Community vote distribution

A (67%) C (33%)

BigITGuy 3 months ago

Selected Answer: A

For a SIEM system to function properly, it is essential that all data sources are synchronized to a common time reference (typically via Network Time Protocol (NTP)). This ensures that events from multiple sources can be correlated correctly, sequenced accurately and used effectively for incident investigation and forensic analysis. Privacy considerations are important but are not a primary SIEM administrator requirement — this is usually handled during data classification and collection policies.

upvoted 1 times

CCNPWILL 7 months ago

A is correct. Without NTP/timestamps, doesnt matter which log format the data arrives in. we MUST have the timestamps to correlate data.

upvoted 2 times

homeysl 1 year, 2 months ago

Selected Answer: A

SIEM needs that for correlation

upvoted 3 times

ccKane 1 year, 2 months ago

Selected Answer: A

C is not a MUST do for an SIEM Administrator. I go with A.

upvoted 1 times

MShaaban 1 year, 4 months ago

It is clearly A.

upvoted 2 times

DeepCyber 1 year, 6 months ago

Selected Answer: C

Time synchronization is important but it is asking about most Important. We need to ensure data sources does not contain information infringing upon privacy regulations. We need to either mask, anonymize or remove privacy data before sending to SIEM. This should be most important task.

upvoted 3 times

JAlexander35 6 months ago

True but that's not your SIEM admin's job.

upvoted 1 times

dmo_d 1 year, 7 months ago

Selected Answer: C

Time synchronisation is obviously the most important thing.

But how can the SIEM administrator influence the time of each reporting system??

Even if the SIEM admin tries to insert some correction in the received timestamps, the source systems time could deviate more and more over time.

IMHO there is no way for the receiver to ensure a synchronous time.

upvoted 1 times

Ernestokoro 1 year, 9 months ago

CISSP OFFICIAL GUIDE 9TH EDITION. PG829:Logging systems should also make use of the Network Time Protocol (NTP) to ensure
that clocks are synchronized on systems sending log entries to the SIEM as well as the SIEM

itself. This ensures that information from multiple sources has a consistent timeline.
Information security managers should also periodically conduct log reviews, particularly
for sensitive functions, to ensure that privileged users are not abusing their privileges. For
example, if an information security team has access to eDiscovery tools that allow searching
through the contents of individual user files, security managers should routinely review the
logs of actions taken by those administrative users to ensure that their file access relates to legitimate eDiscovery initiatives and does not violate user privacy

upvoted 2 times

jackdryan 1 year, 7 months ago

A is correct

upvoted 1 times

conur87 1 year, 11 months ago

Selected Answer: C

Privacy regulations compliance is a must for SIEM administrator to ensure that the data sources do not contain information infringing upon privacy regulations.

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: A

It is important that all sources are synchronized with a common time reference because it ensures that the events being logged and analyzed are correctly correlated and accurately reflect the order in which they occurred. This is important for properly identifying and investigating security incidents, as well as for creating reports and performing analytics on the data. If the sources are not synchronized, the data may be misleading or confusing, which can hinder the effectiveness of the SIEM system.

upvoted 2 times

Ivanchun 2 years ago

Selected Answer: A

Time sync is most important

upvoted 1 times

rdy4u 2 years, 2 months ago

Selected Answer: A

Time is one of the most important things when it comes to the analysis of log information collected from security devices.

https://resources.infosecinstitute.com/certification/security-technologies-and-tools-siem/

upvoted 4 times

Question #204 *Topic 1*

An organization wants to share data securely with their partners via the Internet. Which standard port is typically used to meet this requirement?

A. Setup a server on User Datagram Protocol (UDP) port 69

B. Setup a server on Transmission Control Protocol (TCP) port 21

C. Setup a server on Transmission Control Protocol (TCP) port 22

D. Setup a server on Transmission Control Protocol (TCP) port 80

Suggested Answer: *C*

Community vote distribution

C (100%)

Skittle4710 6 months, 3 weeks ago

Selected Answer: C

C. SSH (Secure Shell) is indeed the only protocol among the listed options that inherently provides secure transmission of data. It encrypts the data transmitted between the client and server, which ensures confidentiality, integrity, and authenticity.

upvoted 3 times

klarak 8 months, 1 week ago

LOL. Is this actually part of the test? This isn't how data's shared in 2024...

upvoted 1 times

gjimenezf 11 months, 2 weeks ago

SFTP Secure FTP on port 22

upvoted 1 times

John520 1 year, 8 months ago

ecure Shell (SSH) is a good example of an end-to-end encryption technique. This suite of programs provides encrypted alternatives to common internet applications such as the File Transfer Protocol (FTP), Telnet, and rlogin. There are actually two versions of SSH. SSH1 (which is now considered insecure) supports the Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption Algorithm (IDEA), and Blowfish algorithms. SSH2 drops support for DES and IDEA but adds several security enhancements, including support for the Diffie–Hellman key exchange protocol and the ability to run multiple sessions over a single SSH connection. SSH2 provides added protection against man-in-the-middle (on-path) attacks, eavesdropping, and IP/DNS spoofing.

upvoted 2 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: C

C. Setup a server on Transmission Control Protocol (TCP) port 22. The Secure Shell (SSH) protocol, which is used for secure remote login and other secure network services, uses TCP port 22 as its default port. It is a common choice for securely exchanging data between organizations over the Internet.

upvoted 4 times

Jamati 2 years, 1 month ago

Selected Answer: C

Easy-peasy

upvoted 1 times

franbarpro 2 years, 2 months ago

Yep - SSH

upvoted 2 times

Question #205 *Topic 1*

When designing a business continuity plan (BCP), what is the formula to determine the Maximum Tolerable Downtime (MTD)?

A. Estimated Maximum Loss (EML) + Recovery Time Objective (RTO)

B. Business impact analysis (BIA) + Recovery Point Objective (RPO)

C. Annual Loss Expectancy (ALE) + Work Recovery Time (WRT)

D. Recovery Time Objective (RTO) + Work Recovery Time (WRT)

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 9 months, 1 week ago

Selected Answer: D

Quote: "Downtime consists of two elements, the systems recovery time and the work recovery time. Therefore, MTD = RTO + WRT."

Quote: "Work recovery time (WRT). [...] It takes time to get critical business functions back up and running once the systems (hardware, software, and configuration) are restored. Upstream and downstream systems or interfaces need to be synchronized, data need to be tested to ensure backups are correct and in sequence, data captured manually during a downtime needs to be input, validated, and integrated into existing data. This is an area that some planners overlook, especially from IT. If the systems are back up and running, they're all set from an IT perspective. From a business function perspective, there are additional steps that must be undertaken before it's back to business."

Source: Business Impact Analysis
Susan Snedaker, Chris Rima, in Business Continuity and Disaster Recovery Planning for IT Professionals (Second Edition), 2014

upvoted 4 times

georgegeorge125487 10 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

DJOEK 1 year, 5 months ago

Selected Answer: D

Correct, according to the CISSP exam objectives, the formula to determine the Maximum Tolerable Downtime (MTD) is the Recovery Time Objective (RTO) + Work Recovery Time (WRT). The RTO is the maximum length of time that a business process can be unavailable before it begins to have an impact on the business, while the WRT is the time required to restore the business process to its normal state after an incident occurs. Together, these two factors help to determine the maximum amount of time that a business can tolerate being without a particular process before it begins to suffer significant consequences.

upvoted 4 times

jackdryan 1 year, 1 month ago

D is correct

upvoted 1 times

rdy4u 1 year, 8 months ago

Selected Answer: D

Maximum allowable downtime = RTO + WRT
For example, if a critical business process has a three-day maximum allowable downtime, the RTO for systems, networks and data might be one day. This is the time the organization needs to recover technology. The remaining two days are for work recovery.

upvoted 4 times

bherto39 1 year, 9 months ago

the answer is correct .. verified by looking at this ref
https://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

upvoted 2 times

⊟ **Cww1** 1 year, 9 months ago

Correct, Maximum allowable downtime = RTO + WRT

upvoted 3 times

Question #206 *Topic 1*

In systems security engineering, what does the security principle of modularity provide?

A. Minimal access to perform a function

B. Documentation of functions

C. Isolated functions and data

D. Secure distribution of programs and data

Suggested Answer: *C*

Community vote distribution

C (100%)

stickerbush1970 Highly Voted 👍 2 years, 3 months ago

Selected Answer: C

This security designing principle says that the security mechanism must be generated as separate and protected modules and the security mechanism must be generated using the modular architecture.

This principle helps in updating the security mechanism independently without modifying the entire system.

upvoted 7 times

jackdryan 1 year, 7 months ago

C is correct

upvoted 2 times

Soleandheel Most Recent 1 year ago

The security principle of modularity in systems security engineering provides isolated functions and data. This principle isolates functions into well-defined logical units, allowing them to be composed and managed independently. It extends functional modularity to include considerations based on trust, trustworthiness, privilege, and security policy. This means that different functions and data are separated and not dependent on each other, reducing the risk of compromise of one function or piece of data. Therefore, the correct answer is:

C. Isolated functions and data

upvoted 3 times

homeysl 1 year, 2 months ago

Selected Answer: C

NASA says "The security principle of modularity services is to isolate functions into well-defined logical units so that they can be composed. Layering relates to the application layer, network layer, and security kernel/device layer."

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: C

Although CISSP CBK does not tell anything about modularity, the secure design principle of modularity is mentioned in NIST Special Publication 800-53:

"These core security principles include, for example, simplicity, modularity, layering, domain isolation, least privilege, least functionality, and resource isolation/encapsulation. [...] The reduction in inter-module interactions helps to constrain security functions and to manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between the different functions within a particular module. Good software engineering practices rely on modular decomposition, layering, and minimization to reduce and manage complexity, thus reducing
software modules that are highly cohesive and loosely coupled. The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules."

upvoted 1 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: C

C is correct

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: C

The security principle of modularity provides isolated functions and data. This means that different functions and data are separated and not dependent on each other. This can help to reduce the risk of a compromise of one function or piece of data affecting other functions or data. Modularity can also make it easier to identify and fix security vulnerabilities, as it allows for a more targeted approach to security testing and remediation.

upvoted 3 times

⊟ **Jamati** 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 2 times

Question #207 *Topic 1*

Which of the following is the strongest physical access control?

A. Biometrics, a password, and personal identification number (PIN)

B. Individual password for each user

C. Biometrics and badge reader

D. Biometrics, a password, and badge reader

Suggested Answer: *D*

Community vote distribution

D (67%) C (33%)

stickerbush1970 Highly Voted 2 years, 3 months ago

Selected Answer: D

Something you are

Something you know

Something you have

upvoted 21 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 2 times

liledag Highly Voted 1 year, 9 months ago

Please Read the question carefully is asking for physical! That's the keyword a password is not considered physical because it is a piece of information that is stored electronically or in a person's memory. Physical access controls refer to measures that use physical objects or devices to restrict access, such as badges, keys, or biometric readers.

upvoted 5 times

eboehm 8 months, 3 weeks ago

isnt a pin(password) entered into an electronic lock a form of password?

upvoted 1 times

95f6f48 Most Recent 4 months, 1 week ago

Selected Answer: D

Something you are

Something you know

Something you have

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: D

Types 1 to 3, AIO

upvoted 2 times

629f731 11 months, 3 weeks ago

Selected Answer: C

A password is not a typical PACS.

upvoted 2 times

homeysl 1 year, 2 months ago

Selected Answer: D

D. Type 1, 2 & 3. All in one.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: D

The combination of access controls provides multiple factors of authentication, including something the user is (biometrics), something the user knows (password), and something the user has (badge) makes it much harder for an unauthorized person to gain access to a secure area or system.

Although a password may not be necessary in a physical access control scenario where biometrics and a badge reader are already present (biometrics and a badge reader alone can provide a strong physical access control mechanism), however, the addition of a password as a third factor of authentication can further increase security and may be required in some high-security environments.

Sine the question emphasizes "strongest" physical access control, option D is correct.

upvoted 2 times

georgegeorge125487 1 year, 4 months ago

Selected Answer: C

A password is not a typical PACS.

upvoted 3 times

Clay 1 year, 12 months ago

Selected Answer: C

Badges, identification cards, and security IDs are forms of physical identification and/or access to electronic control devices. CISSP 9th Edition pg 456 kindle reader

upvoted 5 times

Ivanchun 2 years ago

Selected Answer: D

PIN is not strongest physical control, D combination would be the strongest

upvoted 1 times

Nickolos 2 years ago

Selected Answer: C

It's c. Hint - physical access control, not logical.

upvoted 4 times

WiDeBarulho 2 years, 2 months ago

Selected Answer: C

A password is not "physical" access control. So "C" is the most correct answer.

upvoted 4 times

jon1991 2 years, 3 months ago

Why not C? Its' asking for physical access control.

upvoted 3 times

jon1991 2 years, 3 months ago

Got it :)

upvoted 2 times

DERCHEF2009 2 years, 3 months ago

Yea but pysical access and password? Never see a password. A PIN yes but no password ....

upvoted 1 times

Question #208 *Topic 1*

An access control list (ACL) on a router is a feature MOST similar to which type of firewall?

A. Stateful firewall

B. Packet filtering firewall

C. Application gateway firewall

D. Heuristic firewall

Suggested Answer: *B*

Community vote distribution

B (91%) 9%

Soleandheel 1 year ago

An access control list (ACL) on a router is most similar to a packet filtering firewall.

upvoted 2 times

Soleandheel 1 year ago

B. Packet filtering firewall

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

Stateful firewalls are designed to keep track of the state of network connections and use this information to make decisions about whether to allow or block traffic. While stateful firewalls provide more advanced security features than ACLs, they are not the most similar to ACLs on a router. This is because ACLs are typically used to control access to network resources based on more basic criteria, such as IP address and port number, whereas stateful firewalls are more focused on the state of a connection. Therefore, the most similar type of firewall to an ACL on a router is a packet filtering firewall.

upvoted 2 times

MShaaban 1 year, 4 months ago

Answer is B. Packet filtering is stateless

upvoted 1 times

jens23 1 year, 5 months ago

Selected Answer: B

It's B, but router can also utilize ACLs that are stateful.
That's the function of extended ACLs on a Cisco router for example.
It' a feature that's well beyond decade old.

upvoted 2 times

omarin25 1 year, 11 months ago

Network ACLs are stateless: This means any changes applied to an incoming rule will not be applied to the outgoing rule. If you allow an incoming port 22, you would also need to apply the rule for outgoing traffic.

upvoted 2 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 2 times

trawa05 2 years ago

Selected Answer: B

router is not stateful

upvoted 2 times

krassko 2 years, 3 months ago

Selected Answer: B

Yes ACL is stateless so I choose B

upvoted 4 times

stickerbush1970 2 years, 3 months ago

Selected Answer: A

An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination

upvoted 1 times

Yanjun 2 years, 3 months ago

Yes, the best answer is stateless firewall, but A is Stateful Firewall

upvoted 3 times

stickerbush1970 2 years, 3 months ago

You are correct and after reading into the question more, I believe the answer to be B.

upvoted 2 times

Question #209 *Topic 1*

While dealing with the consequences of a security incident, which of the following security controls are MOST appropriate?

A. Detective and recovery controls

B. Corrective and recovery controls

C. Preventative and corrective controls

D. Recovery and proactive controls

Suggested Answer: *B*

Community vote distribution

B (93%) 7%

Jamati Highly Voted 2 years, 1 month ago

Selected Answer: B

The incident has already happened. You're not trying to detect anything or be proactive or prevent anything. You're just interested in recovery and corrective controls.

upvoted 9 times

Mann0302 2 years, 1 month ago

Did you take the exam already? You seem to know all the answers lol. I love it.

upvoted 2 times

maawar83 Most Recent 1 year ago

Answer should be C:

Consequences = the aftermath of the incident which is mainly at the lesson learned.

Preventive so it does not happen again whether after restoring this incident or new incident

Corrective They are crucial for not only resolving the immediate impact of an incident but also for strengthening an organization's security defenses and resilience against future threats.

upvoted 2 times

Soleandheel 1 year ago

B. Corrective and recovery controls

upvoted 1 times

homeysl 1 year, 2 months ago

Selected Answer: B

B is correct. I thought it was A but looking at the CISSP IR Steps, detect is Step 1.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

Corrective controls are designed to correct or fix an issue that has already occurred, while recovery controls are designed to restore systems and data to their normal operating state after an incident. These controls are critical for minimizing the damage caused by security incidents and restoring normal business operations as quickly as possible.

Detective controls are designed to detect security incidents, whereas preventative controls are designed to prevent security incidents from occurring in the first place. Proactive controls are designed to proactively identify and mitigate security risks before they can cause harm. While all of these controls are important components of a comprehensive security program, they are not the MOST appropriate controls when dealing with the consequences of a security incident.

upvoted 2 times

Skinbaggy 2 years, 1 month ago

If you Look at this termonology

Before the event, preventive controls are intended to prevent an incident from occurring e.g. by locking out unauthorized intruders;

During the event, detective controls are intended to identify and characterize an incident in progress e.g. by sounding the intruder alarm and alerting the security guards or police;

After the event, corrective controls are intended to limit the extent of any damage caused by the incident e.g. by recovering the organization to normal working status as efficiently as possible.

It's A

upvoted 1 times

Skinbaggy 2 years, 1 month ago

Sorry B

upvoted 3 times

Nickolos 2 years ago

Lmao all the nice writeup and you ended with "a" I was like "is this guy for real?" and then noticed you corrected xd

upvoted 4 times

jackdryan 1 year, 7 months ago

B is correct

upvoted 2 times

franbarpro 2 years, 2 months ago

Selected Answer: B

You are dealing with the consequences of a security incident. Detective controls are out of the door here. This thing has already happened and now you're dealing with the consequences. So, I am going with "B".

upvoted 3 times

rc7 2 years, 2 months ago

Answer is B. Question asks/incudes "dealing with the consequences" which implies that the most appropriate security controls includes corrective and recovery controls.

upvoted 2 times

WiDeBarulho 2 years, 2 months ago

Selected Answer: A

Always check your detective controls to understand what they detected and/or failed to detect before applying any corrective controls.

upvoted 1 times

Nickolos 2 years ago

Always check? Even after the incident has been documented and everything has already been checked by specialists, you have the workflow documented, you have your incident resolution and prb record, you're going to go to the same people and say "hey guys so yeah thanks for the great work, now do all of that again, okay?"

upvoted 1 times

[Removed] 2 years, 2 months ago

Agree with B

upvoted 3 times

JAckThePip 2 years, 2 months ago

Answer is A

"Detective controls are designed to find errors or problems after the transaction has occurred. Detective controls are essential because they provide evidence that preventive controls are operating as intended, as well as offer an after-the-fact chance to detect irregularities."

upvoted 1 times

Question #210 *Topic 1*

A cloud hosting provider would like to provide a Service Organization Control (SOC) report relevant to its security program. This report should an abbreviated report that can be freely distributed. Which type of report BEST meets this requirement?

A. SOC 1

B. SOC 2 Type 1

C. SOC 2 Type 2

D. SOC 3

Suggested Answer: *B*

Community vote distribution

D (100%)

⊟ **matt1976** Highly Voted 👍 2 years, 3 months ago

Answer is D - A SOC 3 report is basically a redacted SOC2 report. It's intended for a public audience, and is usually available on an organization's website.

upvoted 16 times

⊟ **jackdryan** 1 year, 7 months ago

D is correct

upvoted 2 times

⊟ **74gjd_37** Highly Voted 👍 1 year, 3 months ago

Selected Answer: D

This is expressly mentioned on page 26 of the Official ISC2 CISSP CBK reference that SOC3 is a light version for distribution.

upvoted 5 times

⊟ **041ba31** Most Recent 🕓 7 months, 1 week ago

Its quite concerning to see the amount of questions that are that incorrect answers marked as "Correct Answer". SOC 2 type 1 report is clearly incorrect, it focuses on the could provider's CIA+ processes and procedures, generating a report that is CONFIDENTIAL. Correct answer should be D, SOC 3, which focuses on the same principles as SOC 2 but generates a "high view" report thatcan be freely distributed.

upvoted 1 times

⊟ **Dtony66** 7 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

⊟ **Soleandheel** 1 year ago

SOC 3 report is essentially a summary of the SOC 2 report. SOC 3 can be freely distributed while SOC 2 is not for distribution.

upvoted 2 times

⊟ **Soleandheel** 1 year ago

Therefore, the answer is D. SOC 3

upvoted 1 times

⊟ **georgegeorge125487** 1 year, 4 months ago

Selected Answer: D

D is correct

upvoted 1 times

⊟ **MShaaban** 1 year, 4 months ago

Answer is D. SOC3. SOC2 is not for distribution.

upvoted 1 times

⊟ **Dee83** 1 year, 11 months ago

D. SOC 3

upvoted 1 times

⊟ **olulado** 1 year, 12 months ago

Ans B . What is SOC 2 Type 1? SOC 2 Type 1 compliance evaluates an organization's cybersecurity controls at a single point in time. The goal is to determine whether the internal controls put in place to safeguard customer data are sufficient and designed correctly.

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: D

SOC3 because they're public.

upvoted 3 times

WiDeBarulho 2 years, 2 months ago

Selected Answer: D

SOC 2 reports are restricted. SOC 3 are to be freely distributed. For more info go here: https://linfordco.com/blog/soc-2-vs-soc-3/

upvoted 3 times

JAckThePip 2 years, 2 months ago

Answer correct

"Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy."

https://www.imperva.com/learn/data-security/soc-2-compliance/

upvoted 1 times

> **Jamati** 2 years, 1 month ago
>
> Given answer is not correct.
>
> upvoted 1 times

inmymind84 2 years, 3 months ago

Selected Answer: D

Correct, D

upvoted 4 times

stickerbush1970 2 years, 3 months ago

Selected Answer: D

Agree with D.

upvoted 4 times

Question #211 *Topic 1*

Which of the following is TRUE for an organization that is using a third-party federated identity service?

A. The organization specifies alone how to authenticate other organization's users

B. The organization defines internal standard for overall user identification

C. The organization establishes a trust relationship with the other organizations

D. The organization enforces the rules to other organization's user provisioning

Suggested Answer: *C*

Community vote distribution

C (100%)

74gjd_37 9 months, 1 week ago

Selected Answer: C

In a federated identity management system, multiple organizations agree to trust each other to authenticate their respective users. The organization that provides the identity service acts as a trusted third party, enabling users from different organizations to access resources using the same set of credentials. The other options are not true for a third-party federated identity service.

upvoted 1 times

georgegeorge125487 10 months, 1 week ago

Selected Answer: C

C. The organization establishes a trust relationship with the other organizations.

upvoted 1 times

DJOEK 1 year, 5 months ago

Selected Answer: C

C. The organization establishes a trust relationship with the other organizations.

Federated identity is a system that allows users from different organizations to access multiple applications with a single set of credentials. In this case, the organization using the third-party federated identity service establishes a trust relationship with the other organizations, meaning that it trusts the other organizations to authenticate their users and allow them access to the shared applications. The organization may also define internal standards for overall user identification, but it does not specify how to authenticate users from other organizations or enforce rules for their user provisioning.

upvoted 1 times

jackdryan 1 year, 1 month ago

C is correct

upvoted 1 times

sphenixfire 1 year, 6 months ago

Selected Answer: C

C us ut

upvoted 1 times

Jamati 1 year, 7 months ago

Selected Answer: C

I'll go with C

upvoted 2 times

Jay_12 1 year, 7 months ago

B - third-party federated identity service will provide trust between other organization. Organizations are only responsible for authentication of users in their ream.

upvoted 1 times

JAckThePip 1 year, 8 months ago

Answeri is correct

Federated identity – also known as Federated Identity Management (FIM) – works on the basis of mutual trust relationships between a Service

Provider (SP) such as an application vendor and an external party or Identity Provider (IdP"

https://www.onelogin.com/learn/federated-identity

upvoted 3 times

Question #212 *Topic 1*

Which of the following describes the BEST method of maintaining the inventory of software and hardware within the organization?

A. Maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools

B. Maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools

C. Maintaining the inventory through a combination of on premise storage configuration, cloud management, and partner management tools

D. Maintaining the inventory through a combination of system configuration, network management, and license management tools

Suggested Answer: *C*

Community vote distribution

D (100%)

Cww1 Highly Voted 👍 2 years, 3 months ago

I prefer D here, license management for sw and network management for hw

upvoted 8 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

klarak 8 months, 1 week ago

Yeah it's just the least bad option.

upvoted 2 times

Amit3 Most Recent 🕘 8 months, 2 weeks ago

The answer is D

upvoted 1 times

amogh2612 1 year, 3 months ago

Selected Answer: D

no doubt..it is D

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: D

Option A, maintaining the inventory through a combination of asset owner interviews, open-source system management, and open-source management tools, may be a useful approach, but it lacks the comprehensive and integrated approach that option D offers. It may not be sufficient for large organizations with complex software and hardware environments.

Option B, maintaining the inventory through a combination of desktop configuration, administration management, and procurement management tools, is focused on managing the desktop environment and procurement of new assets. While this approach may be useful, it does not provide a comprehensive view of all software and hardware assets within the organization.

Option C, maintaining the inventory through a combination of on-premise storage configuration, cloud management, and partner management tools, is focused on managing cloud-based assets and partner relationships. While these are important aspects of managing software and hardware inventory, it does not address the need to manage on-premise assets and may not be suitable for organizations that do not use cloud-based assets extensively.

upvoted 3 times

Nicola_2_Reg 1 year, 3 months ago

Selected Answer: D

Best is to have a CMDB... D is the answer that seems the most accurate

upvoted 2 times

DJOEK 1 year, 11 months ago

Selected Answer: D

D. Maintaining the inventory through a combination of system configuration, network management, and license management tools is the best method of maintaining the inventory of software and hardware within the organization according to cissp. This method combines tools for system and network management, which can provide information about the hardware and software installed on the organization's systems, with tools for license management, which can help track the organization's software licenses and ensure compliance. By using a combination of these tools, the organization can maintain a comprehensive and up-to-date inventory of its hardware and software assets.

upvoted 3 times

oudmaster 2 years ago

by heart, I will go with option D

upvoted 1 times

sphenixfire 2 years ago

Selected Answer: D

Doesn't seem to be a valid question, but d is nearest for me

upvoted 2 times

CuteRabbit168 2 years, 3 months ago

Selected Answer: D

Agree D is the best answer

upvoted 4 times

inmymind84 2 years, 3 months ago

Selected Answer: D

NMS, LMS i CMDB looks file for this task. I think it's D.

upvoted 4 times

Question #213 *Topic 1*

Which of the following outsourcing agreement provisions has the HIGHEST priority from a security operations perspective?

A. Conditions to prevent the use of subcontractors

B. Terms for contract renegotiation in case of disaster

C. Root cause analysis for application performance issue

D. Escalation process for problem resolution during incidents

Suggested Answer: *D*

Community vote distribution

D (72%) A (17%) 11%

ServerBrain 3 months, 2 weeks ago

Selected Answer: D

" from a security operations perspective "

upvoted 1 times

Vasyamba1 9 months, 1 week ago

Selected Answer: C

The root cause analysis often highlights issues that require remediation to prevent similar incidents in the future, so I think it's the most important thing for SecOps.

upvoted 2 times

maawar83 12 months ago

I think the answer is C.

A and B.. are not valid for security operation..

D is the escalation process for problem during incident...

C... will make more sense as RCA for application performance issue that can be cause by Cyber Attack?

upvoted 2 times

homeysl 1 year, 2 months ago

Selected Answer: D

D. It's between A and D but the question mentioned security operations.

upvoted 3 times

74gjd_37 1 year, 3 months ago

Selected Answer: D

Option D, Escalation process for problem resolution during incidents, ensures that there is a clear and effective process in place for resolving security incidents and minimizing the impact of any security breaches. It is critical to have a well-defined escalation process to ensure that security incidents are handled promptly and efficiently. The other provisions listed are also important, but they do not have as high a priority from a security operations perspective as the escalation process for problem resolution during incidents.

An escalation process is necessary for resolving security incidents promptly and efficiently. Outsourcing agreements transfer responsibility and control of certain business functions to a third-party provider, but ultimate responsibility for information security still rests with the organization. Therefore, an escalation process helps maintain security posture and communication and accountability between the organization and the outsourcing provider.

upvoted 3 times

HughJassole 1 year, 6 months ago

The question doesn't mention what is being outsourced, so D might not be applicable. What if you're outsourcing the cafeteria?

A seems to be the best answer, I once used a contractor to do construction and he subcontracted work, it had to be redone. Avoid subcontractors if you can.

upvoted 2 times

dmo_d 1 year, 7 months ago

Selected Answer: D

I'm going for D.

Subcontractors aren't the HIGHEST concern. Yes, it elevates the risks. But, without proper incident handling "our" business could make huge losses. Therefore this is the highest priority of the given options.

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: D

According to the International Association of Computer Science and Information Technology (IACSIT), the outsourcing agreement provision with the highest priority from a security operations perspective is the escalation process for problem resolution during incidents. This is because it is important for organizations to have a clear and efficient process in place for resolving problems that may arise during an incident, in order to minimize the impact on the organization and maintain the security of its systems and data. Other provisions, such as those related to subcontracting and contract renegotiation, may also be important for ensuring the security and integrity of the organization's systems, but the escalation process for problem resolution is typically considered the most critical from a security operations perspective.

upvoted 2 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

oudmaster 2 years ago

If Third-Party Governance process is well managed, then A is excluded.

I would go with D.

upvoted 1 times

sphenixfire 2 years ago

Selected Answer: A

very unclear state questions. anoying. I go for a, most of the rest is not security but system operations

upvoted 2 times

dmo_d 1 year, 7 months ago

Information security incidents have noot necessarily to do with systems operations.

An incident could be that the outsourcing contractor looses some sensitive hardcopy information. This would be covered by proper incident handling.

upvoted 1 times

Jamati 2 years, 1 month ago

Selected Answer: D

Agreed, D

upvoted 1 times

sec_007 2 years, 2 months ago

Selected Answer: A

Will go with A.

Subcontracting increases security risk and compliance perimeter, and ensuring everything is compliant from security point of view is highest priority.

Reference: https://softwarehut.com/blog/it-outsourcing/outsourcing-contract-clauses

upvoted 1 times

dmo_d 1 year, 7 months ago

sure about that?

For me it is more important that the subcontractors are carefully selected.

And much more important is that there is proper incident handling. No one likes if the contractor doesn't provide emergency contact details or handles high priority incidents very slowly.

upvoted 2 times

BDSec 2 years, 3 months ago

Selected Answer: D

D first, A would be second

upvoted 2 times

matt1976 2 years, 3 months ago

you are correct, its A. Not quite sure what I was thinking there.

upvoted 1 times

matt1976 2 years, 3 months ago

Geez, I mean D. Someone give me a drink

upvoted 7 times

CuteRabbit168 2 years, 3 months ago

Selected Answer: D

Selecting D. Question is from security operations (SOC ?) perspective

upvoted 3 times

matt1976 2 years, 3 months ago

Answer is A. Its pretty obvious

upvoted 2 times

Question #214 *Topic 1*

Which of the following is the MOST comprehensive Business Continuity (BC) test?

A. Full interruption

B. Full simulation

C. Full table top

D. Full functional drill

Suggested Answer: *A*

Community vote distribution

A (83%) B (17%)

djedwards 1 week, 4 days ago

Selected Answer: B

The most comprehensive Business Continuity (BC) test among the options provided is "B. Full simulation." A full simulation test involves simulating a real-life disaster scenario to test the organization's response and recovery capabilities.

upvoted 1 times

BigITGuy 3 months ago

Selected Answer: A

A full interruption test is the most comprehensive form of Business Continuity (BC) testing because it involves completely shutting down normal operations

upvoted 1 times

ayadmawla 5 months, 1 week ago

Selected Answer: B

The question is asking for BC not DR
A full simulation test is a business continuity plan (BCP) test that activates the entire BCP. It's a hands-on exercise that mimics a real disaster or disruptive event.

Full interruption test, aka full interruption test, used in disaster recovery testing
as it evaluates an organization's ability to respond to a disruption

upvoted 2 times

> **J_Ko** 3 months ago
>
> Could if be due to, as per the AIO 9th edition p. 101: "BCP and DRP plans are related but different. The DRP is a subset of the BCP & is focussed on the immediate aftermath of a disaster. BCP is much broader & covers any disruption including (but not limited to) disasters."
> So if you see DR as a subset of BC you can see it as correct but it does feel like a bit of a stretch, though "most comprehensive" might be a hint.
> I chose A but mainly because in the AIO I could not remember having read anything about the Full simulation test, only the "regular" simulation.
>
> upvoted 1 times

629f731 11 months, 3 weeks ago

Selected Answer: A

A. de key word is "MOST comprehensive"

upvoted 1 times

Soleandheel 1 year ago

The most comprehensive Business Continuity (BC) test among the options provided is "B. Full simulation." A full simulation test involves simulating a real-life disaster scenario to test the organization's response and recovery capabilities. This type of test is the most rigorous and closely mimics actual emergency situations, allowing for a thorough evaluation of the effectiveness of the business continuity plan. It typically involves the participation of various stakeholders and can be resource-intensive, but it provides the most realistic assessment of an organization's readiness for a crisis.

upvoted 1 times

> **Soleandheel** 1 year ago
>
> Actually, I change my answer to A. Full Interruption. Full interruption is the MOST Comprehensive of all. However, if we want to avoid disrupting business during the BC test, then B. Full simulation will make more sense. Based on the question, A. Full interruption is the correct answer.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: B

"Full simulation" is not expressly metioned in official ISC2 documents, only the "simulation" and "full interruption".

However, full simulation test is considered the most comprehensive test in disaster recovery guidelines.
Quote: "Full Simulation activates the total business continuity plan. The purpose is to simultaneously test as many components as possible in the organization recovery structure. "
Quote: "Full Simulation Test is the ultimate business continuity plan test which activates the total business continuity plan."

A full simulation test involves the entire organization and simulates a disaster scenario, allowing the organization to test its BC plans and procedures across all departments and functions. This type of test is the most comprehensive because it exercises all aspects of the BC plan, including communication, evacuation, recovery, and restoration.

A full interruption test, on the other hand, involves shutting down a system or process to test the effectiveness of the IT Disaster Recovery Plan (ITDRP) and it does not exercise the full range of BC plans and procedures.
upvoted 2 times

l00t 1 year, 10 months ago

Selected Answer: A

Plan Testing includes:

Checklist or Desk Check -- Give each business a copy of the plan, habe them run through a checklist to make sure all relevant points are covered.
Structured walk trough -- Representatives get together in a meeting and review the plan collectively.
Simulation -- A practical drill, mobilizing the personnel.
Parallel -- An operational test at the alternate site, running parallel to production.
Full Interruption -- Shut down the production environment and run a live environment at the alternate site. (Need to have prio: 1) Written management permission 2) At least a parallel testing beforehand)
upvoted 4 times

jackdryan 1 year, 7 months ago

A is correct
upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: A

obvious A if you read the book. I would not know exactly where buti believe it to be the following in order from least to most impact:
Review of procedures
Tabletop Review
Simulation
Parallel
Full Interuption
upvoted 1 times

DJOEK 1 year, 11 months ago

I mean document review as the top one
upvoted 1 times

rdy4u 2 years, 2 months ago

Selected Answer: A

A Full Interruption Test is an exercise which all recovery procedures and strategy are tested. It actually replicates a disaster by halting production.

https://www.bcmpedia.org/wiki/Test_-_Full_Interruption
upvoted 4 times

Question #215 *Topic 1*

A security practitioner needs to implement a solution to verify endpoint security protections and operating system (OS) versions. Which of the following is the
BEST solution to implement?

A. An intrusion prevention system (IPS)

B. Network Access Control (NAC)

C. Active Directory (AD) authentication

D. A firewall

Suggested Answer: *B*

Community vote distribution

B (100%)

74gjd_37 9 months, 1 week ago

Selected Answer: B

There is a chapter on "Network Access Control" in the official ISC2 CBK reference (6th Edition), page 352-354 which explicitly explains why option B is correct.

upvoted 2 times

[Removed] 10 months, 1 week ago

I feel like the last eight questions are from a person that was completely failing the test. A little too easy. When completely failing the test will start throwing easy questions at you until you fail at 125.

upvoted 1 times

> **homeysl** 8 months, 2 weeks ago
>
> did you pass the exam?
>
> upvoted 1 times

DJOEK 1 year, 5 months ago

Selected Answer: B

NAC as there is no better solution. You can allow or deny access to a network based on the characters asked

upvoted 2 times

> **jackdryan** 1 year, 1 month ago
>
> B is correct
>
> upvoted 1 times

sphenixfire 1 year, 6 months ago

Selected Answer: B

correct would be a monitoring system for endpoints (f.e. scom). but NAC would be the nearest solution because it ensures that only maintained devices are on the nework. just another question to make money with failed cissp exams...

upvoted 4 times

Jamati 1 year, 7 months ago

Selected Answer: B

NAC such as posture validation systems will do the trick.

upvoted 2 times

Question #216 *Topic 1*

During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are identified. In which of the following management stages are nonconformities reviewed, assessed and/or corrected by the organization?

A. Assessment

B. Planning

C. Improvement

D. Operation

Suggested Answer: *D*

Community vote distribution

C (76%) D (24%)

⊟ **wook33** Highly Voted 👍 2 years, 1 month ago

WTF is a nonconformity? Why do they have to use these words

upvoted 15 times

⊟ **sphenixfire** 2 years ago

anoying quewstin but it refers to the iso27001 audit findings. a non comfirmity is a finding you need to act on (next to notice). see iso 27001 guide you will find ;)

as I rember it is not a thing of risk assessment or treatment, it is a thing regarding to the improvement of the isms itself (act) therefore improvment.

upvoted 5 times

⊟ **jackdryan** 1 year, 7 months ago

C is correct

upvoted 1 times

⊟ **BoZT** 1 year, 3 months ago

If you ever went through a internal audit, that's a pretty common word.

upvoted 3 times

⊟ **BigITGuy** Most Recent ⊙ 2 months, 4 weeks ago

Selected Answer: C

NOT D. Operation refers to the day-to-day functioning of the ISMS, not specifically to the correction of audit findings.

upvoted 1 times

⊟ **Soleandheel** 1 year ago

C. Improvement Stage

During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are reviewed, assessed, and corrected during the C. Improvement stage. This is evident from the ISO 27001 standard, which requires management reviews to be conducted to ensure the ISMS and its objectives remain suitable, adequate, and effective.

upvoted 1 times

⊟ **74gjd_37** 1 year, 3 months ago

Selected Answer: C

According to ISO-27001, the Improvement stage involves identifying areas for improvement, implementing corrective actions, and continually monitoring and reviewing the ISMS to ensure it remains effective and meets changing organizational needs and objectives.

upvoted 3 times

⊟ **Dee83** 1 year, 11 months ago

During an internal audit of an organizational Information Security Management System (ISMS), nonconformities are reviewed, assessed and/or corrected by the organization in the Improvement stage. (Option C)

upvoted 1 times

⊟ **DJOEK** 1 year, 11 months ago

Selected Answer: C

The answer is C. Improvement. According to the ISO/IEC 27001 standard, which is a widely recognized international standard for information security management systems, the improvement stage is where nonconformities are reviewed, assessed, and corrected by the organization. The purpose of this stage is to identify opportunities for improving the ISMS, including addressing any identified nonconformities. This is an ongoing process that helps the organization continuously improve its information security posture.

Planning
Implementation
Operation
Review
Improvement

upvoted 3 times

⊟ **rajkamal0** 2 years ago

Selected Answer: C

Corrective action in operations is wrong.

The process of correcting errors and taking corrective action can lead to new opportunities for improvement. The situation should be dealt with accordingly. It is necessary to retain sufficient documentation to demonstrate that the organization has dealt with the nonconformity appropriately and that the consequences have been addressed.

Reference:

https://www.solutions-inc.co.uk/iso-27001-clause-10-1-nonconformity-and-corrective-action/

upvoted 3 times

⊟ **Jay327** 2 years, 1 month ago

Selected Answer: C

C
https://www.isms.online/iso-27001/10-1-nonconformity-and-corrective-action/

The corrective action that follows from a nonconformity is also a key part of the ISMS improvement process that needs to be evidenced along with any other consequences caused by the nonconformity.

upvoted 4 times

⊟ **rdy4u** 2 years, 2 months ago

Selected Answer: D

ISO 27001 Clause 10.1 Non conformity and corrective action, Clause 10 containing sections 10.1 and 10.2 covers the “Act” part W. Edwards Deming’s Plan-Do-Check-Act (PDCA) cycle. This clause helps an organisation react to nonconformities, evaluate them and take corrective actions with the end goal of continually improving how it runs its daily activities.

https://info-savvy.com/iso-27001-clause-10-1-non-conformity-and-corrective-action/

upvoted 4 times

Question #217 *Topic 1*

When developing an external facing web-based system, which of the following would be the MAIN focus of the security assessment prior to implementation and production?

A. Ensuring Secure Sockets Layer (SSL) certificates are signed by a certificate authority

B. Ensuring Secure Sockets Layer (SSL) certificates are internally signed

C. Assessing the Uniform Resource Locator (URL)

D. Ensuring that input validation is enforced

Suggested Answer: *A*

Community vote distribution

D (70%) A (30%)

BDSec Highly Voted 2 years, 3 months ago

Selected Answer: D

SSL certificates are insecure. Injection/buffer overflow attacks are major attack vectors.

upvoted 9 times

sphenixfire 2 years ago

statement is wrong. first, it's not an ssl but a x509 certificate and it is secure by securing the transport layer. and it is considered by implementation, therefore d is correct. injections etc. are part of L7 protections like input validation

upvoted 1 times

jackdryan 1 year, 7 months ago

D is correct

upvoted 1 times

franbarpro Highly Voted 2 years, 2 months ago

Selected Answer: D

input validation is the security of alot of application related attacks. Check out the OWASP top 10

upvoted 8 times

BigITGuy Most Recent 3 months ago

Selected Answer: D

Can't be A. Ensuring SSL certificates are signed by a certificate authority is important for encryption and trust, but it doesn't directly protect against application-level attacks.

upvoted 1 times

SangSang 5 months, 1 week ago

Selected Answer: D

With A, not signing your SSL with CA doesn't mean you do not encrypt. But without input validation, you really getting trouble with the failure of security assessment.

upvoted 1 times

homeysl 9 months, 2 weeks ago

Selected Answer: A

Cryptographic failure is #2 after Broken Access Control in OWASP Top 10.

https://owasp.org/www-project-developer-guide/draft/training_education/owasp_top_ten/

upvoted 1 times

maawar83 1 year ago

I would say A. web-based System (is pretty generic that I could have additional components)... in addition, the main focus of the developer during the security assessment is ensuring that base line are met.. which is SSL Certificates are signed by certificate authority. Thinking CIA concept more than security.

upvoted 1 times

Soleandheel 1 year ago

D. Ensuring that input validation is enforced. Think like a manager.

upvoted 1 times

74gjd_37 1 year, 3 months ago

Selected Answer: D

Ensuring that SSL certificates are signed by a certificate authority is an important aspect of web application security, but it can be done at any stage of the development cycle or even after implementation. On the other hand, ensuring that input validation is enforced is critical to the security of web applications, and it should be a primary focus of the security assessment prior to implementation and production. The earlier input validation is implemented in the development cycle, the easier it is to prevent potential security vulnerabilities and attacks.

upvoted 6 times

[Removed] 1 year, 8 months ago

Selected Answer: D

Just don't use SSL anymore. Therefore answer definately should be D.

upvoted 1 times

bsongwk 1 year, 9 months ago

Selected Answer: A

All external web-based system must have public signed certs.

upvoted 2 times

Dee83 1 year, 11 months ago

D- answer

When developing an external facing web-based system, the main focus of the security assessment prior to implementation and production would be D. Ensuring that input validation is enforced.

Input validation is a critical aspect of web application security, as it helps to prevent malicious users from injecting harmful code or data into the system. Input validation can help protect against a wide range of attacks, including SQL injection, cross-site scripting (XSS), and command injection.

upvoted 1 times

DJOEK 1 year, 11 months ago

Selected Answer: D

The main focus of the security assessment prior to implementation and production of an external facing web-based system would be ensuring input validation is enforced, as this helps prevent attacks such as injection attacks, which can allow attackers to execute malicious code or access sensitive information. Ensuring SSL certificates are signed by a certificate authority and assessing the URL are also important considerations, but they are not the main focus of the security assessment. Ensuring SSL certificates are internally signed is not relevant to the security assessment of an external facing web-based system.

upvoted 1 times

oudmaster 2 years ago

Selected Answer: A

D should not be the answer. Because what if that web based application is not made to allow users to insert data? Then input validation is not required. But SSL certificate is always required for websites published to the internet.

upvoted 3 times

zelda923 1 year, 12 months ago

I really like your reasoning but the same logic applies for "A" as well. What if the website doesn't use cookies, doesn't have a user login functionality, and doesn't allow users to enter data? In this case, certificates won't be necessary as well.

upvoted 1 times

dmo_d 1 year, 7 months ago

TLS(SSL) provides protection against MitM-attacks.

It is a common misunderstanding that you might only need transport encryption when the user transfers data or the websites provides sensible data.

But what about an attacker who is modifying a trustworthy static website by injecting malicous code which is then executed in the users browser?

It is the same reason why you hardly find unencrypted FTP downloads nowadays (most users won't do a hashsum check).

upvoted 1 times

marziparzi 9 months ago

"But what about an attacker who is modifying a trustworthy static website by injecting malicous code which is then executed in the users browser?"

I don't think SSL/TLS would provide protection on that. How would SSL/TLS even protect against that?
TLS used in a public website is not mutual authentication (but there can be mutual TLS in other applications that use TLS). It only authenticates the web server but not the client. So, a web server does not authenticates whether it's a valid user or not. I'm assuming when we say "external facing web-based system", we're building the web server, not the client.

TLS is not very important if your attacker is not a man in the middle but actually the end-user. (But if it's a mutual TLS, then there's some point to be made)
upvoted 1 times

sphenixfire 2 years ago

Selected Answer: D

has notthing to do with certificatees. input validation you need to cover while dev. so, its d.
upvoted 1 times

juniorhs86 2 years, 1 month ago

Selected Answer: A

I would say A. because there is no mentioning about security of the website self. So D is not the answer because first step is HTTPS so A. HTTP with answer D looks weird to me
upvoted 5 times

sec_007 2 years, 2 months ago

Selected Answer: D

Prior to implementation and production means we can only enforce input validation. Reast all options are either production or implementation related. Knocking out B as it does not make any sense.
upvoted 3 times

[Removed] 2 years, 2 months ago

to me the key words here are "prior to", SSL is something you would configure during the implementation into production (as it's transitioning from the test environment), so to me, would be part of the provisioning/implementation process... I would certainly want to make sure the web app doesn't accept malformed input which could lead to confidentiality issues after deployment...
upvoted 3 times

Question #218 *Topic 1*

A financial services organization has employed a security consultant to review processes used by employees across various teams. The consultant interviewed a member of the application development practice and found gaps in their threat model. Which of the following correctly represents a trigger for when a threat model should be revised?

A. After operating system (OS) patches are applied

B. A new developer is hired into the team.

C. After a modification to the firewall rule policy

D. A new data repository is added.

Suggested Answer: *D*

Community vote distribution

D (100%)

74gjd_37 9 months, 1 week ago

Selected Answer: D

The correct answer is D. While the other factors (A, B, C) can impact the security of a system, they may not necessarily require a revision of the threat model unless they introduce new potential threats that were not previously considered. The addition of a new data repository, on the other hand, can change the threat landscape of the system and introduce new potential threats that were not previously considered, making it a more likely trigger for revising the threat model.

upvoted 4 times

DJOEK 1 year, 5 months ago

Selected Answer: D

the other options seem of too little impact compared to D

upvoted 1 times

jackdryan 1 year, 1 month ago

D is correct

upvoted 1 times

oudmaster 1 year, 6 months ago

Selected Answer: D

A new data repository is added, means a new a attack surface.
threat Model should be reviewed and revised if needed.

upvoted 2 times

sec_007 1 year, 8 months ago

Selected Answer: D

D is correct.
Adding a new data repository affects the attack vector.

upvoted 2 times

Rollizo 1 year, 9 months ago

Selected Answer: D

"interviewed a member of the application development", then it is related with application modification => new repository

upvoted 2 times

Question #219 *Topic 1*

The Chief Information Security Officer (CISO) of an organization has requested that a Service Organization Control (SOC) report be created to outline the security and availability of a particular system over a 12-month period. Which type of SOC report should be utilized?

A. SOC 1 Type 1

B. SOC 1 Type 2

C. SOC 2 Type 2

D. SOC 3 Type 1

Suggested Answer: *C*

Community vote distribution

C (100%)

ServerBrain 3 months, 2 weeks ago

Selected Answer: C

SOC 2 Type 2

upvoted 1 times

homeysl 8 months, 2 weeks ago

There's no SOC1 Type1

upvoted 1 times

jackdryan 1 year, 1 month ago

C is correct

upvoted 1 times

DJOEK 1 year, 5 months ago

Selected Answer: C

SOC 2 security related, SOC 3 is for the outside world and SOC 1 is for the financial controls

upvoted 2 times

rdy4u 1 year, 8 months ago

Selected Answer: C

While the SOC 2 Type I report signifies that security controls are in place at a particular point in time, the Type II Report validates the presence of the controls over a period of time.

https://www.oslash.com/learning-center/how-to-fast-track-soc-2-compliance-for-your-startup-the-ultimate-guide

upvoted 4 times

Question #220 *Topic 1*

An organization recently upgraded to a Voice over Internet Protocol (VoIP) phone system. Management is concerned with unauthorized phone usage. The security consultant is responsible for putting together a plan to secure these phones. Administrators have assigned unique personal identification number (PIN) codes for each person in the organization. What is the BEST solution?

A. Have the administrator enforce a policy to change the PIN regularly. Implement call detail records (CDR) reports to track usage.

B. Have the administrator change the PIN regularly. Implement call detail records (CDR) reports to track usage.

C. Use phone locking software to enforce usage and PIN policies. Inform the user to change the PIN regularly.

D. Implement call detail records (CDR) reports to track usage.

Suggested Answer: *A*

Community vote distribution

A (91%) 9%

RRabbit_111 6 months, 4 weeks ago

Selected Answer: C

i think the goal is to secure phones from unauth usage and you have to lock the phones down. It doesnt say that (A) locks it down. the CDR reports tracks usage but that doesnt prevent usage.

upvoted 2 times

74gjd_37 1 year, 9 months ago

Selected Answer: A

The best solution is Option A because it ensures that the PIN codes are changed regularly, making it difficult for unauthorized users to access the phone system; additionally, implementing call detail records (CDR) reports allows for tracking of phone usage, which can be used to identify any unauthorized usage and take appropriate action. Option C, using phone locking software, may be a good additional measure, but it is not a complete solution on its own. Option B, having the administrator change the PIN regularly, is not practical as it would be difficult to manage and may cause confusion for users. Option D, implementing CDR reports alone, does not address the issue of unauthorized usage and does not provide a way to prevent it in the first place.

upvoted 3 times

liebeskind 2 years, 1 month ago

can a "Unique" personal ID number be changed arbitrarily? what if two users picked a same PIN? how to distinguish them?

upvoted 2 times

jackdryan 2 years, 1 month ago

A is correct

upvoted 1 times

DJOEK 2 years, 5 months ago

Selected Answer: A

The best solution would be to have the administrator enforce a policy to change the PIN regularly and implement call detail records (CDR) reports to track usage. This would help to prevent unauthorized phone usage and allow the organization to monitor and track usage. Option A would be effective in securing the VoIP phones and ensuring that they are being used appropriately.

upvoted 2 times

rajkamal0 2 years, 6 months ago

Selected Answer: A

A is correct

upvoted 2 times

Ivanchun 2 years, 6 months ago

Selected Answer: A

A vs B, A is enforce - best solution

upvoted 3 times

Li_Rong_Han 2 years, 6 months ago

Did you notice the catch in the answers for A and B?

A is to enforce a policy (Applies to all users) to change the PIN regularly.