



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

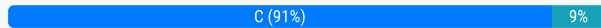
- CertificationTest.net - Cheap & Quality Resources With Best Support

Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?

- A. Security regression testing
- B. Code review
- C. User acceptance testing
- D. Stress testing

Suggested Answer: D

Community vote distribution



amateurguy Highly Voted 2 years, 9 months ago

what just happened? were the questions changed or what? yesterday we had like 291 questions and now we have around 200 and they are completely different. Did comptia change the exam?

upvoted 11 times

Laudy 2 years, 9 months ago

Taking my test in a few hours. I'll report back what it looks like compared to the new questions.

upvoted 5 times

mindhunterX 2 years, 9 months ago

Are the correct answers the voted ones or the ones from the simulation?

upvoted 1 times

Inasepl 2 years, 9 months ago

Same question here!

upvoted 3 times

Laudy Highly Voted 2 years, 9 months ago

Just finished. Passed. About 57 of the 70 questions were listed here. The other 13 weren't too different for the stuff here.

One question on TDEA/TDES(3DES) vs AES-256.

Sadly I forgot the other one that stood out. My bad y'all. Best of luck!!

upvoted 9 times

bigerblue2002 2 years, 9 months ago

Is this 57 from this set or the original set of questions that were here before they changed them?

upvoted 1 times

m025 Most Recent 1 year, 6 months ago

Selected Answer: C

It's a UAT

upvoted 1 times

Sharecyber 1 year, 7 months ago

Selected Answer: C

Key word is usability

upvoted 2 times

chaddman 1 year, 8 months ago

Selected Answer: C

User Acceptance Testing (C): This type of testing involves end-users trying out various scenarios to make sure that the software meets the base requirements in terms of function and usability.

upvoted 1 times

CySAIsHard 1 year, 8 months ago

Selected Answer: C

functionality and usability, definitely falls in line with UAT.

upvoted 1 times

🗨️ 👤 **AlkindyMary** 2 years ago

Please any one passed the exam, Did you relay on the answers from the discussion or the once provided by the website??

Please respond to me urgently. As I the answers vary from one site to another. Not sure which site give the correct answers to the exam questions

upvoted 1 times

🗨️ 👤 **Lungful** 1 year, 8 months ago

If the discussion posts have sources, you read through the sources, and you can find the answer referenced. Then definitely follow the answers in the discussions. Never blindly follow any of the selected answers. Do a little bit of reading to check.

upvoted 1 times

🗨️ 👤 **blehbleh** 2 years, 3 months ago

Hello everyone,

I just passed this. I think only two questions were not from this dump. All of my pbqs were in the dump. I passed with an 800. I wish all of you the best of luck. Everything on this dump is relevant. Study hard and you will pass!

upvoted 5 times

🗨️ 👤 **wdarden2** 2 years, 3 months ago

What answers did you go with? The site generated ones or the answers provided by the community.

upvoted 3 times

🗨️ 👤 **Jacobmy98** 2 years, 3 months ago

did you go with the user answers ?

upvoted 2 times

🗨️ 👤 **bmac1984** 2 years, 1 month ago

Hey, congratulations on passing. Can you help me and let me know if you went for the most voted answers or the answer highlight in green?

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

This is definitely UAT

upvoted 2 times

🗨️ 👤 **Joe00** 2 years, 4 months ago

Passed this exam recently. Be sure to study mostly after the update on these questions. The PBQ's were all there including 1 from CS0-001 version. They also added more questions early in Feb 2023. Solid study guide, but do some hw and cross reference a little to verify answers

upvoted 2 times

🗨️ 👤 **DrVoIP** 2 years, 4 months ago

C. User acceptance testing is the software development process by which function, usability, and scenarios are tested against a known set of base requirements. User acceptance testing (UAT) is the final stage of testing before a software product is released to the market, and it is designed to ensure that the software meets the needs of its intended users. - ChatGPT

upvoted 2 times

🗨️ 👤 **Davar39** 2 years, 4 months ago

Lets ask the chat bot:

The software development process you are referring to is likely to be Acceptance Testing. Acceptance testing is a type of software testing that is performed to verify if a system meets the specified requirements and is ready for delivery to the end-users or clients.

upvoted 1 times

🗨️ 👤 **Joe00** 2 years, 5 months ago

for those who already took exam recently, how many questions actually came from new updated question bank?

upvoted 2 times

🗨️ 👤 **iraidesc** 2 years, 5 months ago

Selected Answer: D

Stress testing (sometimes called torture testing) is a form of deliberately intense or thorough testing used to determine the stability of a given system, critical infrastructure or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.

upvoted 1 times

🗨️ 👤 **Elbasilisk** 2 years, 6 months ago

Passed this one... very few questions from here.

upvoted 2 times

🗨️ 👤 **acbd** 2 years, 5 months ago

About how many would you say were actually on the exam?

upvoted 1 times

🗨️ 👤 **sho123** 2 years, 6 months ago

Selected Answer: D

it is against known set principle i.e beyond known set principle

upvoted 1 times

🗨️ 👤 **Cizzla7049** 2 years, 7 months ago

Selected Answer: C

user acceptance

upvoted 1 times

A security analyst discovers the following firewall log entries during an incident:

Source	Destination	Destination port	Bytes	Flags
10.0.30.100	10.0.40.20	21	0	syn
10.0.30.100	10.0.40.20	22	0	syn
10.0.30.100	10.0.40.20	80	0	syn
10.0.30.100	10.0.40.20	443	0	syn
10.0.30.100	10.0.40.20	3389	0	syn
10.0.30.100	10.0.40.20	445	0	syn

Which of the following is MOST likely occurring?

- A. Banner grabbing
- B. Port scanning
- C. Beaconsing
- D. Data exfiltration

Suggested Answer: C

Community vote distribution

B (95%)

5%

🗳️ 👤 **AlexR76** Highly Voted 2 years, 8 months ago

Selected Answer: B

This is a typical SYN scan. Beaconsing is when the malware communicates with a C2 server asking for instructions or to exfiltrate collected data on some predetermined asynchronous interval

upvoted 17 times

🗳️ 👤 **Joluve** Most Recent 1 year, 3 months ago

Selected Answer: B

multiple ports and zero data tranfered

upvoted 1 times

🗳️ 👤 **Achilles69** 1 year, 4 months ago

Zero data transferred: port scanning

upvoted 1 times

🗳️ 👤 **m025** 1 year, 6 months ago

Selected Answer: B

It's a port scanning, there sin't nothing of others

upvoted 1 times

🗳️ 👤 **CySAlsHard** 1 year, 8 months ago

Selected Answer: B

Port Scanning ftw

upvoted 1 times

🗳️ 👤 **Ayben** 1 year, 8 months ago

Selected Answer: B

This is port scanning.

upvoted 2 times

🗳️ 👤 **rphadol** 1 year, 9 months ago

definetly port Scanning

upvoted 1 times

🗳️ 👤 **ReaperDeathSeal** 1 year, 11 months ago

This is port scanning.

upvoted 3 times

🗳️ 👤 **Temickey** 2 years, 2 months ago

I strongly believe that this is port scanning
upvoted 4 times

🗨️ 👤 **JokerRWild** 2 years, 2 months ago

Why is the answer wrong. Is this meant to spark a discussion with the community?
upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

This is typical port scanning, most beacons will use specific ports and will not show this type of behavior.
upvoted 3 times

🗨️ 👤 **omer123456** 2 years, 4 months ago

Selected Answer: B

I think it is port scan not beaconing
upvoted 1 times

🗨️ 👤 **iraidesc** 2 years, 5 months ago

Selected Answer: C

In networking, beaconing is a term used to describe a continuous cadence of communication between two systems. In the context of malware, beaconing is when malware periodically calls out to the attacker's C2 server to get further instructions on tasks to perform on the victim machine.
upvoted 2 times

🗨️ 👤 **kopib21961** 2 years, 6 months ago

I also think the answer is C.
upvoted 1 times

🗨️ 👤 **kopib21961** 2 years, 6 months ago

Sorry I meant Port Scanning NOT beaconing
upvoted 2 times

🗨️ 👤 **sho123** 2 years, 6 months ago

Selected Answer: B

it is Syn - 3 way tcp handshake has not yet completed. it is port scan
upvoted 2 times

🗨️ 👤 **AndyM112** 2 years, 8 months ago

B: SYN Scan, sometimes called half-open scanning
upvoted 2 times

🗨️ 👤 **35nerd7** 2 years, 8 months ago

B. Port scanning makes the most sense.
upvoted 2 times

A security analyst is revising a company's MFA policy to prohibit the use of short message service (SMS) tokens. The Chief Information Officer has questioned this decision and asked for justification. Which of the following should the analyst provide as justification for the new policy?

- A. SMS relies on untrusted, third-party carrier networks.
- B. SMS tokens are limited to eight numerical characters.
- C. SMS is not supported on all handheld devices in use.
- D. SMS is a cleartext protocol and does not support encryption.

Suggested Answer: D

Community vote distribution

D (71%)

A (29%)

🗳️ **ce797c7** 1 year, 4 months ago

D. SMS is a cleartext protocol and does not support encryption.

The primary justification for prohibiting the use of SMS tokens in a Multi-Factor Authentication (MFA) policy is the lack of security associated with SMS. SMS is considered less secure for several reasons, and one significant concern is that it is transmitted in cleartext, meaning the information is not encrypted during transmission. This makes it more vulnerable to interception and eavesdropping.

Option A (SMS relies on untrusted, third-party carrier networks) is also a valid concern and relates to the potential for interception or SIM swapping attacks. However, the lack of encryption (Option D) directly speaks to the inherent security weakness in using SMS for authentication.

upvoted 1 times

🗳️ **m025** 1 year, 6 months ago

Selected Answer: D

The point is the is cleartext protocol so everything can be seen

upvoted 1 times

🗳️ **samsuna** 1 year, 6 months ago

Key word "A security analyst is revising" which means

If the company is already using Multi-Factor Authentication (MFA) but is considering revising the policy to prohibit the use of SMS tokens, the justification can be based on security concerns associated with SMS. In this case, the analyst should provide reasoning for discontinuing the use of SMS tokens despite their existing implementation. The most suitable justification would be:

D. SMS is a cleartext protocol and does not support encryption.

upvoted 1 times

🗳️ **respect9602** 2 years, 1 month ago

Selected Answer: A

I hate this question and I hate all the idiots on this thread. SMS tokens are the weakest MFA because of SIM swapping attacks. SIM swapping attacks happen from insider attacks or social engineering attacks at third party carriers. Third party carriers are untrusted a-holes that will carelessly port your number for an impersonator or take a bribe.

upvoted 3 times

🗳️ **CySAIsHard** 1 year, 8 months ago

I believe it's D. Sure SMS can branch into being housed by a untrusted 3rd party provider, but SMS itself can be picked up by eavsdropping, mitm attacks due to plaintext.

upvoted 2 times

🗳️ **adrian1188** 2 years, 1 month ago

Selected Answer: A

A. SMS relies on untrusted, third-party carrier networks is the most appropriate justification for prohibiting the use of SMS tokens as part of a company's MFA policy.

upvoted 2 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: D

Agreed, this is D.
upvoted 1 times

  **alayeluwa** 2 years, 4 months ago



This one is tricky
upvoted 1 times

  **DrVoIP** 2 years, 4 months ago

A. SMS relies on untrusted, third-party carrier networks is the most appropriate justification for prohibiting the use of SMS tokens as part of a company's MFA policy.

SMS tokens are a form of two-factor authentication (2FA) that relies on a text message being sent to the user's mobile phone. However, this method has been criticized for its security limitations, including the reliance on untrusted, third-party carrier networks to transmit the text message. These networks are vulnerable to interception and can be compromised by attackers, making SMS tokens less secure than other forms of 2FA, such as hardware tokens or mobile authentication apps. - ChatGPT

upvoted 4 times

  **RCA** 2 years, 7 months ago

Selected Answer: D

The correct answer is D.
upvoted 1 times

  **IT_Master_Tech** 2 years, 8 months ago

Strings sounds better.



<https://www.javatpoint.com/linux-strings-command>

upvoted 2 times

  **Cizzla7049** 2 years, 9 months ago

Selected Answer: D

D is right
upvoted 3 times

  **EVE12** 2 years, 9 months ago

Selected Answer: D

SMS/MMS/Messaging

Short Message Service (SMS) is a text messaging service component of most telephone, World Wide Web, and mobile telephony systems. Multimedia Messaging Service (MMS) handles messages that include graphics or videos. Both technologies present security challenges. Because messages are sent in clear text, both are susceptible to spoofing and spamming.

upvoted 4 times

  **EAart** 2 years, 9 months ago

Selected Answer: D

<https://techcrunch.com/2018/12/25/cybersecurity-101-guide-encrypted-messaging-apps/>
upvoted 1 times

  **Laudy** 2 years, 10 months ago

Selected Answer: D

CompTIA proper doesn't seem to discuss "sms tokens", but from what I can gather, this question is asking about SMS OTP for SSO. Link discusses some of the concerns of that. Biggest issue, is that it's better to use an OTP App that uses encryption vs using plain text sms to deliver OTPs.
<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/authentication-methods/>



upvoted 1 times

  **justauser** 2 years ago

your own link...

"The use of SMS message, is generally considered to be less secure than other methods. It's relatively easy for someone to reassign a phone number so that the SMS message is redirected into another person's phone."

upvoted 2 times

  **m025** 1 year, 6 months ago

An the same said: Or it could be that the app is not using encryption, and that push notification is being sent to the phone, in the clear rather than using some type of protected mechanism. With the right app, however, this is a relatively safe process, and probably more secure than something like SMS

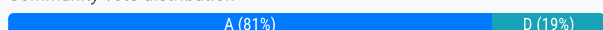
upvoted 1 times

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following should the analyst use to extract human-readable content from the partition?

- A. strings
- B. head
- C. fsstat
- D. dd

Suggested Answer: D

Community vote distribution



rodwave Highly Voted 2 years, 6 months ago

Selected Answer: A

Answer: strings

The strings command returns strings of printable characters in files. It's mainly used for extracting text (strings) from non-text files like binary/data files and help us understand the contents of the files.

Binary files can contain non-printable characters which doesn't work well with the terminal. We can assume printable characters means human-readable which works for the situation.

The dd (disk duplicator/destroyer) command is used in forensics for raw images of a system that can be used in tools like Autopsy or FTK for analysis. You can extract raw data with the command but it doesn't mean that the extracted data is human-readable so it doesn't mean it would work for the situation.

=====

Other Info:

head - command that prints the first line(s) in a file

fsstat - command shows file system information

upvoted 18 times

f405aa0 Most Recent 1 year, 7 months ago

Selected Answer: D

I would say D, since this is DURING an incident response, using dd will not modify any changes to files. Afterwards, then you can use the strings command

upvoted 1 times

NerdAlert 2 years, 2 months ago

Selected Answer: A

*"Strings" grabs and lists Strings of characters in a file, making it easy to notice human-readable words and phrases.

*"dd" is a command used to clone a hard drive and bit by bit copy (an image).

*"fststat" shows info about a File System (FS)

*"head" prints out the top of a file (the head)

upvoted 1 times

NerdAlert 2 years, 2 months ago

*meant to say "FSstat" = File System stats

answer is still Strings

upvoted 1 times

2Fish 2 years, 3 months ago

Selected Answer: A

Yup, this is Strings.

upvoted 3 times

🗳️ 👤 **boletri** 2 years, 4 months ago

Selected Answer: D

Answer is D.

Disassemblers and Decompilers

Disassemblers and decompilers are software that translate low-level machine language code into higher level code.

upvoted 1 times

🗳️ 👤 **Lunarr** 2 years, 4 months ago

Option D (dd) can be used to create a bit-by-bit copy of a partition, but it does not extract human-readable content. Answer is A - Strings

upvoted 2 times

🗳️ 👤 **DrVoIP** 2 years, 4 months ago

A. strings is the tool that can be used to extract human-readable content from a Linux swap partition. The Linux swap partition is used as virtual memory and contains data that has been swapped out of RAM to free up space. The data in the swap partition is not in a human-readable format, but it may contain fragments of files or other data that can be extracted using the "strings" tool. - ChatGPT

upvoted 1 times

🗳️ 👤 **encxorblood** 2 years, 5 months ago

Selected Answer: A

First can use dd to secure the disc as a image. But the answer is A - strings.

upvoted 1 times

🗳️ 👤 **mrodmv** 2 years, 7 months ago

Strings without doubt

<https://forensicswiki.xyz/wiki/index.php?title=Strings>

upvoted 1 times

🗳️ 👤 **Just2a** 2 years, 7 months ago

Linux partition uses strings

upvoted 1 times

🗳️ 👤 **Cizzla7049** 2 years, 7 months ago

Selected Answer: A

Some people said its A. unsure of this one

upvoted 1 times

🗳️ 👤 **Angie_1** 2 years, 7 months ago

dd is bit by bit disk image , so dd is a good choice

upvoted 1 times

🗳️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: A

question asks human readable context, so string provides it.

upvoted 1 times

🗳️ 👤 **Smolz** 2 years, 7 months ago

DD would be the most appropriate answer because we're being told its an incident response and as a rule of thumb when you conduct IR you need to clone your source evidence b4 any forencis investigation, then with the cloned image one can now mount it, after mounting thats when it becomes readable! So DD makes the most appropriate for this question your views are welcome.

upvoted 2 times

🗳️ 👤 **IT_Master_Tech** 2 years, 8 months ago

I have looked for answers about dd and it doesn't mention anywhere about human-readable text.

upvoted 2 times

🗳️ 👤 **CW4901** 2 years, 8 months ago

So in the Compitia CySA+ study guide book in chapter 18 under dd utility is says: "dd can duplicate data across files, devices, partitions, and volumes."

So would that make this answer "D"?

upvoted 2 times

🗳️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: A

Strings is the correct answer

upvoted 1 times

A consultant is evaluating multiple threat intelligence feeds to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

- A. Ask for external scans from industry peers, look at the open ports, and compare information with the client.
- B. Discuss potential tools the client can purchase to reduce the likelihood of an attack.
- C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
- D. Meet with the senior management team to determine if funding is available for recommended solutions.

Suggested Answer: A

Community vote distribution

C (90%)

10%

🗳️ **msey2** Highly Voted 2 years, 6 months ago

Selected Answer: C

A is an absurd answer. "Hi company B, I'm from your rival, company A. Would you mind giving us scans of your network so we can see which ports you keep open? It's not for anything sinister, I promise."

upvoted 29 times

🗳️ **kill_chain** 1 year, 12 months ago

no... a consultant is not working for company A or B. he is consulting for Company A and probably many others along with his peers. His peers in this case are fellow consultants who are also not attached to company A or B.

upvoted 3 times

🗳️ **Stiobhan** 2 years, 5 months ago

Love the feedback 🤔

upvoted 3 times

🗳️ **KhanhMicheal** Most Recent 9 months, 4 weeks ago

Selected Answer: C

why this so correct answer is A

upvoted 1 times

🗳️ **goku1** 2 years, 1 month ago

How do you "Look at attacks against similar industry peers"? You google it?

upvoted 2 times

🗳️ **JoInn** 2 years, 3 months ago

Selected Answer: A

I think the key word here is consultant.

They are looking for the best way to find out as much as possible, so actual scans would be it. They aren't asking competitors, but other consultants. This would be sharing, in the same fashion as threat intelligence. That's at least how I see it.

upvoted 2 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: C

C is the most reasonable answer here. Agree with msey2, A is absurd.

upvoted 2 times

🗳️ **DrVoIP** 2 years, 4 months ago

C. Look at attacks against similar industry peers and assess the probability of the same attacks happening would be the best approach for the consultant to consider when modeling the client's attack surface. By examining similar industry peers, the consultant can gain insight into what types of threats and attacks are most prevalent in that industry, and use that information to assess the potential risks for the client. This approach can help the consultant to identify which threats are most likely to impact the client and prioritize the resources needed to mitigate those risks. - ChtGPT

upvoted 3 times

🗳️ **prud31** 2 years, 7 months ago

Selected Answer: C

External scans details cannot be disclosed for comparison with other clients. This will be a security breach for a companies scan reports being accessible for comparison.

upvoted 3 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: C

this is about industry specific feeds about threat intelligence, so it should be C.

upvoted 4 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

You cannot just ask for External scans from peers. This needs approval and paperwork..it is not your peers that have been tasked with this job, it is you...Answer is C

upvoted 4 times

🗨️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: C

C is correct. Look for vuln and attacks that affect your industry the most

upvoted 2 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: C

I would say C. Asking scans from other companies would reveal their vulnerabilities and impossible to get.

upvoted 2 times

🗨️ 👤 **Belijmag** 2 years, 9 months ago

Selected Answer: C

It is C

upvoted 2 times

🗨️ 👤 **EAart** 2 years, 9 months ago

Selected Answer: A

A.

This answer satisfies the attack surface of the client and potential risks faced by industry.

upvoted 2 times

🗨️ 👤 **Adonist** 2 years, 9 months ago

Selected Answer: C

C makes more sense to me

upvoted 1 times

🗨️ 👤 **Laudy** 2 years, 10 months ago

Selected Answer: A

I'm really torn with A and C. Only picking A because it asks specifically asks about modelling their attack surface. This question seems like one of those stupid comptia questions where you shouldn't over think things....

With that said - if I was a consultant, I would rather perform C and help my client build and develop their network. Plus, just because others have a certain attack surface, it doesn't mean we should mirror it. It may not work for the client or simply be poorly configured. Smh.

upvoted 1 times

SIMULATION -

You are a penetration tester who is reviewing the system hardening guidelines for a company's distribution center. The company's hardening guidelines indicate the following:

- ⇒ There must be one primary server or service per device.
- ⇒ Only default ports should be used.
- ⇒ Non-secure protocols should be disabled.
- ⇒ The corporate Internet presence should be placed in a protected subnet.

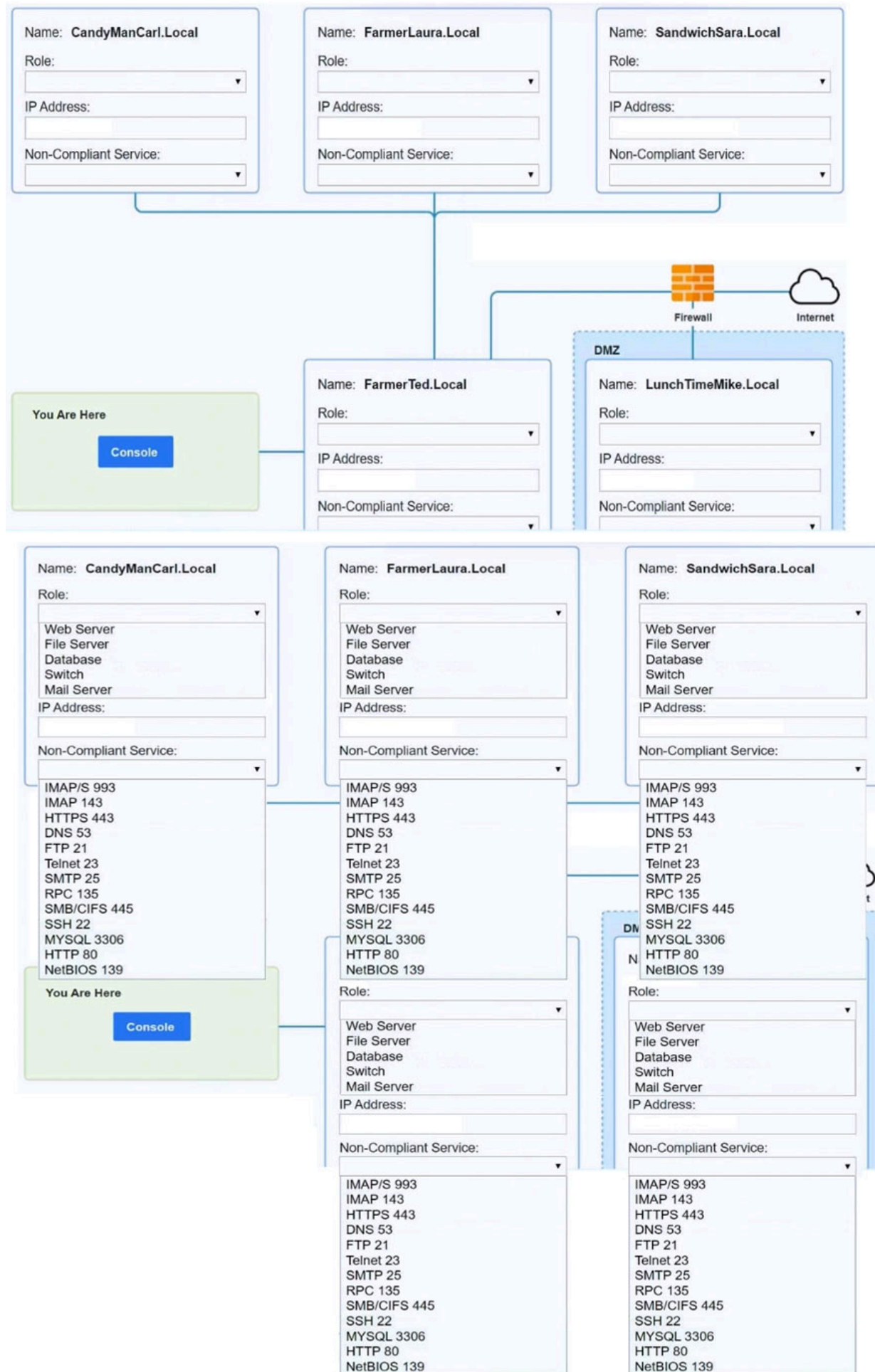
INSTRUCTIONS -

Using the tools available, discover devices on the corporate network and the services that are running on these devices.

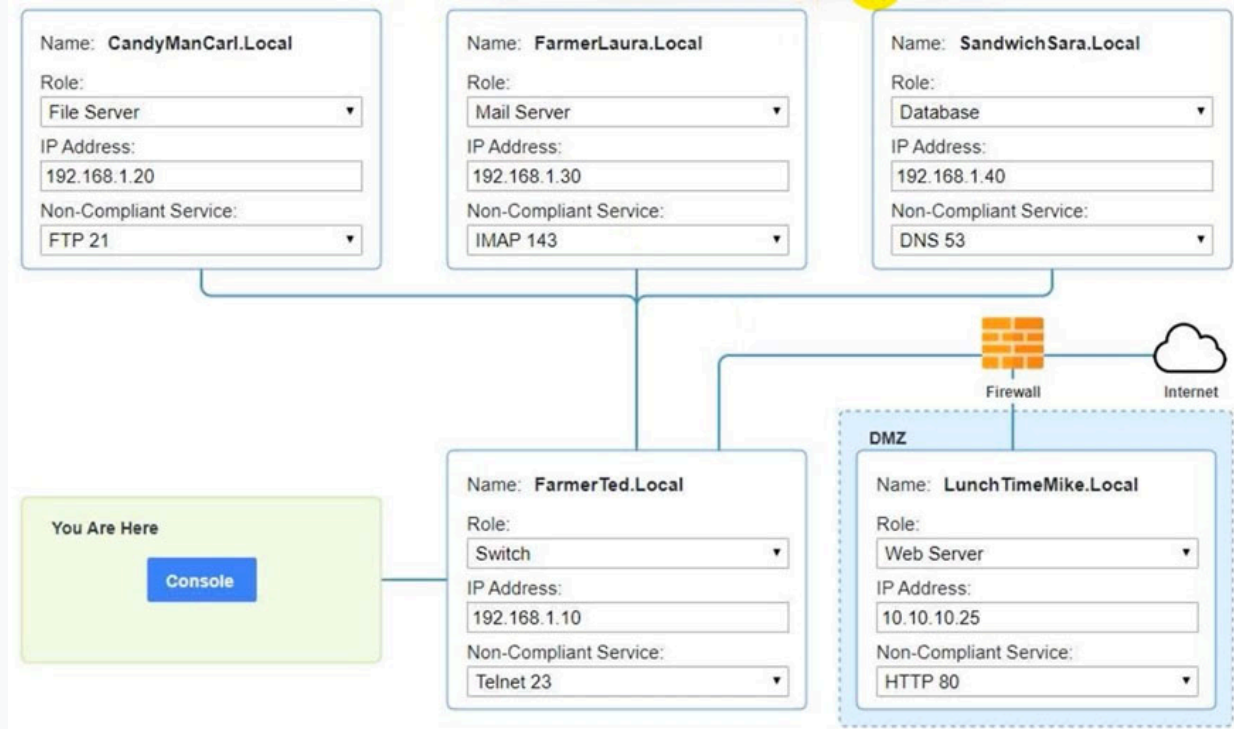
You must determine:

- ⇒ The IP address of each device.
- ⇒ The primary server or service of each device.
- ⇒ The protocols that should be disabled based on the hardening guidelines.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Suggested Answer: See explanation below.



```
nmap <host>
ping <host>
help
```

```
[root@server1 ~]# nmap candymancarl.local
```

```
Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on CandyManCarl.Local (192.168.1.20):
Not shown: 1676 closed ports
PORT      STATE      SERVICE
21/tcp    open      ftp
135/tcp    open      msrpc Microsoft Windows RPC
139/tcp    open      netbios-ssn
445/tcp    open      microsoft-ds
MAC Address: 09:00:27:D9:8E:D4 (Symmetrical Systems Industries Consortium)
```

```
Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds
```

```
[root@server1 ~]# nmap farmerlaura.local
```

```
Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on FarmerLaura.Local (192.168.1.30):
Not shown: 1678 closed ports
PORT      STATE      SERVICE
143/tcp    open      imap
993/tcp    open      imap/s
MAC Address: 09:00:27:D9:8E:D3 (Symmetrical Systems Industries Consortium)
```

```
Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds
```

```
[root@server1 ~]# nmap sandwichsara.local
```

```
Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on SandwichSara.Local (192.168.1.40):
```

```

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on SandwichSara.Local (192.168.1.40):
Not shown: 1677 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
53/udp    open       dns
3306/tcp  open       mysql
MAC Address: 09:00:27:D9:8E:D1 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap farmerted.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on FarmerTed.Local (192.168.1.10):
Not shown: 1678 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
23/tcp    open       telnet
MAC Address: 09:00:27:D9:8E:D6 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]# nmap lunchtimemike.local

Starting Nmap 7.01 ( http://www.insecure.org/nmap/ ) at 2016-03-02 16:20 EST
Interesting ports on LunchTimeMike.Local (10.10.10.25):
Not shown: 1677 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
80/tcp    open       http
443/tcp   open       https
MAC Address: 09:00:27:D9:8E:D5 (Symetrical Systems Industries Consortium)

Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds

[root@server1 ~]#

```

NBE Highly Voted 1 year, 11 months ago

Please note that you have to type the nmap commands yourself nmap and the computer name for each one
upvoted 16 times

Pesos 1 year, 1 month ago

So is the question not actually pull down multiple choice?
upvoted 1 times

voiddraco 10 months, 1 week ago

nmap <Host>
ping <Host>
help
upvoted 1 times

ptbuchanan 11 months ago

Ditto!
upvoted 1 times

Kickuh06 Highly Voted 1 year, 10 months ago

Passed CS0-003 last week (757), this question was on it! 69 questions, 3 PBQ/SIMs. 25 questions that are in the first 200 questions of this board.
upvoted 16 times

Director 3 months ago

Congrats! what other PBQ's you encountered?
upvoted 1 times

dave_delete_me Most Recent 1 year, 1 month ago

Someone asked how we know FarmerTed.Local is a switch? Here is my logic:

- other servers are shown on topology to plug into FarmerTed.local
- The very "CONSOLE" on the test question is usually the terminology when you "CONSOLE" into a switch... Sure this can be done on a Server to

using iLO ports or OOB management switches, but given the ports are ONLY 23 (telnet) and 22 (ssh), it's a dead giveaway that this is a network device / switch.

upvoted 1 times

🗨️ 👤 **RT7** 1 year, 7 months ago

Hi turki_1993,

I suppose the reason why FarmerTed.local is a switch is because the only secure protocol left is SSH and because SSH access is a preferred option to login to a Switch.

upvoted 7 times

🗨️ 👤 **turki_1993** 1 year, 10 months ago

how can you know that FarmerTed.local is a switch? can anyone explain?

upvoted 3 times

🗨️ 👤 **iwonttellyou** 2 years ago

Passed it the other day, this one was on it.

upvoted 5 times

🗨️ 👤 **ghjhjh** 1 year, 12 months ago

Thanks mate!, How many questions from examtopic?. is it a lot?

upvoted 2 times

🗨️ 👤 **[Removed]** 2 years ago

This was on my exam and I passed.

upvoted 3 times

🗨️ 👤 **ApexPredator84** 2 years, 4 months ago

was on mine today and applied as ispassed the exam and the all the pbqs. thank you

upvoted 3 times

🗨️ 👤 **db97** 2 years, 4 months ago

Was there any other PBQ from CS0-001 version?

upvoted 2 times

🗨️ 👤 **SylFlo** 2 years, 5 months ago

this sim was on my test today

i remembered the nmap command to get the ips and tried to remember the functions... i deduced the ports from the nmap output

upvoted 1 times

🗨️ 👤 **Freddy90** 2 years, 5 months ago

I got this sim today. I believe CandyMan should have a non-compliant service port 135 not FTP 21. This is a file server and blocking FTP will affect the functionality right?

upvoted 3 times

🗨️ 👤 **db97** 2 years, 5 months ago

Port 135 is needed within the network so the clients can connect properly. File servers use port 445 as well for network shares. Port 21 is not needed at all so the default answer is correct!

upvoted 6 times

🗨️ 👤 **cmllsu** 2 years, 6 months ago

One of the 3 sims I got today, answer is correct.

upvoted 6 times

🗨️ 👤 **mandimus** 2 years, 7 months ago

Just took the test yesterday. This was one of four sims on the test.

upvoted 6 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

In database server, port 3306 is unencrypted as I know. Ok this is database server and we need to disable dns as an unnecessary port, but why we keep using unencrypted port 3306. Please someone explain. Thank you

upvoted 3 times

🗨️ 👤 **throdrido** 2 years, 7 months ago

MySQL uses 3306 and can use SSL over this port or any other to encrypt the connection.

upvoted 2 times

🗨️ 👤 **wtkao** 2 years, 8 months ago

In database server, the non-compliance service should be MySQL 3306. Because Port 3306 is unencrypted.
upvoted 2 times

🗨️ 👤 **PTcruiser** 2 years, 9 months ago

Does anyone have an explanation on why DNS should be disabled?
upvoted 2 times

🗨️ 👤 **Treymb6** 2 years, 9 months ago

Because it's a database and not a domain server. SSH is a secure protocol. Granted, SSH could be disabled if it is unnecessary but it seems like the given answer is correct in my opinion.
upvoted 5 times

🗨️ 👤 **TheSkyMan** 2 years, 9 months ago

I keep wondering why these questions disable services needed for a server. Looks like per hardening guidelines, unencrypted services should be disabled.

"Another area of concern is systems that are configured to use unencrypted protocols. Common unencrypted protocols include HTTP, TELNET, and FTP. If a system is using an unencrypted protocol, sensitive information such as usernames and passwords could be sent in clear text over the network. An attacker who is monitoring network traffic could potentially intercept this information."

<https://www.tracesecurity.com/blog/articles/system-hardening-standards>
upvoted 4 times

A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the following types of testing does this describe?

- A. Acceptance testing
- B. Stress testing
- C. Regression testing
- D. Penetration testing

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: A

A. this is UAT for sure.

upvoted 1 times

🗳️ **Goat54** 2 years, 6 months ago

answer-A) reason-Analyst received and PULLED ARTIFACTS FROM recent INCIDENT.

upvoted 1 times

🗳️ **amateurguy** 2 years, 7 months ago

Selected Answer: A

A is correct.

upvoted 1 times

🗳️ **AndyM112** 2 years, 8 months ago

A: "asked users to conduct testing to ensure an application meets the needs of the business"

upvoted 1 times

🗳️ **MortG7** 2 years, 8 months ago

Again, key word is "asking users..."...thus user acceptance testing

upvoted 1 times

🗳️ **Belijmag** 2 years, 9 months ago

Selected Answer: A

Agree with A

upvoted 2 times

🗳️ **Laudy** 2 years, 10 months ago

Selected Answer: A

It's not B, C, or D.....Smh. I don't like their wording for how their asking this stuff.

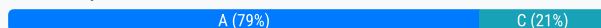
upvoted 1 times

An analyst receives artifacts from a recent intrusion and is able to pull a domain, IP address, email address, and software version. Which of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

- A. Infrastructure
- B. Capabilities
- C. Adversary
- D. Victims

Suggested Answer: C

Community vote distribution



rivo3 Highly Voted 2 years, 3 months ago

Selected Answer: A

Per CompTIA, and makers of Diamond Model(<https://www.comptia.org/blog/think-like-a-hacker-3-cybersecurity-models-used-to-investigate-intrusions>):

Adversary: The persona of the individual or group attacking you

Infrastructure: IP addresses, domain names or email addresses

Capabilities: What the adversary can do (e.g., malware, exploits, manipulate infrastructure)

Victim: Can include people, services, network assets or information

upvoted 26 times

Learner213 Most Recent 7 months ago

Selected Answer: A

I initially thought that "C" was the correct answer but, based on the description of "Infrastructure" it is definitely "A":

Infrastructure

The technical resources and assets used by the attacker to perform the attack, such as servers, domains, and IP addresses

upvoted 1 times

nelombg 1 year, 6 months ago

C=Infrastructure

The infrastructure includes the physical or logical communication structures such as IP or e-mail addresses, domain names, and others, employed by an adversary to deliver a capability.

upvoted 1 times

581777a 1 year, 8 months ago

Selected Answer: C

The information about the domain, IP address, email address, and software version represents the "Infrastructure" point of the Diamond Model of Intrusion Analysis.

So the correct answer is:

A. Infrastructure

upvoted 2 times

581777a 1 year, 8 months ago

oops I meant A

upvoted 1 times

Kwame25 1 year, 10 months ago

Selected Answer: A

infrastructure includes the physical or logical communication structures such as IP or e-mail addresses, domain names, and others, employed by an adversary to deliver a capability. cyware website gives clear definition.

upvoted 1 times

🗨️ 👤 **Kwame25** 1 year, 10 months ago

Selected Answer:A

upvoted 1 times

🗨️ 👤 **Kainas** 2 years, 2 months ago

Selected Answer: A

Chatgpt went with A as the correct answer. When asked why it picked A over C, this is what it said...

The domain, IP address, email address, and software version are all part of the infrastructure that the adversary used to carry out the intrusion. Therefore, this intelligence would represent the "Infrastructure" point in the Diamond Model of Intrusion Analysis, which is why option A is the correct answer. The "Adversary" point in the Diamond Model would represent information about the identity, motivations, and tactics of the attackers themselves, which is not directly represented by the artifacts listed in the question.

upvoted 4 times

🗨️ 👤 **Snkrsnaker1** 2 years, 2 months ago

Answer is C.

I think you guys are making this question harder than it is supposed to be. In the Diamond Model of Intrusion Analysis, it talks about analytical pivoting, meaning IP address, domain name, and email address can also be the victim, it all depends on where in the diamond you are coming from. In this case, we are the analyst and all we have is an IP address, an email address, and software version. This would point to the Adversary responsible for the recent intrusion. There is no way you can tell what the infrastructure is based on just an IP, email address, and software version. That's how I am approaching this question.

upvoted 3 times

🗨️ 👤 **OnA_Mule** 2 years, 3 months ago

Selected Answer: C

The key to this question is how you interpret the first 8 words of the sentence, "An analyst receives artifacts from a recent Intrusion." If you believe that these artifacts are from the local system, then the answer would be A.

In this context, artifacts would be referring to the breadcrumb trail left behind by the attacker. So that would make the correct answer C as this information would belong to the Adversary

upvoted 4 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. Per Jason Dion CYSA Udemy class.

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 3 months ago

Selected Answer: A

Infrastructure

The information provided in the question, such as domain, IP address, email address, and software version, falls under the "Infrastructure" point of the Diamond Model of Intrusion Analysis. This information can be used to identify the infrastructure that the adversary used during the intrusion, including the tools, networks, and systems that were compromised. By analyzing the infrastructure, analysts can identify the tactics, techniques, and procedures (TTPs) used by the adversary and create a better understanding of the overall intrusion.

upvoted 1 times

🗨️ 👤 **boletri** 2 years, 4 months ago

Selected Answer: C

Answer is C.

Official Compitia Cysa+ Course Material Diagram of Diamond Model. Can t submit the Image here because is not support.

upvoted 1 times

🗨️ 👤 **encxorblood** 2 years, 4 months ago

Selected Answer: C

The BEST approach for the consultant to consider when modeling the client's attack surface would be to answer the question: "What are the most likely attack vectors for this particular client?"

Option C is the best approach for the consultant to take, as it involves analyzing attacks against similar industry peers and assessing the probability of the same attacks happening. This approach would help the consultant to identify the most likely attack vectors and prioritize their attention on those areas.

Option A is helpful in understanding external scans, but may not give the full picture of the client's attack surface.

Option B is focused on potential solutions to reduce the likelihood of an attack, but it does not provide insight into the specific risks that the client may be facing.

Option D is focused on funding for solutions, which may not be the primary concern at this stage.

upvoted 1 times

🗨️ 👤 **omer123456** 2 years, 5 months ago

Selected Answer: A

Correct answer is A

The infrastructure includes the physical or logical communication structures such as IP or e-mail addresses, domain names, and others, employed by an adversary to deliver a capability.

upvoted 1 times

🗨️ 👤 **omer123456** 2 years, 5 months ago

Correct answer is A

The infrastructure includes the physical or logical communication structures such as IP or e-mail addresses, domain names, and others, employed by an adversary to deliver a capability.

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: A

Google DIAMOND Model and you will see A is the answer.

upvoted 2 times

🗨️ 👤 **iraidesc** 2 years, 7 months ago

Selected Answer: C

<https://teamt5.org/en/posts/what-is-diamond-model-of-intrusion-analysis/>

upvoted 1 times

While conducting a network infrastructure review, a security analyst discovers a laptop that is plugged into a core switch and hidden behind a desk. The analyst sees the following on the laptop's screen:

[*] [NBT-NS] Poisoned answer sent to 192.169.23.115 for name FILE-SHARE-A (service: File Server)

[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A

[*] [LLMNR] Poisoned answer sent to 192.168.23.115 for name FILE-SHARE-A

[SMBv2] NTLMv2-SSP Client : 192.168.23.115

[SMBv2] NTLMv2-SSP Username : CORP\jsmith

[SMBv2] NTLMv2-SSP Hash : F5DBF769CFEA7...

[*] [NBT-NS] Poisoned answer sent to 192.169.23.24 for name FILE-SHARE-A (service: File Server)

[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A

[*] [LLMNR] Poisoned answer sent to 192.168.23.24 for name FILE-SHARE-A

[SMBv2] NTLMv2-SSP Client : 192.168.23.24

[SMBv2] NTLMv2-SSP Username : CORP\progers

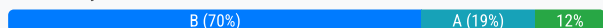
[SMBv2] NTLMv2-SSP Hash : 6D093BE2FDD70A...

Which of the following is the BEST action for the security analyst to take?

- A. Force all users in the domain to change their passwords at the next login.
- B. Disconnect the laptop and ask the users jsmith and progers to log out.
- C. Take the FILE-SHARE-A server offline and scan it for viruses.
- D. Initiate a scan of devices on the network to find password-cracking tools.

Suggested Answer: C

Community vote distribution



nonjabusiness Highly Voted 2 years, 9 months ago

Selected Answer: B

The output on the laptop looks like the authentication service has been poisoned, and 2 accounts have been compromised.

Requiring all users to change their passwords could be overkill, if there isn't more to this output.

Though taking the server offline and scanning for viruses may be a good idea, this answer however does nothing to remediate the compromised accounts which would be my main concern given the scenario.

Disconnecting the laptop, and remediating the compromised hashes would be the best course of action for this in my opinion. As this would stop the poisoning, and prevent any unauthorized access from cracking the hashes.

upvoted 17 times

db97 2 years, 4 months ago

Totally agree

upvoted 1 times

Xoomalla 1 year, 10 months ago

Agree on B.

Was confused between A and B. But since,

- Nothing mentioned about disconnecting the Laptop and only mentioned Password reset this is not correct.

hmm, but asking the users to logout only, would this prevent there password from being cracked offline?

upvoted 1 times

Laudy Highly Voted 2 years, 10 months ago

Selected Answer: B

Obviously scanning the file sever would be good, but it doesn't stop the DNS poisoning... Feels more like the users have a better chance of being infected than the file server...Maybe I'm wrong, but I feel like disconnecting the known bad laptop, and having the two users who tried navigating to the "file server" log off, would be better than just scanning the File Server.

upvoted 6 times

JimmyJams Most Recent 2 years, 1 month ago

Selected Answer: B

Defo not A as the server itself isn't infected. The laptop is poisoning traffic not a device
upvoted 1 times

  **DerekM** 2 years, 1 month ago

Selected Answer: B

Based on the provided information, the BEST action for the security analyst to take in this scenario is:

B. Disconnect the laptop and ask the users jsmith and progers to log out.

The analyst has discovered a suspicious laptop connected to the network infrastructure, and the screen displays indications of potentially malicious activity related to network poisoning and SMBv2 communication. To contain the potential threat and prevent further compromise, the immediate action should be to disconnect the laptop from the network. Asking the users "jsmith" and "progers" to log out from the laptop is also important to ensure that they do not continue any unauthorized activities.

While other actions like changing passwords, scanning the FILE-SHARE-A server, or initiating network scans may be necessary as part of a broader incident response plan, the immediate focus should be on isolating the suspicious device and preventing any further potential harm.


upvoted 1 times

  **SimonR2** 2 years, 2 months ago

This is an attack using the command line Responder Tool which poisons responses to NetBIOS, LLMNR and MDNS name resolution requests. It basically performs a man in the middle attack and allows retrieval of password hashes over a file sharing network.

The simple answer here is to get the laptop off the network as soon as possible and prevent the MITM attack from occurring so answer is B.



upvoted 2 times

  **2Fish** 2 years, 3 months ago

Selected Answer: B

B. Stop the assumed threat and then have a look at the server.



upvoted 1 times

  **DrVoIP** 2 years, 4 months ago

B. Disconnect the laptop and ask the users jsmith and progers to log out is the best action for the security analyst to take.

The laptop is using the responder tool to perform a man-in-the-middle attack, and the output on the screen indicates that it has successfully obtained NTLMv2-SSP hashes for two users on the network: jsmith and progers. This attack could be used to steal user credentials and gain access to sensitive information on the network. ChatGPT

upvoted 4 times

  **CL_QRT** 2 years, 4 months ago

another tricky COMPTIA questions again. Guys, after the analyst discovered the event, what is the BEST NEXT action to take?

Answer is B. - then from there do the other necessary steps

upvoted 3 times

  **Sweety_Certified7** 3 months, 3 weeks ago

The question does not mention "next": Which of the following is the BEST action for the security analyst to take? If it says "best action to take" (without specifying order), then A is a better choice because it neutralizes the most critical risk (compromised credentials).

upvoted 1 times

  **Stiobhan** 2 years, 5 months ago

The log output is a capture of traffic flow for said users as they have requested access to the file server and (in this case) the requests have been captured by a malicious tool such as Responder (available in Kali). The best answer here is B, but if I had the option to pick 2 then I would also pick D. Even at that, the choice of answers are poor because on their own this incident will not resolve, have a wee read at this to help you understand what is really happening here - <https://www.cynet.com/attack-techniques-hands-on/llmnr-nbt-ns-poisoning-and-credential-access-using-responder/> . On reading the scenario more in depth, I'd say the laptop is a plank with Responder installed and the threat is internal! So, disconnect the laptop (which only solves part of the issue, if it were real). The laptop should then be investigated, possibly forensically.

upvoted 1 times

  **sho123** 2 years, 7 months ago

Selected Answer: B

No answer here yet. the correct answer should be disconnect the laptop and scan the file server for malicious input.

upvoted 1 times

🗨️ 👤 **Dcfc_Doc** 2 years, 7 months ago

I feel like I would do all of these steps. The only thing that i would debate is the order in Which i would do them.

Voting B

upvoted 2 times

🗨️ 👤 **Kelz56** 2 years, 7 months ago

Selected Answer: C

Prevention is better than cure. Server is possibly compromise base on logs so we should check the server first. Resetting the user's passwords is a good option but will not remediate the possible server issue.

upvoted 1 times

🗨️ 👤 **Goat54** 2 years, 5 months ago

Scanning the server will check for vulnerabilities but what about the compromised accounts of the 2 users? Answer B may be a better choice.

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 7 months ago

Selected Answer: B

B seems like the best answer.

upvoted 1 times

🗨️ 👤 **IT_Master_Tech** 2 years, 8 months ago

What is the RIGHT answer?

upvoted 2 times

🗨️ 👤 **TeyMe** 2 years, 8 months ago

A tool called Responder will generate such output, the tool can intercept LLMNR and NBT-NS requests and an attacker can obtain Password hashes in the process. I would say answer: D

upvoted 3 times

🗨️ 👤 **TeyMe** 2 years, 7 months ago

B is correct

upvoted 2 times

🗨️ 👤 **AcidoNZ** 2 years, 7 months ago

Its D for sure

<https://0xdf.gitlab.io/2019/01/13/getting-net-ntlm-hashes-from-windows.html>

upvoted 1 times

🗨️ 👤 **A_core** 2 years, 8 months ago

Selected Answer: C

although not best step but this is the only option make sense in the choices. B is close but, it talked about reset an account which does not constitute best action. Best action is take action on the source and the target

upvoted 1 times

🗨️ 👤 **wico** 2 years, 8 months ago

Selected Answer: A

A few things happening here. Big part is gathered credentials. We see two credentials on the screen, but who knows how many other credentials we dont see?

What are our options? We can have the users immediately log out, but what will that protect? If the attacker has the user's credentials, we can spend time telling each user to log off and disconnect the laptop. Meanwhile the attacker will be using their credentials to steal DATA from the file server and do whatever else they want with the credentials. The only reasonable option here is to have all users change their passwords while also disconnecting the laptop.

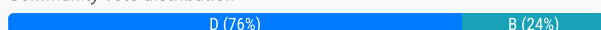
upvoted 2 times

A Chief Executive Officer (CEO) is concerned the company will be exposed to data sovereignty issues as a result of some new privacy regulations. To help mitigate this risk, the Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

- A. Data masking procedures
- B. Enhanced encryption functions
- C. Regular business impact analysis functions
- D. Geographic access requirements

Suggested Answer: B

Community vote distribution



Laudy Highly Voted 2 years, 10 months ago

Selected Answer: D

Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner.

You're only worried about that if you're in multiple locations. Hence the best answer is D.

<https://www.virtu.com/blog/gdpr-data-sovereignty-matters-globally>

upvoted 25 times

bootleg 2 years, 8 months ago

If the question would've said (INTEGRITY) then you think encryption. Geo is absolutely locale. Move the instance to a location in which you have control.

upvoted 2 times

Goat54 2 years, 5 months ago

Integrity=hashing

Confidentiality=encryption

upvoted 5 times

kopib21961 2 years, 6 months ago

D is correct. Also because data sovereignty would not restrict certain customers from doing business with an organization. Geographic access requirements could block potential customers from accessing an organization's resources from within a geographic location.

upvoted 1 times

2Fish 2 years, 3 months ago

Agree. D is the correct answer here.

upvoted 2 times

DerekM Most Recent 2 years, 1 month ago

Selected Answer: D

To mitigate the risk of data sovereignty issues resulting from new privacy regulations, the Chief Information Security Officer (CISO) should implement geographic access requirements (option D).

Geographic access requirements involve implementing technical controls that ensure data is stored and accessed only within specific geographic regions or jurisdictions. This control helps address concerns related to data sovereignty by ensuring that data is stored and processed in compliance with the applicable regulations of the specific regions where the data is located.

upvoted 1 times

JokerRWild 2 years, 2 months ago

Selected Answer: D

D. Geographic access requirements would help mitigate the risk of data sovereignty issues. This control would ensure that data is only accessible from approved geographic locations, helping to ensure the data sovereignty of certain countries or regions is maintained. Data masking procedures,

enhanced encryption functions, and regular business impact analysis functions can help address other types of risks, but would not specifically address data sovereignty concerns.

upvoted 2 times

🗨️ 👤 **1oldman** 2 years, 2 months ago

Technical controls consist of the hardware and software components that protect a system against cyberattack. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.

upvoted 2 times

🗨️ 👤 **Snkrsnaker1** 2 years, 2 months ago

Answer is B

Think along the lines of...Geo access requirements is just that, an access control based on geolocation. It doesn't actually protect data. The most widely accepted meaning to Data sovereignty refers to the understanding that data which are stored outside of an organizations host country and still subject to the laws in the country where the data is stored. How this question is asked, the answer is B. Data sovereignty has nothing to do with where its accessed but more of how the data is protected based on their laws. Hope this helps.

upvoted 4 times

🗨️ 👤 **josbornx** 2 years, 3 months ago

To mitigate the risk of data sovereignty issues, the appropriate technical control would be D. Geographic access requirements. This control ensures that data is only stored and processed in geographic locations that comply with relevant privacy regulations, thereby reducing the risk of the company being exposed to such issues.

Option A, data masking procedures, is a technique used to obfuscate sensitive data in a system, but it may not be sufficient to address the specific concerns related to data sovereignty.

Option B, enhanced encryption functions, can be an effective control to protect data confidentiality, but it may not necessarily address the concerns related to data sovereignty.

Option C, regular business impact analysis functions, are an important aspect of risk management but are not directly related to addressing data sovereignty issues.

Therefore, option D is the best choice to help mitigate the risk of data sovereignty issues.

ChatGPT

upvoted 2 times

🗨️ 👤 **uday1985** 2 years, 1 month ago

Dude! dont rely on ChatGPT! it gave me wrong answers 50% of the times!

upvoted 3 times

🗨️ 👤 **kiduuu** 2 years, 3 months ago

Selected Answer: D

Data masking procedures (option A) can be used to protect sensitive data by replacing it with fictitious data, but it does not address the issue of data sovereignty.

Enhanced encryption functions (option B) can be used to protect sensitive data, but it does not address the issue of data sovereignty directly.

Regular business impact analysis functions (option C) are important for identifying potential risks and developing mitigation strategies, but it does not address the issue of data sovereignty.

Therefore, option D. Geographic access requirements would be the most appropriate technical control to implement to address the CEO's concern about data sovereignty issues resulting from new privacy regulations.

upvoted 2 times

🗨️ 👤 **DrVoIP** 2 years, 4 months ago

B. Enhanced encryption functions would be an appropriate technical control to help mitigate the risk of data sovereignty issues due to new privacy regulations.

-ChatGPT

upvoted 1 times

🗨️ 👤 **boletri** 2 years, 4 months ago

Geographic Access Requirements

Geographic access requirements fall into two different scenarios.

Storage locations might have to be carefully selected to mitigate data sovereignty issues. Most cloud providers allow choice of data centers for processing and storage, ensuring that information is not illegally transferred from a particular privacy jurisdiction without consent. Employees needing access from multiple geographic locations. Cloud-based file and database services can apply constraint-based access controls to validate the user's geographic location before authorizing access.

Official CompTia Cysa+ Course Material.

upvoted 1 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: D

D. Sovereignty refers to location specific governance

upvoted 1 times

🗨️ 👤 **Cock** 2 years, 4 months ago

Selected Answer: D

D. In the UK, you need to give permissions to cookies

upvoted 1 times

🗨️ 👤 **zainulimti** 2 years, 5 months ago

The Chief asked for technical control. Encryption is a technical control, not option D

upvoted 3 times

🗨️ 👤 **catastrophie** 2 years, 5 months ago

The correct answer is D. You can encrypt and mask the data all you want, however, the issue lies within the location in which the data is contained. For example, the UK has a strict privacy regulation called General Data Protection Regulation (GDPR) which protects their citizens PII and data rights. Under this regulation, only countries with verified similar regulations can store data on UK citizens. The United States cannot because we do not have federal regulations to protect the individual rights of data privacy. This is an example of type Geographical access requirements based on a sovereignty privacy regulation.

upvoted 3 times

🗨️ 👤 **omer123456** 2 years, 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

🗨️ 👤 **albano23412415** 2 years, 6 months ago

Selected Answer: B

They are saying the data will be exposed due to new privacy rules. Using encryption to protect data against prying eyes. If a foreign government demands that a cloud provider give them access to your data, they won't be able to read it if you hold the decryption key.

upvoted 3 times

🗨️ 👤 **Cyril_the_Squirrel** 2 years, 7 months ago

B is correct.

The CISO wants to apply Technical Controls, B is correct.

D is wrong because it's an Administrative or Managerial Control.

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

upvoted 2 times

🗨️ 👤 **1oldman** 2 years, 2 months ago

Correct. Technical controls consist of the hardware and software components that protect a system against cyberattack. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.

upvoted 1 times

🗨️ 👤 **sho123** 2 years, 7 months ago

Selected Answer: B

there is always an access control but i haven't seen the words like Geographic access requirements in cybersecurity. so the next answer should be enhance encryption. i

upvoted 2 times

Which of the following is a difference between SOAR and SCAP?

- A. SOAR can be executed faster and with fewer false positives than SCAP because of advanced heuristics.
- B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope.
- C. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does.
- D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts.

Suggested Answer: B

Community vote distribution

B (100%)

 **Laudy** Highly Voted 2 years, 10 months ago

Selected Answer: B

I think this was supposed to be a very easy question if you know and understand what these two things are. But these are very different things. But I'll do my best to spell it out.

SOAR is used to automatically detect known bad traffic and implement a series of preapproved steps to alleviate the need of more workers. There are many tools that perform this function.

<https://www.fortinet.com/resources/cyberglossary/what-is-soar>

Tool Examples:

<https://geekflare.com/best-soar-tools/>

SCAP automates vulnerability management and policy compliance evaluation. It was developed by RHEL and the US Gov't to automate the implementation of STIGs. It scans for those STIGs/VULNs and will patch them automatically based on the defined rules implemented. It was originally a single tool that is now a suite that covers different areas of concern.

<https://www.youtube.com/watch?v=5PA9r9oaHUY>

Ultimately, SOAR is a conceptualization that many tools are built for while SCAP is a Tool Suite that has a much smaller scope and almost completely different purpose.

upvoted 12 times

 **2Fish** 2 years, 3 months ago

Agreed.

upvoted 1 times

 **R00ted** Highly Voted 2 years, 9 months ago

Selected Answer: B

Security Orchestration, Automation, and Response (SOAR)

-A class of security tools that facilitates incident response, threat hunting, and security configuration by orchestrating automated runbooks and delivering data enrichment

-SOAR is primarily used for incident response.

Security Content Automation Protocol (SCAP)

-A NIST framework that outlines various accepted practices for automating vulnerability scanning by adhering to standards for scanning processes, results reporting and scoring, and vulnerability prioritization

-SCAP is used to uphold internal and external compliance requirements

upvoted 9 times

 **NickDrops** 2 years, 5 months ago



Best explanation! TY sir!

upvoted 3 times

 **gokra** Most Recent 11 months, 1 week ago

Agreed.



upvoted 1 times

  **m025** 1 year, 6 months ago

Selected Answer: B

It's the only logic

upvoted 1 times

  **DrVoIP** 2 years, 4 months ago

B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope is the difference between SOAR and SCAP. - ChatGPT

upvoted 2 times

  **RobThaBlak** 2 years, 5 months ago

I pick A. Because the question explicitly states that the server should be used for one function and the other 3 are used for web but FTP is for file transfer.

upvoted 1 times

  **Cizzla7049** 2 years, 9 months ago

Selected Answer: B

SOAR is B

upvoted 1 times

An organization has a policy that requires servers to be dedicated to one function and unneeded services to be disabled. Given the following output from an Nmap scan of a web server:

```
Starting Nmap 5.10 (https://nmap.org) at 2020-01-11 17:43 Interesting ports on 192.168.10.3:
```

```
Not shown: 997 closed ports
```

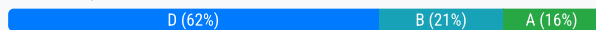
PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https
1433/tcp	open	sql

Which of the following ports should be closed?

- A. 21
- B. 80
- C. 443
- D. 1433

Suggested Answer: B

Community vote distribution



MortG7 Highly Voted 2 years, 8 months ago

"servers to be dedicated to one function..." http/s and SQL are two functions. I will select D, but agree with folks that the question is horribly written, and the person who wrote it was most likely drunk.

upvoted 24 times

SolventCourseisSCAM Highly Voted 2 years, 7 months ago

Selected Answer: D

question asks for a "WEB SERVER", so you may need to use FTP to download and upload files. Also, http and https are must for web server. Do not think it like http is not secure, so it should be closed. No, this is not how the system works in real life. HTTP and HTTPS are used by companies by providing reliable secure configurations on HTTP. There is one port left 1433 SQL DATABASE server. You do not need that on web server. Remember, you may need FTP on web server when you are dealing with files download/upload.

upvoted 15 times

fuzzyguzzy Most Recent 6 months, 4 weeks ago

Selected Answer: D

A SQL database shouldn't be on the server if the goal is to dedicate a server to one function. Also, it's generally not correct to expose a sql server port, if it's being used on the host.

upvoted 1 times

Learner213 7 months ago

Selected Answer: D

Since the sole purpose of this server is to deliver web services, insecure port 1433 should be closed. I could also make a case for closing insecure port 21.

upvoted 1 times

m025 1 year, 6 months ago

Selected Answer: D

Database would be another function

upvoted 1 times

kmordalv 1 year, 8 months ago

Selected Answer: D

Gentlemen, a database on a web server? It is not the right thing to do. If port 1433 were not available, the answer would be B (80).

upvoted 1 times

skibby16 1 year, 8 months ago

Selected Answer: A

If the server is dedicated to one function (web server) and unneeded services are disabled, then port 21 should be closed, because FTP is not necessary for a web server and could pose a security risk if exploited. Port 80, port 443, and port 1433 are ports that are needed for a web server, because they are used for HTTP, HTTPS, and SQL Server respectively. Reference: <https://www.ssh.com/ssh/port>

upvoted 1 times

🗳️ 👤 **attesco** 2 years ago

Selected Answer: B

The questions says one function and unneeded services. Port 80 is irrelevant when port 443 is available. 1433 and 21 could be a backend server that webserver is connected to

upvoted 4 times

🗳️ 👤 **DerekM** 2 years, 1 month ago

Selected Answer: D

Based on the organization's policy that requires servers to be dedicated to one function and unneeded services to be disabled, if I have to choose only one port to be closed based on the given Nmap scan output, I would recommend closing port 1433/TCP (SQL) if it is not required for the web server's intended function.

upvoted 1 times

🗳️ 👤 **uday1985** 2 years, 1 month ago

Web server=80+443

SQL is not needed and closing only HTTP "80", wont serve the question requirements

upvoted 2 times

🗳️ 👤 **JoInn** 2 years, 2 months ago

Selected Answer: B

Clearly B. Question states we need to basically have one port per service, and the rest disabled. 1433 is the only port for SQL opened on this server, but why would we have both HTTP and HTTPS open? Close port 80, job done.

upvoted 2 times

🗳️ 👤 **JokerRWild** 2 years, 2 months ago

Selected Answer: D

D. The server is dedicated as a web server (function) and the unneeded service to be disabled is 1433(sql). This is directly based of the question itself.

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: D

D. Just from experience, I would most definitely want to separate SQL from a Web Server. "Dedicated to one function". So my take is remove SQL (1433)

upvoted 1 times

🗳️ 👤 **Orean** 2 years, 4 months ago

Selected Answer: D

You can have separate server for databasing (which is often advisable), but you'll most likely need FTP for file transfers. The web-server is where you store all the necessary files (including HTML contents), after all, and file-transfer protocols are the most efficient avenue.

upvoted 1 times

🗳️ 👤 **DrVoIP** 2 years, 4 months ago

As they do not say what type server it is, we have to assume port 21 should be closed because the other ports would all be required to support either a webserver or a database server.

upvoted 1 times

🗳️ 👤 **DrVoIP** 2 years, 4 months ago

Based on the information provided, it is not possible to determine whether the organization should close any of the ports. However, if the policy of the organization is to dedicate servers to one function and to disable unneeded services, then it is likely that some of these ports should be closed.

In this case, assuming that the server is intended to be a web server, port 21 (FTP) and port 1433 (Microsoft SQL Server) are likely not necessary and should be closed. Port 80 and port 443 are necessary for web traffic, and should be left open. However, it is important to ensure that only necessary services are running on these ports, and that they are properly secured to reduce the risk of cyber attacks. - ChatGPT

upvoted 1 times

🗳️ 👤 **aisling** 2 years, 4 months ago

Selected Answer: A

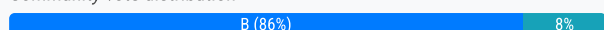
Webservers usually link back to an SQL database for orders etc, for FTP you would want both ports 20 and 21 open one is of no use
upvoted 2 times

An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

- A. Monthly vulnerability scans, biweekly topology scans, daily host discovery scans
- B. Monthly topology scans, biweekly host discovery scans, monthly vulnerability scans
- C. Monthly host discovery scans, biweekly vulnerability scans, monthly topology scans
- D. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans

Suggested Answer: C

Community vote distribution



adrianlacatus Highly Voted 3 years, 4 months ago

Selected Answer: B

The schedule should accomodate enterprise-wide changes & minimize the impact
 infrastructure upgrades each month -> monthly vulnerability scans (biweekly option is overkill therefore condition 2 does not apply)
 workstation installs every other week -> biweekly host discovery scan
 option A has daily host discovery scans therefore it is ruled out
 Only possible option is B.
 upvoted 16 times

Davar39 Highly Voted 3 years ago

Selected Answer: B

Workstation installs every other week = biweekly host discovery
 Infrastructure upgrades each month = monthly vuln scan
 Topology scans are slow and prompt all hosts/servers in the network, so that would be the "impact to the network" part = monthly
 The answer is B.
 upvoted 14 times

cyberwolfhooah Most Recent 1 year, 4 months ago

Selected Answer: D

.....
 upvoted 1 times

cfb30e6 1 year, 7 months ago

Selected Answer: D

This schedule provides a balance by conducting topology scans monthly to understand the overall network structure, host discovery scans every two weeks to keep track of connected devices, and weekly vulnerability scans to proactively identify and address security vulnerabilities.
 upvoted 1 times

salmonIsDecent 1 year, 10 months ago

Selected Answer: B

It is B, because biweekly vulnerability scans are expensive and can affect business operations, so I really do not think it can't be C.
 upvoted 1 times

Niitetteh 2 years, 2 months ago

B. From comptia website. Monthly vuln scan.
<https://www.comptia.org/content/guides/it-security-perimeter-health-check#:~:text=You%20should%20perform%20vulnerability%20scans,services%20exposed%20to%20the%20internet.>
 upvoted 1 times

JokerRWild 2 years, 2 months ago

Selected Answer: D

This schedule is the most appropriate because it ensures that the vulnerability scans are conducted weekly to detect and address potential security risks, while minimizing the impact on the network. The biweekly host discovery scans ensure that any new workstations or devices are detected in a

timely manner, while monthly topology scans help monitor changes to the network infrastructure.

upvoted 1 times



  **JoInn** 2 years, 3 months ago

Selected Answer: C

Reasons why I believe it's C and not B:

topology scan monthly, and we all agree. Vulnerabilities biweekly, because that's when workstations are added, and they are a good way of monitoring without heavily loading network, which is what the question is asking. In addition, host discovery monthly, so you can find out what is on your network (just to be on the safe side). That definitely doesn't need done once every two weeks, and network isn't heavily impacted this way.

upvoted 1 times

  **tatianna** 2 years, 3 months ago

B

Therefore, option D is a better choice as it strikes a balance between the various scanning requirements while also accommodating the phased approach to network and workstation upgrades.

upvoted 1 times

  **2Fish** 2 years, 3 months ago

Selected Answer: B

B. Makes the most sense in this case.

upvoted 1 times

  **DrVoIP** 2 years, 4 months ago

D. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans is the schedule that BEST addresses the requirements of upgrading the network and workstations in phases while minimizing the impact to the network. ChatGPT

upvoted 1 times

  **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

B makes sense for what the question is asking. It minimizes the impact and accommodates the enterprise-wide changes. Vulnerability scans take up a lot resources.

upvoted 1 times

  **kimi3155** 2 years, 6 months ago

I will be taking my exam this coming week. Anyone that just did the exam, please what is the correct answer. I am leaning on C.

upvoted 1 times

  **SoonT** 2 years, 6 months ago

Choose B, you need to accommodate the enterprise-wide changes. They are only making changes every month (infrastructure upgrades) and workstation installs (every other week or biweekly)

upvoted 1 times

  **david124** 2 years, 7 months ago

Selected Answer: B

b Correct answer.



upvoted 1 times

  **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: B

biweekly host discovery scans, monthly vulnerability scans

upvoted 1 times

  **amateurguy** 2 years, 7 months ago

Selected Answer: B

Go for B as the best answer.

upvoted 1 times

  **Fastytop** 2 years, 8 months ago

Selected Answer: C

the teacher in the course said to me the correct one is C. so I am not sure but I will take it in the exam.

upvoted 2 times

SIMULATION -

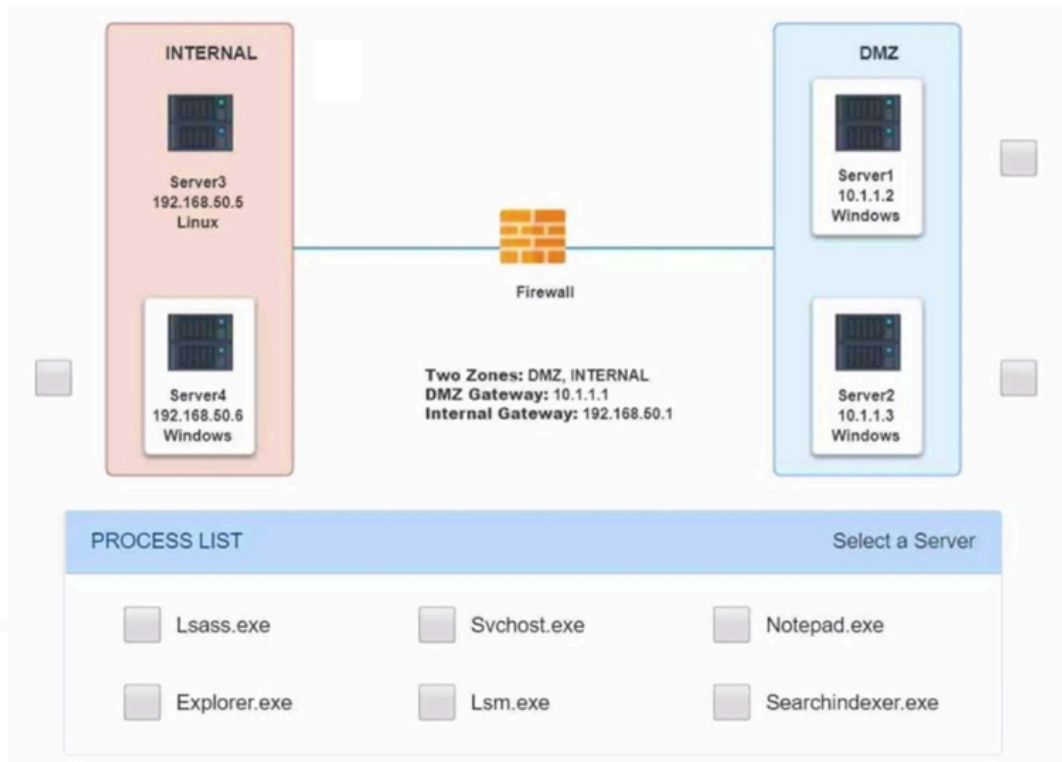
Malware is suspected on a server in the environment.

The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.

INSTRUCTIONS -

Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Diagram for Company A

```
C:\Users\Team3>netstat -oan
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	636
TCP	0.0.0.0:49184	0.0.0.0:0	LISTENING	540
TCP	0.0.0.0:49190	0.0.0.0:0	LISTENING	532
TCP	192.168.50.6:443	10.1.1.2:57433	ESTABLISHED	348
TCP	192.168.50.6:445	10.1.1.2:50125	ESTABLISHED	540
TCP	192.168.50.6:139	10.1.1.2:52349	ESTABLISHED	540
TCP	192.168.50.6:139	0.0.0.0:0	LISTENING	4
TCP	192.168.50.6:3389	172.30.0.148:49242	ESTABLISHED	348
TCP	192.168.50.6:50741	172.30.0.101:445	ESTABLISHED	4
TCP	192.168.50.6:50777	172.30.0.4:135	TIME_WAIT	0
TCP	192.168.50.6:50778	172.30.0.4:49157	TIME_WAIT	0
TCP	:::135	:::0	LISTENING	1720
TCP	:::445	:::0	LISTENING	4
TCP	:::3389	:::0	LISTENING	348

```
C:\Users\Team3>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	636	Services	0	6,864 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K
explorer.exe	2500	RDP-Tcp#0	1	66,444 K
splwow64.exe	2960	RDP-Tcp#0	1	4,152 K
cmd.exe	1260	RDP-Tcp#0	1	2,652 K
conhost.exe	2616	RDP-Tcp#0	1	5,256 K
audiodg.exe	980	Services	0	13,256 K
csrss.exe	2400	Console	3	3,512 K
winlogon.exe	2492	Console	3	5,772 K
LogonUI.exe	2864	Console	3	17,056 K
taskhost.exe	2812	Services	0	9,540 K
tasklist.exe	1208	RDP-Tcp#0	1	5,196 K
WmiPrvSE.exe	1276	Services	0	5,776 K

C:\Users\Team3>netstat -oan

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	884
TCP	0.0.0.0:49184	0.0.0.0:0	LISTENING	540
TCP	0.0.0.0:49190	0.0.0.0:0	LISTENING	532
TCP	10.1.1.2:57433	192.168.50.6:443	ESTABLISHED	1276
TCP	10.1.1.2:50125	192.168.50.6:445	ESTABLISHED	276
TCP	10.1.1.2:52349	192.168.50.6:139	ESTABLISHED	276
TCP	10.1.1.2:139	0.0.0.0:0	LISTENING	4
TCP	10.1.1.2:3389	172.30.0.148:49242	ESTABLISHED	348
TCP	10.1.1.2:50741	172.30.0.101:445	ESTABLISHED	4
TCP	10.1.1.2:50777	172.30.0.4:135	TIME_WAIT	0
TCP	10.1.1.2:50778	172.30.0.4:49157	TIME_WAIT	0
TCP	[::]:135	[::]:0	LISTENING	540
TCP	[::]:445	[::]:0	LISTENING	4

C:\Users\Team3>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	1,340 K
smss.exe	300	Services	0	884 K
csrss.exe	384	Services	0	3,048 K
wininit.exe	432	Services	0	3,284 K
services.exe	532	Services	0	7,832 K
lsass.exe	540	Services	0	9,776 K
lsm.exe	560	Services	0	5,164 K
svchost.exe	884	Services	0	22,528 K
svchost.exe	276	Services	0	9,860 K
svchost.exe	348	Services	0	12,136 K
spoolsv.exe	1036	Services	0	8,216 K
svchost.exe	1068	Services	0	7,888 K
svchost.exe	2020	Services	0	17,324 K
notepad.exe	1276	Services	0	4,324 K
svchost.exe	1720	Services	0	3,172 K
SearchIndexer.exe	864	Services	0	14,968 K
OSPPSVC.EXE	2584	Services	0	13,764 K
csrss.exe	372	RDP-Tcp#0	1	7,556 K
winlogon.exe	460	RDP-Tcp#0	1	5,832 K
rdpclip.exe	1600	RDP-Tcp#0	1	4,356 K
dwm.exe	772	RDP-Tcp#0	1	5,116 K
taskhost.exe	1700	RDP-Tcp#0	1	8,720 K
explorer.exe	2500	RDP-Tcp#0	1	66,444 K
splwow64.exe	2960	RDP-Tcp#0	1	4,152 K
cmd.exe	1260	RDP-Tcp#0	1	2,652 K
conhost.exe	2616	RDP-Tcp#0	1	5,256 K
audiodg.exe	980	Services	0	13,256 K
csrss.exe	2400	Console	3	3,512 K
winlogon.exe	2492	Console	3	5,772 K
LogonUI.exe	2864	Console	3	17,056 K
notepad.exe	376	Services	1	5,636 K
taskhost.exe	2812	Services	0	9,540 K
tasklist.exe	1208	RDP-Tcp#0	1	5,196 K
WmiPrvSE.exe	1276	Services	0	5,776 K

```
C:\Windows\system32>netstat -ano
```

Active Connections

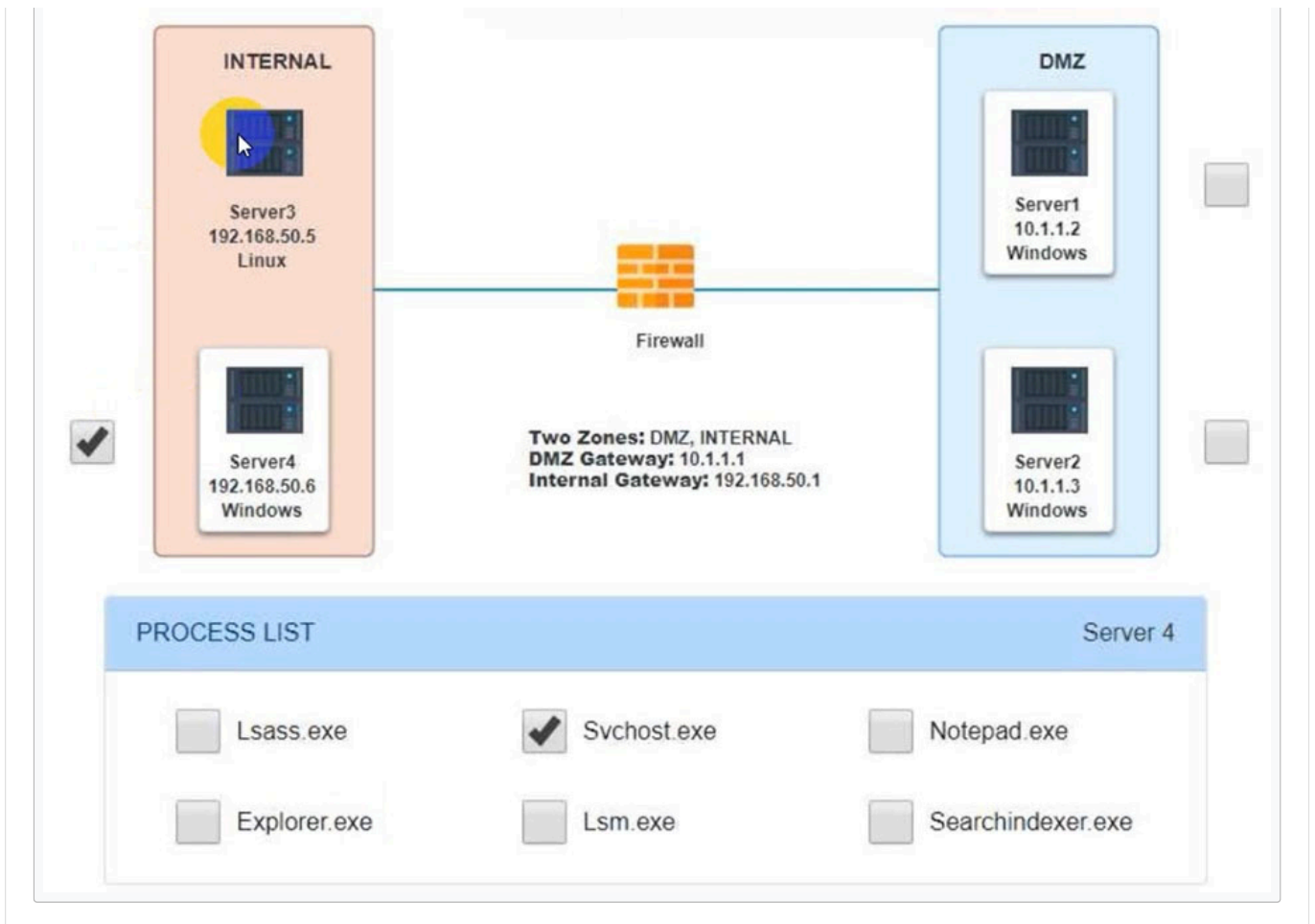
Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	716
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	516
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	440
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	808
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	920
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	536
TCP	0.0.0.0:49185	0.0.0.0:0	LISTENING	528
TCP	10.1.1.3:139	0.0.0.0:0	LISTENING	4
TCP	10.1.1.3:3389	192.168.50.5:49335	ESTABLISHED	516
TCP	10.1.1.3:50276	192.168.50.6:445	ESTABLISHED	4
TCP	:::135	:::0	LISTENING	716
TCP	:::445	:::0	LISTENING	4
TCP	:::3389	:::0	LISTENING	516

```
C:\Users\Team3>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	24 K
System	4	Services	0	636 K
smss.exe	300	Services	0	900 K
csrss.exe	384	Services	0	3,252 K
wininit.exe	440	Services	0	3,272 K
services.exe	528	Services	0	8,212 K
lsass.exe	536	Services	0	10,140 K
lsm.exe	548	Services	0	5,360 K
svchost.exe	648	Services	0	6,572 K
svchost.exe	716	Services	0	6,472 K
svchost.exe	808	Services	0	14,372 K
svchost.exe	884	Services	0	44,856 K
svchost.exe	920	Services	0	22,580 K
svchost.exe	100	Services	0	8,700 K
svchost.exe	516	Services	0	13,236 K
spoolsv.exe	952	Services	0	9,964 K
svchost.exe	1060	Services	0	7,716 K
svchost.exe	904	Services	0	15,228 K
svchost.exe	2208	Services	0	3,156 K
SearchIndexer.exe	2252	Services	0	15,720 K
csrss.exe	848	Console	3	3,444 K
winlogon.exe	2864	Console	3	5,620 K
LogonUI.exe	1976	Console	3	17,080 K
csrss.exe	1408	RDP-Tcp#0	1	5,256 K
winlogon.exe	1520	RDP-Tcp#0	1	6,228 K
rdpclip.exe	1380	RDP-Tcp#0	1	4,504 K
dwm.exe	2656	RDP-Tcp#0	1	4,132 K
explorer.exe	2328	RDP-Tcp#0	1	58,948 K
taskhost.exe	1396	RDP-Tcp#0	1	5,504 K
conhost.exe	472	RDP-Tcp#0	1	5,120 K
conhost.exe	3004	RDP-Tcp#0	1	5,204 K
tasklist.exe	308	RDP-Tcp#0	1	5,180 K
WmiPrvSE.exe	372	Services	0	5,780 K

Suggested Answer: See explanation below.

Server 4, Svchost.exe -



R00ted Highly Voted 2 years, 9 months ago

The correct answer to the question is Server 4 & the process infected is SvcHost.exe.

Explanation:-

The IPs are within the RFC1918 class B range of 172.16.0.0 – 172.31.255.255

Both Servers 1 & 4 (internal) have the same communication with the same IPs for the same RDP(Remote Desktop Protocol [responsible for remote connecting to servers or computers with the same Windows OS])

which shows the system administrator remotely manages them

A connection between Server 1 & 4 is established with notepad.exe on server1 is connecting to port 443 on server 4

As per the question from a logical perspective, the server can be the web server where svchost.exe is listening to a different port rather than 443 & server 1(on DMZ) is trying to access the internal network on Server4 [which is malicious]

upvoted 52 times

Treymb6 2 years, 8 months ago

I think someone finally has the right answer with explanation here. Seems to be the only thing that makes sense.

Thank you for the detailed explanation.

upvoted 8 times

ApexPredator84 Highly Voted 2 years, 4 months ago

Got this one today!! Used Server 1 and notepad.exe. I didnt fail any pbqs...thanks for the deliberations fellas

upvoted 12 times

simpfemboy 2 years, 2 months ago

I understand server 1 & 4 but I'm having trouble finding an explanation for server 2 if you could help me out.

upvoted 1 times

NerdAlert 2 years, 2 months ago

how can you tell you didnt fail any pbqs?!

upvoted 4 times

Hershey2025 1 year, 11 months ago

It seems if you fail the exam, the exam will tell you at the end what questions you failed on.

upvoted 1 times

🗨️ 👤 **NerdAlert** 1 year, 11 months ago

no, it just says how well you did on different topics / exam objectives, not specific questions

upvoted 6 times

🗨️ 👤 **fuzzyguzzy** Most Recent 6 months, 4 weeks ago

Server 4 -> C2 (via svchost.exe)

Server 4 -> Server 1 (connection established from svchost.exe to notepad.exe via process injection)

Server 1 -> C2 (via notepad.exe, still through the injected process)

The attacker malware is pivoting from Server 4 to Server 1 through process injection. Svchost.exe from server 4 is malware as it's the source of infection.

upvoted 1 times

🗨️ 👤 **charles_carmichael** 11 months, 3 weeks ago

Despite instantly rejecting the idea of notepad being responsible for network connections, I did some research about this matter since there is so much divergence between Server 1 - notepad.exe and Server 4 - svchost.exe. I could be wrong and would gladly accept any corrections, but I have to say that I'd opt for the one with the notepad occurrence because of the following explanation:

Even though Notepad could use HTTPS (443) for its traffic, it wouldn't run as a service but as a console. You can test it yourself by opening some URL and URI. Anyway, it isn't common for this process to make network connections, and to run as a service it would have to be previously configured to do so.

Cobalt Strike and the Metasploit Framework use notepad.exe as a default process to spawn and inject into, as can be corroborated by their documentation and code.

Due to its high presence on Windows, notepad can often be used as the target for PE

Forti.SIEM has an integrated rule (medium severity) that triggers when there's any connection specifically made by the notepad process.

upvoted 1 times

🗨️ 👤 **JimmyJohnSubs** 1 year, 1 month ago

I am surprised no one has mentioned Metasploit and Meterpreter. You (as students) should use these tools and see what is possible. It is possible to get a foothold onto a system and then move the malicious process to another service. I have personally moved the malicious process to Notepad and executed actions on the local system and network.

upvoted 1 times

🗨️ 👤 **bettyboo** 1 year, 3 months ago

I don't think it's notepad.exe <https://www.file.net/process/notepad.exe.html>

upvoted 1 times

🗨️ 👤 **JakeH** 1 year, 8 months ago

This was one of the PBQ's on my exam - 10/12/23.

upvoted 4 times

🗨️ 👤 **AAASSAA** 1 year, 11 months ago

Server4 192.168.50.6

Server1 10.1.1.1

10.1.1.2:57433 >> 192.168.50.6:433 PID 1276 (notepad.exe)

192.168.50.6:433 << 10.1.1.2:57433 PID 348 (svchost.exe)

Answer is Server4 (svchost.exe)

upvoted 5 times

🗨️ 👤 **Starburst** 1 year, 12 months ago

This question and #321 are duplicates. This question has the proper exhibits where 321 does not. The conclusion from both discussions is that Server4 and Svchost.exe are correct.

upvoted 1 times

🗨️ 👤 **iwontellyou** 2 years ago

Passed it the other day, this one was in it.

I selected Server 4, svchost.exe.

Read the question carefully, it asks specifically which server & process HOSTS the malware. Realistically you'd select both, but you can only choose one. Then why serv 4 svchost and not serv 1 notepad its counter part? Simple. It asks who hosts the malware, it has to be server 4 because even if notepad was malware of some kind on server 1 it shouldn't ever be able to talk to a server in the internal network without some compromise on that end. It has to cross the DMZ barrier. Being port 443 this looks like a reverse shell, where they've chosen port 443 to obfuscate it

upvoted 8 times

🗨️ 👤 **alayeluwa** 2 years, 2 months ago

Server 1 and Notepad is the correct answer. Notepad should be running as a console if it was legitimate.

upvoted 2 times

🗨️ 👤 **Nouuv** 2 years ago

notepad appearing as a service in task manager is not considered malware, it is a legitimate system process running in background as a service for other applications or processes. This is usually found in situations where Notepad is being used as part of a larger system or software component, and is not meant to be interacted with directly by the user.

upvoted 2 times

🗨️ 👤 **Hershey2025** 2 years, 3 months ago

Server1 nodepad.exe because notepad.exe is not a service, it would run as console.

upvoted 2 times

🗨️ 👤 **Joshey** 2 years, 3 months ago

People, the question is why would notepad process be communicating out to another host...OVER BL**DY 443.....BRAAAAAAAA THATS SUSPICIOUS ENOUGH FOR ME MATE

upvoted 8 times

🗨️ 👤 **lovegate229** 2 years, 3 months ago

Fellas. All you need to remember is that svchost.exe is an executable that Windows use to aggregate a lot services that need access to the same Dynamic Link Libraries (DLL) to run processes, hence svchost.exe could be masqueraded as a virus, it is not in this instance. Now, understand that notepad,msword, pdf, jpeg, pnf or something of that nature is not an executable hence if you see something like that running on your system as an executable, it is a clear indicator of compromise, and you should further look into it. Therefore Server1 has been compromised.

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

I am still mulling over this one, but here is more discussions in case anyone wanted to read more.

<https://www.examttopics.com/discussions/comptia/view/20574-exam-cs0-001-topic-1-question-141-discussion/>

upvoted 4 times

🗨️ 👤 **sho123** 2 years, 6 months ago

the answer is server 2 and csrss.exe . it is running as multiple application on server 2

upvoted 1 times

🗨️ 👤 **Nouuv** 2 years ago

that's normal

upvoted 2 times

🗨️ 👤 **david124** 2 years, 7 months ago

server 4 and svchost.exe

upvoted 1 times

While reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with political propaganda. Which of the following BEST describes this type of actor?

- A. Hacktivist
- B. Nation-state
- C. Insider threat
- D. Organized crime

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. For sure, this is an Activist.
upvoted 1 times

🗳️ 👤 **david124** 2 years, 7 months ago

Selected Answer: A

A Correct answer.
upvoted 1 times

🗳️ 👤 **loveyuki147** 2 years, 9 months ago

Selected Answer: A

CompTIA CySA Study Guide Page 104: Hacktivists are activists who use hacking as a means to a political or philosophical end.
upvoted 2 times

🗳️ 👤 **Fastyt0p** 2 years, 9 months ago

Selected Answer: A

Server 1 and Notepad.exe
upvoted 1 times

🗳️ 👤 **cyberseckid** 2 years, 9 months ago
can you clarify why ?
upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

hacktivist.
upvoted 1 times

🗳️ 👤 **Laudy** 2 years, 10 months ago

Selected Answer: A

"political propaganda" is the key term here.
upvoted 3 times

🗳️ 👤 **Belijmag** 2 years, 10 months ago

Selected Answer: A

Answer A correct
upvoted 1 times

A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

- A. detection and prevention capabilities to improve.
- B. which systems were exploited more frequently.
- C. possible evidence that is missing during forensic analysis.
- D. which analysts require more training.
- E. the time spent by analysts on each of the incidents.

Suggested Answer: A

Reference:

<https://www.recordedfuture.com/diamond-model-intrusion-analysis/>

Community vote distribution

A (100%)

🗳️ 👤 **Davar39** Highly Voted 📅 3 years, 1 month ago

Correct answer.
upvoted 5 times

🗳️ 👤 **HereToStudy** Most Recent 📅 2 years, 2 months ago

Selected Answer: A
Those other choices are strange
upvoted 2 times

🗳️ 👤 **Leonidasss** 📅 2 years, 3 months ago

Selected Answer: A
correct is the way
upvoted 1 times

🗳️ 👤 **2Fish** 📅 2 years, 3 months ago

Selected Answer: A
A. Is correct, Per Jason Dion.
upvoted 1 times

🗳️ 👤 **david124** 📅 2 years, 7 months ago

Selected Answer: A
A Correct answer.
upvoted 1 times

🗳️ 👤 **Study4America** 📅 2 years, 8 months ago

I will go with A
upvoted 1 times

🗳️ 👤 **EVE12** 📅 2 years, 9 months ago

The Diamond Model of Intrusion Analysis

Finalized in 2013, the Diamond Model of Intrusion Analysis serves as a practical analytical methodology for cybersecurity analysts to utilize before, during, and after cybersecurity intrusions. Aimed at strengthening our intrusion analysis, it's the first model of its kind that scientifically incorporates both the fundamentals of threat actors/activities (offense) and the analytical techniques needed to discover, understand, and counteract these threat actors/activities (defense).

upvoted 1 times

🗳️ 👤 **amateurguy** 📅 2 years, 9 months ago

Selected Answer: A
A is correct.
upvoted 1 times

🗨️ 👤 **Laudy** 2 years, 10 months ago

Selected Answer: A

"an incident" = so not B.... Diamond Model has nothing to do with tracking training or time tracked, so not D or E.

I was think C because the Diamond model is very evidence based, but it states forensics. That's likely outdated unless harddrives were kept.

But A seems like a decent possibility as Diamond Model also focuses on enumerating the adversary and developing countermeasures.

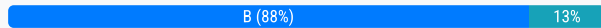
upvoted 3 times

An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

- A. SCADA
- B. CAN bus
- C. Modbus
- D. IoT

Suggested Answer: B

Community vote distribution



boletri Highly Voted 2 years, 4 months ago

Selected Answer: B

Answer is B.

Vehicles and Drones (CAN Bus)

Automobiles and unmanned aerial vehicles (UAV), or drones, contain sophisticated electronics to control engine and power systems, braking and landing, and suspension/stability. Modern vehicles are increasingly likely to have navigation and entertainment systems, plus driver-assist or even driverless features, where the vehicle's automated systems can take control of steering and braking. The locking, alarm, and engine immobilizer mechanisms are also likely to be part of the same system. Each of these subsystems is implemented as an electronic control unit (ECU), connected via one or more controller area network (CAN) serial communications buses. The principal external interface is an Onboard Diagnostics (OBD-II) module. The OBD-II also acts as a gateway for multiple CAN buses.

Official CompTia Cysa+ Course Material

upvoted 5 times

LayinCable Most Recent 1 year, 9 months ago

Selected Answer: B

CAN Buses is the topology used in vehicle's today. This is the only answer, and it's pretty straight forward.

upvoted 2 times

Calvin616 2 years, 3 months ago

Selected Answer: B

Per ChatGpt: The issue with the code excerpt is that it uses the strcpy function to copy data from a file to a buffer without checking the size of the data being copied, which can result in a buffer overflow and cause the program to crash.

Therefore, a security analyst should recommend replacing the strcpy function with a safer alternative, such as strncpy, which allows specifying the maximum number of bytes to copy to the buffer. Additionally, it would be best to perform input sanitization to ensure that the data being read from the file is in the expected format and size, and to increase the size of the file data buffer if needed.

Therefore, the correct answer is B. Replace the strcpy function.

upvoted 2 times

rmwilson 2 years, 3 months ago

wrong question bro

upvoted 7 times

Leonidasss 2 years, 3 months ago

Selected Answer: B

Agree with all of you

upvoted 1 times

2Fish 2 years, 3 months ago

Selected Answer: B

B. Agree with most everyone on this.

upvoted 1 times

🗨️ 👤 **bdub16** 2 years, 7 months ago

Selected Answer: B

B is correct. CAN Bus is the Attack Vector
upvoted 1 times

🗨️ 👤 **david124** 2 years, 7 months ago

Selected Answer: B

b Correct answer.
upvoted 1 times

🗨️ 👤 **Weezyfbaby** 2 years, 8 months ago

Selected Answer: B

The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.
upvoted 4 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: B

I might be overthinking this, but the questions specifically states these are new vehicles, I take that to mean these are recent models. CAN bus has next to no security features, leaving it up to the manufacturer to implement them. In older models of cars, there is less external communication from CAN bus, leading me to believe B is the correct answer
upvoted 1 times

🗨️ 👤 **piotr3439** 2 years, 9 months ago

Selected Answer: B

After researching, I correct my answer to the CAN BUS.
upvoted 1 times

🗨️ 👤 **EVE12** 2 years, 9 months ago

CAN Bus

While autonomous vehicles may still be a few years off, when they arrive they will make use of a new standard for vehicle-to-vehicle and vehicle-to-road communication. Controller Area Network (CAN bus) is designed to allow vehicle microcontrollers and devices to communicate with each other's applications without a host computer. Sounds great, huh?

It turns out CAN is a low-level protocol and does not support any security features intrinsically. There is also no encryption in standard CAN implementations, which leaves these networks open to data interception.

Failure by vendors to implement their own security measures may result in attacks if attackers manage to insert messages on the bus. While passwords exist for some safety-critical functions, such as modifying firmware, programming keys, or controlling antilock brake actuators, these systems are not implemented universally and have a limited number of seed/key pairs (meaning a brute-force attack is more likely to succeed). Hopefully, an industry security standard for the CAN bus will be developed at some point.

upvoted 1 times

🗨️ 👤 **Felix010** 2 years, 9 months ago

it's B. if it doesn't have any network capacity, it won't be an IoT device
upvoted 1 times

🗨️ 👤 **Belijmag** 2 years, 9 months ago

Also agree with D
upvoted 1 times

🗨️ 👤 **Belijmag** 2 years, 9 months ago

Selected Answer: D

Agree with D
upvoted 1 times

🗨️ 👤 **piotr3439** 2 years, 9 months ago

Selected Answer: D

"Some of the most critical IoT deployments are those found on vehicles and drones. These systems have a dramatic impact on the safety of human life and should be carefully monitored for security issues." CySA+ Study Guide Mike Chapple, David Seidl
IoT include CAN bus and Modbus.



upvoted 2 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: B

B - can bus

upvoted 1 times

  **Laudy** 2 years, 10 months ago

Selected Answer: B

I was thinking "CAN bus" before I saw the answer.

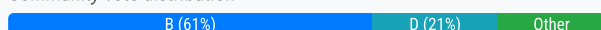
upvoted 2 times

An internally developed file-monitoring system identified the following excerpt as causing a program to crash often: `char filedata[100]; fp = fopen("access.log", "r"); strcpy(filedata, fp); printf("%s\n", filedata);`
Which of the following should a security analyst recommend to fix the issue?

- A. Open the access.log file in read/write mode.
- B. Replace the strcpy function.
- C. Perform input sanitization.
- D. Increase the size of the file data buffer.

Suggested Answer: B

Community vote distribution



Abyad Highly Voted 2 years, 8 months ago

B
comptia study guide
Use of insecure functions can make it much harder to secure code.
Functions like strcpy, which don't have critical security features built in, can result in code that is easier for attackers to target. In fact, strcpy is the only specific function that the CySA+ objectives call out, likely because of how commonly it is used for buffer overflow attacks in applications written in C. strcpy allows data to be copied without caring whether the source is bigger than the destination. If this occurs, attackers can place arbitrary data in memory locations past the original destination, possibly allowing a buffer overflow attack to succeed.
upvoted 15 times

wico1337 2 years, 8 months ago
Sure, that fixes the security issue. But this isn't a question about security. It's a question about application crashing...
upvoted 2 times

ra774ra7 2 years, 5 months ago
The question clearly states security
"Which of the following should a security analyst recommend to fix the issue?"
upvoted 4 times

2Fish 2 years, 3 months ago
Agree. 'strcpy' should be replaced with something like 'strncpy'. 'strncpy' is used to avoid buffer overflow issues that can arise when copying strings using functions like strcpy that do not have a parameter to specify the maximum number of characters to copy.
upvoted 1 times

AbdallaAM Most Recent 1 year, 8 months ago

Selected Answer: B

****Incorrect Usage of 'strcpy'**: The 'strcpy' function is used to copy a string from one memory location to another. However, in this snippet, 'fp' (a file pointer) is being passed as an argument to 'strcpy', which is incorrect. 'strcpy' expects a character pointer as its source argument, not a file pointer.**

B. Replace the strcpy function:

- This is a step in the right direction. Replacing 'strcpy' with a function like 'fgets' or 'fread' would be more appropriate for reading data from a file.
upvoted 1 times

kiduuu 2 years, 3 months ago

Selected Answer: B

The code snippet provided shows that the program is reading data from the "access.log" file and then copying it into a buffer using the "strcpy" function. However, the size of the buffer is fixed at 100 bytes, which could cause a buffer overflow if the data in the file is larger than 100 bytes. This can lead to a crash or other security vulnerabilities.

To fix this issue, the security analyst should recommend replacing the "strcpy" function with a safer alternative, such as "strncpy" or "memcpy," which take a size parameter to ensure that only a certain number of bytes are copied to the buffer. Additionally, the size of the buffer should be increased to accommodate larger files if necessary.

upvoted 2 times

🗨️ 👤 **Qongo** 2 years, 4 months ago

I think Option B is correct.

Increasing the size of the buffer may temporarily fix the symptom of the issue, but it does not address the underlying problem of a potential buffer overflow vulnerability.

upvoted 1 times

🗨️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: B

I taked from book;

C and C++ contain built-in functions suchas strcpy that do not provide a default mechanism for checking if data will overwritethe boundaries of a buffer.

So i going with B.

upvoted 1 times

🗨️ 👤 **encxorblood** 2 years, 5 months ago

Selected Answer: B

The strncpy() function is insecure because if the NULL character is not available in the first n characters in the source string then the destination string will not be NULL terminated.

upvoted 1 times

🗨️ 👤 **smudder** 2 years, 5 months ago

Selected Answer: C

C. Perform input sanitization.

The issue with the code excerpt is that it is not properly handling user input, which can lead to a program crash if the access.log file contains unexpected or malicious data. Input sanitization is the process of ensuring that user input is valid and safe to use. This can involve checking for and removing invalid characters, validating the input against a known set of acceptable values, or implementing other techniques to ensure that the input is safe to use. By performing input sanitization, the security analyst can help to prevent the program from crashing due to unexpected or malicious input.

upvoted 2 times

🗨️ 👤 **jleonard_ddc** 2 years, 5 months ago

Selected Answer: B

B for sure. But that's not just because every study guide says strcpy is bad. More importantly, it's about why.

strcpy is bad because it's susceptible to buffer overflow. The hint that the program is crashing is implying it's because of "buffer overflow".

A and D bot had me going at first, but are eliminated after further review for this reason:

strcpy parameters are (dest, src) [https://www.tutorialspoint.com/c_standard_library/c_function_strcpy.htm]

So for this question

src = fp (the access.log file)

dest = the filedata array

This means the file buffer is irrelevant, as are the permissions. The array is too small - that's why the buffer is having issues. But that's not the file buffer but the string buffer.

Input sanitization is not even related to the discussion.

upvoted 3 times

🗨️ 👤 **david124** 2 years, 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

Sybex Study Guide & Sybex 1000 Practice Exam Books: "The CySA+ exam objectives mention strcpy, so you should be sure you know why it is a concern. Outside of the exam, we suggest reading more about buffer overflows instead of just knowing about strcpy." "The strcpy() function is notorious for leading to buffer overflow vulnerabilities and must be used very carefully." Only choosing B because it's covered in the objectives so much.

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

I choose B based on Exam Objectives

upvoted 1 times

🗨️ 👤 **trainingsmits** 2 years, 5 months ago

Selected Answer: B

strcpy is an insecure code function specifically called out in the comptia study guides

upvoted 2 times

🗨️ 👤 **trojan123** 2 years, 6 months ago

Selected Answer: D

D.

Although there are some alternatives to some of these functions advertised as safe, those functions may themselves be vulnerable to other types of attacks. The strncpy() function, for example, is said to be a safer version of strcpy(), because it enables a maximum size to be specified. However, the strncpy() function doesn't null terminate the destination if the buffer is completely filled, which may lead to stability problems in code. As a security analyst, it's important that you not take alternative recommendations for granted. Doing so can give you a false sense of security and may introduce additional vulnerabilities.

Proposing other functions can lead to a different issues, to fix this one we can increase the buffer.

upvoted 1 times

🗨️ 👤 **trojan123** 2 years, 6 months ago

Selected Answer: B

According to written code data copies from access.log to array, even if you will increase the size of the buffer, you never know the size of access.log, next time it might be bigger than your new buffer value, such vulnerable functions like strcpy should be avoided to use.

The answers are tricky, of course increasing of the buffer can help, but this is not the best solution.

upvoted 1 times

🗨️ 👤 **trojan123** 2 years, 6 months ago

Changing my answer to D.

Although there are some alternatives to some of these functions advertised as safe, those functions may themselves be vulnerable to other types of attacks. The strncpy() function, for example, is said to be a safer version of strcpy(), because it enables a maximum size to be specified. However, the strncpy() function doesn't null terminate the destination if the buffer is completely filled, which may lead to stability problems in code. As a security analyst, it's important that you not take alternative recommendations for granted. Doing so can give you a false sense of security and may introduce additional vulnerabilities.

upvoted 1 times

🗨️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: B

B is the correct answer

upvoted 2 times

🗨️ 👤 **Abyad** 2 years, 7 months ago

strcpy is

the only specific function that the CySA+ objectives call out

upvoted 3 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: D


buffer needs to be bigger than 100 bytes to not crash, so the answer should be D

upvoted 3 times

  **forklord72** 2 years, 8 months ago

ignoring the typo, am I crazy for thinking D is the only viable answer? How does read/write access prevent a program from crashing? I think maybe it could be B but I have no idea what that even means.

upvoted 1 times

  **581777a** 1 year, 8 months ago

yepppp

upvoted 1 times

A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?

- A. VDI
- B. SaaS
- C. CASB
- D. FaaS

Suggested Answer: C

Community vote distribution

B (69%)

C (31%)

🗳️ **SolventCourseisSCAM** Highly Voted 2 years, 8 months ago

Selected Answer: B

CASB doesn't store the data and it's NOT a cloud model.

upvoted 14 times

🗳️ **catastrophe** Highly Voted 2 years, 5 months ago

The answer is C. The question isn't asking which cloud model is to be used. It's asking which of the following choices will ALLOW (give permission, authorization, unhindered access) to keep ALL DATA (could be PII or other sensitive data) on THIRD-PARTY NETWORK (Cloud Service Provider's Network). Assuming the IT Management team has chosen SaaS as their cloud model, this doesn't mention how the data will be monitored, secured and other requirements to ensure the company is within compliance. What if the cloud provider is located in a location that doesn't allow specific data to be stored in that location? With a CASB deployed either locally or within the cloud the security team would be able to ensure policies are still enforced, monitor user activity, maintain logs, etc. This means if you are in the US and for reasons you have data that contains PII on a citizen from another country that doesn't allow the US to maintain or collect that data, the CASB would be able to prevent that data from being stored. Staying in compliance and providing proper threat management allows all data to be kept on a third part network.

upvoted 13 times

🗳️ **jiggly** Most Recent 6 months, 2 weeks ago

Selected Answer: C

Data storage would typically use a PaaS cloud model. A SaaS model has more 3rd party involvement, which is a potential security risk, and the question did not mention anything about software hosting, just data. The question is not specifically asking what cloud model should be used, but it is asking about security recommendations and that alone would probably rule out a SaaS model based on the info given. CASB appears to be the correct answer to "allow all data to be kept on the third-party network."

upvoted 1 times

🗳️ **taistein** 1 year, 6 months ago

This would be similar to One Drive (For Storage), which would be classed as SaaS

VDI (Virtual Desktop Infrastructure) provides virtual desktops but does not necessarily store all data on the third-party network.

CASB (Cloud Access Security Broker) is a service that monitors and controls user access and data sharing across multiple cloud platforms. It does not store all data.

FaaS (Functions as a Service) provides execution environments for event-driven code snippets called functions. It is not primarily for data storage.

upvoted 1 times

🗳️ **dickchappy** 1 year, 7 months ago

Selected Answer: B

Everyone saying C is overthinking it, the question is almost certainly stating that the security team is being asked to recommend a cloud model. CASB is not a cloud model, it manages access to the cloud and has nothing to do with how much data is stored. SaaS has all of your data stored on it.

upvoted 2 times

🗳️ **581777a** 1 year, 8 months ago

Selected Answer: B

B. SaaS (Software as a Service).

SaaS is a cloud computing model where the third-party provider hosts applications and data on their infrastructure. With SaaS, data and applications are stored on the third-party network, and users access them over the internet. This allows the company to leverage the provider's infrastructure while maintaining control and access to their data.

upvoted 2 times

🗳️ 👤 **kumax** 1 year, 8 months ago

Selected Answer: C

ChatGPT:

To allow all data to be kept on a third-party network, the best choice among the options provided is "Cloud Access Security Broker (CASB)." CASB solutions help organizations monitor and manage the use of cloud services and data that is stored in the cloud. CASB provides visibility and control over data, even when it's stored in third-party cloud services. This allows the organization to maintain security and compliance when utilizing cloud-based storage services.

While SaaS (Software as a Service) can indeed involve using third-party cloud applications, it doesn't inherently ensure that all data is kept on the third-party network. The location of data storage can vary depending on the SaaS provider and the specific service being used.

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 8 months ago

Today ChatGPT said B...

Please, let's not base our answer on what chatgpt says.

upvoted 1 times

🗳️ 👤 **AbdallaAM** 1 year, 8 months ago

Selected Answer: B

B

B. SaaS (Software as a Service):

SaaS provides software applications on a subscription basis and hosts data on the provider's infrastructure. This model can effectively offload the risks of data storage to a third-party network.

C. CASB (Cloud Access Security Broker):

CASBs provide visibility, compliance, data security, and threat protection for cloud services. While they add a layer of security, they don't inherently host or store data themselves.

upvoted 1 times

🗳️ 👤 **Dree_Dogg** 1 year, 9 months ago

Selected Answer: B

"All Data." Gotta go with with SaaS

upvoted 1 times

🗳️ 👤 **Nucleric** 1 year, 9 months ago

According to what I have read, CASB already includes IaaS, SaaS and PaaS so the answer should be C

upvoted 1 times

🗳️ 👤 **kill_chain** 1 year, 10 months ago

Selected Answer: B

Is CASB a cloud model?

upvoted 1 times

🗳️ 👤 **attesco** 1 year, 11 months ago

Selected Answer: C

The question ask here is- Which choices listed will allow. Therefore, CASB is a gatekeeper, allowing organisation to extend the reach of their security policies, authentication, DLP, and firewalls beyond their own infrastructure.

upvoted 1 times

🗳️ 👤 **Nouuv** 2 years ago

it's VDI - "with VDI, company can completely offload their IT infrastructure to a 3rd party service enterprise" - from certmaster.

upvoted 1 times



🗳️ 👤 **Kainas** 2 years, 2 months ago

Selected Answer: C

IT already picked the cloud model and is now just asking input from the sec team. Sec team should recommend the use of a CASB to make sure all data is allowed to be stored and remains on the third-parties network.

Would say poor wording for the question though.

upvoted 1 times

  **2Fish** 2 years, 3 months ago

Selected Answer: B



B. "Offloading risks", "security model", to me points to SaaS. CASB would giving visibility into the platform.

upvoted 2 times

  **2Fish** 2 years, 3 months ago

Hmmm... after coming back to this question.. I will have to change my response to C.



upvoted 2 times

  **kiduuu** 2 years, 3 months ago

Selected Answer: B

SaaS is a cloud computing model in which software applications are provided by a third-party provider over the internet. The software and data are hosted on the provider's servers, allowing the organization to offload the risks of data storage to the third-party. With SaaS, the organization can access the software and data from any device with an internet connection, and the third-party provider is responsible for maintaining the software and data security.

upvoted 3 times

  **Cock** 2 years, 4 months ago

Selected Answer: C

CASB (Cloud Access Security Broker) is a security tool that acts as a gateway between an organization's on-premises infrastructure and a cloud provider's infrastructure. It provides visibility into the cloud environment, and the capability to enforce security policies for data stored on the cloud, ensuring that all data remains on the third-party network. CASB also enables the IT team to monitor and manage data access by providing controls such as data loss prevention (DLP), user behavior analytics (UBA), and identity and access management (IAM).

upvoted 4 times

A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Date/time	Destination	Protocol	Host	Info
2020-08-20	92.168.4.52	HTTP	utoftor.com	POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:

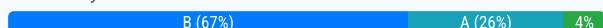
```
Post /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$$.0.k..4.4.RQA.6.... HTTP/1.1 200 OK
Server: nginx/1.6.2
```

Which of the following describes what has occurred?

- A. The host attempted to download an application from utoftor.com.
- B. The host downloaded an application from utoftor.com.
- C. The host attempted to make a secure connection to utoftor.com.
- D. The host rejected the connection from utoftor.com.

Suggested Answer: D

Community vote distribution



Lobo Highly Voted 2 years, 8 months ago

It's POST - there's no downloading here... it's upload... so A/B are out.

Code 200 so nothing was rejected - D is out.

That leaves C except it says HTTP not HTTPS so don't see any attempt of a secure connection... - bad question...

upvoted 32 times

Kainas Highly Voted 2 years, 2 months ago

Selected Answer: A

1. 92.168.4.52 made an HTTP POST request to utoftor.com, sending an "application/octet-stream" content type.

2. Application/octet-stream type is binary that can be used for any kind of data, including audio, video, images, or executable files and used when the content being transmitted is unknown or can be any type of data, such as in the case of file uploads or downloads.

3. "HTTP/1.1 200 OK" indicates that the request was successfully received and processed by the server, but it does not confirm a download or transfer.

Correct choice:

A. The host attempted to download an application from utoftor.com.

upvoted 7 times

alialzehhawi Most Recent 9 months ago

A is the correct answer. B is not correct because If the host were downloading an application or file, you would typically see an HTTP GET request and possibly some content coming back in the response (such as a file or application data)

upvoted 1 times

dickchappy 1 year, 7 months ago

Selected Answer: C

Even if you were to use POST to download something, which seems odd, application/octet-stream does not guarantee it's an application. Its a general term covering many different file types. C is the only reasonable answer here I think.

upvoted 1 times

🗨️ **JaronW214** 1 year, 7 months ago

Comptia really just wants you to focus on HTTP/1.1 ERROR CODE 200 OK (The questions is looking to know if you understand what the error codes stand for) In this case 200 OK means the request was successful, and the server has returned the requested data.

upvoted 1 times

🗨️ **2Fish** 2 years, 3 months ago

Selected Answer: B

B. Mostly because of the "application/octet-stream"

upvoted 1 times

🗨️ **kiduuu** 2 years, 3 months ago

Selected Answer: B

The server responded with an HTTP 200 OK status code, which means that the request was successful, and the server was able to process it. Connection close is only to close the connection after the transaction finishes

upvoted 1 times

🗨️ **encxorblood** 2 years, 5 months ago

Selected Answer: B

The HTTP 200 OK success status response code indicates that the request has succeeded. A 200 response is cacheable by default.

upvoted 2 times

🗨️ **xyz47** 2 years, 5 months ago

There's no good answer in here.

POST is HTTP method for upload not for download.

Connection: close is there only to close the connection after the transaction finishes.

HTTP 1.1 is just the protocol version that should be used in this conversation between client and server and has nothing to do with establishing secure or unsecure connection at this point.

The security header is HSTS that's absent.

upvoted 2 times

🗨️ **kiduuu** 2 years, 3 months ago

POST is an HTTP method used to send data to a web server to create or update a resource on the server. When a client, such as a web browser, sends a POST request to a server, it includes a payload, which can be any data that the client wants to send to the server

upvoted 2 times

🗨️ **HNICA** 2 years, 6 months ago

If the connection was closed, please ask yourself = how could you download a file without Internet?

upvoted 1 times

🗨️ **CertKid** 2 years, 5 months ago

are you retarded...?

upvoted 4 times

🗨️ **CatoFong** 2 years, 4 months ago

c'mon kid...wtf is that?

upvoted 2 times

🗨️ **sudoptgoaway** 1 year, 8 months ago

lmao..

upvoted 1 times

🗨️ **prntscrn23** 2 years, 6 months ago

Selected Answer: B

I think this is B. The host downloaded an application that has an unknown file extension or a file that needs to be opened by a specific application i.e. word, spreadsheet etc..

This is based from the Info "(Application/octet-stream)

<https://isotropic.co/what-is-octet-stream/>

upvoted 3 times

🗨️ **david124** 2 years, 7 months ago

Selected Answer: B

B correct answer

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: B

very bad wordy question. Post means sending data, so it is uploading, not downloading. 210 and 200 codes means that the attempts are successful.

There is no answer because whole options are wrong. If I get this question on the exam, I will choose B.

upvoted 3 times

🗨️ 👤 **Tascjfbosafj** 2 years, 8 months ago

Selected Answer: B

It's B.

upvoted 1 times

🗨️ 👤 **gwanedm** 2 years, 8 months ago

post means send data to the server for processing and 201 means the post/put request was successful.

upvoted 2 times

🗨️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: B

Post and 200 means they were successful

upvoted 2 times

🗨️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: B

Code 200...b is answer

upvoted 1 times

A security team implemented a SIEM as part of its security-monitoring program. There is a requirement to integrate a number of sources into the SIEM to provide better context relative to the events being processed. Which of the following BEST describes the result the security team hopes to accomplish by adding these sources?

- A. Data enrichment
- B. Continuous integration
- C. Machine learning
- D. Workflow orchestration

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. Absolutely Data Enrichment
upvoted 2 times

🗳️ 👤 **david124** 2 years, 7 months ago

Selected Answer: A

A correct answer
upvoted 1 times

🗳️ 👤 **Jimmycyber123** 2 years, 8 months ago

Selected Answer: A

data Enrichment is the right answer
upvoted 1 times

🗳️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: A

Data Enrichment
-The process of incorporating new updates and information to organizations existing database to improve accuracy
upvoted 2 times

🗳️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: A

A- Adding sources to the SIEM to provide more accurate results
upvoted 1 times

🗳️ 👤 **Laudy** 2 years, 10 months ago

Selected Answer: A

Definitely A.
upvoted 4 times

Which of the following organizational initiatives would be MOST impacted by data sovereignty issues?

- A. Moving to a cloud-based environment
- B. Migrating to locally hosted virtual servers
- C. Implementing non-repudiation controls
- D. Encrypting local database queries

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. Moving your data to the cloud could cause issues depending on the location.
upvoted 1 times

🗳️ 👤 **david124** 2 years, 7 months ago

Selected Answer: A

a correct answer
upvoted 1 times

🗳️ 👤 **Jimmycyber123** 2 years, 8 months ago

Selected Answer: A

cloud is correct as you are moving your data to someone else hardware.
upvoted 1 times

🗳️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: A

A is the correct answer
upvoted 1 times

🗳️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: A

Data sovereignty is the idea that data is subject to the laws/governance of the country it resides.
By moving to a cloud-based environment, the organization will be subject to the laws of where the data is being hosted, and also the laws of the country the organization resides in also
upvoted 3 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

cloud based environment.
upvoted 1 times

🗳️ 👤 **Laudy** 2 years, 10 months ago

Selected Answer: A

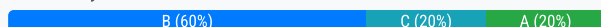
Moving to a cloud-based environment. Definitely. You have to look into where the data is stored across their servers. Could be around the world in several places...
Not to mention where you're accessing from. Yeesh.
upvoted 1 times

A help desk technician inadvertently sent the credentials of the company's CRM in cleartext to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident. According to the incident response procedure, which of the following should the security team do NEXT?

- A. Contact the CRM vendor.
- B. Prepare an incident summary report.
- C. Perform postmortem data correlation.
- D. Update the incident response plan.

Suggested Answer: D

Community vote distribution



🗳️ **moonash** Highly Voted 2 years, 5 months ago

The technician sent to employees PERSONAL EMAIL. I think that is the key word. The actions technician took don't seem to contain the issue at hand. How does resetting Corporate Account or Corporate Email affect PERSONAL email? The incident report document needs to be updated or technician needs to contact CRM. I would go with A to contain.

upvoted 6 times

🗳️ **nomad421** Highly Voted 2 years, 4 months ago

First of all, I despise all these questions as they are structured badly. But I can see why they claim the answer is D. Their incident response plan is is flawed or they at least need to train their help desk better. However, based on the incident response plan,, containment should be achieved by contacting the CRM and resetting the password for the CRM account. My vote is A

upvoted 5 times

🗳️ **fuzzyguzzy** Most Recent 6 months, 4 weeks ago

Selected Answer: C

The actions technician took haven't resolved the issue because:

- * The CRM credentials haven't been reset
- * The credentials were sent to a personal email

The security team needs to investigate this further and do further resets, thus C is the answer.

upvoted 1 times

🗳️ **glenn Dexter** 1 year, 2 months ago

Selected Answer: B

After the incident has been handled by the help desk technician and reported to the security team, the immediate next step in the incident response process is to prepare an incident summary report.

This report should document the details of the incident, including what happened, when it occurred, how it was discovered, and the actions taken to mitigate and remediate the incident.

The incident summary report provides a formal record of the incident for internal documentation purposes and may also be used for reporting to senior management, compliance purposes, or future incident response planning.

While updating the incident response plan (Option D) may be necessary in the long term to incorporate lessons learned from the incident, it is not the immediate next step following the incident.

upvoted 1 times

🗳️ **RobV** 1 year, 6 months ago

Selected Answer: C

Based on the official steps, the NEXT step after recovery is a postmortem.

Recovery:

Restore affected systems and services to normal operation.

Lessons Learned:

Conduct a postmortem analysis of the incident.

upvoted 2 times

🗨️ **dymson** 1 year, 7 months ago

Selected Answer: C

I agree with skibby16

upvoted 1 times

🗨️ **skibby16** 1 year, 8 months ago

Selected Answer: C

The security team should perform postmortem data correlation next after receiving notification of the incident from the help desk technician. Postmortem data correlation is an activity that involves analyzing data from various sources (such as logs, alerts, reports, etc.) to identify root causes, impacts, indicators of compromise (IoCs), lessons learned, and recommendations for improvement after an incident³. Postmortem data correlation can help the security team to Determine how the incident occurred and how it was detected and resolved, Assess the scope and severity of the incident and its effects on confidentiality, integrity, and availability, Identify any gaps or weaknesses in security controls or processes that contributed to the incident, Develop action plans or remediation strategies to prevent recurrence or mitigate future incidents

upvoted 2 times

🗨️ **AbdallaAM** 1 year, 8 months ago

Selected Answer: B

Among the given options, performing a postmortem data correlation (Option C) seems to be a logical next step as it will help the security team to analyze the incident in detail, learn from it, and identify measures to prevent such incidents in the future. However, preparing an incident summary report (Option B) could also be a viable next step for documentation and initial analysis. The specific next step would depend on the organization's established incident response procedures.

upvoted 2 times

🗨️ **sudoptgoaway** 1 year, 9 months ago

Given the context of the situation, the most appropriate next step is:

B. Prepare an incident summary report.

This step allows the security team to document the incident and its initial response, which is crucial for maintaining a record of the incident and ensuring that all relevant information is captured for further analysis and decision-making. After this step, the team can proceed with a more detailed analysis, data correlation, and any necessary follow-up actions, such as contacting the CRM vendor or updating the incident response plan.

-chatGPT

upvoted 1 times

🗨️ **581777a** 1 year, 8 months ago

It cracks me up when people use chatgpt. It just gave me a different answer than the one you have posted lol According to the incident response procedure described, the next step the security team should take is:

C. Perform postmortem data correlation.

Performing postmortem data correlation involves analyzing the incident to understand the full scope of the incident, how it occurred, and what data was potentially exposed. This analysis helps the security team identify any potential risks, vulnerabilities, or areas for improvement in the organization's security practices. It's an important step in incident response to ensure that similar incidents can be prevented in the future.

While the other options (A, B, and D) may be necessary in the broader incident response process, the immediate next step, in this case, should be to perform postmortem data correlation to understand the incident's details and implications.

upvoted 1 times

🗨️ **Dree_Dogg** 1 year, 9 months ago

Selected Answer: A

I would go with A. They're asking what should be done NEXT... not the near future.

upvoted 1 times

🗨️ **MartinRB** 1 year, 12 months ago

Selected Answer: A

This incident has nothing to do with the users account but with the CRM credentials, I would go with A, contact the CRM to change their credentials

upvoted 2 times

🗨️ **JokerRWild** 2 years, 2 months ago

Selected Answer: A

A. There is a longer period of time to assess the environment.

A longer period of time to assess the environment during a vulnerability assessment/penetration test can be more dangerous to the client environment as it provides an opportunity for attackers to exploit vulnerabilities and take advantage of any weaknesses in the system. This potentially gives attackers more time to gather sensitive information, create persistent backdoors into the system, and launch attacks against the organization.

The other options are not as dangerous as a longer period for assessment.

upvoted 2 times

🗲️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. This verbiage is terrible, but B looks to be the best option for what would come next from an IR team.

upvoted 2 times

🗲️ 👤 **marc4354345** 2 years, 6 months ago

When you look at what the technician did to "remedy" the mistake, it clearly contains some odd actions. Could be that the incident response procedure is wrong and needs to be updated. That's the only aspect I could see that would justify D.

upvoted 1 times

🗲️ 👤 **MrRobotJ** 2 years, 7 months ago

I feel like it is A.

upvoted 3 times

🗲️ 👤 **david124** 2 years, 7 months ago

Selected Answer: B

b correct answer

upvoted 1 times

🗲️ 👤 **Jimmycyber123** 2 years, 8 months ago

Selected Answer: B

B is the best answer here

upvoted 2 times

Which of the following is MOST dangerous to the client environment during a vulnerability assessment/penetration test?

- A. There is a longer period of time to assess the environment.
- B. The testing is outside the contractual scope.
- C. There is a shorter period of time to assess the environment.
- D. No status reports are included with the assessment.

Suggested Answer: C

Community vote distribution

B (97%)

  **Laudy** Highly Voted 2 years, 10 months ago

Selected Answer: B

I think someone changed what they were trying to ask halfway through writing this garbage question.... Verbiage on stuff is wack....

Being afforded a short window to perform Vuln Scans/Pentests is unbeneficial, not dangerous though...

What would be dangerous to the client's network would be to scan things that weren't in the Scoping Document. That's what outlines the (5 W's/How) of your scans/tests.

Two things you don't want are unauthorized tests and scope creep.

God forbid you break something outside the scope... You're liable.

upvoted 14 times

  **Laudy** 2 years, 10 months ago

The point is that scans outside the scope can accidentally break it. That's dangerous to the customer's environment.

upvoted 4 times

  **35nerd7** Highly Voted 2 years, 8 months ago

From my experience on the red side, my biggest fear is always involves systems that are out of scope. Definitely B.

upvoted 7 times

  **FEITH** Most Recent 9 months, 3 weeks ago

Selected Answer: B


I think it s B

upvoted 1 times

  **Sebatian20** 1 year, 7 months ago

They are making assumption that the pentester is incompetent. I am surprised Nuclear detonation isn't one of the option.

upvoted 1 times

  **64fc66a** 1 year, 7 months ago

Selected Answer: B

B. Testing Outside Contractual Scope

upvoted 1 times

  **AbdallaAM** 1 year, 8 months ago

Selected Answer: B

B. Testing Outside Contractual Scope:

This scenario is potentially the most dangerous. When testing goes beyond the agreed-upon scope, it could lead to legal issues, unintended disruptions, or damages to systems and networks that were not prepared or authorized for testing. There's a significant risk of causing operational, reputational, and financial harm.

upvoted 2 times

  **CyberCEH** 1 year, 9 months ago

Selected Answer: B

It's answer B

upvoted 1 times

  **JokerRWild** 2 years, 2 months ago

A. There is a longer period of time to assess the environment.

A longer period of time to assess the environment during a vulnerability assessment/penetration test can be more dangerous to the client environment as it provides an opportunity for attackers to exploit vulnerabilities and take advantage of any weaknesses in the system. This potentially gives attackers more time to gather sensitive information, create persistent backdoors into the system, and launch attacks against the organization.

The other options are not as dangerous as a longer period for assessment.

upvoted 1 times

🗲️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. Always B, hitting systems out of scope ramps up the pucker factor from a red teamer.

upvoted 2 times

🗲️ 👤 **JoInn** 2 years, 3 months ago

Selected Answer: C

The fact that the pentest is against client suggests that is within the scope. Although, it being just pentesting and not an actual attack, you are also trying to keep it short to minimise disruption. Correct answer is C.

upvoted 1 times

🗲️ 👤 **david124** 2 years, 7 months ago

Selected Answer: B

b correct answer

upvoted 2 times

🗲️ 👤 **Jimmycyber123** 2 years, 8 months ago

Selected Answer: B

Acting outside the scope is really dangerous.

upvoted 2 times

🗲️ 👤 **Eze2two** 2 years, 8 months ago

It's B, I work as a Cyber Security Analyst, and the Right to Audit is a must in a contract.

upvoted 2 times

🗲️ 👤 **Tascjfbosafj** 2 years, 8 months ago

Selected Answer: B

It's B.

upvoted 1 times

🗲️ 👤 **ruha_ali** 2 years, 8 months ago

Selected Answer: B

B sure

upvoted 2 times

🗲️ 👤 **enduser9000** 2 years, 9 months ago

Selected Answer: B

I think its B

upvoted 1 times

🗲️ 👤 **Adonist** 2 years, 9 months ago

Selected Answer: B

Definitely B

upvoted 1 times

An organization is adopting IoT devices at an increasing rate and will need to account for firmware updates in its vulnerability management programs. Despite the number of devices being deployed, the organization has only focused on software patches so far, leaving hardware-related weaknesses open to compromise.

Which of the following best practices will help the organization to track and deploy trusted firmware updates as part of its vulnerability management programs?

- A. Utilize threat intelligence to guide risk evaluation activities and implement critical updates after proper testing.
- B. Apply all firmware updates as soon as they are released to mitigate the risk of compromise.
- C. Sign up for vendor emails and create firmware update change plans for affected devices.
- D. Implement an automated solution that detects when vendors release firmware updates and immediately deploy updates to production.

Suggested Answer: D

Community vote distribution

A (81%)

D (19%)

 **Laudy** Highly Voted 2 years, 9 months ago

I had also picked A.

D is a terrible answer. lmao

upvoted 13 times

 **FEITH** Most Recent 9 months, 3 weeks ago

It should be B

upvoted 1 times


 **glenn Dexter** 1 year, 2 months ago

Selected Answer: A

Option D suggests implementing an automated solution to detect and deploy firmware updates immediately, which may introduce risks if updates are not properly evaluated or tested before deployment.

I will go with A.

upvoted 1 times

 **dickchappy** 1 year, 7 months ago

Selected Answer: A

You NEVER immediately deploy updates without testing them. A is the only real answer.

upvoted 3 times

 **Dree_Dogg** 1 year, 9 months ago

Selected Answer: A

Gotta go with A.

upvoted 1 times

 **Muculus478** 1 year, 10 months ago

Selected Answer: D

Which of the ((following best practices)) will help the organization to track and deploy trusted firmware updates as part of its vulnerability management programs?

Based on the question it seems it's assuming that all of these are ((best practices)), but which one will "help the organization to track and deploy trusted firmware updates." This is why the answer is implement an automated solution. While I agree with most everybody else that we would test before pushing it to the production environment. This is what we do in our organization and test to ensure operational impact. The question seems to be testing detailed reading to throw one off from the answer they want.

upvoted 3 times

 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. "Best Practice" is key here. Best to implement after testing, else you risking bricking your gear. However, in the real world, sometimes you do not have a platform to test first.

upvoted 2 times

🗨️ 👤 **nooooo** 2 years, 3 months ago

Selected Answer: D

It's D. The key verbiage here is "Trusted firmware".

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: A

"after proper testing." is why I choose A, because that is "best practice" as the question asks.

upvoted 1 times

🗨️ 👤 **knister** 2 years, 5 months ago

I dont know why you would use Threat Intelligence here. Looks like a manager wrote that answer.

upvoted 1 times

🗨️ 👤 **NickDrops** 2 years, 5 months ago

You can't go around patching/updating just because a new update came out. The update needs to be evaluated, especially based on risk. If its a super unlikely exploit that wouldn't accomplish a whole lot against your system, it may not be worth the downtime or the effort.

upvoted 2 times

🗨️ 👤 **gwerin** 2 years, 5 months ago

Selected Answer: A

What's up with D? Who is just blindly smashing things out to their live prod environment without any real testing or oversight?

upvoted 4 times

🗨️ 👤 **david124** 2 years, 7 months ago

Selected Answer: A

A is correct answer

they arent saying all answers are incorrect, but they are asking best practice.

receiving emails from vendors about updates is okay but you still didnt implement any changes to the hardware.

changing and making hardware patches without proper testing or evaluation can cause you critical issues specially if a patch breaks your system

upvoted 3 times

🗨️ 👤 **dnc1981** 2 years, 8 months ago

Why not C?

upvoted 2 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

D? really?...just blindly install without testing in lab first ?..I think not...A

upvoted 2 times

🗨️ 👤 **Tascjfbosafj** 2 years, 8 months ago

Selected Answer: A

It's A.

upvoted 1 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: A

D sounds like a nightmare, A is the correct answer here

upvoted 1 times

🗨️ 👤 **enduser9000** 2 years, 9 months ago

Can anyone explain why it is not A?

upvoted 1 times

🗨️ 👤 **hypertweeeky** 1 year, 10 months ago

No company should blindly install without testing. It could break other systems!

upvoted 1 times

🗨️ 👤 **hypertweeeky** 1 year, 10 months ago

meaning, it is A.

upvoted 1 times

A company's blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

- A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.
- B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed.
- C. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist and remove the lower-severity threats from it.
- D. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.

Suggested Answer: D

Community vote distribution



cysa_1127 Highly Voted 3 years, 4 months ago

Selected Answer: C

Correct option is C.

Statement: Review the current clocklist the prioritize it based on the level of threat severity. Add the domains with the highest severity of the blocklist and remove the lower-severity threats from it.

Explanation:

Since Adding domains with the highest severity of the blocklist will help in better configuration management and reduce risks of security breaches and outages and can also be sometimes very cost effective.

upvoted 13 times

JENNER_ROCKA 3 years, 3 months ago

I agree!. It says too, "to improve performance"

upvoted 3 times

zecomeia_007 Most Recent 11 months, 2 weeks ago

Selected Answer: D

D. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures.

upvoted 1 times

RobV 1 year, 6 months ago

Selected Answer: D

Option C involves reviewing the current blocklist and prioritizing it based on the level of threat severity, adding the domains with the highest severity and removing the lower-severity threats. While this approach might help in prioritizing the blocklist, it doesn't necessarily address the issue of an overgrown blocklist and the limitations of the existing technologies.

The challenge described in the scenario is that the ACLs are at maximum, and the IPS signatures have limited space for domains. Prioritizing based on threat severity might help in focusing on the most critical threats, but it doesn't directly address the issue of the blocklist exceeding the capacity of the existing controls.

Option D, on the other hand, directly addresses the overgrown blocklist by reviewing and removing domains that are no longer necessary or pose lower risks. This action helps optimize the use of ACLs and IPS signatures, leading to improved performance without compromising security.

upvoted 1 times

Sebatian20 1 year, 7 months ago

Selected Answer: D

"remove the lower-severity threats from it"

Who would still allowed Website with threats to access their network - regardless of threat level?

upvoted 4 times

🗨️ 👤 **sansoculus** 1 year, 7 months ago

Selected Answer: D

By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly.

upvoted 1 times

🗨️ 👤 **TacosInMyBelly** 1 year, 7 months ago

Selected Answer: D

Given the context of improving performance and the limitation on ACLs and IPS signatures, option D seems to be the most appropriate. It focuses on optimizing the blocklist by removing unnecessary domains, which can alleviate the constraints on ACLs and IPS signatures.

upvoted 1 times

🗨️ 👤 **Big_Dre** 1 year, 9 months ago

Selected Answer: D

i think D allow no risk appetite while C allows know malicious domains although they are low.

upvoted 2 times

🗨️ 👤 **Dree_Dogg** 1 year, 9 months ago

Selected Answer: D

Gotta go with D.

C ended with "remove the lower-severity threats." This doesn't sit right with me.

upvoted 3 times

🗨️ 👤 **iamfoozy** 1 year, 10 months ago

Selected Answer: C

chatgpt

upvoted 2 times

🗨️ 👤 **Aliyan** 1 year, 10 months ago

Selected Answer: D

I believe answer is D. Its better to remove inactive domains rather than low threat vulnerabilities.

Explanation

It allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs by reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

upvoted 1 times

🗨️ 👤 **Pavel019846457** 1 year, 10 months ago

Selected Answer: C

answer is c

upvoted 1 times

🗨️ 👤 **POWNED** 1 year, 11 months ago

Selected Answer: D

There is a major difference in why the answer is D. C talks nothing about ACLs and IPS. This means that D is your best answer. Basically doing exactly what C is, but updating the ACL's and IPS as well.

upvoted 2 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: D

I think it's D removing threats doesnt sound good on C

upvoted 4 times

🗨️ 👤 **kiduuu** 2 years, 3 months ago

Selected Answer: D

Review the current blocklist to determine which domains can be removed from the list and then update the ACLs and IPS signatures is the MOST appropriate configuration change to improve performance. As the ACLs and IPS signatures have reached their maximum limits, it is essential to review the current blocklist to identify domains that are no longer relevant or pose a lower level of threat. This will help to reduce the size of the blocklist and create space for additional domains that may pose a higher level of risk. Once the review is complete, the ACLs and IPS signatures can be updated with the new list, improving the overall performance of the controls.

upvoted 3 times

🗨️ 👤 **AaronS1990** 2 years, 5 months ago

Surely D is the MOST appropriate?

I understand why people say C, but C doesn't address the ACL or IPS issues and the question talks about improving performance. Surely D will improve it the most given it addresses the 3 issues the network has....

upvoted 3 times

🗨️ 👤 **jstad** 2 years, 5 months ago

Selected Answer: C

ANSWER: C

This option would improve performance by ensuring that the most critical threats are being blocked, while also reducing the number of domains on the blocklist and therefore reducing the load on the existing controls. This would make the most efficient use of the limited space available in the ACLs and IPS signatures.

upvoted 1 times

🗨️ 👤 **david124** 2 years, 7 months ago

Selected Answer: C

C correct answer

upvoted 1 times

HOTSPOT -

A security analyst suspects that a workstation may be beaconing to a command and control server.

Inspect the logs from the company's web proxy server and the firewall to determine the best course of action to take in order to neutralize the threat with minimum impact to the organization.


INSTRUCTIONS -

Modify the Firewall Access Control rule to mitigate the issue.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

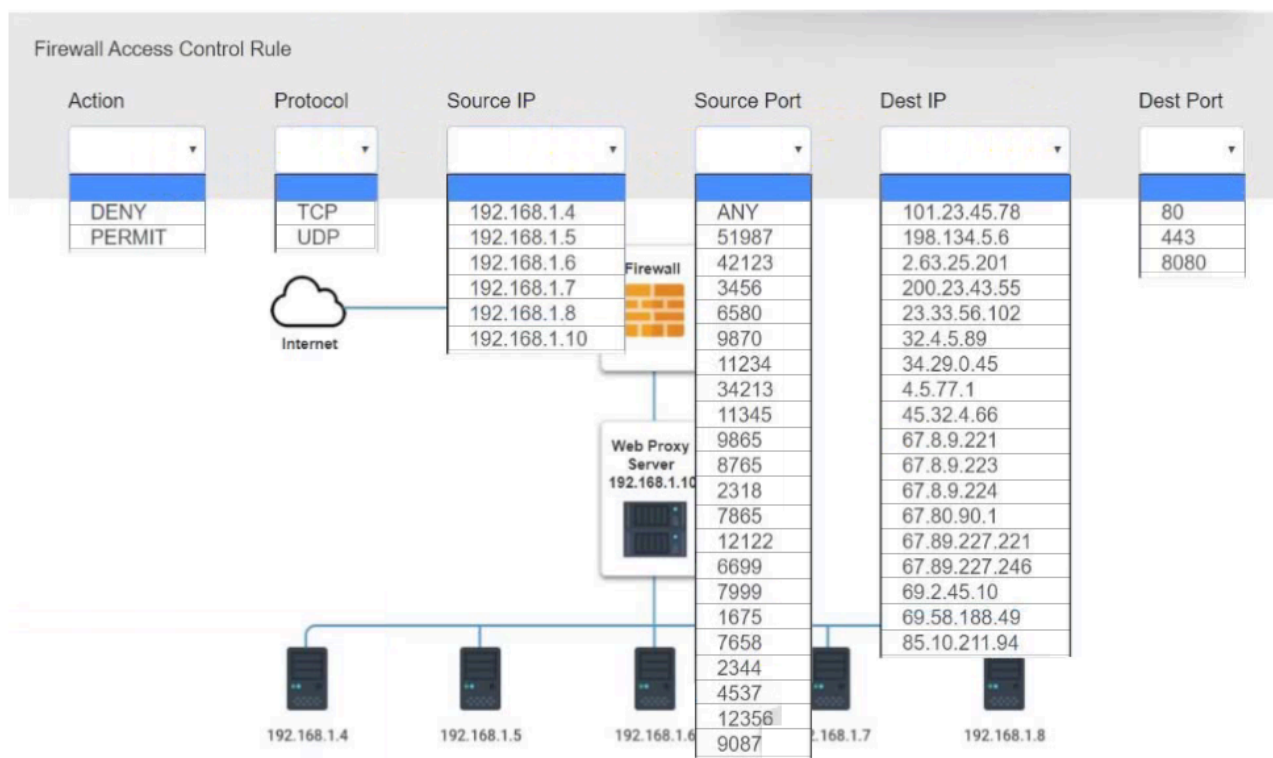


Web Server Log						
Time	SIP	SPort	DIP	DPort	Request Code	URL
12:01:00 PM	192.168.1.4	2344	67.89.227.246	443	GET	company.cn
12:01:01 PM	192.168.1.5	7658	67.89.227.221	443	GET	google.ru
12:01:02 PM	192.168.1.7	9087	85.10.211.94	80	GET	provider.il
12:01:03 PM	192.168.1.6	3456	2.63.25.201	80	POST	bqtest2.ru
12:01:04 PM	192.168.1.8	12356	69.58.188.49	80	POST	testsite.jp
12:01:05 PM	192.168.1.5	42123	198.134.5.6	443	POST	network.org
12:01:06 PM	192.168.1.4	2318	4.5.77.1	443	GET	mynews.com
12:01:07 PM	192.168.1.8	9865	32.4.5.89	80	GET	catala.com
12:01:08 PM	192.168.1.6	9870	2.63.25.201	80	POST	bqtest2.ru
12:01:09 PM	192.168.1.8	4537	69.2.45.10	80	POST	lillte.cn
12:01:10 PM	192.168.1.5	7865	45.32.4.66	80	POST	portal.co.jp
12:01:11 PM	192.168.1.6	51987	101.23.45.78	443	POST	malware.com
12:01:12 PM	192.168.1.5	34213	200.23.43.55	443	GET	vortex.net
12:01:13 PM	192.168.1.6	11234	2.63.25.201	80	POST	bqtest2.ru
12:01:14 PM	192.168.1.6	8765	34.29.0.45	80	GET	colocation.com
12:01:15 PM	192.168.1.4	1675	67.80.90.1	443	GET	johnson.com
12:01:16 PM	192.168.1.7	11345	23.33.56.102	80	POST	college.edu
12:01:17 PM	192.168.1.7	12122	67.8.9.221	443	GET	lalala.gov
12:01:18 PM	192.168.1.6	6580	2.63.25.201	80	POST	bqtest2.ru
12:01:19 PM	192.168.1.7	6699	67.8.9.223	80	POST	mystuff.ac.jp
12:01:20 PM	192.168.1.5	7999	67.8.9.224	8080	GET	erdas.com

Firewall Log						
Action	Time	SIP	SPort	DIP	DPort	
PERMIT	12:01:00 PM	192.168.1.10	2344	67.89.227.246	443	
DENY	12:01:01 PM	192.168.1.10	7658	67.89.227.221	443	
PERMIT	12:01:02 PM	192.168.1.10	9087	85.10.211.94	80	
PERMIT	12:01:03 PM	192.168.1.10	3456	2.63.25.201	80	
PERMIT	12:01:04 PM	192.168.1.10	12356	69.58.188.49	80	
PERMIT	12:01:05 PM	192.168.1.10	42123	198.134.5.6	443	
PERMIT	12:01:06 PM	192.168.1.10	2318	4.5.77.1	443	
PERMIT	12:01:07 PM	192.168.1.10	9865	32.4.5.89	80	
PERMIT	12:01:08 PM	192.168.1.10	9870	2.63.25.201	80	
PERMIT	12:01:09 PM	192.168.1.10	4537	69.2.45.10	80	
DENY	12:01:10 PM	192.168.1.10	7865	45.32.4.66	80	
PERMIT	12:01:11 PM	192.168.1.10	51987	101.23.45.78	443	
PERMIT	12:01:12 PM	192.168.1.10	34213	200.23.43.55	443	
PERMIT	12:01:13 PM	192.168.1.10	11234	2.63.25.201	80	
PERMIT	12:01:14 PM	192.168.1.10	8765	34.29.0.45	80	
PERMIT	12:01:15 PM	192.168.1.10	1675	67.80.90.1	443	
PERMIT	12:01:16 PM	192.168.1.10	11345	23.33.56.102	80	
PERMIT	12:01:17 PM	192.168.1.10	12122	67.8.9.221	443	
PERMIT	12:01:18 PM	192.168.1.10	6580	2.63.25.201	80	
PERMIT	12:01:19 PM	192.168.1.10	6699	67.8.9.223	80	
DENY	12:01:20 PM	192.168.1.10	7999	67.8.9.224	8080	

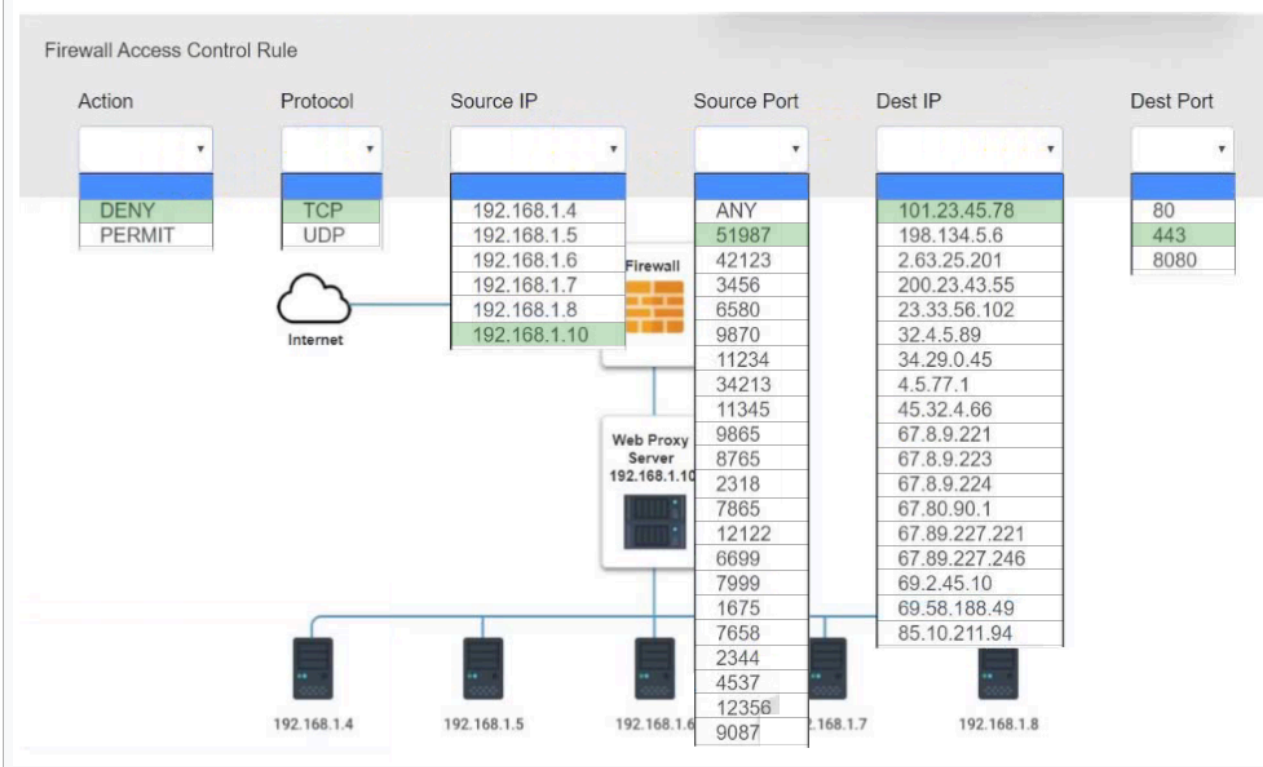
Hot Area:

Answer Area



Suggested Answer:

Answer Area



TheSkyMan Highly Voted 2 years, 9 months ago

With internal computers beaconing to C2 servers, many times you'll see a trend of traffic calling out at set intervals. In this case 192.168.1.6 is beaconing out to 2.63.25.201 (bqtest2.ru) every 5 seconds. Since we have a proxy server (192.168.1.10), we need to deny the proxy servers IP.

Action = DENY | Protocol = TCP | Source IP = 192.168.1.10 | Source Port = ANY | 2.63.25.201 | Dest Port = 80

Side note: I would block all traffic (ANY) to the destination port too, but that's not an option on this question.

upvoted 63 times

AaronS1990 2 years, 5 months ago

It's also beaconing out to malware.com on port 443 though...

upvoted 2 times

  **justauser** 2 years ago



Seems like a red herring, obviously with only 1 rule to provide, it should be what TheSkyMan said.

upvoted 3 times

  **Mr_BuCh3th34D** 2 years, 6 months ago



I agree 100%

upvoted 2 times

  **2Fish** 2 years, 3 months ago




Agree. Thanks for the break down.

upvoted 2 times

  **attesco** 1 year, 11 months ago

Good explanation

upvoted 2 times

  **CyberNoob404**  2 years, 5 months ago


DENY | TCP | 192.168.1.10 | ANY | 2.63.25.201 | 80

upvoted 12 times

  **RT7**  1 year, 7 months ago

Is the correct answer: Source Port:51987, DST IP:101.23.45.78, DST Port:443?

upvoted 1 times


  **Big_Dre** 1 year, 9 months ago

what about

Action = DENY | Protocol = TCP | Source IP = 192.168.1.10 | Source Port = ANY | 2.63.25.201 | Dest Port = 8080

destination port should be 8080 and not 80 since the beaconing will be done over the proxy and we know the default port is 8080?



upvoted 1 times

  **rg00** 1 year, 11 months ago

DENY, TCP, 192.168.1.10, ANY, 2.63.25.201, 80

Notice that the source port is inconsistent on logs. Therefore, Source Port should be any.

upvoted 2 times

  **SimonR2** 1 year, 11 months ago

If there was no firewall in the path of the proxy server to the internet and no address translation was done, it would be:

DENY > TCP > 192.168.1.6 > ANY > 2.63.25.201 > ANY



However, since we are natting the source ip to that of the proxy server (this caught me out), the actual answer would be:

DENY > TCP > 192.168.1.10 > ANY > 2.63.25.201 > ANY

Ideally in the real world we would use the following rule, but this isnt an option:



DENY > ANY > ANY > ANY > 2.63.25.201 > ANY

upvoted 1 times

  **SimonR2** 1 year, 11 months ago

Sorry, for the actual destination port answer it should be 80*

upvoted 2 times

  **kiduuu** 2 years, 1 month ago

DENY | TCP | 192.168.1.6 | 51987 | 101.23.45.78 | 443

upvoted 1 times

  **[Removed]** 2 years, 2 months ago

DENY | TCP | 192.168.1.10 | ANY | 2.63.25.201 | 80

upvoted 5 times

  **ChrisRM** 2 years, 3 months ago

MailClient.exe

7 Clicked

4 infected

.134 x
.254 x
.9 x
.70 x
.188 x
.24 x
.132 x

4 Logons: cpuziss/ jlee/ asmith/ kmathews (IP's matched those who clicked on the mailclient.exe link)

upvoted 1 times

🗨️ 👤 **ChrisRM** 2 years, 3 months ago

Wrong post sorry guys

upvoted 3 times

🗨️ 👤 **msellars** 2 years, 7 months ago

Found this from an earlier study guide CSO-001. They have Dent -> TCP -> 192.168.1.6 ->ANY -> 2.63.25.201 ->80. Although the FW will only recognize the next hop which would be the proxy server, so replace .6 with .10.

upvoted 3 times

🗨️ 👤 **david124** 2 years, 7 months ago

Action = DENY | Protocol = TCP | Source IP = 192.168.1.10 | Source Port = ANY | 2.63.25.201 | Dest Port = 80

upvoted 3 times

🗨️ 👤 **A_core** 2 years, 8 months ago

A=Deny | Protocol = TCP | SIP=192.168.1.6 Sport=Any DIP=2.63.25.201 Dport=80

upvoted 2 times

🗨️ 👤 **CW4901** 2 years, 8 months ago

Have you taken the exam yet? If so, did you stick with this answer?

upvoted 1 times

🗨️ 👤 **bigerblue2002** 2 years, 9 months ago

Looks like DENY TCP .10 ANY 2.63.25.201 80. The given answer only shows up once, would that really be beaconing?

upvoted 4 times

🗨️ 👤 **fablus78** 2 years, 10 months ago

Wrong, the beaconing destination address is 2.63.25.101 , so this is the address to block on all ports

upvoted 7 times

🗨️ 👤 **twobuckchuck** 2 years, 10 months ago

I agree with the answer but wouldn't it be smart to block any service port. Not just 51987

upvoted 3 times

SIMULATION -

Approximately 100 employees at your company have received a phishing email. As a security analyst, you have been tasked with handling this situation.

INSTRUCTIONS -

Review the information provided and determine the following:

1. How many employees clicked on the link in the phishing email?
2. On how many workstations was the malware installed?
3. What is the executable file name of the malware?

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

View Phishing Email

How many workstations were infected?

Select the malware executable name.

How many users clicked the link in the fishing e-mail?

Internal Network

Email Server
192.168.0.20

File Server
192.168.0.102

SIEM
192.168.0.15

Internal Router
192.168.0.1

Proxy
192.168.0.50

192.168.0.0/24

Firewall

Internet

View Phishing Email

How many users clicked the link in the fishing e-mail?

How many workstations were infected?

Select the malware executable name.

winlogon.exe

excel.exe

iexplore.exe

notepad.exe

chrome.exe

explorer.exe

time.exe

cmd.exe

lsass.exe

winword.exe

outlook.exe

mailclient.exe

firefox.exe

svchost.exe

putty.exe

Internal Network

Email Server
192.168.0.20

File Server
192.168.0.102

SIEM
192.168.0.15

Internal Router
192.168.0.1

Proxy
192.168.0.50

192.168.0.0/24

Firewall

Internet

Phishing Email



From: IT HelpDesk <it-helpdesk@sobergrill.com>

Sent: Mon 3/7/2016 4:00 PM

To: Global Users <globalusers@sobergrill.com>

Hi,

In the upcoming days, we will be moving our mail servers from MS Outlook to the new Netscape Navigator. Check out the new SoberGrill webmail and know if it has started working for you.

Visit the new SoberGrill webmail to see all the new features.

Use your current username and password at [SoberGrill Webmail](#).

Download the latest mail client [here](#).

Thank you.

IT HelpDesk

Email Server Logs - Email Server 192.168.0.20



Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com;jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sboaz@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ibenz@anycorp.com
3/7/2016 4:01:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsutherland@anycorp.com
3/7/2016 4:01:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrossiter@anycorp.com
3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ahynson@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mdillion@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jwayman@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrehn@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lrogge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aaveritt@anycorp.com
3/7/2016 4:01:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lephraim@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wmcnemey@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	imarable@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfausto@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kdefranco@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mworley@anycorp.com

Email Server Logs - Email Server 192.168.0.20



Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltreiber@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mgameau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hfossu@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	trhoda@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ctsui@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bmonteone@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cfenstermacher@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgarinkel@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cheroux@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mkamen@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	zdodgen@anycorp.com
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhammonds@anycorp.com
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	onorth@anycorp.com
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mroane@anycorp.com
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kbowling@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nrachal@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jdegenhardt@anycorp.com
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wracette@anycorp.com
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lhammond@anycorp.com
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dmilazzo@anycorp.com
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kneubauer@anycorp.com
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bboyko@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dicrofoot@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmemmott@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	chodgin@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aholler@anycorp.com
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	abattaglia@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	halberti@anycorp.com
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	myeoman@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wbobadilla@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lkam@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jcooks@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpolice@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mwagener@anycorp.com
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com

Email Server Logs - Email Server 192.168.0.20



Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltaor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	loller@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kwilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tshack@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmanson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dstivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mslstrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgallipeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckroeker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuziss@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morwig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingbury@anycorp.com

Email Server Logs - Email Server 192.168.0.20

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ltabor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	loller@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kwilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tshack@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmanson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dstivers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	msistrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenware@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgalipeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmathews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckroeker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuziss@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morvig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com

File Server Logs - File Server 192.168.0.102

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55947	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tilapia.com	GET

File Server Logs - File Server 192.168.0.102							
Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request	
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET	
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET	
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tlapi.com	GET	
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET	
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET	
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.190.57.150	80	freefood.com	POST	
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST	
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET	
3/7/2016 3:57:59 PM	192.168.0.59	33145	209.240.152.67	80	bestpurchase.com	GET	
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.83.170.116	80	goodguys.se	POST	
3/7/2016 3:55:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET	
3/7/2016 3:54:31 PM	192.168.0.152	30520	141.217.181.243	80	goodguys.se	POST	
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.201.191	80	pastebucket.cn	POST	
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET	
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.192	80	funweb.cn	POST	
3/7/2016 3:49:54 PM	192.168.0.126	40815	171.140.162.96	80	stopthebotnet.com	GET	
3/7/2016 3:49:07 PM	192.168.0.9	47625	18.23.47.44	80	stopthebotnet.com	GET	
3/7/2016 3:47:38 PM	192.168.0.131	44579	139.58.55.91	80	funweb.cn	GET	
3/7/2016 3:45:58 PM	192.168.0.186	62683	31.133.137.225	80	chatforfree.ru	POST	
3/7/2016 3:44:05 PM	192.168.0.181	38937	150.119.71.249	80	anti-malware.com	GET	
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET	
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET	
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET	
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET	
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.208.164.237	443	searchforus.de	GET	
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET	
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET	
3/7/2016 3:35:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET	
3/7/2016 3:35:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET	
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	POST	

SIEM Logs - SIEM 192.168.0.15									
Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name	
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe	
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe	
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe	
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe	
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe	
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe	
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe	
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe	
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe	
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe	
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe	
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe	
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe	
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe	
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe	
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe	
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe	
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe	
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe	
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe	
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe	
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe	

SIEM Logs - SIEM 192.168.0.15									
Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name	
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe	
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe	
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe	
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe	
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe	
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe	
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe	
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe	
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe	
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe	
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe	
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe	
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe	
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe	
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe	
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe	
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe	
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe	
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe	
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe	
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe	
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe	

Suggested Answer: See explanation below.

How many workstations were infected?


Select the malware executable name.

How many users clicked the link in the fishing e-mail?

 **V4Vendetta** Highly Voted 2 years, 5 months ago

The answer is as shown, this question was on my exam, when you hover over the email link it shows the domain name, you then check which users accessed that domain (There are 7) then you cross reference those with the mailclient.exe on SIEM (you can't see because it's a screenshot and you need to scroll) also you can organize the processes alphabetically and you will see 4 users were infected!

upvoted 37 times

 **jleonard_ddc** Highly Voted 2 years, 5 months ago

First, I somewhat worked out that mailclient.exe was suspicious; it even has '1234' for the target port. And, as mentioned - the phishing e-mail even says "download the latest client here". Apparently others are stating this is even more obvious in the real exam.

In any event, with that information alone, that EXE only shows up on the .188 machine. The only request from that machine in the logs is a GET for chzweb.tilapia.com This tells me that is the target URL.

From there, you can tell for sure that 7 workstations made requests to that URL. (fell victim to the scam)

192.168.0.134

192.168.0.254

192.168.0.9

192.168.0.70

192.168.0.188

192.168.0.24

192.168.0.132

As for the users infected, that might be easier to verify if the 2 SIEM screenshots weren't identical.

Be suspicious of people saying they passed, and what their answer was - but not why it was right or if they had a perfect score. (do they know they got that question right?)

I'm a CySA by trade so kinda trusting my gut here.

upvoted 16 times

  **AaronS1990** 2 years, 4 months ago

Good point well made. So many say they got the question right on the day but CompTIA exams only give you a steer with what questions you got wrong at the end. They don't actually let you see for sure which ones you got right

upvoted 2 times

  **Achilles69** 1 year, 9 months ago



You're wrong. I thought the same thing at first but you made the mistake of believing a Process ID was a Port Number.

upvoted 2 times

  **T1bii** Most Recent 1 year, 3 months ago

The answer is correct : 7 click, 4 infected with mailclient.exe, why, because when passing the exam, you just has to count how many time you may find mailclient.exe : 4 times.

upvoted 1 times

  **JakeH** 1 year, 8 months ago

Confirmed this was one of the PBQ's on my exam - 10/12/23 - Answered as it is shown

upvoted 2 times

  **hypertweeeky** 1 year, 9 months ago

Unrelated to this question.. but I accidentally took CYSA 003 series instead of the 002 and I failed. Not by much (I got a 740). There was a LOT more log interpreting and NIST standard questions. The CYSA 003 also available on this site has about 40% (so far) of those questions.

upvoted 8 times

  **sorinttt** 2 years, 1 month ago

Hello, I passed yesterday with 793. The answer is 7 clicked, 4 infected and mailclient.exe. why? Three reasons. 1. User Jlee who clicked the phishing link at 4:08 has lsass.exe started at 3:56, and mailclient.exe started at 4:08 after a few seconds from when he clicked, if you have experience with SIEM you will see this. And 2. When mailclient.exe starts the message is: a new process is created, when lsass.exe starts the message is an account was logged on. 3. Bonus, not all who clicked have lsass.exe. good luck.

upvoted 6 times

  **ChrisRM** 2 years, 3 months ago

MailClient.exe
7 Clicked
4 infected

.134 x
.254 x
.9 x
.70 x
.188 x
.24 x
.132 x

4 Logons: cpuziss/ jlee/ asmith/ kmathews (IP's matched those who clicked on the mailclient.exe link)

upvoted 8 times

  **PhillyCheese** 2 years, 4 months ago

I am leaning toward 7 clicks, 5 infected, and lasass.exe. Below is my thought process:

The common URL in the logs is a GET for chzweb.tilapia.com This tells me that is the target URL.

From there, you can tell that 7 workstations made requests to that URL.(clicked the link in the phishing email).

192.168.0.134
192.168.0.254
192.168.0.9
192.168.0.70
192.168.0.188
192.168.0.24
192.168.0.132

5 Logons: cpuziss/ dfritz/ jlee/ asmith/ kwilliams

-To me, a successful Logon = an infected workstation

-As you can see, account name "cpuziss" successfully logs on 2x with lsass.exe w/the same IP of .70 and don't think this is correct bc can you really infect a workstation twice? Same user, same IP address.

Any thoughts?

upvoted 1 times

🗨️ 👤 **SylFlo** 2 years, 5 months ago

on my test today, i went with the 7, malicent.exe and 4

upvoted 2 times

🗨️ 👤 **1oldman** 2 years, 2 months ago

Did you pass?

upvoted 2 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Workstations: 6

Executable: lsass.exe

Clicked: 7

upvoted 1 times

🗨️ 👤 **tendaisanyamahwe** 2 years, 7 months ago

How do you get the:

6 infected

7 clicked

lsass.exe

as an answer?

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

someone please explain how 6 infected and 7 clicked?

upvoted 3 times

🗨️ 👤 **kdubb2307** 2 years, 8 months ago

Okay now I could be wrong but hear me out I believe 7 users clicked the link, and the lsass.exe is the malware executable due to it is a system file not a user file and should be labeled as such not by username but that doesn't mean all the users that clicked the link are infected, rather they all have downloaded the malware executable in question. Although, the user: Jlee in the log looks like he might indeed be infected for this reason he not only has the malware executable, but it looks like it installed as well due to him also having the cmd.exe and the file explorer.exe (explorer.exe). In that case 7 clicked, 1 infected, and lsass.exe?

upvoted 1 times

🗨️ 👤 **Weezyfbaby** 2 years, 8 months ago

Passed the exam today and I went with 6 infected, 7 clicked, and lsass.exe.

upvoted 9 times

🗨️ 👤 **Tag** 2 years, 8 months ago

6 infected

7 clicked

lsass.exe

dont ask me to explain, just know thats the answer.

upvoted 6 times

🗨️ 👤 **MrRobotJ** 2 years, 7 months ago

How do you know? for me it is about learning not passing

upvoted 8 times

🗨️ 👤 **Yerfez** 2 years, 8 months ago

Is it not 4 , 7 and lsass.exe?

upvoted 2 times

🗨️ 👤 **bootleg** 2 years, 6 months ago

I passed today, I picked this. there were 4 executables when you top click the SIEM in the far right hand side, I believe the lsass was the exe but I can't remember.

upvoted 1 times

  **TheSkyMan** 2 years, 9 months ago

This sim has duplicate log screen shots, so can't determine the real answer (answer may be right?!). Since the phishing email has a download link to a mail client, it makes sense that the malware will be mailclient.exe. Also I'm pretty sure the mailclient.exe malware is connecting to chatforfree.ru. To confirm this, we need to correlate the time line of events with all of the server logs.



This how I plan on working this sim (method could change as I start the sim):

SIEM - look for users that have "mailclient.exe" in the process name to get how many workstations were infected.

File Server - look for users connecting to "chatforfree.ru" to determine how many users clicked the phishing email.

Email Server - used as a reference confirming users received the email and the time line of events support infection times.

upvoted 3 times

  **Treymb6** 2 years, 9 months ago

I agree with most of this except that the IP that the mailclient.exe is running on is .188. If you go back to the file server logs and look at what is close in time and for that .188 IP it looks like it should be that tilapia.com website.

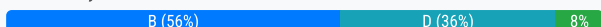
upvoted 5 times

A company is experiencing a malware attack within its network. A security engineer notices many of the impacted assets are connecting outbound to a number of remote destinations and exfiltrating data. The security engineer also sees that deployed, up-to-date antivirus signatures are ineffective. Which of the following is the BEST approach to prevent any impact to the company from similar attacks in the future?

- A. IDS signatures
- B. Data loss prevention
- C. Port security
- D. Sinkholing

Suggested Answer: B

Community vote distribution



fuzzyguzzy 6 months, 4 weeks ago

Selected Answer: B

Sinkholing is a reactive measure not a preventative measure. The answer that is reactive and will detect exfiltrated data is B
upvoted 1 times

sireym1 1 year, 3 months ago

I would go with dlp, no signature, so we may be looking at a zero day exploit, it is probably not linked to any malicious group so sinkhole might fail if data exfiltration is not noticed by analysts but dlp involves protecting data at rest, in transit.
upvoted 2 times

skibby16 1 year, 6 months ago

Selected Answer: D

Sinkholing can help prevent any impact to the company from similar attacks in the future by redirecting the malicious traffic from the compromised assets to a sinkhole server, where it can be monitored, analyzed, or blocked. Sinkholing can also prevent the compromised assets from communicating with their command and control servers or exfiltrating data to remote destinations
upvoted 1 times

Sebatian20 1 year, 7 months ago

Selected Answer: D

Sink hole.

Stop the Malware at its source and you won't need to worry about DLP.
upvoted 1 times

dickchappy 1 year, 7 months ago

Selected Answer: D

Straight from the official study guide:
"Black holes and sinkholes can be configured using routing policies, but you can also use DNS-based sinkholing to capture malicious traffic trying to exit from your network."

This is about malicious traffic exiting your network. DLP is more tailored toward dealing with insider threats, not malware attacks.

Another source: <https://www.egress.com/blog/data-loss-prevention/five-tips-prevent-exfiltration#:~:text=Sinkholing%20is%20a%20network%20engineering,exfiltration%20from%20doing%20any%20harm.>

"Sinkholing is a network engineering technique where you redirect traffic from a malicious program to an IP address of your choosing. This technique means you can see exactly what the malware program is attempting to exfiltrate while preventing the exfiltration from doing any harm. You can then study the malware at your leisure to understand how it got there and mitigate future attempts."
upvoted 1 times

Chilaqui1es 1 year, 7 months ago

Im going to DLP as the answer because from a google search "can dlp work against cyber attacks?" Multiple sources say "Companies that use DLP have a security strategy to detect, prevent data loss, and cyber-attacks. DLP is also used to eliminate unwanted data that will harm the system's

security."

I looked into Sinkholes and I just feel sketchy about it. Maybe or maybe but I think its unlikely. A big reason too I am going with DLP a lot people who passed the test went with this answer as well.

upvoted 2 times

🗨️ 👤 **chaddman** 1 year, 8 months ago

The best approach to prevent any impact from similar attacks in the future is "D. Sinkholing."

A sinkhole redirects traffic from the infected machines to a trusted server, effectively isolating them and preventing data exfiltration to malicious destinations. This can be especially useful when traditional antivirus measures are proving ineffective, as it can stop the communication between the malware and its command and control servers.

upvoted 1 times

🗨️ 👤 **skibby16** 1 year, 8 months ago

Selected Answer: D

Sinkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to the server of your choosing. It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks. Sinkholing can help prevent any impact to the company from similar attacks in the future by redirecting the malicious traffic from the compromised assets to a sinkhole server, where it can be monitored, analyzed, or blocked. Sinkholing can also prevent the compromised assets from communicating with their command and control servers or exfiltrating data to remote destinations.

upvoted 1 times

🗨️ 👤 **MiDirtyTip** 1 year, 10 months ago

Im choosing D, solely because its saying it sending resources to outbound sources which is why i would use sinkholing to prevent loss of information same as DLP but my opinion giving you more control on the sink hole server

upvoted 2 times

🗨️ 👤 **karpal** 2 years ago

Selected Answer: D

I went through all 405 questions.

I am now reviewing the questions I got wrong and I am so puzzled by the comments and voting here.

Is for SURE not DLP man. DLP prevents human exfiltration not exfil done by malware attacks (for example exfiltration would mean dns exfiltration - DLP has no way to detect this).

I asked chatGPT and said also DLP. I told it : "DLP is useful to protect exfiltration done by humans not malware attacks. I think that IDS signatures is a method to do it (it will detect malware and then the analyst can stop it to happen) or Sinkhole the malicious IPs or domain names used in the malware attack. I do not think DLP is the answer here."

Answer came back: You're correct, and I apologize for the incorrect response. In the context of preventing the impact of malware attacks and exfiltration, the more appropriate approach would be option D: Sinkholing.

So the only active useful method from the options to really have an impact is the sinkhole for the remote destinations.

I choose D.

upvoted 4 times

🗨️ 👤 **Aliyan** 1 year, 10 months ago

I am also coming back to the questions and i was thinking why not sinkholing also because that was the answer i picked when i didnt look at the comments and answer key but after going back to my notes and talking to GPT a bit I think we are forgetting what the main reason for sinkholing is..

Sinkholing primarily focuses on redirecting malicious traffic to a controlled server for analysis or monitoring. It doesn't inherently prevent data exfiltration or address the root cause of the attack. It can be more effective for understanding the scope and scale of an attack or for gathering threat intelligence but may not directly prevent sensitive data from leaving the network.

Sinkholing does not necessarily prevent this data transfer from occurring; it merely redirects the communication to a different location.



Sinkholing may not have full control over the malware or its actions. Sophisticated malware can adapt and change its behavior, potentially evading sinkholing measures.

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago



Selected Answer: B

The best approach to prevent any impact to the company from similar attacks in the future is to implement data loss prevention (DLP).
upvoted 2 times



  **2Fish** 2 years, 3 months ago

Selected Answer: B

B. This is DLP for sure.
upvoted 2 times

  **timhk** 2 years, 5 months ago

It says "prevent any impact to the company from similar attacks in the future?". That means the attack still exists in the future within the company. So to prevent any impact to the company is to use DLP.
upvoted 2 times



  **Kelz56** 2 years, 7 months ago

Data loss prevention (DLP) is a set of technologies and processes that monitor and inspect data on a corporate network to prevent exfiltration of critical data as a result of cyberattacks, such as phishing or malicious insider threats.
upvoted 2 times

  **Study4America** 2 years, 8 months ago

Selected Answer: B

Exfiltrating data is DLP no doubt
upvoted 3 times



  **TeyMe** 2 years, 8 months ago

Selected Answer: D

Context: So devices are connecting to outbound remote destinations (C2), attack via malware, Since malware signatures couldnt be detected, this is Unknown Unknowns so we can rule out A, However, Malware analysis will reveal Source info and get IPs from that, then we can SinkHole with the hope of getting alerted!
upvoted 1 times

  **TeyMe** 2 years, 8 months ago

Also, notice the "Prevent ""ANY"" impact, this means for both Malware and DLP, not just DLP.. contextually...
upvoted 1 times

  **MortG7** 2 years, 8 months ago

Selected Answer: B

The little nugget here is "exfiltrating data" DLP
upvoted 3 times

The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues. The steering committee wants to rank the risks based on past incidents to improve the security program for next year.

Below is the incident register for the organization:

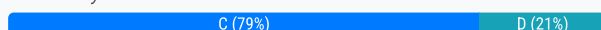
Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop \$1,250

Which of the following should the organization consider investing in FIRST due to the potential impact of availability?

- A. Hire a managed service provider to help with vulnerability management
- B. Build a warm site in case of system outages
- C. Invest in a failover and redundant system, as necessary
- D. Hire additional staff for the IT department to assist with vulnerability management and log review

Suggested Answer: C

Community vote distribution



mcNik Highly Voted 4 years ago

Only possible's are B and C , but given the scenario C seems closer to a right answer.
upvoted 10 times

Sebatian20 Most Recent 1 year, 7 months ago

Another stupid question from Comptia.

So if you go for C - you invest in better IT infrastructure but lack the manpower to run it.
upvoted 1 times

LayinCable 1 year, 9 months ago

The key word is availability, so in that case it would have to be B or C. You can't be available for business with no storage or ways to access it if the primary goes down. Although I do agree that they do need to do some kind of company change to looking at their logs, this question seems to be leaning towards storage.
upvoted 1 times

Dree_Dogg 1 year, 9 months ago

Selected Answer: C

C is the best answer
upvoted 1 times

Pavel019846457 1 year, 10 months ago

My choice is A. As patching critical vulnerabilities should go first. Managed services can promptly respond.
upvoted 1 times

🗨️ 👤 **attesco** 1 year, 11 months ago

Selected Answer: C

Explanation:

Investing in a failover and redundant system, as necessary, is the best solution to improve the availability of the organization's systems based on past incidents. A failover system is a backup system that automatically takes over the operation of a primary system in case of a failure or outage. A redundant system is a duplicate system that runs simultaneously with the primary system and provides backup functionality if needed. Investing in a failover and redundant system can help to ensure that the organization's systems are always available and can handle the workload without interruption or degradation.

upvoted 2 times

🗨️ 👤 **Bubu3k** 1 year, 11 months ago

Selected Answer: D

I would go for D

You'd still need some manpower to help/oversee the backups. To me is obvious they're lacking in that department, failed to review logs, wipe out credentials (which might be the reason for the ransomware) etc

upvoted 2 times

🗨️ 👤 **thenewpcgamer** 2 years, 1 month ago

Selected Answer: D

The question mentions systematic issues. 5/7 of these issues would be negated by proper log review/vulnerability scans reviews.. also, a warm site has not data... therefore, if your backups dont work.. your warm site is useless.

To fix the systemic issue at this organization you need to hire more staff to help with log review and vulnerability management.

FYI. if someone would review logs... the would see that backups are failing.

upvoted 1 times

🗨️ 👤 **uday1985** 2 years, 1 month ago

lets build a redundant site without patching! nice appraoch!

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. Is the best answer. If there was an answer regarding improving better backup and restore systems, I would have chosen that.

upvoted 2 times

🗨️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: C

My choice is C

upvoted 1 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: C

Between B and C, a hot site is a mirrored production environment for temporary use. Given the scenario of their backups failing multiple times, C seems like it's the best choice

upvoted 3 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

C looks right

upvoted 1 times

🗨️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: C

looks good to me

upvoted 1 times

🗨️ 👤 **Practice_all** 3 years, 11 months ago

looking at question "investing in FIRST due to the potential impact of availability"

C seems appropriate answer which is mainly related to restoring the data.

upvoted 2 times

🗨️ 👤 **SniipZ** 4 years ago

Answer is C. Both on July 31 and November 24, the organization could not restore multiple days due to missing disaster recovery plan. Therefore, failover systems are very important for this organization.

upvoted 3 times

  **mcNik** 4 years ago

and in addition Warm site won't help you if you don't have up to date backups . As we know Warm sites has the hardware and everything else except the data which needs to be restored. C seems correct

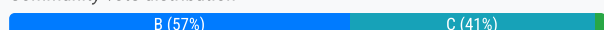
upvoted 2 times

The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's single Internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT department?

- A. Require the guest machines to install the corporate-owned EDR solution
- B. Configure NAC to only allow machines on the network that are patched and have active antivirus
- C. Place a firewall in between the corporate network and the guest network
- D. Configure the IPS with rules that will detect common malware signatures traveling from the guest network

Suggested Answer: B

Community vote distribution



🗳️ 👤 **zecomeia_007** 11 months, 2 weeks ago

Selected Answer: C

B. Configure NAC to only allow machines on the network that are patched and have active antivirus: While Network Access Control (NAC) is a good security practice, it might not be feasible to enforce patching and active antivirus on all guest devices.

upvoted 1 times

🗳️ 👤 **skibby16** 1 year, 6 months ago

Selected Answer: C

A firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules or policies. A firewall can help prevent unauthorized or malicious traffic from entering or leaving a network, and protect network resources from external threats. Placing a firewall in between the corporate network and the guest network can help prevent a guest device from infecting machines on the corporate network or taking down the company's single internet connection, as it can block or filter any unwanted or harmful traffic from the guest network.

upvoted 3 times

🗳️ 👤 **dickchappy** 1 year, 7 months ago

Selected Answer: B

SINGLE internet connection, meaning its likely they do not even have a guest network. If that was not stated I would likely say C to segment the networks, but it seems like that is not an option.

upvoted 1 times

🗳️ 👤 **kumax** 1 year, 9 months ago

Selected Answer: B

ChatGPG:

Implement Network Access Control (NAC) solutions to enforce policies on guest device access. NAC can check guest devices for compliance with security policies before allowing them to connect to the network.

upvoted 2 times

🗳️ 👤 **turki_1993** 1 year, 9 months ago

Selected Answer: B

i think answer is B

Network Access Control (NAC)

- A general term for the collected protocols, policies, and hardware that authenticate and authorize access to a network at the device level

upvoted 1 times

🗳️ 👤 **Aliyan** 1 year, 10 months ago

Selected Answer: B

NAC can be configured to place guest devices in a restricted network segment or VLAN, isolating them from critical corporate resources. This limits the potential impact of any compromise.



upvoted 3 times

🗳️ 👤 **kill_chain** 1 year, 10 months ago

Selected Answer: B

Taking down the company's single internet connection is a concern being fixed....

upvoted 1 times

  **attesco** 1 year, 11 months ago

Selected Answer: C

What are the general capabilities of a NAC solution?

NAC solutions help organizations control access to their networks through the following capabilities:

Policy lifecycle management: Enforces policies for all operating scenarios without requiring separate products or additional modules.

Profiling and visibility: Recognizes and profiles users and their devices before malicious code can cause damage.



Guest networking access: Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal.

Security posture check: Evaluates security-policy compliance by user type, device type, and operating system.

Incidence response: Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention.

Bidirectional integration: Integrate with other security and network solutions through the open/RESTful API.

upvoted 2 times

  **attesco** 1 year, 11 months ago

take it or leave it. The answer is C

upvoted 1 times

  **karpal** 2 years ago

Selected Answer: C

You always segment the guest network from the corporate network. B would still allow the guests on your corporate network which is a huge risk by itself.

upvoted 3 times

  **kyky** 2 years ago

Selected Answer: C

C: Place a firewall between the corporate network and the guest network.

Placing a firewall between the corporate network and the guest network is a common and effective security measure to isolate and protect the corporate network from potential threats originating from guest devices. By implementing a firewall, you can control and monitor the traffic flowing between the two networks, allowing you to enforce security policies and restrict unauthorized access

upvoted 2 times

  **jreverte** 2 years, 1 month ago

Selected Answer: B

The point of the questions is the access to the single internet point of the office. Normally will be C if we have more than one point to internet but for a single point option C is not viable

upvoted 1 times

  **LukaszL** 2 years, 2 months ago

Selected Answer: C

I am voting for C. Using NAC on guest computers does not make sense to me. Usually guests should be separated from corporate.



upvoted 3 times

  **Mounted0608** 2 years, 2 months ago

Selected Answer: C

It's standard practice to put guest devices on a separate network with a firewall. To allow guest devices on a corporate network would be unwise.

upvoted 2 times

  **kiduuu** 2 years, 2 months ago

Selected Answer: C

A firewall can be configured to restrict network traffic between the corporate network and the guest network. This will prevent any infected guest device from infecting the corporate network and protect the company's single Internet connection from being taken down

upvoted 2 times

  **HereToStudy** 2 years, 2 months ago

Selected Answer: B

B) would ensure that only devices that meet the company's security standards are allowed to connect to the network, minimizing the risk of malware infections or attacks.

C) is a good security measure, but it may not be enough to prevent guest devices from infecting machines on the corporate network
upvoted 2 times

🗨️ 👤 **Joshey** 2 years, 3 months ago

Selected Answer: C

Even if the machine is up-to-date with patches and has an active AV running, why would you allow a guest on your corporate network ????? what if the guest performs a 0-day that the AV can't, or performs reconnaissance?? or brings down the second....segmentation with a firewall is the best option
upvoted 4 times

🗨️ 👤 **chuck165** 2 years, 5 months ago

I'm going with C.

In order for you NAC configuration to verify patches and antivirus, it would need client installed on every machine, including your guests, which isn't feasible, same reason A isn't correct.

CYSA+ seems to be big on segmentation which all points to C being the correct answer.

upvoted 1 times

🗨️ 👤 **db97** 2 years, 4 months ago

NAC works in agent and/or agentless mode.

upvoted 3 times

🗨️ 👤 **CCNPsec** 1 year, 9 months ago

Looks like you never worked with BYOD products, that won't let you into the network until you login to a portal where you will install the onboarding software to allow you as a guest in the corporate network.

B should be the correct answer.

upvoted 1 times

Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night. Which of the following actions should the analyst take NEXT?

- A. Disable the privileged account.
- B. Initiate the incident response plan.
- C. Report the discrepancy to human resources.
- D. Review the activity with the user.

Suggested Answer: D

Community vote distribution



🗳️ 👤 **JayMus** Highly Voted 3 years, 4 months ago

I think initiating an IR plan will be the best, because the employee might be an insider threat or maybe he might be using it for other reasons. Approaching him without first knowing his intent will be a bad idea.

upvoted 25 times

🗳️ 👤 **mhop321** 2 years, 5 months ago

Totally agree that they might be an insider threat so wouldn't be D, however it states there has been a security breach so I assume the IR plan has already initiated? As there is an ongoing investigation?

upvoted 1 times

🗳️ 👤 **Joshey** 2 years, 3 months ago

So I'll go with B

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree. Following a breach, meaning post breach where that incident is likely over. Then company decides to monitor off hour logins. Discovers a pattern, what happens next? We initiate the IR plan as this event has kicked off a new investigation. Through the IR process we will find out if it is or is not related to the previous breach.

upvoted 2 times

🗳️ 👤 **mmm55555** 3 years, 4 months ago

I'm going to have to agree with B - initiate IR plan. The threat of an insider makes me think answer D is not a good idea. Yes the activity may be legitimate, but it can also be nefarious. Better to over-react then under-react and tip off an insider about an investigation.

upvoted 8 times

🗳️ 👤 **forklord72** Highly Voted 2 years, 8 months ago

Selected Answer: A

Read the question everyone. There's been a security breach, there's already an ongoing investigation, the only correct option is A. The activity is being conducted during non-business hours, that alone is a policy violation. Not D. Not B either because there's already an ongoing investigation. The next step is to contain.

upvoted 13 times

🗳️ 👤 **NickDrops** 2 years, 5 months ago

Pls disregard my last reply. The question said that it was consistent. No one is patching every night. Could be a service running under a user account instead of a service account, like it should.

upvoted 1 times

🗳️ 👤 **White_T_10** 2 years, 6 months ago

I agree. A it is

upvoted 1 times

🗳️ 👤 **NickDrops** 2 years, 5 months ago

Midnight patches and upgrades are a thing. Hopefully, they have an incident response plan for such occasions. I'd hope that one of the 1st steps in that plan would be to check change controls that were planned.

upvoted 2 times

🗄️ 👤 **zecomeia_007** Most Recent 11 months, 2 weeks ago

Selected Answer: B

B. Initiate the incident response plan.

upvoted 1 times

🗄️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: D

As someone who works in a SOC environment, the first thing you do after seeing a user related suspicious behavior is reach out to the user first.

Answer is D.

upvoted 2 times

🗄️ 👤 **Sebatian20** 1 year, 7 months ago

I think B is the correct answer.

The IR plan MIGHT include reaching out to the user, but it will also contain a flow chart of what to do after.

upvoted 2 times

🗄️ 👤 **[Removed]** 1 year, 7 months ago

I agree what you are saying but just because a user is working during off-hours, it doesn't automatically correlate to the user is doing something bad. You ask the user what they are doing and based on that and the logs you determine the next step.

upvoted 2 times

🗄️ 👤 **dickchappy** 1 year, 7 months ago

Selected Answer: B

FOLLOWING a recent security breach, meaning that breach has already been dealt with. They are investigating potential issues after already resolving the incident, finding a suspicious privileged account should initiate the incident response process. It's absolutely NOT D since it could be an insider threat. A could also be a bad choice since you would immediately alert the attacker.

upvoted 1 times

🗄️ 👤 **Chilaqui1es** 1 year, 7 months ago

Selected Answer: D

I spent too much time reviewing this question but hear me out....

It sounds like D is the answer. Its a tricky worded question.

"FOLLOWING a recent security breach (it doesn't say during) ...a company decides to INVESTIGATE account usage... "

IRP should not be implemented because there is no proof this is an actual breach thus it should be investigated (as said in the question) "Review the activity with the user." to find out more information before going in to IRP.

The account should not be disabled before investigating.

upvoted 3 times

🗄️ 👤 **AhmedSameer** 1 year, 8 months ago

Selected Answer: D

Probably answer will be disabling the account but at first I will review logs to get more info about this activity then I will disable it

upvoted 1 times

🗄️ 👤 **Dree_Dogg** 1 year, 9 months ago

what sucks is that it doesn't say a PRIV account was consistently accessed in the middle of the night...

upvoted 1 times

🗄️ 👤 **Big_Dre** 1 year, 9 months ago

Selected Answer: B

initiate incident response plan. it might include reviewing with the account user or disabling the account.

upvoted 1 times

🗄️ 👤 **Big_Dre** 1 year, 9 months ago

Selected Answer: B

best option

upvoted 1 times

🗄️ 👤 **Dree_Dogg** 1 year, 9 months ago

Selected Answer: B

B seems to be the best answer. Follow the IRP/SOP and get more eyes on this.

upvoted 1 times

🗄️ 👤 **Kickuh06** 1 year, 10 months ago

Passed CS0-003 last week (757), this question was on it! 69 questions, 3 PBQ/SIMs. 25 questions that are in the first 200 questions of this board.

upvoted 3 times

🗨️ 👤 **Dree_Dogg** 1 year, 9 months ago

congrats! i wonder where the CS0-002 questions will come from!

upvoted 1 times

🗨️ 👤 **douglas_smith1** 1 year, 10 months ago

Kickuh06 which answer is it since you just took the exam?

upvoted 1 times

🗨️ 👤 **attesco** 1 year, 11 months ago

Selected Answer: B

Read Below -

An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will provide guidance on key activities. It should also include a cybersecurity list of key people who may be needed during a crisis.

upvoted 2 times

🗨️ 👤 **attesco** 1 year, 11 months ago

In this case - the guy with Privileged Acct is suspected

upvoted 1 times

🗨️ 👤 **rg00** 1 year, 11 months ago

Selected Answer: D

I won't do any action without conducting further investigation.

upvoted 1 times

🗨️ 👤 **MartinRB** 1 year, 12 months ago

Selected Answer: B

Reviewing the activity with the user is part of the incident response, disabling the account is not a good option as the activity might have been legitimate. HR is not an option at this point.

upvoted 1 times

🗨️ 👤 **Nouuv** 2 years ago

D -

Disabling the privileged account or initiating the incident response plan without further investigation could be an overreaction and may cause unnecessary disruption to business processes. Reporting the discrepancy to human resources may be necessary at some point, but it should not be the first immediate action.

The next step should be to review the activity with the user to determine if there is a legitimate reason for accessing the account during non-business hours. This conversation can provide further insight into the situation and help the security analyst determine if any malicious activity or policy violations have occurred. Based on the outcome of the conversation, the analyst can then take appropriate actions such as escalating the issue or disabling the account.

upvoted 2 times

🗨️ 👤 **JoshuaXIV** 2 years, 2 months ago

Selected Answer: A

I believe the answer is A because the company has a recent security breach, it make sense here that incident response is still on-going. We tend to isolate or contain it first for checking.

upvoted 1 times

Which of the following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Choose two.)

- A. Message queuing telemetry transport does not support encryption.
- B. The devices may have weak or known passwords.
- C. The devices may cause a dramatic increase in wireless network traffic.
- D. The devices may utilize unsecure network protocols.
- E. Multiple devices may interfere with the functions of other IoT devices.
- F. The devices are not compatible with TLS 1.2.

Suggested Answer: BD

Community vote distribution

BD (88%)

6%

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: BD

B D, seem to be the best fit here.

upvoted 3 times

🗳️ 👤 **Mouhammad1** 2 years, 5 months ago

Weak password and unsecure protocol IOT

upvoted 2 times

🗳️ 👤 **Ondall_1** 2 years, 7 months ago

Selected Answer: BD

BD are correct answers

upvoted 2 times

🗳️ 👤 **TeyMe** 2 years, 8 months ago

Selected Answer: DE

IoT devices can communicate and pass data between themselves and other traditional systems like computer servers. machine-to-machine (M2M) communication.

upvoted 1 times

🗳️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: BD

BD because some android OS devices compatible with TLS

upvoted 2 times

🗳️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: BD

<https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8228.pdf>

upvoted 3 times

🗳️ 👤 **wico1337** 2 years, 8 months ago

Thank you... I was thinking C/D. I figured that people can change passwords. But according to NIST, certain IOT devices passwords cannot be changed.

upvoted 2 times

🗳️ 👤 **wico1337** 2 years, 8 months ago

OOPS, I meant D/E

upvoted 1 times

🗳️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: BD

I think BD is better than BF

Some Android devices are compatible with TLS 1.2 so this statement is false

upvoted 2 times

🗨️ 👤 **Fastytop** 2 years, 9 months ago

Selected Answer: BF

Weak password and the Tls1.2 . I think they are the correct answer.

upvoted 1 times

🗨️ 👤 **NickDrops** 2 years, 5 months ago

Some, but not all IOT devices support Tls 1.2. D is right, because lack of firmware updates to bring these devices to the most up to date security protocols.

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: BD

B and D are the most likely reason.

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

B/D sounds right to me

upvoted 2 times

In response to an audit finding, a company's Chief Information Officer (CIO) instructed the security department to increase the security posture of the vulnerability management program. Currently, the company's vulnerability management program has the following attributes:

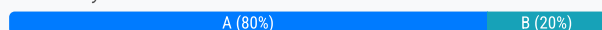
- ⇒ It is unauthenticated.
- ⇒ It is at the minimum interval specified by the audit framework.
- ⇒ It only scans well-known ports.

Which of the following would BEST increase the security posture of the vulnerability management program?

- A. Expand the ports being scanned to include all ports. Increase the scan interval to a number the business will accept without causing service interruption. Enable authentication and perform credentialed scans.
- B. Expand the ports being scanned to include all ports. Keep the scan interval at its current level. Enable authentication and perform credentialed scans.
- C. Expand the ports being scanned to include all ports. Increase the scan interval to a number the business will accept without causing service interruption. Continue unauthenticated scanning.
- D. Continue scanning the well-known ports. Increase the scan interval to a number the business will accept without causing service interruption. Enable authentication and perform credentialed scans.

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Riwon** 2 years, 3 months ago

B. The interval is the time lapse between the completion of the previous scan and the start of the next scan, so increase scan interval means "decrease the frequency of scans".

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 2 months ago

I see what your saying, however, the question states "...business will accept without causing service interruption". I would think that "decreasing the scans" would not be a disruption to service. unless I have misinterpreted this whole thing.

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. This makes the most sense and currently they are at the "minimum" level. Does not mean we cannot improve the cadence.

upvoted 2 times

🗳️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: A

"A" makes sense for a real world scenario.

upvoted 2 times

🗳️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: B

the question says: In response to an audit finding: It is at the minimum interval specified by the audit framework.

so I guess you should keep the scan interval at its current level

upvoted 2 times

🗳️ 👤 **Big_Dre** 1 year, 10 months ago

no the scans are at a minimum meaning when increased it still falls under the acceptable frame. so to increase security we should definitely increase the number of scans too.

upvoted 1 times

🗳️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: A

A is correct

upvoted 2 times

🗳️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: A

A credentialed scan takes more time but, is more thorough.

This answer will not impact availability

All ports should be scanned to catch any malicious high numbered ports

upvoted 1 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: A

A is right imo.

upvoted 1 times

  **Laudy** 2 years, 9 months ago

Only A makes sense.

upvoted 1 times

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct business overseas must have their mobile devices checked for malicious software or evidence of tampering upon their return. The information security department oversees this process, and no executive has had a device compromised. The Chief Information Security Officer wants to implement an additional safeguard to protect the organization's data.

Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

- A. Implement a mobile device wiping solution for use if a device is lost or stolen.
- B. Install a DLP solution to track data flow.
- C. Install an encryption solution on all mobile devices.
- D. Train employees to report a lost or stolen laptop to the security department immediately.

Suggested Answer: A

Community vote distribution

C (66%)

A (34%)

🗳️ 👤 **Apollo28** 1 year, 7 months ago

Selected Answer: A

I chose A for the main reason of my video watching: "Privacy is about the individual, confidentiality is about the data. Encryption is used for confidentiality"

upvoted 2 times

🗳️ 👤 **Chilaqui1es** 1 year, 7 months ago

"It can't be wiped if a device is turned off, in airplane mode, or otherwise cut off from the network." I am choosing encryption.

upvoted 1 times

🗳️ 👤 **Dree_Dogg** 1 year, 9 months ago

Selected Answer: C

C.

Gotta have encryption. Don't over think it.

upvoted 2 times

🗳️ 👤 **supernewtechnewbie** 1 year, 10 months ago

A would be the best answer. This is back from security plus. In order to secure data at rest, data in transit on mobile devices, laptops etc, you should have a mobile device management solution active in the case the device is lost or stolen, a remote wiping solution is needed. The answer is actually A.

upvoted 3 times

🗳️ 👤 **Big_Dre** 1 year, 10 months ago

anytime you hear privacy encryption is the way to go. All data at rest or in use should be encrypted if you are looking for confidentiality/privacy

upvoted 3 times

🗳️ 👤 **Dutch012** 2 years ago

He wants an additional safeguard to protect the organization's data, so I think that means data is already encrypted,

90% remote wiping is the correct answer.

upvoted 2 times

🗳️ 👤 **alayeluwa** 2 years, 2 months ago

Stop overthinking it with all these some countries does not allow encryption.

Encryption is the best answer here. You have to be able to connect to the device MDM to wipe (Goodluck). With encryption, take it 5 million feet deep with no signal, data will still be encrypted.

upvoted 4 times

🗳️ 👤 **uday1985** 1 year, 10 months ago

what if the attacker had the credentials to login ? how good encryption in this scenario ?

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

What if the device is in airplane mode? Device can't be wiped. Data protection = encryption. C is the right answer.

upvoted 1 times

🗳️ 👤 **NerdAlert** 2 years, 2 months ago

This question is kicking my butt because what if the device is stolen and unlocked - what good will encryption do?!

At the same time, what if remote wipe is enabled, but airplane mode is turned on. What good will remote wipe do?!

upvoted 3 times

🗳️ 👤 **NerdAlert** 2 years, 2 months ago

also this question is just like #168 but the remote wipe answer is written differently

upvoted 1 times

🗳️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: C

Encryption

upvoted 1 times

🗳️ 👤 **DUD899** 2 years, 3 months ago

AI says encryption

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

A or C? I hope I don't get this one. While there are countries that do not allow encryption on mobile devices, you are also able to apply for an import license, or may fall under "personal use". Encryption can be used for nefarious reasons. Data wipes are possible as long as the device can connect to the internet, check in, and kick the task to wipe. Many times those devices never get put back on the internet. Ugh.. I guess would go with C.

upvoted 1 times

🗳️ 👤 **alayeluwa** 2 years, 2 months ago

CompTIA's questions are all U.S. based.

upvoted 1 times

🗳️ 👤 **kill_chain** 1 year, 11 months ago

granted but the question does say offices located globally

upvoted 1 times

🗳️ 👤 **Cyber_Guru** 2 years, 4 months ago

Selected Answer: A

Encryption of mobile devices is not allowed in all countries, since the question says employees travel overseas Mobile Device Wiping solution is the correct answer.

upvoted 2 times

🗳️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: C

In this scenario, the organization wants to implement an additional safeguard to protect the privacy of its data if a mobile device is stolen. One of the best controls to achieve this goal would be to enable full-disk encryption on the devices.

Full-disk encryption protects the data stored on a device by encrypting all of its contents, including the operating system and system files. This makes it more difficult for unauthorized individuals to access the data, even if the device is stolen or lost.

Other possible controls that the organization may consider implementing include implementing strong password policies, enforcing multi-factor authentication, and using mobile device management (MDM) solutions to remotely wipe data from lost or stolen devices.

However, given that the question is specifically asking for the BEST control to protect the privacy of the data in case of a stolen device, full-disk encryption is the most appropriate option.

upvoted 3 times

🗳️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: C

C would be the best. Remote wipe also would protect well but it may be some time between the loss/theft of the device and you realizing it is gone and initiating the wipe.

upvoted 1 times

🗳️ 👤 **david124** 2 years, 5 months ago

Selected Answer: C

chat GPT says C LUL

upvoted 2 times

🗨️ 👤 **AaronS1990** 2 years, 5 months ago

Another unhelpful comment of you just telling us what chat GPT says...
upvoted 8 times

🗨️ 👤 **corboonstra** 2 years, 6 months ago

I would go for C encryption, if the thieves really want to have the data they can put it in a Faraday cage and extract the data later in a secure room with no signal... Remote wipe is not going to help then.
upvoted 1 times

🗨️ 👤 **lordguck** 2 years, 6 months ago

I'd prefer C but have to go with A, as there are countries which prohibit the use of encryption.
upvoted 1 times

🗨️ 👤 **Mr_BuCh3th34D** 2 years, 6 months ago

You're overthinking the question. Even if you can remotely wipe a device, that doesn't mean one will have available time to do it before any data loss. If a device is encrypted, it doesn't matter if it was lost/stolen, no one can tamper with its content.
upvoted 6 times

🗨️ 👤 **db97** 2 years, 5 months ago

This completely makes sense
upvoted 1 times

🗨️ 👤 **NerdAlert** 1 year, 10 months ago

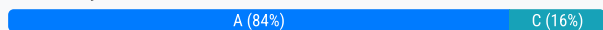
unless it is stolen and unlocked
upvoted 1 times

A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

- A. Static analysis
- B. Dynamic analysis
- C. Regression testing
- D. User acceptance testing

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Charlieb123** Highly Voted 3 years, 5 months ago

Selected Answer: A

Agreed it's A.

What is static analysis in cyber security?

Image result for static analysis cyber security

Static application security testing (SAST), or static analysis, is a testing methodology that analyzes source code to find security vulnerabilities that make your organization's applications susceptible to attack.

Regression testing is a software testing practice that ensures an application still functions as expected after any code changes, updates, or improvements. Which would fall into the Security Analyst remit.

upvoted 9 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree.. this is Static Analysis.

upvoted 1 times

🗳️ 👤 **awad1997** Highly Voted 3 years, 4 months ago

Selected Answer: A

Clearly its A

upvoted 5 times

🗳️ 👤 **iraidesc** Most Recent 2 years, 6 months ago

Selected Answer: A

Process of reviewing uncompiled source code either manually or using automated tools

-Automated tools can reveal issues ranging from faulty logic to insecure libraries before the app even runs

▪ Code Review

• The process of peer review of uncompiled source code by other developers

upvoted 1 times

🗳️ 👤 **MrRobotJ** 2 years, 7 months ago

Why not B?

upvoted 2 times

🗳️ 👤 **okioki** 2 years, 7 months ago

Selected Answer: C

Answer from the Course Class

upvoted 1 times

🗳️ 👤 **gwanedm** 2 years, 8 months ago

the answer is A

A regression test evaluates whether changes in software have caused previously existing functionality to fail

upvoted 1 times

🗳️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: A

"Unlike many other methods, static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do. Static code analysis can be conducted using automated tools or manually by reviewing the code—a process sometimes called "code understanding." Automated static code analysis can be very effective at finding known issues, and manual static code analysis helps identify programmer-induced errors." CompTIA CYSA Dstudy Guide

upvoted 3 times

🗳️ 👤 **Fastytop** 2 years, 9 months ago

Selected Answer: C

Regression testing.

upvoted 2 times

🗳️ 👤 **cyberseckid** 2 years, 9 months ago

definitely not , please read regression testing definition first.

upvoted 2 times

🗳️ 👤 **IT_Master_Tech** 2 years, 7 months ago

<https://www.guru99.com/regression-testing.html>

upvoted 1 times

🗳️ 👤 **EVE12** 2 years, 10 months ago

Static analysis refers to testing or examining software when it is not running. The most common type of static analysis is code review. Code review is the systematic investigation of the code for security and functional problems. It can take many forms, from simple peer review to formal code review. Code review was covered earlier in this chapter. More on static analysis was covered in Chapter 4.

upvoted 1 times

🗳️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: A

looks good to me

upvoted 1 times

🗳️ 👤 **FrancisBakon** 2 years, 11 months ago

People who are confused why it is not Dynamic (B) or Regression (C) the keyword here is 'code'. You perform dynamic or regression testing while running the program.

upvoted 3 times

🗳️ 👤 **FrancisBakon** 2 years, 11 months ago

Selected Answer: A

It is not regression testing. Because that is not job of Analyst. Regression testing is in general of QA/Test team. Analyst usually performs either perform static (code scanning) or Dynamic (VA/fuzzing)

upvoted 1 times

🗳️ 👤 **Threat_Analyst** 3 years ago

A security analyst reviewing code should be done with a Dynamic analysis tool as coding is not a usual strength of security analysts just scripting.

upvoted 2 times

🗳️ 👤 **f3lix** 3 years, 1 month ago

This is indeed a very tricky one.

Statistic analysis - code analysis (not software analysis)

Regression Testing - Software Test to ensure it functions as it should.

Questions asks about examining code and not software, I think here I'll be going with A.

upvoted 1 times

🗳️ 👤 **encxorblood** 3 years, 2 months ago

C - Regression testing is testing existing software applications to make sure that a change or addition hasn't broken any existing functionality.

upvoted 1 times

🗳️ 👤 **RoPsur** 3 years, 3 months ago

Selected Answer: C

Regression testing is making sure past vulnerabilities are not resurfaced when implementing new code. We are not software developers to pick A...

upvoted 2 times

🗳️ 👤 **wazowski1321** 3 years, 3 months ago

Selected Answer: A

A. static analysis
upvoted 4 times

A security analyst inspects the header of an email that is presumed to be malicious and sees the following:

Received: from sonic306-20.navigator.mail.company.com (77.21.102.11) by mx.google.com with ESMTPS id qu22a111129667eaa.101.2020.02.21.01.22.55 for (version=TLS1.0 cipher-ECDEMRSA-AES128-GCM-SHA256 bits=128/128); Mon, 21 Feb 2020 01:22:55 -0600 (MST)

From: smith@yahoo.com
To: jones@gmail.com
Subject: Resume Attached

Which of the following is inconsistent with the rest of the header and should be treated as suspicious?

- A. The use of a TLS cipher
- B. The sender's email address
- C. The destination email server
- D. The subject line

Suggested Answer: B

Community vote distribution

B (100%)



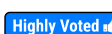
  **Laudy**  2 years, 9 months ago

Its B, but it was sent by "sonic306-20.navigator.mail.company.com", not yahoo.

The google server is to be expected since "to" is a gmail.com email. (It's like by-direction-of)

Just check your own gmail headers.

upvoted 9 times

  **anon0621**  2 years, 9 months ago

The sender is yahoo but the header indicates google

upvoted 5 times

  **alayeluwa** 2 years, 2 months ago

The google there is expected since it's sent to a google mail, that's the delivery. It's the sonic address that does not correspond with senders yahoo email.

upvoted 1 times

  **sorinttt**  2 years, 1 month ago

unbelievable what a lack of attention on your part! Sonic306 is not an email address but a server through which the email passed, if you have GMAIL, open an email and look in the header.

Received: from mail1.static.mailgun.info (mail1.static.mailgun.info. [104.130.122.1])

by mx.google.com with UTF8SMTPS id r9-20020a05622a034900b003f52c2fa74dsi4072172qtw.146.2023.05.22.09.48.04

for <43534322@gmail.com>



upvoted 2 times

  **2Fish** 2 years, 3 months ago

Selected Answer: B

B. The From and "received from" domains do not match.

upvoted 1 times

  **R00ted** 2 years, 9 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: B

I say B

upvoted 4 times

A team of network security analysts is examining network traffic to determine if sensitive data was exfiltrated. Upon further investigation, the analysts believe confidential data was compromised. Which of the following capabilities would BEST defend against this type of sensitive data exfiltration?

- A. Deploy an edge firewall.
- B. Implement DLP.
- C. Deploy EDR.
- D. Encrypt the hard drives.

Suggested Answer: B

Community vote distribution



🗳️ 👤 **_Bihari_** 1 year, 6 months ago

Selected Answer: B

B. Implement DLP (Data Loss Prevention)

The BEST capability to defend against sensitive data exfiltration is to implement Data Loss Prevention (DLP). DLP solutions are designed to monitor, detect, and prevent unauthorized access, use, or transmission of sensitive data, thereby safeguarding against data exfiltration.

upvoted 1 times

🗳️ 👤 **_Bihari_** 1 year, 6 months ago

B. Implement DLP (Data Loss Prevention).

Data Loss Prevention (DLP) is specifically designed to defend against sensitive data exfiltration. DLP solutions monitor, detect, and prevent unauthorized transmission of sensitive information across a network. They can identify and block attempts to transfer sensitive data through various channels, such as email, web traffic, or other network protocols.

While the other options (deploying an edge firewall, implementing EDR, and encrypting hard drives) are important security measures, they may not be as directly focused on preventing the unauthorized transmission of sensitive data outside the network

upvoted 1 times

🗳️ 👤 **dickchappy** 1 year, 7 months ago

Selected Answer: D

I disagree with DLP. It's asking for the BEST method, encrypting the confidential data makes any attack against it irrelevant.

upvoted 1 times

🗳️ 👤 **geenoe** 1 year, 7 months ago

all data is encrypted in real world. even so, the data is still exfiltrated and used in malicious purposes. i agree and going with b

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. DLP will help mitigate this issue.

upvoted 1 times

🗳️ 👤 **f3lix** 2 years, 5 months ago

Selected Answer: B

DLP - Data Loss Prevention; Prevent data exfiltration. B

upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

B obviously.

upvoted 1 times

🗳️ 👤 **anon0621** 2 years, 9 months ago

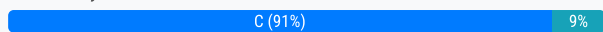
If you want to keep data from being exfiltrated, DLP is the way to go
upvoted 4 times

After a series of Group Policy Object updates, multiple services stopped functioning. The systems administrator believes the issue resulted from a Group Policy Object update but cannot validate which update caused the issue. Which of the following security solutions would resolve this issue?

- A. Privilege management
- B. Group Policy Object management
- C. Change management
- D. Asset management

Suggested Answer: B

Community vote distribution



🗳️ 👤 **jiggly** 6 months, 1 week ago

Selected Answer: C

While better GPO management practices could prevent future issues, they do not help pinpoint the specific causing update or resolve the current problem.

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. Change management takes into account a roll-back procedure, while also providing more insight of what could go wrong so you are better prepared.,

upvoted 1 times

🗳️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: C

c is the best answer

upvoted 1 times

🗳️ 👤 **TeyMe** 2 years, 8 months ago

Selected Answer: C

With Change Management, you can roll back to be known working condition.

upvoted 1 times

🗳️ 👤 **MortG7** 2 years, 8 months ago

There is no such thing as "Group Policy Object management" answer is C

upvoted 2 times

🗳️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: C

I think C is correct.

upvoted 1 times

🗳️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: C

The answer is C

Change Management:

o The process through which changes to the configuration of information systems are monitored and controlled as part of the organization's overall configuration management efforts

o Each component should have a separate document or database record that describes its initial state and subsequent changes

- Configuration information
- Patches installed
- Backup records

- Incident reports/issues
 - o Change management ensures all changes are planned and controlled to minimize the risk of a service disruption
 - o Changes are categorized according to their potential impact and level of risk
 - Major
 - Significant
 - Minor
 - Normal
- upvoted 3 times

🗨️ 👤 **RoVasq3** 2 years, 9 months ago

Implement change management for Group Policy

Group Policy can get out of control if you let all your administrators make changes as they feel necessary. But tracking changes to Group Policy can be difficult because security logs cannot give you full picture of exact which setting was changed and how. You can take a look at how you can track changes to Group Policy in the Group Policy Auditing Quick Reference Guide.

The most important GPO changes should be discussed with management and fully documented. In addition, you should set up email alerts for changes to critical GPOs because you need to know about these changes ASAP in order to avoid system downtime. You can do this using PowerShell scripts or, more conveniently, with IT auditing software like Netwrix Auditor for Active Directory.

upvoted 2 times

🗨️ 👤 **RoVasq3** 2 years, 9 months ago

Selected Answer: C

looks good to me

upvoted 1 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: B

B, GPO Management has it's own way to perform auditing

C is the better answer, but is doing more than what the question is asking for

upvoted 1 times

🗨️ 👤 **AaronS1990** 2 years, 5 months ago

Then why did you put B as the selected aswer...

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

C seems like the correct answer because change management would best solve this issue but maybe im wrong.

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

I thought it was C, but I guess it is B...

<https://www.lepide.com/how-to/audit-changes-made-to-group-policy-objects.html>

upvoted 2 times

🗨️ 👤 **slizla** 2 years, 9 months ago

It is actually C in my opinion, if the company had a change management Admin would know which update to GP cause the issue since he could see the configuration before the update. - The problem here is the admin couldn't validate which update caused the issue.

upvoted 1 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

I agree that change management would holistically be a better option for the network as a whole, GPO Management specifically has it's own audit policy that tracks this stuff. Only reason why I would stick with B as the answer.

upvoted 1 times

Which of the following describes the main difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

- A. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
- B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
- C. Unsupervised algorithms are not suitable for IDS systems, while supervised algorithms are.
- D. Unsupervised algorithms produce more false positives than supervised algorithms.

Suggested Answer: D

Community vote distribution

B (63%)

D (37%)

🗳️ **kmanb** Highly Voted 2 years, 5 months ago

Literally both D and B are right. Just pray this question doesn't come up
upvoted 6 times

🗳️ **dickchappy** 1 year, 7 months ago

While both are correct, it is asking for the MAIN difference, which is the requirement of feedback.
upvoted 1 times

🗳️ **glenn Dexter** Most Recent 1 year, 2 months ago

Selected Answer: B

In supervised machine learning, algorithms require labeled training data, where each data point is associated with a known output label. The algorithm learns to predict the output based on input features and the provided labels. Supervised algorithms rely on human experts (security analysts) to provide feedback on the correctness of predictions and to adjust the model as needed.
upvoted 1 times

🗳️ **d8viev** 1 year, 7 months ago

Selected Answer: B

B. Supervised learning algorithms are trained on a labeled dataset, which means they require prior knowledge of input-output pairs. In cybersecurity, this could mean a dataset where network traffic data is labeled as 'malicious' or 'benign'. A security analyst might provide feedback or labels for the training data.
Unsupervised learning algorithms, on the other hand, do not require labeled data. They work on identifying patterns or anomalies without prior training on what constitutes normal or abnormal behavior.
upvoted 1 times

🗳️ **Dree_Dogg** 1 year, 9 months ago

Selected Answer: B

B is best.
The key phrase is "main difference..."
upvoted 1 times

🗳️ **yanyan20** 2 years, 1 month ago

Selected Answer: D

unsupervised algorithms may require security analyst feedback to interpret results or adjust settings, so B is not correct
upvoted 2 times

🗳️ **kiduuu** 2 years, 2 months ago

Selected Answer: D

Supervised learning algorithms are trained on labeled data, while unsupervised learning algorithms are used to identify patterns and anomalies in data without prior knowledge of what constitutes normal or abnormal behavior.

Option A is incorrect because both supervised and unsupervised algorithms can be used to block attacks, depending on the application.

Option C is incorrect because unsupervised algorithms are often used in intrusion detection systems (IDS) to identify anomalous behavior.
upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. Question asks for the main difference here.

upvoted 1 times

🗨️ 👤 **Stiobhan** 2 years, 4 months ago

Selected Answer: B

To be honest, it could be either B or D depending on how you interpret the answers - <https://www.ibm.com/cloud/blog/supervised-vs-unsupervised-learning#:~:text=The%20main%20difference%20between%20supervised,unsupervised%20learning%20algorithm%20does%20not.>

upvoted 2 times

🗨️ 👤 **Soldier** 2 years, 4 months ago

Selected Answer: D

Supervised machine learning algorithm is a machine learning approach that's defined by its use of labeled datasets. These datasets are designed to train or "supervise" algorithms into classifying data or predicting outcomes ACCURATELY.

On the other hand, unsupervised learning models work on their own to discover the inherent structure of unlabeled data leading to many false positives.

Note that they still require some human intervention for validating output variables but the question is asking for a key difference

upvoted 3 times

🗨️ 👤 **Soldier** 2 years, 4 months ago

The answer is C

Supervised machine learning algorithm is a machine learning approach that's defined by its use of labeled datasets. These datasets are designed to train or "supervise" algorithms into classifying data or predicting outcomes ACCURATELY.

On the other hand, unsupervised learning models work on their own to discover the inherent structure of unlabeled data leading to many false positives.

Note that they still require some human intervention for validating output variables but the question is asking for a key difference

upvoted 1 times

🗨️ 👤 **Soldier** 2 years, 4 months ago

The answer is D and C. That's a typo

upvoted 2 times

🗨️ 👤 **david124** 2 years, 5 months ago

Selected Answer: B

B is correct.

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: B

Changing me answer to B

The main difference between supervised vs unsupervised learning is the need for labelled training data. Supervised machine learning relies on labelled input and output training data, whereas unsupervised learning processes unlabelled or raw data.

upvoted 2 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: D

D is the correct one.

upvoted 4 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

On the fence with this one:

"While supervised learning models tend to be more accurate than unsupervised learning models, they require upfront human intervention to label the data appropriately."

So technically both are correct.

upvoted 1 times

🗨️ 👤 **Tascjfbosafj** 2 years, 8 months ago

Selected Answer: B

It's B.

upvoted 1 times

🗨️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: B

B is correct.

upvoted 2 times

🗨️ 👤 **arctanx** 2 years, 8 months ago

Selected Answer: B

The question asks for main difference so it should be B. if it was asking for cons and pros the answer would be D then.

The main difference between supervised vs unsupervised learning is the need for labelled training data. Supervised machine learning relies on labelled input and output training data, whereas unsupervised learning processes unlabelled or raw data.

[https://www.seldon.io/supervised-vs-unsupervised-learning-](https://www.seldon.io/supervised-vs-unsupervised-learning-explained#:~:text=The%20main%20difference%20between%20supervised,processes%20unlabelled%20or%20raw%20data.)

[explained#:~:text=The%20main%20difference%20between%20supervised,processes%20unlabelled%20or%20raw%20data.](https://www.seldon.io/supervised-vs-unsupervised-learning-explained#:~:text=The%20main%20difference%20between%20supervised,processes%20unlabelled%20or%20raw%20data.)

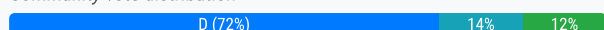
upvoted 4 times

The SOC has received reports of slowness across all workstation network segments. The currently installed antivirus has not detected anything, but a different anti-malware product was just downloaded and has revealed a worm is spreading. Which of the following should be the NEXT step in this incident response?

- A. Send a sample of the malware to the antivirus vendor and request urgent signature creation.
- B. Begin deploying the new anti-malware on all uninfected systems.
- C. Enable an ACL on all VLANs to contain each segment.
- D. Compile a list of IoCs so the IPS can be updated to halt the spread.

Suggested Answer: A

Community vote distribution



jeonard_ddc Highly Voted 2 years, 5 months ago

Selected Answer: D

I think people are confused because all of the steps are valid ones to take. The key is the question asks which step to take NEXT. That means you have to fit the steps into the IR process.

We're past identification as we have a live worm spreading. Next step is containment.

- A) This needs to happen, but could take a long time fo results. This is a post-incident activity.
- B) Changes like this are part of remediation / recovery. But it only says it revealed the worm; not that it stopped it.
- C) This would make sense, but slowness is being reported for "all workstation segments". In other words, it's hit every VLAN already.
- D) Updating your IPS is the best chance you have at stopping it. You don't need much for IOC's, just anything that you're getting from the anti-malware. An EXE, a port, a signature...

upvoted 26 times

Dutch012 2 years ago

Your comment makes sense, thanks!

upvoted 2 times

uday1985 1 year, 10 months ago

Imagine ! just imagine ! that the script of the malware is obfuscated! how long it will take you to deobfuscate and extract IOC's?

upvoted 1 times

novolyus 1 year, 7 months ago

100%. If it is already spread in all vlans, contain each vlan would do nothing because worm will spread in the vlan itself. And that, will happen in every vlan, so you won't stop the worm spreading.

upvoted 1 times

Sebatian20 1 year, 7 months ago

Can't be D.

"across all workstation network segments"

Can't stop something that's already been spread. I believe A or C are the better answer.

upvoted 1 times

fuzzyguzzy Most Recent 6 months, 4 weeks ago

- A) This takes too long
- B) The question says all work stations are slow, implying all devices are infected.
- C) The malware hit all segments, so there's nothing to contain
- D) Again, the worm spread, so there's nothing to contain.

All these options are terrible lol

upvoted 1 times

🗨️ **fuzzyguzzy** 6 months, 4 weeks ago

Thinking this over, I would to D. Contain the malware on each machine. This way when you clean the malware, a host doesn't get reinfected.
upvoted 1 times

🗨️ **zecomeia_007** 11 months, 1 week ago

Selected Answer: C

C. Enable an ACL on all VLANs to contain each segment.
upvoted 1 times

🗨️ **Pavel019846457** 1 year, 8 months ago

ChatGPT says it's C...

Well, might be a point.

upvoted 1 times

🗨️ **Gwatto** 1 year, 8 months ago

"Slowness across ALL network segments" Which means the worm has already spread across all work stations. You cannot halt what has already spread. I'm going with A also

upvoted 1 times

🗨️ **Pavel019846457** 1 year, 10 months ago

Selected Answer: D

D is correct one for NEXT action to be taken
upvoted 1 times

🗨️ **karpal** 2 years ago

Selected Answer: C

I went several times on this question. days have passed. i looked at everyone. all answer make sense.

The thing is they say all workstation segments. and while the word ALL is important, but also workstation. What about the rest that are NOT workstations ? servers , databases etc ? We want to contain it as it an WORM that spreads allone - think SQL Slammer

https://en.wikipedia.org/wiki/SQL_Slammer . So I think the ACL - segmenting ALL segments is the best answer, closing the ports that the worm is using. It is fast and it contains it in the workstation segments that are already infected. the signature and the new anti malware could be done later the Remediation step.

upvoted 2 times

🗨️ **thenewpcgamer** 2 years, 1 month ago

Everyone keeps saying "this has hit every vlan already" as there reasoning for not choosing C.

So let me ask you this.. Do servers also live on vlan segments ... that have not potentially been affected yet?

upvoted 3 times

🗨️ **PartialNarwhal** 2 years, 1 month ago

Yeah they're saying it's hit every network segment, but then choose D to stop the spread. It makes no sense. I'm still leaning towards C.

upvoted 2 times

🗨️ **Kainas** 2 years, 2 months ago

Selected Answer: B

B is a more immediate response to the incident. Deploying the new anti-malware on all uninfected systems will help prevent further infections and reduce the spread of the worm. D is not an immediate response to the incident and may take some time to complete.

Both options are important, but in this specific scenario, B is the more urgent and effective next step to take.

upvoted 2 times

🗨️ **Joshey** 2 years, 3 months ago

Selected Answer: D

C looks appealing but, why would you use ACLs on all vlans, when the IOC/Incident was identified on just the workstation subnet...even sef such action could cause lots of service outages

upvoted 1 times

🗨️ **2Fish** 2 years, 3 months ago

Selected Answer: D



D. I have to agree that we can contain the spread. Then Send a sample (hashs, etc) to the vendor. Perhaps this could be done in tandem if you have more than one Analyst working on the event.

upvoted 1 times

🗨️ **tatianna** 2 years, 4 months ago

Containment is key

upvoted 1 times

  **absabs** 2 years, 4 months ago

Selected Answer: D

This virus already in all workstation, so not C.

A is post-incident activity.

When you deploying new anti-malware, it takes so many time. not B.

D is make sense, IPS is in your system already.

upvoted 1 times

  **IanRogerStewart** 2 years, 4 months ago

Selected Answer: D

Question notes it has already spread to all network segments. At this stage to quote Princess Leia, "Help me Intrusion Prevention System, you're my only hope!"

upvoted 3 times

  **NickDrops** 2 years, 5 months ago



C is a bad answer " Enable an ACL on all VLANs to contain each segment.". Its already on all segments. This won't do anything.

upvoted 3 times

  **HereToStudy** 2 years, 2 months ago

Good catch. I was leaning towards C until I noticed this

upvoted 1 times

  **reidssel** 2 years, 5 months ago

Selected Answer: A

hard to choose, a or d is all fine. But more prefer A since slowness is already on all workstations.

upvoted 1 times

  **MrRobotJ** 2 years, 7 months ago

Selected Answer: D

Should be D

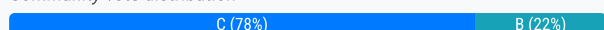
upvoted 1 times

A vulnerability assessment solution is hosted in the cloud. This solution will be used as an accurate inventory data source for both the configuration management database and the governance, risk, and compliance tool. An analyst has been asked to automate the data acquisition. Which of the following would be the BEST way to acquire the data?

- A. CSV export
- B. SOAR
- C. API
- D. Machine learning

Suggested Answer: B

Community vote distribution



🗳️ **cyberseckid** Highly Voted 2 years, 9 months ago

Selected Answer: C

from some one who has 1.5 years expirince in SOAR , SOAR has nothing to do with this question , its API
upvoted 16 times

🗳️ **IT_Master_Tech** 2 years, 7 months ago

So we can rely that the answer is C since you work with SOAR and confirm that it is not related with the question....?
upvoted 2 times

🗳️ **2Fish** 2 years, 3 months ago

I would agree, a SOAR can ingest data from many sources, but its primary function is to automate responses to that data. This question does not mention that part.
upvoted 2 times

🗳️ **indyrckstar** Most Recent 1 year, 5 months ago

Selected Answer: C

API - Automate
upvoted 1 times

🗳️ **Ayben** 1 year, 8 months ago

Selected Answer: B

An API is too broad of an answer. APIs are built for many different solutions. SOAR would be more of a COTS solution for specific tasks.
upvoted 1 times

🗳️ **Dree_Dogg** 1 year, 9 months ago

Selected Answer: C

APIs allow for the automated administration, management, and monitoring of a cloud service
upvoted 2 times

🗳️ **uday1985** 1 year, 10 months ago

API is used for the purpose! but SOAR is required to trigger/automate request
upvoted 1 times

🗳️ **uday1985** 2 years, 1 month ago

Highly doubt that SOAR isnt capable of automating this somehow!
upvoted 1 times

🗳️ **Cosmic_robot** 2 years, 3 months ago

They put automate in there to throw you off. Read the question again - "Which of the following would be the BEST way to 'ACQUIRE' the data?" API is the answer.
upvoted 1 times

🗳️ **josbornx** 2 years, 3 months ago

The BEST way to acquire data for this use case would be through an API (Application Programming Interface). APIs allow for automated data retrieval in a structured manner, which would be suitable for feeding data to both the configuration management database and the governance, risk, and

compliance tool. CSV export may be suitable for periodic manual exports, but it would not be the most efficient or reliable way to automate data acquisition. SOAR (Security Orchestration, Automation, and Response) and machine learning are not directly related to data acquisition and may not be the best fit for this use case.

ChatGPT

upvoted 1 times

🗳️ 👤 **Jolnn** 2 years, 3 months ago

Selected Answer: B

API is literally an interface. It's a vector to get things done, not what actually gets the thing done itself. It's SOAR.

upvoted 1 times

🗳️ 👤 **boletri** 2 years, 4 months ago

Selected Answer: C

Answer: C

Cloud APIs supply access to most CSP services and components for provisioning and configuration. Many also supply access to data exchange for client or third-party application integration. Naturally, services that are accessed through APIs should be secured to prevent unauthorized access to data and configuration. Here are a few examples how cloud APIs might be used:

- To provision resources used in a cloud solution including compute, storage, and networking services.

- To provide third-party or integrated connectivity for data exchange or interaction with a SaaS software suite.

- To configure CSP-specific application platform services such as message queuing or other back-end architecture services required for building highly scalable, feature-rich applications.

It is a SaaS, the solution is hosted in the cloud.

upvoted 2 times

🗳️ 👤 **ddcnsd65** 2 years, 5 months ago

What is SOAR API?

The SOAR platform is built on the REST API. It provides comprehensive access to platform capabilities: to read and write incident data, and to perform a wide range of administrative functions. The REST API is supported by documentation, client libraries and example code for Python, .NET and Java.

upvoted 1 times

🗳️ 👤 **david124** 2 years, 5 months ago

Selected Answer: C

C : API is correct

upvoted 1 times

🗳️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

"An analyst has been asked to AUTOMATE the data acquisition."

SOAR = Security Orchestration, Automation, and Response

upvoted 2 times

🗳️ 👤 **Osagie** 2 years, 6 months ago

Anytime you see automation, just know it is SOAR.

upvoted 2 times

🗳️ 👤 **NickDrops** 2 years, 5 months ago

No. The R stands for response. We aren't responding to any threats.

upvoted 2 times

🗳️ 👤 **mhop321** 2 years, 5 months ago

"and response". The automation still stands.

upvoted 1 times

🗳️ 👤 **MrRobotJ** 2 years, 7 months ago

Selected Answer: C

In my organization sometimes we use API to feed the SIEM sometimes

upvoted 1 times

🗨️ 👤 **arctanx** 2 years, 8 months ago

Selected Answer: C

C. API

Simply lets say they need a vulnerability scanner such as Acunetix, they want to integrate their vulnerabilities into their Jira etc. as far as I saw from my prev. exp. this is by done API. If I didn't get the question wrong.

upvoted 2 times

🗨️ 👤 **edudarl** 2 years, 8 months ago

Selected Answer: B

[https://www-03.ibm.com/software/sla/sladb.nsf/8bd55c6b9fa8039c86256c6800578854/a2b13dc6ac6a13c7852586a80009db9d/\\$FILE/i126-8508-04_03-2021_en_US.docx](https://www-03.ibm.com/software/sla/sladb.nsf/8bd55c6b9fa8039c86256c6800578854/a2b13dc6ac6a13c7852586a80009db9d/$FILE/i126-8508-04_03-2021_en_US.docx)

upvoted 1 times

Which of the following is MOST closely related to the concept of privacy?



- A. The implementation of confidentiality, integrity, and availability
- B. A system's ability to protect the confidentiality of sensitive information
- C. An individual's control over personal information
- D. A policy implementing strong identity management processes

Suggested Answer: C

Community vote distribution

C (81%)

Other

  **jchutch2** Highly Voted 2 years, 9 months ago

Selected Answer: C

From CompTIA CySA+ Domain 5: Compliance and Assessment:

"Privacy refers to whatever control you have over your personal information and how it is utilized."

upvoted 17 times

  **2Fish** 2 years, 3 months ago

Agreed. Thanks for the excerpt.

upvoted 2 times

  **HereToStudy** Most Recent 2 years, 2 months ago

Selected Answer: C

C is the answer

upvoted 1 times

  **talosDevbot** 2 years, 4 months ago

Selected Answer: C

C

Security - focuses on an organization protecting its own data by achieving CIA

Privacy - focuses on the ways that an organization can use and share information it has collected about individuals.

A, B, and D is more related to the concept of Security

upvoted 1 times

  **CyberNoob404** 2 years, 5 months ago

Selected Answer: C

From CySA+ Sybex Book: "Privacy controls have a different focus. Instead of focusing on way that an organization can protect its own information, privacy focuses on the ways that an organization can use and share information that it has collected about INDIVIDUALS. This data is also known as PII. (Privacy)

upvoted 1 times

  **MrRobotJ** 2 years, 7 months ago

I'm confused between B and C

upvoted 1 times

  **Abyad** 2 years, 7 months ago

Selected Answer: B

if we think like a cybersecurity analyst the best answer is B



answer c is general

upvoted 1 times

  **IT_Master_Tech** 2 years, 7 months ago

Question states "sensitive information". You can protect any data's privacy, not only sensitive data. I go with answer C..

upvoted 1 times

  **th3man** 2 years, 7 months ago

Selected Answer: B

Confidentiality is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.

upvoted 1 times

🗨️ 👤 **david124** 2 years, 8 months ago

c it is

upvoted 1 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

Answer is NOT A. Availability has NOTHING to do with privacy.

upvoted 1 times

🗨️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: B

Answer is B...not A

upvoted 2 times

🗨️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: A

Answer is A. Confidentiality is privacy...integrity is unaltered info...availability is having info to right party when needed

upvoted 1 times

🗨️ 👤 **Cizzla7049** 2 years, 9 months ago

I meant B...not A

upvoted 1 times

🗨️ 👤 **Fastytop** 2 years, 9 months ago

Selected Answer: C

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

<https://en.wikipedia.org/wiki/Privacy>

upvoted 2 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

I was thinking A because that gets the most mention when reading about confidentiality when reading textbooks about the topic, but I could be wrong.

upvoted 1 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

You are wrong.

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

C sounds right

upvoted 2 times

An organization is focused on restructuring its data governance programs, and an analyst has been tasked with surveying sensitive data within the organization.

Which of the following is the MOST accurate method for the security analyst to complete this assignment?

- A. Perform an enterprise-wide discovery scan.
- B. Consult with an internal data custodian.
- C. Review enterprise-wide asset inventory.
- D. Create a survey and distribute it to data owners.

Suggested Answer: A

Community vote distribution

D (67%)

A (33%)

  **skibby16**  1 year, 8 months ago

Selected Answer: A


A data governance program is a collection of practices, policies, and procedures that manage, leverage, and protect the data assets of an organization¹. It requires changing the workplace culture and adding some software¹. To survey sensitive data within the organization, the most accurate method is to perform an enterprise-wide discovery scan that can identify and classify data from various sources and systems². This way, the analyst can have a comprehensive view of the data landscape and its quality, security, accessibility, and usage. Consulting with an internal data custodian (B) or reviewing enterprise-wide asset inventory © may provide some insights, but not as accurate or complete as a discovery scan. Creating a survey and distributing it to data owners (D) may be time-consuming and unreliable, as data owners may not have the full knowledge or awareness of their data

upvoted 5 times

  **RyanMccar** 1 year, 8 months ago

Not sure where this answer is from but it sounds official and correct




upvoted 1 times

  **skibby16** 1 year, 6 months ago

References: 1: <https://www.analytics8.com/blog/8-steps-to-start-your-data-governance-program/> 2:

<https://solutionsreview.com/data-management/the-best-data-governance-tools-and-software/>

upvoted 1 times

  **Sebatian20**  1 year, 7 months ago

Selected Answer: A

Both C and D are relying on the knowledge of a third party - and they could be wrong.

B is logical as you actually talk to those who knows about the system but A is the more logical first step.

upvoted 2 times

  **2Fish** 2 years, 3 months ago

Selected Answer: D

D. Is the best option here, specifically how it mentions "Data Owners"

upvoted 2 times

  **uday1985** 2 years, 1 month ago

Really? are you giving a survey to a random guy to fill and trust them they answered accurately?

upvoted 7 times

  **boletri** 2 years, 4 months ago

Selected Answer: D

Data owner—A senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity, and availability of the information asset. The owner is responsible for labeling the asset (such as determining who should have access and determining the asset's criticality and

sensitivity) and ensuring that it is protected with appropriate controls (access control, backup, retention, and so forth). The owner also typically selects a steward and custodian and directs their actions and sets the budget and resource allocation for sufficient controls.

upvoted 2 times

🗳️ **tboi** 2 years, 6 months ago

I would go with A simply because a survey of "sensitive" data might lead to loss of data confidentiality. A survey also is also a cumbersome task and might be inefficient.

upvoted 3 times

🗳️ **Tascjfbosafj** 2 years, 8 months ago

Selected Answer: D

It's D

upvoted 2 times

🗳️ **uday1985** 2 years, 1 month ago

Really? are you giving a survey to a random guy to fill and trust them they answered accurately?

upvoted 5 times

🗳️ **arctanx** 2 years, 8 months ago

Selected Answer: D

A Data Owner is the person accountable for the classification, protection, use, and quality of one or more data sets within an organization. This responsibility involves activities including, but not limited to, ensuring that: The organization's Data Glossary is comprehensive and agreed upon by all stakeholders.

<https://blog.satoricyber.com/the-datamasters-data-owners-vs-data-stewards-vs-data-custodians/#:~:text=A%20Data%20Owner%20is%20the,agreed%20upon%20by%20all%20stakeholders>

upvoted 1 times

🗳️ **SAAVYTECH** 2 years, 9 months ago

Selected Answer: D

Data owners are the people who classify the Data and they also set permission to who access it, so they are the only ones who can provide the most accurate information.

upvoted 2 times

🗳️ **nonjabusiness** 2 years, 9 months ago

Selected Answer: D

Through the process of elimination, D makes the most sense

A- Enumerate OS/ports/services/etc, not dealing with data

B- Data custodian handles the technical details of the data

C- Assets the company owns, though data is an asset this wouldn't be of much use

upvoted 1 times

🗳️ **amateurguy** 2 years, 9 months ago

Selected Answer: D

D seems correct by process of elimination, none of the other ones are related to sensitive data.

upvoted 1 times

🗳️ **amateurguy** 2 years, 9 months ago

Also, if you know what discovery scans and asset inventory is, you would know that they have nothing to do with the actual sensitive data. They have more to do with hardware and software that are being used so A and C are eliminated.

upvoted 1 times

🗳️ **cyberseckid** 2 years, 9 months ago

data discovery scan seems related , can you elaborate on it ?

<https://it.cornell.edu/data-discovery/how-scan-data-discovery>

upvoted 1 times

🗳️ **EAart** 2 years, 9 months ago

Selected Answer: D

D, as this is the only answer that mentions data ownership.

upvoted 1 times

🗳️ **Laudy** 2 years, 9 months ago

A Sounds good to me

upvoted 2 times

  **Joshgip95** 2 years, 4 months ago

Can somebody ban this dude?

upvoted 8 times

Which of the following is the BEST security practice to prevent ActiveX controls from running malicious code on a user's web application?

- A. Deploying HIPS to block malicious ActiveX code
- B. Installing network-based IPS to block malicious ActiveX code
- C. Adjusting the web-browser settings to block ActiveX controls
- D. Configuring a firewall to block traffic on ports that use ActiveX controls

Suggested Answer: C

Reference:

<https://support.microsoft.com/en-us/windows/use-activex-controls-for-internet-explorer-11-25738d05-d357-39b4-eb2f-fdd074bbf347>

ActiveX controls

ActiveX controls are small apps that allow websites to provide content such as videos and games. They also let you interact with content like toolbars and stock tickers when you browse the web. However, these apps can sometimes malfunction, or give you content that you don't want. In some cases, these apps might be used to collect info from your PC, damage info on your PC, install software on your PC without your agreement, or let someone else control your PC remotely.

ActiveX Filtering

ActiveX Filtering in Internet Explorer prevents sites from installing and using these apps. This can help keep you safer as you browse, but it can also affect the performance of certain sites. For example, when ActiveX Filtering is on, videos, games, and other interactive content might not work.

To turn on ActiveX Filtering for all sites



Turn off ActiveX Filtering for individual sites



Turn off ActiveX Filtering for all sites



Adjust ActiveX settings in Internet Explorer

Internet Explorer might not be set up to download or run ActiveX controls for security reasons. Changing some advanced security settings will let you download, install, or run the control, but your PC might be more vulnerable to security threats. Only change advanced ActiveX settings if you're sure about increasing the level of risk to your PC.

Community vote distribution

C (96%)

4%

MacherGaming Highly Voted 3 years ago

Selected Answer: C

So... you made it this far. Congrats! Just wanted to let you know that I passed CySA+ today using this guide, the "All In One" book by Brent Chapman/Fernando Maymi, and the Udemmy course with Jason Dion. There were several question and sims not covered in this guide, but by reviewing and learning from it I was able to score above 85%. Good luck, fellow cyber nerds.

-Macher, New Sr. CyberSec Analyst

P.S. From what I read, the answer here is C.

upvoted 24 times

[Removed] 2 years, 10 months ago

Did some or any questions/sims come from this guide?

upvoted 4 times

2Fish 2 years, 3 months ago

Agree, answer is C

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 2 months ago

I is dangerous to say your name in this site "Macher, New Sr" I might find who you are
upvoted 2 times

🗨️ 👤 **MacherNewSrCyberSecAnal** 2 years, 2 months ago

I know who you are next time don't send everyone your name
upvoted 6 times

🗨️ 👤 **Stiobhan** **Most Recent** 2 years, 3 months ago

Be great if Exam Topics "Experts" could provide this level of answer detail in all of the questions.....isn't that what we are paying for!
upvoted 2 times

🗨️ 👤 **Walloper** 2 years, 7 months ago

Surely completely blocking all ActiveX is not the BEST solution? There would be an unnecessary loss of fuctionality. A or B make more sense for best case solutions imo
upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

C seems like the easiest / quickest solution.
upvoted 1 times

🗨️ 👤 **juninho12** 2 years, 11 months ago

Selected Answer: A

I believe A is the correct answer
upvoted 1 times

A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot be reused. Which of the following is the BEST approach?

- A. Degaussing
- B. Shredding
- C. Formatting
- D. Encrypting

Suggested Answer: B

Community vote distribution

B (76%)

A (24%)

🗳️ 👤 **2Fish** Highly Voted 2 years, 3 months ago

Selected Answer: B

B. Ugh.. this verbiage. While Degaussing will "Sanitize" a HD and render is useless, it will not do the same to Flash or SSDs. So since we are not sure which it is.. I would lean to Shredding.

upvoted 5 times

🗳️ 👤 **PrincePazol** Most Recent 1 year, 8 months ago

Degaussing does not work on SSDs, because SSDs do not use magnetic fields to store data like traditional hard drives do. Running an SSD through a degaussing machine will not destroy the device or the data on it. For destroying SSDs, shredding is recommended in order to physically destroy the device beyond the possibility of repair or recovery.

upvoted 1 times

🗳️ 👤 **jade290** 1 year, 10 months ago

Selected Answer: B

I've seen this question in other CompTIA exams. Although degaussing permanently and securely deletes data using the power of magnets that cannot be recovered with existing or future technology, the answer is always shredding because maybe there was an error with the degaussing and a part of the info is still readable. But if the disk is in pieces, recovery isn't possible.

upvoted 1 times

🗳️ 👤 **tutita** 2 years ago

Selected Answer: A

I will choose A degaussing, best practice is that the disk should be overwritten or degaussed prior to destruction.

upvoted 1 times

🗳️ 👤 **rg00** 1 year, 11 months ago

Based on the question, you should be choosing best approach, not first approach.

upvoted 1 times

🗳️ 👤 **JoshuaXIV** 2 years, 2 months ago

Selected Answer: A

Based on the Storage Device Sanitization and Destruction Manual for NSA.

Shredding is not included only Degaussing and Incineration.

upvoted 1 times

🗳️ 👤 **ComradeBoris** 2 years, 3 months ago

This question is the split difference between the right answer and the most right answer. While degaussing is the right answer, shredding would be the most right answer.

upvoted 3 times

🗳️ 👤 **catastrophie** 2 years, 5 months ago

Just throwing this out there but not storage devices are susceptible to degaussing such as SSD. Shredding gets the job done every time.

upvoted 3 times

🗳️ 👤 **NerdAlert** 2 years, 2 months ago

that is the best point as to why it is better! not all storage devices are affected like SSD's. great idea

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

"so the drives CANNOT BE REUSED." B. Shredding (They will be destroyed making them unusable).

upvoted 2 times

🗨️ 👤 **ref** 2 years, 5 months ago

I am going with Shredding cuz, "storage media files" can be HDD, SSD, RAM, NVM, and CD.

upvoted 3 times

🗨️ 👤 **ms200** 2 years, 6 months ago

chatgpt says Degaussing

upvoted 1 times

🗨️ 👤 **tboi** 2 years, 6 months ago

Degaussing a drive will ensure you cannot reuse it. A

upvoted 1 times

🗨️ 👤 **Cizzla7049** 2 years, 7 months ago

Selected Answer: A

keyword is sanitize. Not physical destroy. it is degaussing

upvoted 1 times

🗨️ 👤 **A_Shadows_Soul** 2 years, 8 months ago

Selected Answer: B

Straight from CompTIA Learn platform:

Secure disposal means physical destruction by mechanical shredding or incineration. It leaves the media device unusable. The company, by policy, does not allow reusing hard drives.

A secure erase (SE) utility is commonly available from vendors to perform sanitization of flash-based devices, especially those that use wear-leveling routines such as TRIM. The media is still usable after using this utility.

In a cryptographic erase (CE), the media is encrypted by default. To apply the erase operation, the encryption key itself is destroyed. The media is still usable after a CE.

Degaussing is an erase method for a hard drive disk (HDD). It rearranges the magnetic field on electronic media to completely erase it. The media is still usable afterward.

upvoted 2 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

Leaning towards A.

Reuse Degaussed Media

Many people are unsure of what to do with degaussed disks, hard drives, tapes, et cetera. Since the devices don't appear damaged, people often think they can reuse them. Unfortunately, degaussing usually renders the device unusable. Hard drives, disks, and more modern devices cannot be reused. However, older devices, such as reel tapes, can occasionally be reused after the process.

upvoted 1 times

🗨️ 👤 **Adrian831** 2 years, 8 months ago

"so the drives cannot be reused".

That is really the point here, so the driver can not be reused ever again.

B is the correct answer here.

upvoted 2 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

Adrian831..I have to agree with you. Went back and did some additional research, and I think Comptia is looking for shredding...changed my answer to B

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: B

The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding

upvoted 1 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: B

B, question doesn't specify if it's a HDD or an SSD

Degaussing will only work on a HDD

upvoted 2 times

🗨️ 👤 **TheSkyMan** 2 years, 9 months ago

Selected Answer: B

It's hard drive shredding. Our company just purchased one... not cheap!

<https://legalshred.com/degaussing-vs-hard-drive-shredding/>

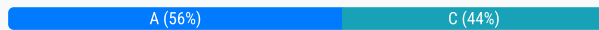
upvoted 2 times

During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the NEXT step the analyst should take?

- A. Validate the binaries' hashes from a trusted source.
- B. Use file integrity monitoring to validate the digital signature.
- C. Run an antivirus against the binaries to check for malware.
- D. Only allow whitelisted binaries to execute.

Suggested Answer: A

Community vote distribution



🗳️ **R00ted** Highly Voted 2 years, 9 months ago

Selected Answer: A

I would check the hash against virustotal before doing anything else
upvoted 5 times

🗳️ **RobV** Most Recent 1 year, 6 months ago

Selected Answer: C

C. Run an antivirus against the binaries to check for malware.
upvoted 1 times

🗳️ **CCNPsec** 1 year, 9 months ago

I see people leaning to C option but how would an analyst know that a machine is compromised??? they do already have AV in place that flagged the machine.
The analyst wants to confirm if that payload is malicious only, so he will open Virus total and check the hash if it was flagged by other sources.
Option A is the correct one.
upvoted 1 times

🗳️ **POWNED** 1 year, 10 months ago

Selected Answer: C

I was leaning toward C, and verified with other websites that others are leaning toward C as well. Why would you ask and wait for an answer from a trusted source when you could just quickly run a scan and get the answer you are looking for?
upvoted 1 times

🗳️ **kiduuu** 2 years, 2 months ago

Selected Answer: C

Validating the binaries' hashes from a trusted source or using file integrity monitoring to validate the digital signature may be helpful, but they do not guarantee that the binaries are not malicious. Similarly, only allowing whitelisted binaries to execute can be a good security practice, but it does not address the immediate concern of the potentially compromised machine. Therefore, running an antivirus is the most appropriate step in this scenario.
upvoted 1 times

🗳️ **Joshey** 2 years, 3 months ago

"after extracting strings..unexpected content"....gives direction to what he is trying to confirm
upvoted 1 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: A

My thought process is that the AV should have already caught those binaries if they have the signatures or hash. I would check the binaries hash first. So A for me.
upvoted 3 times

🗳️ **talosDevbot** 2 years, 4 months ago

Selected Answer: C

Question is asking for the NEXT step.
We already know that binaries are already compromised as the questions stated that the analyst observed abnormal behavior and unexpected strings

in the file.

NEXT step to take is to run an antivirus against the binaries.

upvoted 2 times

🗨️ 👤 **Decatur** 1 year, 11 months ago

The question states that "binaries that are exhibiting abnormal behaviors", so we do not know that they are compromised, therefore we run a scan to detect malware.

upvoted 1 times

🗨️ 👤 **db97** 2 years, 4 months ago

Well... I would run the full anti-malware scan first, in the meantime (while the scanning is in progress), I would go and compare the hash. Both actions at the same time, but the first one it's to rule out/discard/contain/delete a threat in place. If the hash is clean and/or the report shows no results for threats, then we are good :) I talked based on my experience.

upvoted 2 times

🗨️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: A

Validate the hash is first action i think.

upvoted 1 times

🗨️ 👤 **gnnggnngnng** 2 years, 4 months ago

Selected Answer: C

Validating the hashes of the binaries from a trusted source and using file integrity monitoring to validate the digital signature can be important steps in the forensic analysis process, but they do not directly address the issue of the unexpected content found in the binaries. Running an antivirus against the binaries to check for malware is a more direct step to determine if the abnormal behaviors are a result of malicious activity. If the binaries are found to contain malware, then steps can be taken to mitigate the threat and prevent further harm, such as only allowing whitelisted binaries to execute.

upvoted 1 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

Selected Answer: A

"...After extracting the strings, the analyst finds unexpected content..." something different or something that should not be there...you validate the hash to confirm why data was altered/changed/edited and is not what is expected

upvoted 4 times

🗨️ 👤 **david124** 2 years, 8 months ago

A it is

upvoted 1 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: C

A wouldn't hurt to do, but C seems like the more thorough answer

upvoted 2 times

🗨️ 👤 **bigerblue2002** 2 years, 9 months ago

Hey amateurguy, I literally said the exact same thing. I also checked another site and they have C as the answer as well. I selected C too.

I searched more before Submitting this and found another site for C and another for A.

I am going for C!

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

This is confusing, why would you try to validate the binaries against a trust source when you already know its a compromised machine and you know theres binaries exhibiting abnormal behaviour. Wouldn't C be the most reasonable thing to do?

upvoted 4 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

to determine the diff between his binaries and a confirmed good source..the diff being what changed

upvoted 3 times

🗨️ 👤 **jchutch2** 2 years, 8 months ago

To determine which binaries were actually infected or if the malware is coming from elsewhere.

upvoted 1 times

An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by public users accessing the server. The results should be written to a text file and should include the date, time, and IP address associated with any spreadsheet downloads. The web server's log file is named `webserver.log`, and the report file name should be `accessreport.txt`. Following is a sample of the web server's log file:

```
2017-10-12 21:01:12 GET /index.html - 84.102.33.7 - return=200 1622
```

Which of the following commands should be run if an analyst only wants to include entries in which a spreadsheet was successfully downloaded?

- A. `more webserver.log | grep *.xls > accessreport.txt`
- B. `more webserver.log > grep "\.xls" | egrep "E 'success'" > accessreport.txt`
- C. `more webserver.log | grep "E return=200 | \.xls" > accessreport.txt`
- D. `more webserver.log | grep "A *.xls" < accessreport.txt`

Suggested Answer: B

Community vote distribution

C (50%)

C (43%)

7%

 **R00ted** Highly Voted 2 years, 9 months ago

Selected Answer: C

The answers should read:

Options:

A.

```
more webserver.log | grep *.xls > accessreport.txt
```

B.

```
more webserver.log > grep ".xls" > egrep -E 'success' > accessreport.txt
```

C.

```
more webserver.log | grep "E return=200 | \.xls" > accessreport.txt
```

D.


```
more webserver.log | grep -A *.xls < accessreport.txt
```

upvoted 21 times

 **2Fish** 2 years, 3 months ago

Agree. I had to look at this for a bit. Thanks for deciphering that chicken scratch.

upvoted 7 times

 **JENNER_ROCKA** Highly Voted 3 years, 3 months ago

Selected Answer: C

The HTTP 200 OK success status response code indicates that the request has succeeded.

upvoted 8 times

 **zecomeia_007** Most Recent 11 months, 1 week ago

Selected Answer: C

```
grep 200
```

upvoted 1 times

 **[Removed]** 2 years, 4 months ago

It is certainly C. However, the formatting is missing a few quotes.

```
more webserver.log | grep "E return=200" | grep "\.xls" > accessreport.txt
```

upvoted 3 times

 **david124** 2 years, 5 months ago

Selected Answer: C

C is correct

upvoted 2 times

🗨️ **ryanzou** 2 years, 8 months ago

Selected Answer: C

C is correct

upvoted 2 times

🗨️ **jchutch2** 2 years, 8 months ago

Selected Answer: C

It's absolutely C

Tested

upvoted 1 times

🗨️ **Fastytop** 2 years, 9 months ago

Selected Answer: C

is the correct answer

upvoted 2 times

🗨️ **EVE12** 2 years, 9 months ago

Selected Answer: A

A is the correct one

upvoted 1 times

🗨️ **amateurguy** 2 years, 9 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗨️ **miabe** 2 years, 11 months ago

Selected Answer: C

looks good to me

upvoted 1 times

🗨️ **Davar39** 3 years, 1 month ago

Selected Answer: C

Besides the 200 status code, answer C is the only syntax that makes sense.

upvoted 1 times

🗨️ **cysa_1127** 3 years, 2 months ago

Selected Answer: C

C is correct

upvoted 3 times

🗨️ **Xyz_40** 3 years, 2 months ago

C correct

upvoted 3 times

🗨️ **thegreatnivram** 3 years, 2 months ago

B is not also the proper answer because "success" is present on the log (as shown by the sample log), so although the command is well structured, would not result succesful downloads.

upvoted 1 times

🗨️ **thegreatnivram** 3 years, 2 months ago

HTTP 200 ok indicates success, but the command is not properly formulated, the third pipe "| xls&€ > accessreport.txt" does not start with a valid command. No answer is valid here, but C would be closer.

upvoted 2 times

🗨️ **lionleo** 3 years, 3 months ago

The answer is C 200 successful status

upvoted 3 times

A security analyst is running a tool against an executable of an unknown source. The input supplied by the tool to the executable program and the output from the executable are shown below:

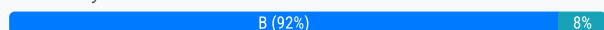
Input supplied by tool	Output from executable
asdfnerlajnvjanjkdfnvkjanakjdv	asdfnerlajnvjanjkdfnvkjanakjdv
klrejfkalsdjfkklasdjffjladsf892	klrejfkalsdjfkklasdjffjladsf892
ADSFQEDVASDASDFASDF;ADSFASDWDF	command not found
qscTRGvcaDFcaDCasDC23rdcasdfAS	qscTRGvcaDFcaDCasDC23rdcasdfAS
lqkejfc934ejcjvsad:cmaoiwefasd	lqkejfc934ejcjvsad:cmaoiwefasd

Which of the following should the analyst report after viewing this information?

- A. A dynamic library that is needed by the executable is missing.
- B. Input can be crafted to trigger an injection attack in the executable.
- C. The tool caused a buffer overflow in the executable's memory.
- D. The executable attempted to execute a malicious command.

Suggested Answer: D

Community vote distribution



Bayoneh 1 year, 7 months ago

Guys,

I will point at an obvious here but let's do each other a favor and not comment if not backing your answer with a reason. Apart from being useless, only "I am thinking B or B is the correct answer" also hide the comments that provide meaningful information.

Cheers

upvoted 4 times

2Fish 2 years, 3 months ago

I am thinking B here as well.

upvoted 1 times

Q23 2 years, 4 months ago

the question shows the input and outputs. If the input can be crafted to trigger an injection attack, and the output reveals "command not found" then the executable did in fact attempt to execute a malicious or untrusted command after all. Both answers are correct, but D validates a command was already entered

upvoted 1 times

AaronS1990 2 years, 4 months ago

I agree that it validates it was entered but was it malicious? I don't think so

upvoted 1 times

MrRobotJ 2 years, 7 months ago

Selected Answer: B

B is the correct answer.

upvoted 3 times

Tascjfbosafj 2 years, 8 months ago

Selected Answer: B

It's B.

upvoted 2 times

R00ted 2 years, 9 months ago

Selected Answer: B

B. Input can be crafted to trigger an injection attack in the executable.

upvoted 2 times

adamhoms 2 years, 9 months ago

Selected Answer: B

Sure is B

upvoted 3 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: B

The command not found output could be caused by an issue with an environment path, using this, a malicious payload could be crafted and executed by leveraging the invalid path

upvoted 1 times

🗨️ 👤 **Merc16** 2 years, 9 months ago

Selected Answer: D

D makes sense to me. For B, I think the application is performing input validation and that's why the statement "Command not found" was returned.

upvoted 1 times

🗨️ 👤 **cyberseckid** 2 years, 9 months ago

I think its B

upvoted 1 times

🗨️ 👤 **TheSkyMan** 2 years, 9 months ago

Pretty sure this is B:

"In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program."

<https://www.acunetix.com/blog/articles/injection-attacks/>

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

B makes the most sense to me.

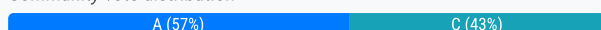
upvoted 2 times

A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verify that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

- A. Automate the use of a hashing algorithm after verified users make changes to their data.
- B. Use encryption first and then hash the data at regular, defined times.
- C. Use a DLP product to monitor the data sets for unauthorized edits and changes.
- D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Suggested Answer: A

Community vote distribution



MortG7 Highly Voted 2 years, 8 months ago

DLP primary function is to prevent data exfiltration based on tagging. It is not used nor marketed to track authorized versus non-authorized changes...File Integrity Monitoring would be more suited for that..A is correct
upvoted 10 times

Davar39 Highly Voted 3 years, 1 month ago

Selected Answer: C

The question states privacy regulations - which translates to compliance regulations. DLP solutions provide capabilities that can assist you in compliance audits.
upvoted 9 times

zecomeia_007 Most Recent 11 months, 1 week ago

Selected Answer: A

Therefore, automating the use of a hashing algorithm after verified user changes is the most appropriate and efficient method to verify data integrity in this scenario
upvoted 2 times

zhuzhu123 1 year, 7 months ago

Would go for A:
DLP is mainly used to prevent data leakage:
"The value of a DLP system resides in the level of precision with which it can locate and prevent the leakage of sensitive data."
From the official cert guide for 002
Answer A also includes a verification of the user.
upvoted 3 times

32d799a 1 year, 7 months ago

Selected Answer: C

Data Loss Prevention (DLP) products are designed to monitor, detect, and prevent unauthorized access and changes to sensitive data. They can be configured to identify and alert on any unauthorized modifications to data, ensuring that any alterations can be investigated promptly.
upvoted 1 times

SimonR2 1 year, 11 months ago

C

Data Loss Prevention (DLP) products are designed to monitor and protect sensitive data from being lost, leaked, or altered in an unauthorized manner. DLP solutions can help organizations identify and prevent data breaches, unauthorized modifications, and data exfiltration.

In this context, using a DLP product would be a suitable approach because it allows continuous monitoring of the data sets for any unauthorized changes. The DLP solution can be configured to detect and alert on suspicious activities, ensuring that any unauthorized modifications trigger an immediate response.
upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 11 months ago

C for me

The Official CompTIA CySA+ about DLP said

Document matching—A whole document can be matched using a fingerprint, but it is quite easy to modify a file so that it no longer matches the fingerprint. To compensate for this risk, partial document matching creates a series of hashes for overlapping parts of the document. These hashes can match content that has been copied from the document or used in a different order in another file (458 page)

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: C

A Data Loss Prevention (DLP) product is designed to monitor and protect sensitive data from unauthorized access, use, or disclosure. It can help detect and prevent unauthorized edits and changes to user data by monitoring data sets for any suspicious activity. By implementing a DLP solution, the company can enforce policies and rules to prevent unauthorized alterations without the user's consent.

upvoted 1 times

🗨️ 👤 **bolubeyi** 2 years, 2 months ago

using a DLP product to monitor the data sets for unauthorized edits and changes may be useful for detecting unauthorized access to the data, but it does not address the issue of data integrity. A is the correct answer

upvoted 2 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: A

Using a Data Loss Prevention (DLP) product to monitor the data sets for unauthorized edits and changes (Option C) would not be an appropriate course of action for verifying that a user's data is not altered without their consent. DLP products can help protect sensitive data from loss or theft, but they do not provide a means to verify the integrity of the data or detect unauthorized changes.

upvoted 5 times

🗨️ 👤 **Stiobhan** 2 years, 3 months ago

Selected Answer: A

So the give away here is "verify that a user's data is not altered without the user's consent" Answer A will not allow changes unless user has been verified (logged on and authenticated), answer C will only monitor the situation and report if a change is made, that is not what the CISO is requesting!

upvoted 4 times

🗨️ 👤 **IanRogerStewart** 2 years, 4 months ago

Selected Answer: A

The idea of using DLP to monitor data at rest on a server is just nonsensical. This Q has nothing to do with Confidentiality (what DLP is about), it is about Integrity. Hashing is 100% your solution.

upvoted 3 times

🗨️ 👤 **JohnMangley** 2 years, 4 months ago

Selected Answer: A

What can DLP Prevent?

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations.

Correct me if I am wrong, but so far as the info online shows, DLP does not really compare the before and after data for alteration checks.

[https://www.imperva.com/learn/data-security/data-loss-prevention-](https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/#~:text=Data%20Loss%20Prevention%20(DLP)%20is,data%20and%20comply%20with%20regulations.)

[dlp/#~:text=Data%20Loss%20Prevention%20\(DLP\)%20is,data%20and%20comply%20with%20regulations.](https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/#~:text=Data%20Loss%20Prevention%20(DLP)%20is,data%20and%20comply%20with%20regulations.)

upvoted 3 times

🗨️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: C

I going with C because it seems more sysmatic. suit for comptia.

upvoted 1 times

🗨️ 👤 **david124** 2 years, 5 months ago

Selected Answer: A

Chat GPT says A

upvoted 4 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

It also says C

upvoted 3 times

🗨️ 👤 **xyz47** 2 years, 5 months ago

This is tough question due to the fact is not precisely asked.

I think the correct answer is A. Why?

The CISO tasked a security analyst to find a control function to 'verify' that a user's data is not altered without the user's consent.

DLP is more about preventing alteration, and it is more about preventing data leak or exfiltration outside of the company. It is frequently connected to sensitive data.

If the question is only about verification answer A should be enough.

Also I am not sure how good DLP is with tracking the file changes especially changes performed by the authorized users from inside of the company's network.

I guess if system administrator makes a change this change is also authorized, but still it was done without user's consent. I guess DLP won't do anything about such a change.

upvoted 2 times

🗨️ 👤 **mrodmy** 2 years, 6 months ago

Selected Answer: C

<https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/>

upvoted 1 times

An employee was found to have performed fraudulent activities. The employee was dismissed, and the employee's laptop was sent to the IT service desk to undergo a data sanitization procedure. However, the security analyst responsible for the investigation wants to avoid data sanitization. Which of the following can the security analyst use to justify the request?

- A. GDPR
- B. Data correlation procedure
- C. Evidence retention
- D. Data retention

Suggested Answer: C

Community vote distribution

C (77%)

D (23%)

🗳️ 👤 **EVE12** Highly Voted 🍌 2 years, 9 months ago

Selected Answer: C

Evidence Retention

If the incident involved a security breach and the incident response process gathered evidence to prove an illegal act or a violation of policy, the evidence must be stored securely until it is presented in court or is used to confront the violating employee. Computer investigations require different procedures than regular investigations because the time frame for the computer investigator is compressed, and an expert might be required to assist in the investigation. Also, computer information is intangible and often requires extra care to ensure that the data is retained in its original format. Finally, the evidence in a computer crime is difficult to gather.

upvoted 9 times

🗳️ 👤 **fuzzyguzzy** Most Recent ⌚ 6 months, 4 weeks ago

Selected Answer: C

C: Makes sense given the context. "Evidence Retention" is in the exam objectives in the context of incident response.

upvoted 1 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

Evidence retention would be the most appropriate justification for the security analyst to request avoiding data sanitization

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. This is basically the same as putting data on Legal Hold.

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years, 3 months ago

Evidence Retention = Legal Hold

upvoted 4 times

🗳️ 👤 **MrRobotJ** 2 years, 7 months ago

Selected Answer: C

most likely C

upvoted 1 times

🗳️ 👤 **TeyMe** 2 years, 7 months ago

The option should be "Legal Hold" not Evidence retention..

upvoted 3 times

🗳️ 👤 **MortG7** 2 years, 8 months ago

Selected Answer: D

I am leaning towards D. How do we know that the evidence came from the laptop which resulted in fraudulent activity. The evidence could have come from a DLP, Firewall, proxy server...IMHO it is D.

upvoted 1 times

🗨️ 👤 **TheStudiosPeepz** 2 years, 8 months ago

"How do we know that the evidence came from the laptop which resulted in fraudulent activity"

You would still want to check his computer for evidence of fraud regardless, no?

He committed a crime and its likely that the org wants to pursue him legally. If they wipe the drive they have no evidence to provide to legal counsel. It's no longer just "data" it is now also evidence.

upvoted 1 times

🗨️ 👤 **MortG7** 2 years, 7 months ago

evidence? "...An employee was found to have performed fraudulent activities.." he has been found guilty and dismissed. They already have proof, and there is evidence already..thus the dismissal.

upvoted 1 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: C

Evidence retention

upvoted 1 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: C

Evidence retention is the process of keeping any evidence of an incident for the entire duration of the legal process

upvoted 2 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: D

I would have to go with D because I dont think ive ever heard the term "evidence retention" being used in any courses. What do you guys think?

upvoted 4 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Exam objective 4.2 under post-incident activities has specially has "Evidence retention"

upvoted 2 times

🗨️ 👤 **ititititcomcocomcom** 2 years, 9 months ago

evidence retention is in exam obj 4.2

upvoted 1 times

As part of an intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several domains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for intelligence gathering?

- A. Update the whitelist.
- B. Develop a malware signature.
- C. Sinkhole the domains.
- D. Update the blacklist.

Suggested Answer: D

Community vote distribution

C (100%)

🗳️ **amateurguy** Highly Voted 2 years, 9 months ago

Selected Answer: C

Sinkhole the domains would be best for INTELLIGENCE GATHERING but updating the blacklist would be the best way to prevent future issues. So i would assume Sinkhole is what they want.

upvoted 10 times

🗳️ **2Fish** 2 years, 3 months ago

Agree. It took me a minute, but the verbiage INTELLIGENCE GATHERING leads me to think C.

upvoted 2 times

🗳️ **R00ted** Highly Voted 2 years, 9 months ago

Selected Answer: C

"intelligence gathering"

upvoted 6 times

🗳️ **RobV** Most Recent 1 year, 6 months ago

Selected Answer: C

C. Sinkhole the domains.

In this scenario, sinkholing the domains would be the most appropriate configuration change for intelligence gathering. Sinkholing involves redirecting traffic from malicious domains to a controlled infrastructure, allowing security professionals to monitor and analyze the malicious activity without exposing the targeted individuals to actual threats. This helps in gathering intelligence on the tactics, techniques, and procedures (TTPs) of the potential threat actors.

The other options, such as updating the whitelist, developing a malware signature, or updating the blacklist, are more focused on reactive measures and may not be as effective in gathering intelligence on the threat actors and their activities. Sinkholing, on the other hand, provides an opportunity for proactive intelligence gathering while protecting the targeted individuals from potential harm.

upvoted 1 times

🗳️ **novolyus** 1 year, 7 months ago

Selected Answer: C

Like many others said "INTELLIGENCE GATHERING" are the keywords to choose C

upvoted 1 times

🗳️ **Hershey2025** 1 year, 10 months ago

D is the correct answer... why sinkhole? You are not asked to investigate it further...it was already investigated by a trusted source.

upvoted 2 times

🗳️ **CyberNoob404** 2 years, 5 months ago

Selected Answer: C

If you are trying to gather intelligence, you would Sinkhole. (C)

upvoted 2 times

🗳️ **f3lix** 2 years, 5 months ago

Selected Answer: C

Just read this not too long - Sinkholing it is: [C]

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

Selected Answer: C

"A sinkhole is a server designed to capture malicious traffic and prevent control of infected computers by the criminals who infected them"

<https://www.wired.com/story/what-is-sinkholing/>

upvoted 3 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

Key words are "intelligence gathering"

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

D sounds right

upvoted 1 times

🗨️ 👤 **TheStudiosPeepz** 2 years, 8 months ago

What did you score on the Cysa+ ?

upvoted 2 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

she failed third time because of this question :D

upvoted 2 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

this is the reason you failed three times, right :D

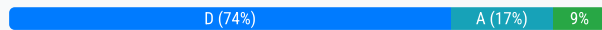
upvoted 2 times

A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentiality protection. Which of the following is the BEST technical security control to mitigate this risk?

- A. Switch to RADIUS technology.
- B. Switch to TACACS+ technology.
- C. Switch to MAC filtering.
- D. Switch to the WPA2 protocol.

Suggested Answer: D

Community vote distribution



🗳️ **nonjabusiness** Highly Voted 2 years, 9 months ago

Selected Answer: D

This is my train of thought for this question

- A- Radius only encrypts passwords
- B- TACAS+ is Cisco proprietary, this question doesn't say they're using Cisco products
- C- MAC address could be spoofed to gain access to the network
- D- WPA2 is difficult to crack

Between C and D, D provides the most security; cracking a WPA2 handshake would require an extremely beefy system and take a long time. On the other hand, MAC spoofing is very easy to accomplish

upvoted 10 times

🗳️ **A_Shadows_Soul** 2 years, 8 months ago

WPA2 is not difficult to crack unless its an enterprise solution. D is still the correct answer tho

upvoted 3 times

🗳️ **uday1985** Most Recent 2 years, 1 month ago

WPA2 is secure ? anymore?

upvoted 1 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: D

Going with D, we are talking confidentiality.

upvoted 2 times

🗳️ **absabs** 2 years, 4 months ago

I going to B. Tacas encrypt all data, but radius encrypt only password !!!

<https://www.geeksforgeeks.org/difference-between-tacacs-and-radius/>

upvoted 1 times

🗳️ **Stiobhan** 2 years, 5 months ago

It has got to be A, this would give most protection. Chances are that WPA2 is the high risk element!

upvoted 1 times

🗳️ **david124** 2 years, 5 months ago

Selected Answer: D

chat GPT says D

upvoted 3 times

🗳️ **Maniact165** 2 years, 7 months ago

Selected Answer: A

please correct me if I am wrong, but wouldn't implementing RADIUS ensure only those with AD accounts could access the WiFi hence Confidentiality is improved?

upvoted 2 times

🗨️ 👤 **TeyMe** 2 years, 8 months ago

Selected Answer: A

Weak WPA/WPA2 passphrases can be recovered via brute force password cracking
enterprise networks should use RADIUS authentication, which is not susceptible to this attack.
upvoted 2 times

🗨️ 👤 **TeyMe** 2 years, 8 months ago

Scrap that, changed to D correct answer
upvoted 2 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: D

This is terrible question. I would say best answer is D as well.
upvoted 1 times

🗨️ 👤 **Merc16** 2 years, 9 months ago

Selected Answer: D

I think D is the correct answer. Radius is used in conjunction with NAC for user authentication. We still need to think of how to encrypt users' data.
upvoted 1 times

🗨️ 👤 **Fastytop** 2 years, 9 months ago

Selected Answer: B

TACACS (Terminal Access Controller Access Control System) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS.
upvoted 2 times

🗨️ 👤 **dnc1981** 2 years, 8 months ago

Has nothing to do with confidentiality though
upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

I thought it would be tacacs because it provides remote authentication for network access which would protect data. But maybe D is correct since im unsure, we need an expert here.
upvoted 1 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

D is the only one specific to Wireless Security
upvoted 2 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

In an 802.1x system, the device attempting to join the network runs a NAC supplicant, which communicates with an authenticator on the network switch or wireless access point. The authenticator uses RADIUS to communicate with an authentication server.
upvoted 1 times

Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?

- A. H-ISAC
- B. Dental forums
- C. Open threat exchange
- D. Dark web chatter

Suggested Answer: A

Reference:

<https://h-isac.org/>

Health-ISAC Inc. (H-ISAC, Health Information Sharing and Analysis Center), is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other.

Health-ISAC is a trusted community of critical infrastructure owners and operators within the Healthcare and Public Health sector (HPH). The community is primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material. Sharing can occur via machine to machine or human to human. Health-ISAC also fosters the building of relationships and networking through a number of educational events in order to facilitate trust. Working groups and committees focus on topics and activities of importance to the sector. Shared Services offer enhanced services to leverage the Health-ISAC community for the benefit of all.

Community vote distribution

A (100%)

 **sasquatch111** Highly Voted 3 years, 5 months ago

most idiotic question, are we memorize every healthcare as well, A is correct but shame on comptia if this is a real question
upvoted 7 times

 **Merc16** Most Recent 2 years, 9 months ago

Selected Answer: A


I choose A because of the label ISAC. But to be far, H-ISAC is mentioned within Comptia notes as follows

Healthcare

Healthcare providers are targeted by criminals seeking blackmail and ransom opportunities by compromising patient data records or by interfering with medical devices. The Health ISAC is at h-isac.org.- Healthcare

Healthcare providers are targeted by criminals seeking blackmail and ransom opportunities by compromising patient data records or by interfering with medical devices. The Health ISAC is at h-isac.org.

upvoted 2 times

 **2Fish** 2 years, 3 months ago

Concur. ISACs are a great source for threat intel.

upvoted 1 times

 **amateurguy** 2 years, 9 months ago

Selected Answer: A

A is correct.

upvoted 1 times

 **Laudy** 2 years, 9 months ago

Wasn't sure what A was off the jump, but I knew it wasn't B, C, or D. lol

upvoted 2 times

 **miabe** 2 years, 11 months ago

Selected Answer: A

looks good to me

upvoted 1 times

 **f3lix** 3 years, 1 month ago

What country does this Health Care Intel Sharing community covers? This is a really dumb question if I'm being honest, will someone from a totally different country have to cram this?



upvoted 4 times

  **dommain** 3 years, 5 months ago

Selected Answer: A

This is correct.

upvoted 2 times

  **Remilia** 3 years, 6 months ago

I concur.

upvoted 2 times

Which of the following incident response components can identify who is the liaison between multiple lines of business and the public?

- A. Red-team analysis
- B. Escalation process and procedures
- C. Triage and analysis
- D. Communications plan

Suggested Answer: D

Community vote distribution

D (89%)

11%

  **Davar39**  3 years ago

Selected Answer: D



CySA+ study guide v2 (sybex) pages 391-392.

upvoted 6 times

  **2Fish** 2 years, 3 months ago

Agree, the comm plan should have all the listed contacts.

upvoted 2 times

  **MortG7**  2 years, 8 months ago

Looks like examtopics has dropped comptia all together



upvoted 2 times

  **miabe** 2 years, 11 months ago

Selected Answer: D



looks good to me

upvoted 1 times

  **blehbleh** 2 years, 11 months ago

Hello everyone, I see most of us have agreed but I believe answer D is correct. "One of the critical components of your incident response plan is a communications plan that covers both internal and external communications." Good luck everyone!

upvoted 3 times

  **RoPsur** 3 years, 3 months ago

Selected Answer: B

B because it includes Communications plan if the incident were to require it.



upvoted 2 times

  **wazowski1321** 3 years, 3 months ago

Selected Answer: D

d is right

upvoted 1 times

  **bzpunk** 3 years, 4 months ago

Selected Answer: D

"Once a security incident has occurred, communication is key to carrying out the plans your organization has developed for such cases. Having a set process for escalating communication will facilitate the knowledge and teamwork needed to resolve the incident and bring the organization's operations back to normal. The CSIRT should have a single point-of-contact to handle requests and questions from stakeholders outside the incident response team, including both executives within the company and contacts external to the company."


upvoted 4 times

  **cysa_1127** 3 years, 4 months ago

Selected Answer: D

going with d

upvoted 1 times

  **carlo479** 3 years, 4 months ago

Selected Answer: D

D all day long. smh

upvoted 3 times

🗨️ 👤 **XYZ_40** 3 years, 4 months ago

D is the answer

upvoted 2 times

🗨️ 👤 **Hawkeyexp** 3 years, 5 months ago

Its communication plan. page 266 comptia CYSA official study guide

upvoted 2 times

🗨️ 👤 **Charlieb123** 3 years, 5 months ago

B. Communications Plan - why would you escalate to the public??

upvoted 3 times

🗨️ 👤 **Charlieb123** 3 years, 4 months ago

Correction, I meant D.

upvoted 2 times

🗨️ 👤 **Bat_man_5** 3 years, 5 months ago

Why is the answer not "Communications plan"???

upvoted 2 times

Which of the following threat classifications would MOST likely use polymorphic code?

- A. Known threat
- B. Zero-day threat
- C. Unknown threat
- D. Advanced persistent threat

Suggested Answer: B

Reference:

<https://www.thesslstore.com/blog/polymorphic-malware-and-metamorphic-malware-what-you-need-to-know/>

Community vote distribution



blehbleh Highly Voted 2 years, 10 months ago

The answer should be A. According to the Compita study guide there are only two threat classifications which are known and unknown. APT is a threat actor type and Zero day is a type of malware or threat but not a threat classification. Hope this helps.

upvoted 18 times

2Fish 2 years, 3 months ago

agree. A is the best answer here.

upvoted 1 times

adrianlacatus Highly Voted 3 years, 4 months ago

Selected Answer: A

Polymorphic malware is a type of malware that constantly changes its identifiable features in order to evade detection, therefore its a known threat. While APTs may use polymorphic code, it does not specify anywhere about the characteristics of APTs - coordination, resources, persistence, capability or intent.

upvoted 10 times

akinbas 2 years, 11 months ago

agree with A

upvoted 1 times

SolventCourseisSCAM 2 years, 7 months ago

agree on it. solvent course is scam as you predict

upvoted 1 times

fuzzyguzzy Most Recent 6 months, 4 weeks ago

Selected Answer: D

D. Advanced persistent threat

According to my study guide, there's more than two Threat Classifications and APT is one of them.

upvoted 1 times

zecomeia_007 11 months ago

Selected Answer: A

Polymorphic code is used to evade detection by changing its appearance while maintaining its malicious behavior. Advanced persistent threats (APTs) often employ such sophisticated techniques to remain undetected for extended periods while they target specific organizations or individuals.

upvoted 1 times

anhod1578 1 year, 3 months ago

Selected Answer: B

These are newly discovered vulnerabilities for which no patch or mitigation exists yet. Attackers often exploit zero-days by using sophisticated techniques like polymorphic code to evade detection until security researchers become aware of the threat and develop countermeasures.

upvoted 2 times

skibby16 1 year, 7 months ago

Selected Answer: C

C Unknown Threat here is a good explanation. Definitely a crappy question... <https://www.paloaltonetworks.com/cyberpedia/what-are-unknown-cyberthreats>

upvoted 1 times

🗨️ 👤 **Skywalker89** 1 year, 7 months ago

answer is C:

(reference:CYSA+ certmaster)

Another example of a known unknown is that malware authors can use various obfuscation techniques to circumvent signature-matching. The exact form that such malware will take is unknown, but its likely use and operation within an attack is predictable, at least to some extent.

upvoted 1 times

🗨️ 👤 **kumax** 1 year, 9 months ago

Selected Answer: D

ChatGPT: "Advanced persistent threa" comes first, then "Zero-day".

upvoted 2 times

🗨️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: D

APTs are sophisticated threats that are often targeted at specific organizations. They are designed to avoid detection and evade traditional security measures. Polymorphic code is a type of malware that can change its code each time it is executed. This makes it difficult for antivirus software to detect and block.

upvoted 2 times

🗨️ 👤 **Big_Dre** 1 year, 10 months ago

Selected Answer: A

only 2 types od threat classification (known and unknown)

upvoted 1 times

🗨️ 👤 **Anaser** 2 years, 2 months ago

Selected Answer: B

B. Zero-day threat is the most likely threat classification to use polymorphic code. Polymorphic code is a type of code that can change its structure without changing its functionality, making it difficult for traditional signature-based antivirus systems to detect and block it. Zero-day threats are newly discovered vulnerabilities that have not yet been patched by vendors and are exploited by threat actors to carry out attacks. Since zero-day threats are unknown to security vendors and antivirus systems, attackers may use polymorphic code to evade detection and deliver their payloads.

upvoted 3 times

🗨️ 👤 **justauser** 2 years, 2 months ago

Selected Answer: C

[GPT4] In the context of the CompTIA Security+ exam, polymorphic code can be associated with different types of malware threats. Polymorphic code refers to malicious software that can change its code or behavior to evade detection by antivirus and other security software. Polymorphic malware can be categorized under the following threat classifications:

Known and unknown. Unknown threats or zero-day threats would be the classification MOST likely to use polymorphic code. Polymorphic malware is specifically designed to evade detection and constantly change its code or behavior to avoid signature-based security solutions. This makes it more challenging for security researchers and software to identify and counter unknown polymorphic threats as compared to known ones.

upvoted 2 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: A

Polymorphic code is a technique used by attackers to modify the code of malicious software, such as viruses or trojans, so that it appears different each time it is executed while retaining its original functionality. This technique is often used to evade detection by signature-based antivirus software, which identifies malware based on its signature or pattern.

upvoted 2 times

🗨️ 👤 **khrid4** 2 years, 3 months ago

Selected Answer: C

We know of Polymorphic code concept that it is evading detection by means of changing its signature/appearance while retaining its functionality. As it evades detection, it bypass AV detection making it "Unknown".

Since as everyone pointed out that this asks for threat classification- Known vs Unknown, Jason Dion course from Udemy actually classified "Known Unknowns" as under "Unknown" threat classification.

Known Unknowns - a classification of malware that contains obfuscation techniques to circumvent signature-matching and detection

upvoted 5 times

🗨️ 👤 **boletri** 2 years, 3 months ago

Selected Answer: C

Historically, cybersecurity techniques depended very much on the identification of "static" known threats, such as viruses, rootkits, Trojans, and botnets. It is straightforward to identify and scan for this type of threat with automated software by matching the malicious code to a signature in a database of known malware. Unfortunately, many adversaries now have the capability to develop means of circumventing these security systems.

The sophisticated nature of modern cybersecurity threats means that when classifying threats, it is important to be able to describe and analyze behaviors as well as enumerate known attack signatures. This type of threat classification underpins tools and procedures that can detect unknown threats.

Official CompTia Cysa+ Material
upvoted 2 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Taken directly from comptia CySA 002 exam objectives 1.1

"Threat classification

- Known threat vs. unknown threat
- Zero-day
- Advanced persistent threat"

Surely APT is the most likely to have access to this technology...

upvoted 2 times

🗨️ 👤 **IanRogerStewart** 2 years, 4 months ago

Selected Answer: D

Going with D. APTs have the resources to create polymorphic malware, which traditional actors may not.

upvoted 4 times

🗨️ 👤 **narcosubs** 1 year, 11 months ago

The concept of polymorphic code is to evade detection, as khrid4 mentioned above. And the main goal of APT is persistence, which requires to be undetected.

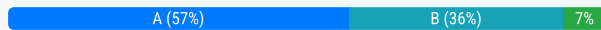
upvoted 4 times

A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to go offline. Which of the following solutions would work BEST prevent to this from happening again?

- A. Change management
- B. Application whitelisting
- C. Asset management
- D. Privilege management

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Dree_Dogg** 1 year, 9 months ago

Selected Answer: B

Change Management doesn't "prevent" it. Whitelisting will absolutely prevent it though.

upvoted 1 times

🗳️ 👤 **Snkrsnaker1** 2 years, 2 months ago

Selected Answer: A

Based on the answers we have to choose from, answer A (Change Management) is the BEST answer. One does not simply just whitelist an application. Even if there is no formal "change management" process, you still have to follow best practices to ensure the application is secure and compliant with your security policy.

upvoted 2 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: A

In this scenario, if the systems administrator had followed a change management process, they would have needed to document and seek approval for the installation of the utility that caused the issue. This would have allowed for a review of the utility and its potential impact on the web server cluster.

upvoted 1 times

🗳️ 👤 **db97** 2 years, 4 months ago

Install a tool = change in the host. So I go for A on this, cuz with a change management control this could be prevented now and in the future as well.

upvoted 3 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree. Change management also incorporates a roll-back plan. In this event, we could roll-back and or recover from and event

upvoted 2 times

🗳️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: A

the only choice

upvoted 1 times

🗳️ 👤 **david124** 2 years, 8 months ago

Selected Answer: A

A it is

upvoted 1 times

🗳️ 👤 **MortG7** 2 years, 8 months ago

Application whitelisting is for authorization..how would that help in the future? The admin already installed it...it is not an authorization issue, it is crappy software issue. Ideally, had "test in a lab/test environment first" been one of the choices, that would be it, but it isn't. Change Management is a crappy answer but sadly the best one.

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years, 9 months ago

I'm going with Change Management.

After doing some research/studying I can see how application whitelisting would work since it is a list of approved applications that can be

downloaded but since it is a critical system that was taken offline and the question is asking you 'prevent' it from happening 'again' I think change management which would require approval to not only install the application but also require testing before hand would be better at preventing this situation from happening again.

upvoted 1 times

🗲️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: A

Change Management

o The process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts

o Each individual component should have a separate document or database record that describes its initial state and subsequent changes

- Configuration information
- Patches installed
- Backup records
- Incident reports/issues

o Change management ensures all changes are planned and controlled to minimize risk of a service disruption

upvoted 2 times

🗲️ 👤 **bigerblue2002** 2 years, 9 months ago

Wouldn't a whitelist be a list of proven applications? If they had that, they wouldn't have used this application at, they would have used one on the list. I think if this had been a blacklist then the answer would be correct as this would be on the list for not using it in the future. If they have a whitelist and this event happens, the whitelist will not change nor help this situation. Blacklist would be a great answer, whitelist is not....in my book anyway. Going with Change Management.

upvoted 2 times

🗲️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: A

I think A is the best answer, because change management is the process of requesting, approval, validating, and logging.

By following this process, the utility would have to be tested to validate it doesn't cause issues before and after installation. Also in this scenario, logging would provide a way to identify the cause and restore the cluster to it's previous state

upvoted 2 times

🗲️ 👤 **Fastyt0p** 2 years, 9 months ago

Selected Answer: B

I think Application whitelisting will be better in this case.

upvoted 1 times

🗲️ 👤 **EVE12** 2 years, 9 months ago

Change Management

All networks evolve, grow, and change over time. Companies and their processes also evolve and change, which is a good thing. But infrastructure change must be managed in a structured way so as to maintain a common sense of purpose about the changes. By following recommended steps in a formal change management process, change can be prevented from becoming the tail that wags the dog. The following are guidelines to include as a part of any change management policy:

All changes should be formally requested.

Each request should be analyzed to ensure it supports all goals and policies.

Prior to formal approval, all costs and effects of the methods of implementation should be reviewed.

After they're approved, the change steps should be developed.

During implementation, incremental testing should occur, relying on a predetermined fallback strategy if necessary.

Complete documentation should be produced and submitted with a formal report to management.

<https://learning.oreilly.com/library/view/comptia-cybersecurity-analyst/9780136747000/ch08.xhtml#ch08lev1sec8>

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

Wouldnt application whitelist be better? as it can make sure the application is safe / approved before we deploy it so that it doesnt crash the server?

upvoted 3 times

🗨️ 👤 **david124** 2 years, 9 months ago

Selected Answer: C

Doesn't Utility = Application = Whitelisting as a solution?

it's weird that change management is the solution tbh.

upvoted 1 times

🗨️ 👤 **david124** 2 years, 9 months ago

sorry answer is B

upvoted 1 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

A sounds right

upvoted 2 times

An analyst must review a new cloud-based SIEM solution. Which of the following should the analyst do FIRST prior to discussing the company's needs?

- A. Check industry news feeds for product reviews.
- B. Ensure a current non-disclosure agreement is on file.
- C. Perform a vulnerability scan against a test instance.
- D. Download the product security white paper.

Suggested Answer: B

Community vote distribution

D (49%)

B (43%)

8%

🗳️ 👤 **[Removed]** Highly Voted 2 years, 3 months ago

Selected Answer: D

It is D and I will explain why:

Part of the question is "analyst do FIRST prior to discussing company's needs?" This eliminates an NDA as we are not discussing our requirements. The only other option that makes sense and is commonly used, is a whitepaper.

A white paper is independent audits, testaments and so on regarding products/services and underlying security, architecture, data governance and so on.

So in summary, you would certainly review the white paper for a cloud SIEM you're interested in, so see if you believe it meets your companies needs. Prior to discussing with the Cloud provider, which could require an NDA.

upvoted 13 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

I'm feeling D as well. I am reading this as we are "reviewing" and new product, not a "we are or have purchased this product" and need an NDA. The NDA, if needed should have happened during the procurement process. So at the review phase, I would be getting white papers.

upvoted 2 times

🗳️ 👤 **forklord72** Highly Voted 2 years, 8 months ago

Selected Answer: B

Keep in mind, the question is asking what to do "FIRST prior to discussing the company's needs?". From this alone, I am assuming the security white papers have already been reviewed and they are about to discuss company needs. Before discussing anything confidential, an NDA is a must. CompTIA wants the world to burn for writing these questions.

upvoted 8 times

🗳️ 👤 **forklord72** 2 years, 8 months ago

This question is haunting me admittedly, i'm starting to believe the answer CompTIA is looking for is D because of the question saying the analyst is reviewing a "new" solution. Ugg

upvoted 3 times

🗳️ 👤 **2Fish** 2 years, 2 months ago

and here I am flopping back to B because NDA is an objective in this CYSA course. geezuz

upvoted 3 times

🗳️ 👤 **zecomeia_007** Most Recent 11 months ago

Selected Answer: D

When reviewing a new cloud-based Security Information and Event Management (SIEM) solution, the analyst should FIRST consider downloading the product security white paper.

upvoted 1 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

B. Ensure a current non-disclosure agreement is on file.

Before delving into discussions about the company's specific needs and potentially sensitive information, it's important to have a non-disclosure agreement (NDA) in place. This agreement helps protect the confidentiality of the information exchanged between the analyst and the provider of the cloud-based SIEM solution. Once the NDA is in place, the analyst can proceed to gather information about the solution's security features and capabilities to better address the company's specific requirements.

upvoted 2 times

🗨️ 👤 **novolyus** 1 year, 7 months ago

Selected Answer: B

NDA is a must, no doubt on this one.

upvoted 1 times

🗨️ 👤 **Sleezyglizzy** 1 year, 11 months ago

B non disc.

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: B

D. Ensure a current non-disclosure agreement is on file.

Before discussing the company's needs and any specific details regarding the cloud-based SIEM solution, it is important for the analyst to ensure that a current non-disclosure agreement (NDA) is on file. This step is crucial to protect the confidentiality of any sensitive information that may be shared during the review process.

upvoted 2 times

🗨️ 👤 **kyky** 2 years ago

By having an NDA in place, the analyst can have open and candid discussions with the company about their needs, without the risk of confidential information being shared or misused. It establishes a legal framework that safeguards both parties' interests and helps create a trustworthy environment for sharing sensitive information.

Once the NDA is in place, the analyst can proceed with further actions like performing a vulnerability scan, downloading the product security white paper, and checking industry news feeds for product reviews. These activities can provide additional insights and information about the cloud-based SIEM solution, helping the analyst make an informed evaluation.

upvoted 1 times

🗨️ 👤 **nomad421** 2 years, 1 month ago

I would choose B because I know Comptia. However, you don't need to have them sign an NDA unless you are sharing data. Letting them know what you want in a product is not sharing data.

upvoted 1 times

🗨️ 👤 **nedeajob12** 2 years, 2 months ago

Selected Answer: D

I think the answer is D, the question asks what we should do FIRST. Why bring in an NDA if we dont even know if this product will do what we want it to do? Dont feel obligated ot agree with me.

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: B

When reviewing a new cloud-based SIEM solution, the analyst may be exposed to sensitive or confidential information about the product, such as its architecture, features, and capabilities. Therefore, it is important for the analyst to ensure that a current NDA is on file before discussing the product with the vendor or any other parties.

upvoted 2 times

🗨️ 👤 **Ryukendo** 2 years, 7 months ago

Selected Answer: A

why do you need NDA if you are discussing your own company needs with YOUR company?
and Nope there is no such thing as product security white paper for SIEMs, etc.

the only option that makes sense is A, it wouldn't kill you to take look at reviews of the product.

upvoted 3 times

🗨️ 👤 **brvndvnwolf** 2 years, 6 months ago

It does not matter, you can still be a part of a company and still be required to sign an NDA.

upvoted 3 times

🗲️ 👤 **david124** 2 years, 8 months ago

Selected Answer: B

B IT is

upvoted 2 times

🗲️ 👤 **CW4901** 2 years, 8 months ago

are we assuming that the analyst has already downloaded the white paper and is ready to discuss it with the company?

upvoted 1 times

🗲️ 👤 **A_core** 2 years, 8 months ago

Ans: B

product was identified, hence its been reviewed. Next is to have NDA before providing company info.

upvoted 2 times

🗲️ 👤 **MortG7** 2 years, 8 months ago

Why the heck would I check NDA if I don't know what the product does/features and whether or not it fits my needs and satisfies my requirements...answer is D

upvoted 2 times

🗲️ 👤 **PTcruiser** 2 years, 9 months ago

Selected Answer: B

Prior to discussing the companies needs

upvoted 4 times

🗲️ 👤 **haykaybam** 2 years, 9 months ago

Selected Answer: D

Prior to discussing the company's needs - Download the product security white paper to find out if the product is useful for your company. I go with option D.

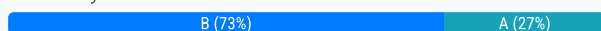
upvoted 3 times

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment. Which of the following is the BEST solution?

- A. Virtualize the system and decommission the physical machine.
- B. Remove it from the network and require air gapping.
- C. Implement privileged access management for identity access.
- D. Implement MFA on the specific system.

Suggested Answer: B

Community vote distribution



🗳️ 👤 **anhod1578** 1 year, 3 months ago

Selected Answer: B

Since the system CANNOT be updated and is considered a potential security risk, physically isolating it (air gapping) from the rest of the network significantly reduces the attack surface and prevents it from being compromised or used as a launching point for attacks against other systems.

upvoted 3 times

🗳️ 👤 **skibby16** 1 year, 6 months ago

Selected Answer: A

A virtualized system is a system that runs on a software layer called a hypervisor that emulates the hardware resources of a physical machine. A virtualized system can have its own operating system, applications, and data that are isolated from other virtualized systems or the host machine. A virtualized system can be a solution for a small organization that has proprietary software that is used internally but cannot be updated with the rest of the environment. By virtualizing the system and decommissioning the physical machine, the organization can achieve several benefits, such as:

Reducing hardware costs and maintenance

Improving performance and scalability

Enhancing security and compliance

Simplifying backup and recovery

Enabling portability and compatibility

upvoted 1 times

🗳️ 👤 **novolyus** 1 year, 7 months ago

Selected Answer: A

Vote for A and here is why.

I understand that the organization has a proprietary software, they want to update this software but while the system where it relies has not been properly maintained and it cannot be upgraded accordingly. So, virtualize the system and install there the software.

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. These questions are terrible. B is the best answer I can see here as it does not specify there is a hardware issue. This appears to be a software update issue.

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years, 4 months ago

Selected Answer: A

The system has not been well maintained. Meaning the software on the system is fine. So virtualization of the system solves the issue.

A

upvoted 1 times

🗳️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: A

Everything i look i see answer is A.

i think say "remove it" in B, it is wrong. Because this software is proprietary. Rather than remove, virtualize. I going to A for a long research. If i am wrong, discuss with me?

upvoted 1 times

🗨️ 👤 **TKW36** 2 years, 5 months ago

Selected Answer: B

I believe it is B. This isn't a hardware vulnerability, it's a SOFTWARE vulnerability. Decommissioning the hardware wouldn't remove the vulnerability. Moving the software to a virtualized environment also wouldn't remove the vulnerability. Air gapping is not the BEST answer, but it's the best on available here..

upvoted 4 times

🗨️ 👤 **lolacryptonite** 1 year, 11 months ago

where does it say software vulnerability?

upvoted 2 times

🗨️ 👤 **Kickuh06** 1 year, 11 months ago

The proprietary software on the system that cant be updated.

upvoted 2 times

🗨️ 👤 **david124** 2 years, 8 months ago

Selected Answer: B

B it is

upvoted 1 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

You know, sometimes there is no BEST answer...although B sounds good, but airgapping means it cannot communicate with any network resources. It becomes a stand alone app..oh hell..B it is.

upvoted 4 times

🗨️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: B

B is the best answer

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is the best answer.

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

agree B

upvoted 2 times

🗨️ 👤 **cyberseckid** 2 years, 9 months ago

just wanted to say thanks for your efforts and hope you pass

upvoted 4 times

A SIEM analyst receives an alert containing the following URL: `http://companywebsite.com/displayPicture?filename=../../../../etc/passwd`
Which of the following BEST describes the attack?

- A. Password spraying
- B. Buffer overflow
- C. Insecure object access
- D. Directory traversal

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ **MetaHack** 1 year, 10 months ago

We all know it's D....

upvoted 2 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: D

D. classic DIR traversal `../../../../`

upvoted 1 times

🗳️ **david124** 2 years, 8 months ago

Selected Answer: D

D it is

upvoted 1 times

🗳️ **R00ted** 2 years, 9 months ago

Selected Answer: D

D is the best answer

upvoted 1 times

🗳️ **Merc16** 2 years, 9 months ago

Selected Answer: D

agreed

upvoted 1 times

🗳️ **DaroKa** 2 years, 9 months ago

Selected Answer: D

`../../../../` = traversal

upvoted 3 times

🗳️ **amateurguy** 2 years, 9 months ago

Selected Answer: D

`../` is a directory traversal.

upvoted 4 times

🗳️ **Laudy** 2 years, 9 months ago

agree D

upvoted 2 times

Which of the following is the BEST way to gather patch information on a specific server?

- A. Event Viewer
- B. Custom script
- C. SCAP software
- D. CI/CD

Suggested Answer: C

Reference:

<https://www.open-scap.org/features/standards>

A green banner with a white square containing a magnifying glass icon with a checkmark inside. To the right of the icon, the text reads: "SCAP Standard", "Security Content Automation Protocol (SCAP) is a multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement.", and "OpenSCAP has received a NIST certification for its support of SCAP 1.2." A "more" button is in the bottom right corner.

SCAP Standard

Security Content Automation Protocol (SCAP) is a multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement.

OpenSCAP has received a **NIST** certification for its support of SCAP 1.2.

[more](#)

Community vote distribution



🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. Agree with the answer given.

upvoted 2 times

🗳️ 👤 **MMK777** 2 years, 5 months ago

Does SCAP gather patch information?

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

It can.. an example of SCAP software is OpenSCAP and Nessus.

upvoted 1 times

🗳️ 👤 **f3lix** 2 years, 5 months ago

Selected Answer: C

Valid - SCAP software is correct //C

upvoted 1 times

🗳️ 👤 **EVE12** 2 years, 9 months ago

SCAP Standard

Security Content Automation Protocol (SCAP) is a multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement.

upvoted 2 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

C is the way



upvoted 1 times

🗳️ 👤 **Laudy** 2 years, 9 months ago

Absolutely C.

The tool was literally developed for this very pupose. lol.

upvoted 3 times

  **miabe** 2 years, 11 months ago

Selected Answer: C

looks good to me

upvoted 2 times

A security analyst reviews SIEM logs and discovers the following error event:

ERROR Event ID 4

The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server DBASVRR4\$. The target name used was GC/PDC1DC.Domain57/Administrator. This indicates that the target server failed to decrypt the ticket provided by the client. Check if there are identically named server accounts in these two domains, or use the fully qualified name to identify the server.

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

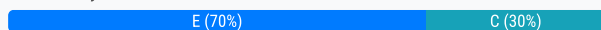
- A. Proxy server
- B. SQL server
- C. Windows domain controller
- D. WAF appliance
- E. DNS server

Suggested Answer: C

Reference:

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-client-krb-ap-err-modified-error>

Community vote distribution



irxkh333 Highly Voted 3 years, 3 months ago

Selected Answer: E

I first picked C, but see that E is correct. Also found this:

Duplicate DNS entries

Most of the configurations gives the KRB_AP_ERR_MODIFIED error because of old DNS entries on your DNS server are not removed. Simply remove these so you only have one IP address per server and one server per IP address (use the sort on the DNS Manager to find duplicates). Also check the reverse lookup zone as the Kerberos use this lookup to make the server-match. And remember the replication delay for other DNS servers and the DNS-timeout on clients before testing – better wait a couple of minutes (or up to 30 min. for auto-repl.)

Source: https://jespermchristensen.wordpress.com/2008/06/12/troubleshooting-the-kerberos-error-krb_ap_err_modified/

upvoted 20 times

2Fish 2 years, 3 months ago

Same here, You are correct, this is E.

upvoted 1 times

Stiobhan Highly Voted 2 years, 3 months ago

Selected Answer: C

The chances are that the Windows Domain Controller is probably acting as the DNS server (as well as other services), so going to go with given answer.

upvoted 5 times

Dee42 Most Recent 1 year, 7 months ago

I think people posting answers from ChatGPT should refrain from voting.

Sometimes, the answers are plain wrong and you're skewing the votes in the wrong direction.

upvoted 4 times

32d799a 1 year, 7 months ago

Selected Answer: C

The error event you provided is related to Kerberos authentication, and it indicates an issue with the decryption of a ticket by the target server. In order to troubleshoot this event, the security analyst should examine the Windows domain controller environment.

upvoted 1 times

kmordalv 1 year, 7 months ago

Selected Answer: C

C for me.

"Check if there are identically named server accounts in these two domains"

The error message specifically mentions a Kerberos error. The target server (DBASVRR4\$) is likely a server in a Windows domain, and issues with Kerberos authentication are often related to problems with domain controllers. This could be due to issues with the domain controller's ability to authenticate and decrypt the Kerberos ticket. In order to know if there is a duplicity of names in the domain, you should first check the DC (Windows Domain Controller)

upvoted 1 times

🗨️ 👤 **LukaszL** 2 years, 2 months ago

Selected Answer: C

ChatGPT convinced me. I have checked because I also chosen C at first:

C. Windows domain controller.

The error message in the SIEM log indicates that there is an issue with Kerberos authentication, specifically that the target server failed to decrypt the ticket provided by the client. This suggests an authentication issue between the client and the server, and the event ID (4) is typically associated with Kerberos errors.

The target name in the error message also indicates that it is related to a Windows domain controller (DC), which is responsible for authenticating users and computers in a Windows domain. Therefore, the security analyst needs to examine the Windows domain controller to continue troubleshooting the event.

upvoted 2 times

🗨️ 👤 **jade290** 1 year, 10 months ago

Okay, but when we look up this error, it makes no mention of the Domain Controller however it does specifically tell us to check the DNS record.

"Verify that each cluster node has been set up with correct DNS settings."

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-client-krb-ap-err-modified-error>

upvoted 1 times

🗨️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: E

"The kerberos client received a KRB_AP_ERR_MODIFIED error from the server host/myserver.domain.com. This indicates that the password used to encrypt the kerberos service ticket is different than that on the target server. Commonly, this is due to identically named machine accounts in the target realm (domain.com), and the client realm. Please contact your system administrator."

Cause

During access to the IIS 6 web site that support Windows Integrated Authentication, the following issues may occur:

Mismatch DNS name resolution. The issue is common in an NLB environment that uses multiple IPs or network adapters.

The user doesn't have a Local NTFS access permission.

The Web Site is using Application Pool with a poor permission setting.

upvoted 1 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Selected Answer: E

The error states '... use the fully qualified name' leading me to believe the DNS Server would be the best place to look at, coincidentally the DNS server could be located on a domain controller

upvoted 2 times

🗨️ 👤 **Fastytop** 2 years, 9 months ago

Selected Answer: C

Windows domain controller

upvoted 2 times

🗨️ 👤 **Fastytop** 2 years, 9 months ago

Resolution

To resolve the error issue, consider to implement the following tests:

Verify that the IIS has been set up with correct NTFS settings.

Integrated Windows Authentication (IIS 6.0)

Verify that each cluster node has been set up with correct DNS settings.

Verify that the node has been set up with correct Application Pool settings:

Configuring Application Pool Identity with IIS 6.0 (IIS 6.0)

Verify that internet explorer has been set up with a correct security setting.

All these steps are through the Windows domain controller.

upvoted 2 times

🗲️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: E

E is correct.

upvoted 1 times

🗲️ 👤 **miabe** 2 years, 10 months ago

Selected Answer: E

looks good to me

upvoted 1 times

🗲️ 👤 **Davar39** 3 years, 1 month ago

Given answer is correct :

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-client-krb-ap-err-modified-error>

upvoted 4 times

🗲️ 👤 **thegreatnivram** 3 years, 2 months ago

Selected Answer: E

E is correct "Check if there are duplicated names on the network" clearly points to DNS.

upvoted 2 times

🗲️ 👤 **Sylwekr** 3 years, 3 months ago

D - is O.K.

upvoted 1 times

🗲️ 👤 **Xyz_40** 3 years, 4 months ago

Correct

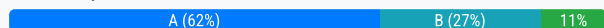
upvoted 3 times

A security analyst needs to develop a brief that will include the latest incidents and the attack phases of the incidents. The goal is to support threat intelligence and identify whether or not the incidents are linked. Which of the following methods would be MOST appropriate to use?

- A. The Cyber Kill Chain
- B. The MITRE ATT&CK framework
- C. An adversary capability model
- D. The Diamond Model of Intrusion Analysis

Suggested Answer: D

Community vote distribution



TKW36 Highly Voted 2 years, 5 months ago

Selected Answer: A

I just took the exam and MITRE ATT&CK wasn't an option so it's A.
upvoted 28 times

jagoichi Highly Voted 2 years, 8 months ago

Selected Answer: A

There are many keys words that point tp this answer being kill chain. (attack phases , incidents are linked)
Chegg has wrong answers all the time
ATT&CK Tactics are unordered and may not all occur in a single intrusion because adversary tactical goals change throughout an operation, whereas the Cyber Kill Chain uses ordered phases to describe high-level adversary objectives
upvoted 16 times

zecomeia_007 Most Recent 11 months ago

Selected Answer: B

Incident Linkage: Comparing ATT&CK patterns across multiple incidents can help determine if they are related, sharing similar tactics or tools.
upvoted 1 times

zecomeia_007 1 year ago

Selected Answer: B

Mitre ATT&CK
upvoted 1 times

RobV 1 year, 6 months ago

Selected Answer: B

B. The MITRE ATT&CK framework

The MITRE ATT&CK framework provides a comprehensive and detailed mapping of tactics, techniques, and procedures (TTPs) used by adversaries during different stages of the attack lifecycle. It covers a wide range of cybersecurity areas and is widely used for threat intelligence analysis. The framework helps security analysts understand the tactics employed by attackers, making it easier to identify patterns, similarities, and potential links between different incidents.

While the Cyber Kill Chain, adversary capability models, and the Diamond Model of Intrusion Analysis are valuable in their own right, the MITRE ATT&CK framework is specifically designed to provide a detailed and structured approach to understanding and analyzing cyber threats.
upvoted 1 times

32d799a 1 year, 7 months ago

Selected Answer: B

The MITRE ATT&CK framework is a knowledge base that describes the actions and tactics commonly observed in cyber threats. It covers a wide range of techniques used by adversaries, including the attack phases.
upvoted 1 times

Gwatto 1 year, 8 months ago

Selected Answer: D

Given Answer is correct.

From Daril Gibson Study guide: The model is intended to help analysts discover more information by highlighting the relationship between elements by following the edges between the events.

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: B

The MITRE ATT&CK framework is a widely recognized and comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs). It provides a standardized taxonomy of cyber threats, organized into various phases and categories, which can be used to analyze and understand the attack lifecycle. The framework covers the entire spectrum of cyber threats, including both traditional and advanced persistent threats (APTs).

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

By using the MITRE ATT&CK framework, the security analyst can map the incidents to the relevant attack phases and identify common TTPs employed by the threat actors. This allows for a standardized and systematic approach to analyzing the incidents, identifying patterns, and determining if there are any links or similarities between them.

While other methods such as the Cyber Kill Chain and the Diamond Model of Intrusion Analysis are also valuable for analyzing cyber incidents, the MITRE ATT&CK framework specifically focuses on the TTPs used by adversaries, making it highly suitable for threat intelligence and identifying potential linkages between incidents.

upvoted 2 times

🗨️ 👤 **DerekM** 2 years, 1 month ago

Selected Answer: B

Wouldn't ATT&CK Tactics link threat actors from past attacks? based off behaviors?

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: B

The Cyber Kill Chain can help identify the stages of a cyber attack and provide insight into the tactics and techniques used by adversaries. However, it may not be the most effective method for identifying whether or not incidents are linked.

The MITRE ATT&CK framework can help identify whether or not incidents are linked. The framework includes information on the tactics and techniques used by adversaries, and organizations can use this information to identify patterns and similarities between different incidents.

To determine whether or not incidents are linked using the Cyber Kill Chain model, an analyst would need to compare the different stages of each incident and look for similarities. Overall, while the Cyber Kill Chain model can provide some insight into the different stages of a cyber attack, the MITRE ATT&CK framework is a more comprehensive resource for identifying and analyzing cyber threats, including determining whether or not incidents are linked.

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 2 months ago

Selected Answer: A

A. Keywords "Attack Phase.."

upvoted 1 times

🗨️ 👤 **doyona** 2 years, 2 months ago

Diamond Model was my first choice.

"The goal is to support threat intelligence..."

The diamond model of intrusion analysis is a valuable tool for any security analysts focused on threat intelligence.

[https://securityboulevard.com/2023/03/diamond-model-of-intrusion-analysis-a-quick-](https://securityboulevard.com/2023/03/diamond-model-of-intrusion-analysis-a-quick-guide/#:~:text=The%20diamond%20model%20of%20intrusion%20analysis%20is%20a%20valuable%20tool,various%20pieces%20of%20threat%20informat)

[guide/#:~:text=The%20diamond%20model%20of%20intrusion%20analysis%20is%20a%20valuable%20tool,various%20pieces%20of%20threat%20informat](https://securityboulevard.com/2023/03/diamond-model-of-intrusion-analysis-a-quick-guide/#:~:text=The%20diamond%20model%20of%20intrusion%20analysis%20is%20a%20valuable%20tool,various%20pieces%20of%20threat%20informat)

upvoted 1 times

🗨️ 👤 **OnA_Mule** 2 years, 3 months ago

Selected Answer: A

The question is asking about the phases of the attack, which would use the Cyber Kill chain. MITRE ATT&CK doesn't use phases and isn't linear analysis and is more focused on the techniques. Diamond also does not use phases and is more focused on connecting the components of the attack.

upvoted 2 times



🗨️ 👤 **boletri** 2 years, 3 months ago

Selected Answer: D

While the Diamond Model is difficult to apply to manual "pen and paper" analysis, it has been used to develop automated threat intelligence analysis engines.

Official Cysa+ Course Material.

upvoted 2 times

  **absabs** 2 years, 4 months ago



Selected Answer: D

I taked from book;

Events can be linked into attack graphs and activity threads, graphed along each vertex, representing the paths an adversary could take (if analyzing an attack in progress) and those that were taken (if analyzing past activity).

i going with D with confidenttaly.

upvoted 5 times

  **absabs** 2 years, 4 months ago

I taked from book;

Events can be linked into attack graphs and activity threads, graphed along each vertex, representing the paths an adversary could take (if analyzing an attack in progress) and those that were taken (if analyzing past activity).

i going with D with confidenttaly.

upvoted 2 times


  **Chrisd636r** 2 years, 4 months ago

The most appropriate method to use in this scenario would be B. The MITRE ATT&CK framework.

The MITRE ATT&CK framework is a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world observations of cyber-attacks. The framework provides a common language and understanding for security teams to discuss and identify the different phases of an attack, helping them to detect and respond to threats effectively. The framework is regularly updated and includes information on the latest incidents and attack techniques.

While the other options listed - A. The Cyber Kill Chain, C. An adversary capability model, and D. The Diamond Model of Intrusion Analysis - are also useful in analyzing and understanding cyber incidents, the MITRE ATT&CK framework is the most appropriate for identifying whether or not incidents are linked, as it includes a vast amount of information on TTPs that can be used to identify patterns and similarities between attacks.

upvoted 1 times

  **knister** 2 years, 5 months ago

Selected Answer: A

Most suitable answer would be A, due to phases.

upvoted 1 times

A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of incident in the future?

- A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
- B. Back up the workstations to facilitate recovery and create a gold image.
- C. Establish a ransomware awareness program and implement secure and verifiable backups.
- D. Virtualize all the endpoints with daily snapshots of the virtual machines.

Suggested Answer: C

Community vote distribution

C (68%)

A (32%)

🗳️ 👤 **TheStudiosPeepz** Highly Voted 2 years, 11 months ago

All of you are wrong. The answer is C. What if the ransomware is transmitted through a plugged in USB? Can't be A. Many people in the discussions for these questions after 200 are wrong. Don't follow the sheep
upvoted 16 times

🗳️ 👤 **absabs** 2 years, 4 months ago

it make sense..
upvoted 3 times

🗳️ 👤 **zhuzhu123** Most Recent 1 year, 7 months ago

Selected Answer: A

An UTM can also include an IPS and endpoint protection, this would cover an USB stick attack and with the IPS prevent the same happening again. Therefore I vote for A
upvoted 1 times

🗳️ 👤 **32d799a** 1 year, 7 months ago

Selected Answer: C

While all the options may contribute to overall security, option C is the most comprehensive and directly addresses the prevention of ransomware incidents
upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C is correct. Users are a huge part of ransomware launches. So User awareness is key. Backups that are verifiable and can actually be restored is the biggest part of recovering from a ransomware attack.
upvoted 2 times

🗳️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: C

As far as CompTIA are concerned backups are the best mitigation against ransomware. Throw in the employee training too and you've got your answer.
upvoted 2 times

🗳️ 👤 **catastrophie** 2 years, 5 months ago

C is correct. It's the only option that consist of a prevention and a recovery method. Employees can be trained to recognize and avoid potential threats, such as not clicking on suspicious links or attachments. Implementing secure and verifiable backups (preferably those in option B the gold image) also ensures that the company has a way to restore their data in the event of an attack. Option A does nothing for recovery if it fails to protect the systems. Option D is the polar opposite of A, it is great for recover but does nothing for prevention.
upvoted 1 times

🗳️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: C

People are always the weakest link. Must train them. This also includes backup solution.
upvoted 3 times

🗳️ 👤 **anap2022** 2 years, 8 months ago

Selected Answer: C

C is the best answer. I currently work in a SOC and we talk about ransomware quite often. Training and awareness is always the first thing to do. For example to pick up random USB's laying around and connect them to your computer.

upvoted 2 times

🗨️ 👤 **Jimmycyber123** 2 years, 8 months ago

Selected Answer: C

This isn't up for debate. The answer is C. Anyone saying otherwise is wrong

upvoted 3 times

🗨️ 👤 **jagoichi** 2 years, 8 months ago

Selected Answer: C

Agree C

Training and awareness is always the BEST answer

upvoted 1 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

Awareness training and having a good backup is the only way to recover from ransomware...or get yourself some good ole Bitcoin for payment to retrieve the keys (if you are Lucky)..for me, C is best

upvoted 2 times

🗨️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: C

C makes more sense.

upvoted 3 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: C

I have to go with C. It's the user awareness that prevents it.

upvoted 3 times

🗨️ 👤 **Fastytop** 2 years, 9 months ago

Selected Answer: A

UTM.. of course.

upvoted 1 times

🗨️ 👤 **Adonist** 2 years, 9 months ago

Selected Answer: C

I agree with C. Most companies that are affected by Ransomware have firewalls and antivirus lol

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

Selected Answer: A

Only one that PREVENTS.

upvoted 2 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

This does not prevent, this mitigates the effects. The only answer that can possibly prevent is C

upvoted 1 times

🗨️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: C

looks good to me

upvoted 1 times

A computer hardware manufacturer is developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

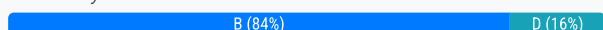
- A. Encryption
- B. eFuse
- C. Secure Enclave
- D. Trusted execution

Suggested Answer: D

Reference:

<https://www.chrislockard.net/posts/ios-android-code-protections/>

Community vote distribution



Merc16 Highly Voted 2 years, 9 months ago

Selected Answer: B

I think B for me

the official CompTIA cysa guide states

Trusted execution—To initialize security functions, the CPU's security extensions invoke a TPM and secure boot attestation to ensure that a trusted operating system is running.

while

eFUSE

eFUSE is an Intel-designed mechanism to allow a software instruction to blow a transistor in the hardware chip. One use of this is to prevent firmware downgrades, implemented on some games consoles and smartphones. Each time the firmware is upgraded, the updater blows an eFUSE. When there is a firmware update, the updater checks that the number of blown eFUSEs is not less than the firmware version number. Another use of eFUSE is one-time programming (OTP), which is used to seal cryptographic keys and other security information during the firmware development process. OTPs can also use a newer technology called antifuse.

upvoted 18 times

2Fish 2 years, 3 months ago

Agree with B, thanks for the detail.

upvoted 3 times

EVE12 Highly Voted 2 years, 9 months ago

Selected Answer: D

The CySA+ exam outline calls out "trusted firmware updates," but trusted firmware itself is more commonly described as part of trusted execution environments (TEEs). Trusted firmware is signed by a chip vendor or other trusted party, and then used to access keys to help control access to hardware. TEEs like those used by ARM processors leverage these technologies to protect the hardware by preventing unsigned code from using privileged features.

upvoted 5 times

Ayben Most Recent 1 year, 8 months ago

Selected Answer: D

A System-on-Chip (SoC) implements secure boot or verified boot. It might support a security version number, which prevents downgrading the current firmware to a vulnerable version. Once downgraded to a previous version, an adversary can launch exploits on the SoC and thus compromise the security of the SoC

<https://cwe.mitre.org/data/definitions/1328.html>

upvoted 1 times

Dree_Dogg 1 year, 9 months ago

Selected Answer: B

Definitely B

upvoted 2 times



nomad421 2 years, 1 month ago

Selected Answer: B

Amazon has blown eFuses on Fire TV devices in the past as a way to seemingly prevent newer devices from taking advantage of older software exploits that allowed the device to be rooted or allowed the bootloader to be unlocked.

<https://www.aftvnews.com/amazon-blows-efuse-on-fire-tv-stick-to-prevent-downgrading-to-old-interface/>



upvoted 2 times

  **LukaszL** 2 years, 2 months ago

Selected Answer: B

Agree with comments on B.

upvoted 2 times

  **Stiobhan** 2 years, 3 months ago

Selected Answer: B

Answer is B - eFuse. This is an excerpt from the CySA Study Guide 2nd Edition, page 457 "Firmware Security
Other defensive technologies can also help to secure systems. IBM's eFuse technology has a number of uses that can help with tuning performance or responding to system degradation, but it also has some interesting security applications. For example, an eFuse can be set at the chip level to monitor firmware levels. This is implemented in the Nintendo Switch, which uses eFuse checking to validate whether the firmware that is being installed is older than the currently installed firmware, preventing downgrading of firmware. When newer firmware is installed, eFuses are "burned," indicating the new firmware level that is installed".

upvoted 3 times

  **NerdAlert** 2 years, 2 months ago

this is on page 338 in my book - Sybex CompTIA CySA Study Guide 2nd Edition

upvoted 1 times

  **saci_frosty** 2 years, 3 months ago

Selected Answer: B


I remember first hearing about eFuse on a lecture about the Xbox 360 security.

upvoted 2 times

  **NerdAlert** 2 years, 2 months ago

Nintendo Switch uses it too for the firmware purpose mentioned in this question!

upvoted 1 times

  **JoInn** 2 years, 3 months ago

Selected Answer: D

Intel Trusted Execution Technology (TXT) uses a TPM and cryptographic techniques to measure software and platform components to prevent malfunctioning or compromised components from running. It protects against software-based attacks that would modify the system configuration. So it would prevent firmware downgrades.

upvoted 1 times

  **boletri** 2 years, 3 months ago

Selected Answer: B

eFUSE is an Intel-designed mechanism to allow a software instruction to blow a transistor in the hardware chip. One use of this is to prevent firmware downgrades, implemented on some games consoles and smartphones. Each time the firmware is upgraded, the updater blows an eFUSE. When there is a firmware update, the updater checks that the number of blown eFUSES is not less than the firmware version number.

Official CompTia Cysa+ Material

upvoted 1 times

  **ddcnsd65** 2 years, 5 months ago

I think the answer is B

According to McGraw Hill's CompTia CySA+ All in One study guide page(s) 242 - 243: Another security application of eFuses is to store data. For example you could use them to keep track of the latest version of "FIRMWARE" you have loaded on a device. This could ensure that nobody could revert the firmware to an earlier (presumably less secure) version. If you have enough eFuses in the chip you could store cryptographic keys on it, which could be used to verify the integrity of a "FIRMWARE" upgrade by checking its digital signature before installing it.

upvoted 2 times

🗄️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

100% eFuse

upvoted 3 times

🗄️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: B

"Other defensive technologies can also help to secure systems. IBM's eFuse technology has a number of uses that can help with tuning performance or responding to system degradation, but it also has some interesting security applications. For example, an eFuse can be set at the chip level to monitor firmware levels. This is implemented in the Nintendo Switch, which uses eFuse checking to validate whether the firmware that is being installed is older than the currently installed firmware, preventing downgrading of firmware. When newer firmware is installed, eFuses are "burned," indicating the new firmware level that is installed." Comptia study guide book

upvoted 3 times

🗄️ 👤 **EVE12** 2 years, 9 months ago

Selected Answer: B

An eFuse allows for the dynamic real-time reprogramming of computer chips. Utilizing a set of eFuses, a chip manufacturer can allow for the circuits on a chip to change while it is in operation.

<https://learning.oreilly.com/library/view/comptia-cybersecurity-analyst/9780136747000/ch10.xhtml#ch10lev1sec5>

upvoted 1 times

🗄️ 👤 **Ruby2021** 2 years, 9 months ago

The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs). The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the Application Processor kernel becomes compromised.

upvoted 1 times

🗄️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is the only hardware manufacturer implementation i believe.

upvoted 1 times

🗄️ 👤 **Laudy** 2 years, 9 months ago

Selected Answer: B

eFuses are perhaps more commonly used as a one-time programmable ROM. This ranges from writing unique information onto CPUs, or in the case of game consoles and other restricted hardware, preventing downgrades by permanently recording a newer version.

<https://en.wikipedia.org/wiki/EFuse#:~:text=eFuses%20are%20perhaps%20more%20commonly,permanently%20recording%20a%20newer%20version.>

upvoted 2 times

An information security analyst on a threat-hunting team is working with administrators to create a hypothesis related to an internally developed web application.

The working hypothesis is as follows:

- ⇒ Due to the nature of the industry, the application hosts sensitive data associated with many clients and is a significant target.
- ⇒ The platform is most likely vulnerable to poor patching and inadequate server hardening, which expose vulnerable services.
- ⇒ The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.

As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SQL injection attacks. Which of the following BEST represents the technique in use?

- A. Improving detection capabilities
- B. Bundling critical assets
- C. Profiling threat actors and activities
- D. Reducing the attack surface area

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ **Practice_all** Highly Voted 3 years, 11 months ago

the hypothesis is for Attack surface so the answer should be D
upvoted 6 times

🗳️ **Yeweja** Highly Voted 4 years ago

D is correct
upvoted 5 times

🗳️ **fuzzyguzzy** Most Recent 6 months, 4 weeks ago

Selected Answer: D
D is the least worst answer.
upvoted 1 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: D
D. For sure, those layers of defense put in place will shrink the attack surface.
upvoted 2 times

🗳️ **NickDrops** 2 years, 5 months ago

D, but realistically the admin is performing device hardening. The admin isn't removing applications or closing ports. The attack surface is really the same.
upvoted 3 times

🗳️ **Sebatian20** 1 year, 7 months ago

Totally agree with you. This is a terrible question
upvoted 1 times

🗳️ **f3lix** 2 years, 5 months ago

Selected Answer: D
Apt - Attach Surface is being compressed, so Answer :D
upvoted 1 times

🗳️ **david124** 2 years, 8 months ago



Selected Answer: D
d it is
upvoted 1 times

🗳️ **amateurguy** 2 years, 9 months ago

Selected Answer: D

yes d is correct.

upvoted 1 times

  **miabe** 2 years, 11 months ago

Selected Answer: D

looks good to me

upvoted 1 times

  **SniipZ** 4 years ago

Going for D here definitely

upvoted 4 times

A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

- A. Make sure the scan is credentialed, covers all hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
- B. Make sure the scan is uncredentialed, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
- C. Make sure the scan is credentialed, has the latest software and signature versions, covers all external hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.
- D. Make sure the scan is credentialed, uses a limited plug-in set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.

Suggested Answer: D

Community vote distribution

D (100%)


 **MortG7** Highly Voted 2 years, 8 months ago

C. Make sure the scan is credentialed, has the latest software and signature versions, *****covers all external hosts in the patch management system*****, and is scheduled during off-business hours so it has the least impact on operations.

D. Make sure the scan is credentialed, uses a limited plug-in set, ****scans all host IP addresses in the enterprise*****, and is scheduled during off-business hours so it has the least impact on operations.

They want to cover all hosts in the Enterprise NOT only external to the patch management system

I am going with D
upvoted 9 times

 **SniipZ** Highly Voted 4 years ago

D is correct. To check for a critical patch, only a few plugins are needed to save time and resources. Also the question mentioned, that all systems should be scanned. I am not really sure though, but I think all hosts in the patch management system are not really all hosts in the enterprise. So I am going for D here definitely.

upvoted 6 times

 **Pen88** 3 years, 8 months ago

Yes, and the question says that the organization has limited resources, so a few plugins will work.

upvoted 2 times

 **STELLO** 3 years, 7 months ago


Low tolerance for risk when it comes to resource availability not limited resources this is a case with amazon where non availability is a major issue that is why they operate on a six 9's. The indicator with this statement is that scan should be done at non business hours not to disrupt business which eliminates option A

upvoted 3 times

 **rayaMooo_Socket2** 3 years, 7 months ago

Yes, scanning all IPs within the network, provides a logical topology. I agree D.

upvoted 3 times

 **Anaser** Most Recent 2 years, 2 months ago

B. Make sure the scan is uncredentialed, covers all hosts in the patch management system, and is scheduled during off-business hours so it has the least impact on operations.

Scanning during business hours with a credentialed scan can impact resource availability and potentially cause operational disruptions. An

uncredentialed scan can still identify if a system is missing a critical security patch and is less intrusive. Scheduling the scan during off-business hours minimizes the impact on operations. It's also important to ensure that all hosts in the patch management system are covered to ensure comprehensive coverage.

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: D

D. Is correct. "...if a critical security patch" = "uses a limited Plug-in set"

upvoted 1 times

🗳️ 👤 **david124** 2 years, 8 months ago

d it is

upvoted 1 times

🗳️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: D

looks good to me

upvoted 2 times

🗳️ 👤 **Manpreet3096** 3 years, 3 months ago

I would like to go fir D as it needs to scan the IPs

upvoted 2 times

🗳️ 👤 **VinciTheTechnic1an** 3 years, 5 months ago

I would go for D, as the question pertain to network so it has to scan the IP blocks.

upvoted 4 times

🗳️ 👤 **STELLO** 3 years, 7 months ago

I would go with C since all systems critical path need to be scanned. Limiting some plug ins might leave some vulnerabilities undetected and since this is done during off business hours it is best to utilize all effort

See: <https://www.tenable.com/blog/4-best-practices-for-credentialed-scanning-with-nessus>

upvoted 3 times

🗳️ 👤 **Manoj1996** 2 years, 11 months ago

They said to look for a sepcific patch

upvoted 2 times

🗳️ 👤 **Davar39** 3 years ago

In addition to what Snipz replied, answer C covers only the systems that are included in the patch management.

upvoted 1 times

🗳️ 👤 **AndreaO** 4 years ago

C and D appear correct, but "...to determine if a critical security patch was applied to all systems in an enterprise." would imply a limited plug-in sets. Thus D seems to be more correct that C.

upvoted 1 times

🗳️ 👤 **mcNik** 4 years ago

I am wondering between C and D but this " uses a limited plugin set " makes me thing actually D might be correct.

upvoted 3 times

🗳️ 👤 **lonestarnj** 4 years ago

I agree tough to choose between C and D. I would also go with D.

upvoted 2 times

🗳️ 👤 **mcNik** 4 years ago

Well I am actively using such scans. If you need to scan particular thing you need just few plugin's which will reduce the impact N times.

upvoted 7 times

A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

From:	Justin O'Reilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	sara.ellis@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

From:	Justin O'Reilly
Subject:	Your tax documents is ready for secure download
Date:	2020-01-30
To:	jason.lee@exampledomain.org
Return-Path:	justinoreilly@provider.com
Received From:	justing@sssofk12awq.com

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

- A. DNSSEC
- B. DMARC
- C. STP
- D. S/IMAP

Suggested Answer: B

Reference:

<https://dmarc.org/>

DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an [email authentication](#), policy, and reporting protocol. It builds on the widely deployed [SPF](#) and [DKIM](#) protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

Community vote distribution

B (100%)

🗳️ **TacosInMyBelly** 1 year, 7 months ago

Selected Answer: B

DMARC allows domain owners to publish policies in their DNS records, specifying what action should be taken if an email fails SPF and/or DKIM checks. The actions can include monitoring, quarantining, or rejecting the email.

upvoted 2 times

🗳️ **narcosubs** 1 year, 11 months ago

Again a silly question as the correct answer is missing here: SPF.

upvoted 1 times

🗳️ **ProNerd** 1 year, 11 months ago

SPF is part of DMARC

upvoted 1 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: B

B. DMARC for sure.

upvoted 1 times

🗳️ **CatoFong** 2 years, 4 months ago

Selected Answer: B

B. for DMARC

upvoted 1 times

🗳️ **amateurguy** 2 years, 9 months ago

Selected Answer: B

go with B

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

Selected Answer: B

DMARC is correct.

<https://dmarc.org/>

upvoted 3 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

To elaborate on answer provided by examtopics...

What is SPF and DKIM?

Image result for spf and dkim

SPF lets you authorize senders that are allowed to send email on behalf of your domain. DKIM signs every outgoing message with your unique signature, so receiving servers can verify the message came from you. SPF and DKIM let receiving servers verify that messages that appear to be from your domain are legitimate.

upvoted 3 times

🗨️ 👤 **Davar39** 3 years, 1 month ago

Correct answer - DMARC

upvoted 4 times

🗨️ 👤 **PoopyPants5000** 3 years, 5 months ago

No, A DMARC is used to stop domain spoofing.

Answer is correct

upvoted 4 times

🗨️ 👤 **Anikulapo** 3 years, 5 months ago

Shouldn't this be C

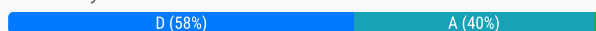
upvoted 1 times

A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with adware. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

- A. Blacklist the hash in the next-generation antivirus system.
- B. Manually delete the file from each of the workstations.
- C. Remove administrative rights from all developer workstations.
- D. Block the download of the file via the web proxy.

Suggested Answer: A

Community vote distribution



🗳️ **MortG7** Highly Voted 2 years, 8 months ago

Laudy, you never explain the reasoning behind any of your answers. I am beginning to have this nasty feeling that you are here simply to throw people off.

upvoted 24 times

🗳️ **TKW36** Highly Voted 2 years, 5 months ago

Selected Answer: D

I'm choosing D. In the question it states that the anti-virus is already preventing the file from executing, but it did not remove the file from the device. Later, more developers tried to DOWNLOAD and execute the same file. If the anti-virus is already preventing the execution of the file, then the real issue is the downloading of the file. By blocking the download, you can prevent anyone else from downloading that file while the AV is already preventing the execution of it. Unless by "blacklist" they also mean automatic deletion of said file when discovered and/or prevent it from being downloaded too. Very confusing question that's not written well...

upvoted 21 times

🗳️ **Anie_diogo28** Most Recent 10 months ago

I choose A.

The reason is that the question is still asking about what would be done to the tool "The next generation Anti-virus solution" It did ask what other solutions can be used.

upvoted 1 times

🗳️ **zecomeia_007** 11 months ago

Selected Answer: A

By blacklisting the hash, the organization can effectively prevent the adware from spreading and compromising more systems.

upvoted 2 times

🗳️ **Lilik** 10 months, 3 weeks ago

what if they upgrade the version of the malware file and you download from the same web a different file with a different hash. what is your NSFW doing?

upvoted 2 times

🗳️ **RobV** 1 year, 6 months ago

Selected Answer: D

D. Block the download of the file via the web proxy.

Explanation:

Blacklisting the hash in the next-generation antivirus system (Option A):

- While blacklisting the hash could prevent the specific file from executing, it may not be a foolproof solution, as attackers can easily modify the file to generate a new hash.

Blocking the download of the file via the web proxy (Option D):

- This is the most proactive and effective solution. By blocking the download at the web proxy level, you prevent the file from reaching the developer

workstations in the first place. This approach stops the problem at its source and helps protect all workstations from potential harm.

Therefore, option D is the best choice in this scenario.

upvoted 2 times

🗳️ 👤 **novolyus** 1 year, 7 months ago

Selected Answer: C

Why nobody said C? A developer should not have administrative rights in the machine he is working with.

Privilege management:

"The principle of least privilege states that an individual should only have the minimum set of privileges necessary to complete their assigned job duties."

upvoted 1 times

🗳️ 👤 **zhuzhu123** 1 year, 7 months ago

Your would be right in some environments about the least privileges, but devs almost always need very specialized software and dev components that require high privileges.

Therefore "...the minimum set of privileges..." are most likely local admin rights (restricted domain + local admin) in my opinion.

upvoted 1 times

🗳️ 👤 **sirpetey** 1 year, 7 months ago

Selected Answer: A

Going with A and not D because it doesn't mention that they are downloading it from a website.

upvoted 2 times

🗳️ 👤 **Big_Dre** 1 year, 9 months ago

Selected Answer: A

A is the best option since blacklisting the app give it no chance of being downloaded at all.

upvoted 2 times

🗳️ 👤 **kmordalv** 1 year, 10 months ago

Selected Answer: D

The most correct option is D.

If at some point the application is updated, the hash will be different, so it will be useless to check the hash in the next-generation antivirus system.

Some people choose option A to prevent installation via USB but do not take into account that if the hash is changed, this option will be invalidated.

Therefore, the most correct option is D

upvoted 2 times

🗳️ 👤 **Rori791** 1 year, 11 months ago

Selected Answer: A

Why D? the web browser will inspect and block any attempts to access the blocked URL or stop the attempt of downloading the malicious file. So what if the developers accessed another URL and download the same file, will the web browser prevent this? A is better because the hash itself will be blocked an any attempts to download the file from other websites or other means (aka usb or email) will be detected and stopped... so A is more comprehensive approach

upvoted 3 times

🗳️ 👤 **Rori791** 1 year, 11 months ago

+ The question didn't mention whether the file was downloaded and executed from a USB drive or other means outside of a web browser, so D would not be effective in preventing the file from being executed.

upvoted 1 times

🗳️ 👤 **nomad421** 2 years, 1 month ago

Selected Answer: A

When I blacklist a file in Cisco Secure Endpoint, it automatically deletes it when someone attempts to download it.

upvoted 4 times

🗳️ 👤 **HotWings8** 1 year, 11 months ago

Comptia is vendor neutral so they shouldn't be specific with certain brand names, for that I'm going with D

upvoted 1 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: A

Blacklist the hash in the next-generation antivirus system would be the BEST approach to remedy the issue. Since the next-generation antivirus software prevented the file from executing but did not remove it from the device, blacklisting the hash in the antivirus system would prevent the file from executing on any workstation in the future, even if a user tries to download it again.

upvoted 3 times

🗨️ 👤 **khrid4** 2 years, 3 months ago

Selected Answer: A

A.

-Can retroactively delete all existing hashes from existing computers

-Immediately detects future download

Hits two birds in one stone compared to D. which shows A is better (question is asking for the Best)

upvoted 3 times

🗨️ 👤 **Stiobhan** 2 years, 3 months ago

Selected Answer: A

You know there is a reason why they keep mentioning NGAV!!! Please read this through.

<https://www.carleton.edu/its/newsletter/news/malwarebytes-next-generation-antivirus/?issue=cybersecurity-2022>

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: D

D. We are trying to mitigate the download. The current AV is already detecting, just not removing. Blacklisting HASHs would not be as efficient as the AV is already detecting it.

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

man.. now I am rethinking, from Stiobhan's post. I can see NGAV being a solution, I wonder though, can you blacklist it yourself or does it require a support ticket with the vendor. For instance in malwarebytes, we do see blocks for downloads and executions "IF" MWB has the hashes already.

Otherwise, we would have to open a support ticket for them to add the hash. ugh.

upvoted 2 times

🗨️ 👤 **encxorblood** 2 years, 4 months ago

Selected Answer: A

Answer is A - Blocking the download of the file via the web proxy (option D) is also a useful security measure, but it may not be sufficient to prevent the file from being downloaded and executed through other means, such as USB drives or email attachments.

upvoted 4 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: D

The proxy will prevent it from being downloaded.

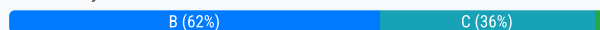
upvoted 1 times

A newly appointed Chief Information Security Officer has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?

- A. Planning
- B. Continuous monitoring
- C. Risk response
- D. Risk analysis
- E. Oversight

Suggested Answer: C

Community vote distribution



db97 Highly Voted 2 years, 4 months ago

Selected Answer: B

It's obviously they will respond, but they want to validate the trend over the time, so continuous monitoring can provide this.
upvoted 10 times

2Fish 2 years, 3 months ago

Agree. Thanks for the input.
upvoted 3 times

db97 2 years, 4 months ago

Continuous monitoring is an approach where an organization constantly monitors its IT systems and networks to detect security threats, performance issues, or non-compliance problems in an automated manner. The goal is to identify potential problems and threats in real time to address them quickly.
upvoted 2 times

m025 Most Recent 1 year, 3 months ago

Selected Answer: A

For me it's planning. He identified the risks that it plan how to response to each one, that implement the response, finally he monitored the result and the new risk restarting the cycle.
upvoted 1 times

skibby16 1 year, 7 months ago

Selected Answer: B

The key is "Which of the following will provide a trend of risk mitigation" How do you find trends? Continuous Monitoring will allow you to see trends and mitigate adverse trends etc...
upvoted 1 times

Rori791 1 year, 11 months ago

Selected Answer: B

The key word here is "trend of risk mitigation".. at first my answer was C but when I searched about the meaning of the word I switched it to B. A trend of risk mitigation refers to the ability to track and monitor the effectiveness of risk mitigation efforts over time. It involves continuously assessing the effectiveness of implemented security controls and risk management strategies to determine if they are reducing the organization's exposure to risk.
upvoted 2 times

kiduuu 2 years, 2 months ago

Selected Answer: C

Risk response involves taking specific actions to reduce, transfer, or mitigate the risks that have been identified through the risk assessment process.
upvoted 2 times

HereToStudy 2 years, 2 months ago

Selected Answer: C

the question states that the risks have already been identified through the risk assessment review, then the option that will provide a trend of risk mitigation would be C. Risk response.

upvoted 2 times

🗨️ **josephconer1** 2 years, 2 months ago

Per the CompTIA CySA+ CS0-002 textbook:

Topic 7A - Speaking on the risk identification process--

"Respond--'Mitigate' each risk factor through the deployment of managerial, operational, and technical security controls.

Key word in the question is mitigation. This clearly means the answer is C

upvoted 1 times

🗨️ **encxorblood** 2 years, 4 months ago

Selected Answer: B

Answer B - Risk response (option C) is focused on addressing risks that have been identified, but it does not provide a trend of risk mitigation.

upvoted 4 times

🗨️ **NerdAlert** 2 years, 2 months ago

I was so sure it was C til I read this - great point, they wanna start a trend not, just respond to this issue

upvoted 1 times

🗨️ **IanRogerStewart** 2 years, 4 months ago

Selected Answer: C

It's the mitigation thing that's critical here. Monitoring isn't mitigating

upvoted 1 times

🗨️ **absabs** 2 years, 4 months ago

Selected Answer: C

Just monitoring without taking action is useless. Easy question, i going with C.

upvoted 1 times

🗨️ **AaronS1990** 2 years, 4 months ago

Selected Answer: C

Which of the following will provide a trend of risk mitigation?

For me this has to be C. He has carried out the risk assesment and identified issues, surely the next stage is risk response... Though i understand people who are saying B, i think some of you (respectfully) are getting too caught up on the term 'trend' and tying that to continuous monitoring

upvoted 1 times

🗨️ **gnnggnnggnng** 2 years, 4 months ago

Selected Answer: B

Risk response is an important part of the risk management process and involves implementing measures to mitigate or transfer the risks identified during the risk analysis. However, risk response alone does not provide a trend of risk mitigation, as it only addresses the risks that have been identified in a specific point in time.

Continuous monitoring, on the other hand, involves ongoing assessment of the organization's security posture and the identification of new risks. By regularly monitoring the organization's security, the CISO can identify trends in risk mitigation and make adjustments to the risk management plan as needed. This provides a more comprehensive view of the organization's risk landscape and the effectiveness of the risk mitigation measures in place.

upvoted 2 times

🗨️ **Stiobhan** 2 years, 4 months ago

This is close, however I'd need to opt for C as to pull trend analysis data, I need to see the how and the why of mitigation over a period of time.

Response actions would give me that better than continuous monitoring. See this article, points 5 and 6 are so close -

<https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation>

upvoted 1 times

🗨️ **david124** 2 years, 5 months ago

Selected Answer: B

chat GBT says B

upvoted 1 times

🗨️ **kmanb** 2 years, 5 months ago

Selected Answer: B

The best option that will provide a trend of risk mitigation is B. Continuous monitoring.

Continuous monitoring is the ongoing process of assessing the security controls in an organization to identify vulnerabilities, threats, and risks. It also involves analyzing the results of security testing, incident response, and other security-related activities to identify trends and patterns that can be used to improve the security of the organization. By continuously monitoring the organization, the Chief Information Security Officer can identify and address new and emerging risks, which will help to reduce the overall risk to the organization.

upvoted 1 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

Selected Answer: C

After risk assessment review --->comes Risk response

upvoted 1 times

🗨️ 👤 **MortG7** 2 years, 8 months ago

risk mitigation is an attempt to minimize the chances of a potential attack...thus Risk Response..C is correct

upvoted 2 times

Which of the following allows Secure Boot to be enabled?

- A. eFuse
- B. UEFI
- C. HSM
- D. PAM

Suggested Answer: C

Community vote distribution

B (92%)

8%

🗳️ 👤 **16561f6** 1 year, 1 month ago

UEFI

To enable Secure Boot, you need to set the BIOS Mode to UEFI1. If your computer supports UEFI, you can switch from Legacy BIOS to UEFI mode1. You can enable or disable Secure Boot from the computer's UEFI firmware settings screen or BIOS confirmation screen2. You can also enable Secure Boot by opening Settings, clicking on Update & Security, clicking on Recovery, and under the "Advanced startup" section, clicking the Restart now button3. You can also enable Secure Boot by contacting your support person for help or enabling Secure Boot from the PC BIOS

upvoted 1 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

B. UEFI

upvoted 1 times

🗳️ 👤 **Big_Dre** 1 year, 10 months ago

Selected Answer: B

are some of these questions answered wrong intentionally? cuz im beginning not to trust this site anymore.

upvoted 4 times

🗳️ 👤 **kill_chain** 2 years ago

WHY DOES IT SEEM LIKE THERE'S A LOT OF WRONG ANSWERS FROM THIS SITE? ANYONE WHO WROTE RECENTLY TO CONFIRM. I WAS TOLD TO BUY THESE... BUT IT SEEMS THESE ARE NOT LEGIT ANSWERS CHOSEN BY THE SITE

upvoted 3 times

🗳️ 👤 **Lungful** 1 year, 8 months ago

Yeah, I am just here for the discussions.

upvoted 3 times

🗳️ 👤 **POWNED** 1 year, 11 months ago

Most Brain dumps are wrong answers, great thing about examtopics is you have the ability to discuss the correct answers.

upvoted 7 times

🗳️ 👤 **supernewtechnewbie** 1 year, 10 months ago

Legally they are not allowed to give the correct answer. They are only allowed to have community discussion about the answers.

upvoted 4 times

🗳️ 👤 **alayeluwa** 2 years, 2 months ago

It's UEFI. CompTIA A+ days, lol

upvoted 3 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. Agree with most here. In order to enable secure boot the device must be capable with UEFI firmware: The computer must have a UEFI firmware instead of the legacy BIOS firmware.

upvoted 2 times

🗳️ 👤 **boletri** 2 years, 3 months ago

Selected Answer: B

Secure Boot, Measured Boot, and Attestation

Secure boot is a security system offered by UEFI. It is designed to prevent a computer from being hijacked by a malicious OS. Under secure boot, UEFI is configured with digital certificates from valid OS vendors. The system firmware checks the operating system boot loader using the stored certificate to ensure that it has been digitally signed by the OS vendor. This prevents a boot loader that has been changed by malware (or an OS installed without authorization) from being used.

Official CompTIA Cysa+ Course Material

upvoted 1 times

🗳️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: B

There is no way this isn't UEFI

upvoted 1 times

🗳️ 👤 **Stiobhan** 2 years, 4 months ago

It is UEFI all day long!!! I was going to just ignore the answer given by Examtopic "Experts" but come on.....this isn't even hard, secondary school students could have answered this. Very poor ExamTopics, some of us are paying for this stuff you know!!! Think you need to get new "Experts" to validate the answers!

upvoted 3 times

🗳️ 👤 **ddcnsd65** 2 years, 5 months ago

I choose B.

Most of what UEFI does is to figure out what code is needed, load it into memory and execute it. By default, it trusts all the code that it uses, but there is an option to do better, Secure boot is a feature in UEFI that establishes the root of trust in the firmware.

upvoted 1 times

🗳️ 👤 **IT_Master_Tech** 2 years, 6 months ago

Secure boot is enabled in system BIOS through UEFI. B is absolutely correct.

upvoted 1 times

🗳️ 👤 **brvndvnwolf** 2 years, 6 months ago

Selected Answer: B

This should be really simple lol, it is B

"allows secure boot to be ENABLED" Keyword enabled

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years, 8 months ago

Selected Answer: B

B UEFI

"Secure Boot requires a recent version of UEFI. Update the firmware with Device Manager if you are in doubt." <https://www.minitool.com/lib/secure-boot.html>

upvoted 1 times

🗳️ 👤 **Treymb6** 2 years, 9 months ago

Selected Answer: C

Sorry but B is wrong.

You literally need a hardware security module to store the encryption keys for secure boot.

While UEFI does enable secure boot when you turn it on, it doesn't make secure boot function in itself.

<https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/secure-boot-key-generation-and-signing-using-hsm--example?view=windows-11>

upvoted 2 times

🗳️ 👤 **ExamTopicsDiscussor** 2 years, 8 months ago

The question literally asks what enables it dude. You're wrong. It's B.

upvoted 4 times

🗳️ 👤 **david124** 2 years, 8 months ago

LMAO @trey, you just played yourself. read the question, its asking you to enable not function.

NPCs everywhere

upvoted 2 times

  **Fastytop** 2 years, 9 months ago

Selected Answer: B

B is correct



upvoted 2 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is the answer.

upvoted 2 times

  **Adonist** 2 years, 9 months ago

Selected Answer: B

B for sure

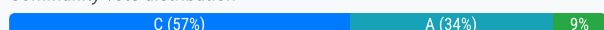
upvoted 1 times

A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

- A. Implement UEM on all systems and deploy security software.
- B. Implement DLP on all workstations and block company data from being sent outside the company.
- C. Implement a CASB and prevent certain types of data from being downloaded to a workstation.
- D. Implement centralized monitoring and logging for all company systems.

Suggested Answer: B

Community vote distribution



🗳️ 👤 **fablus78** Highly Voted 👍 2 years, 10 months ago

Selected Answer: C

Cloud Access Security Broker (CASB): An enterprise management software designed to mediate access to cloud services by users across all types of devices

upvoted 10 times

🗳️ 👤 **kiduuu** Highly Voted 👍 2 years, 2 months ago

Selected Answer: A

UEM stands for Unified Endpoint Management. It is a comprehensive approach to manage and secure all types of endpoint devices (such as laptops, mobile phones, and tablets) in an organization from a single console. UEM software provides capabilities such as device management, security management, application management, content management, and data protection for all endpoints, regardless of the operating system and device ownership model.

In the scenario described in the question, implementing a CASB to prevent certain types of data from being downloaded to a workstation may be a valid solution, but it may not address the issue of unmanaged laptops and users with administrative rights. Implementing UEM (Unified Endpoint Management) on all systems and deploying security software could help address these issues by allowing the security team to manage and secure all endpoints, enforce security policies, and monitor and respond to security incidents in real-time

upvoted 10 times

🗳️ 👤 **grelaman** 1 year, 9 months ago

B. Implement DLP on all workstations and block company data from being sent outside the company.: this solutions are primarily designed to protect data from unauthorized access and transfer (data exfiltration) while it is still on the endpoint device or in transit. DLP won't be able to do much to prevent the access to the data that is already stored in the cloud if a malicious actor gains access with the proper credentials or permissions using those laptops which already have administrative rights. Furthermore, users with administrative privileges can disable the DLP in those devices.

upvoted 1 times

🗳️ 👤 **grelaman** 1 year, 9 months ago

3. Administrative Rights: By using UEM, you can restrict administrative rights for users. Giving all users administrative rights can be a significant security risk, as it allows them to make changes that could compromise the system. With UEM, you can implement the principle of least privilege, ensuring that users have only the necessary permissions.

upvoted 1 times

🗳️ 👤 **Noragretz** 1 year, 11 months ago

ChatGPT agrees with this answer and I do too

upvoted 1 times

🗳️ 👤 **Rori791** 1 year, 11 months ago

I agree with this, but difference between the votes is too huge... I've read the comments here & searched about it and I'm still unconvinced why a lot of people voted for C. CASB doesn't address the root cause of the problem, which is that all company owned laptops are currently unmanaged, and all users have administrative rights. UEM will provide a complete visibility and control over all company-owned laptops, regardless of their location, and enforce security policies such as disabling administrative rights, enforcing data encryption, and enforcing the installation of security software.

upvoted 2 times

🗄️ 👤 **anhod1578** Most Recent 1 year, 3 months ago

Selected Answer: A

(Unified Endpoint Management): UEM provides centralized management of all company endpoints, including laptops, desktops, tablets, and mobile devices.

(Cloud Access Security Broker): A CASB can provide visibility and control over cloud services used by the organization. However, it wouldn't directly address the security vulnerabilities on unmanaged laptops and user administrative rights.

upvoted 1 times

🗄️ 👤 **RobV** 1 year, 6 months ago

C. Implement a CASB and prevent certain types of data from being downloaded to a workstation.

Implement UEM on all systems and deploy security software (Option A):

- While Unified Endpoint Management (UEM) and security software are important components of a security strategy, they might not be sufficient on their own to address the specific concerns of data protection in a cloud-centric environment.

Implement a CASB and prevent certain types of data from being downloaded to a workstation (Option C):

- Cloud Access Security Broker (CASB) solutions are designed to protect data as it moves between on-premises and cloud environments. By implementing a CASB, the company can enforce policies that prevent certain types of data from being downloaded to unmanaged workstations, providing a more granular and cloud-focused approach to data protection.

upvoted 2 times

🗄️ 👤 **edro** 1 year, 7 months ago

As analysts, we face many issues in our day to day, prioritizing asset matters.

While managing devices is necessary, prioritizing the protection of the Confidentiality, Integrity, and Availability (CIA) of the data is paramount. Given that the data is stored in the cloud, implementing a CASB solution becomes instrumental in addressing and enhancing the overall protection of the data.

upvoted 1 times

🗄️ 👤 **grelaman** 1 year, 9 months ago

Selected Answer: A

The problem is shown from the perspective that the primary concern is to protect the company's data from unsafe company-owned laptops, then the best approach would involve addressing the vulnerabilities that could come up from those laptops. In this case, option A would be the most suitable.

1. Unified Endpoint Management (UEM): Implementing UEM allows for centralized control and management of all company-owned laptops. This includes enforcing security policies, ensuring software is up to date, and remotely wiping or locking devices if they are lost or compromised.

2. Deploying Security Software: Deploying security software, including antivirus, anti-malware, and firewall solutions, is essential for protecting laptops from various threats. It can help detect and prevent malware infections and other security risks.

upvoted 2 times

🗄️ 👤 **grelaman** 1 year, 9 months ago

3. Administrative Rights: By using UEM, you can restrict administrative rights for users. Giving all users administrative rights can be a significant security risk, as it allows them to make changes that could compromise the system. With UEM, you can implement the principle of least privilege, ensuring that users have only the necessary permissions.

upvoted 1 times

🗄️ 👤 **grelaman** 1 year, 9 months ago

B. Implement DLP on all workstations and block company data from being sent outside the company.: this solutions are primarily designed to protect data from unauthorized access and transfer (data exfiltration) while it is still on the endpoint device or in transit. DLP won't be able to do much to prevent the access to the data that is already stored in the cloud if a malicious actor gains access with the proper credentials or permissions using those laptops which already have administrative rights. Furthermore, users with administrative privileges can disable the DLP in those devices.

upvoted 1 times

🗄️ 👤 **grelaman** 1 year, 9 months ago

C. Implement a CASB and prevent certain types of data from being downloaded to a workstation. This solutions are intended to provide control access (Accounting), compliance, Threat protection, encryption of the data transferd and DLP to the services that a company has in the cloud. if a laptops have administrative permissions and falls into malicious hands, it can potentially undermine some of the security controls implemented by a CASB. An malicious actor can bypass or disable the security mesures provided by this solutions.

upvoted 1 times

🗄️ 👤 **buchhe** 1 year, 10 months ago

Selected Answer: C

A cloud security broker, or cloud access security broker (CASB), is a software layer that operates as a gatekeeper between an organization's on-premises network and the provider's cloud environment. It can provide many services in this strategic position like:

1. Compliance
2. Data security
3. Threat protection and
4. Data loss prevention

upvoted 3 times

🗳️ 👤 **POWNERD** 1 year, 11 months ago

It is A (UEM). Look at the big picture! UEM is a comprehensive tool which will solve all the issues mentioned in the question.

upvoted 2 times

🗳️ 👤 **HotWings8** 1 year, 11 months ago

I have selected C - There's a reason it included "A Company stores all its data in the cloud"

upvoted 1 times

🗳️ 👤 **msyusa** 2 years, 2 months ago

answer is A: DLP can be bypassed or disabled by an authorized user who has administrative rights.

C: CASB :: can help protect data in the cloud, but it does not address the issue of unmanaged laptops or users with administrative rights.

upvoted 3 times

🗳️ 👤 **MacherNewSrCyberSecAnal** 2 years, 2 months ago

aSBhbSBnYXk=

upvoted 1 times

🗳️ 👤 **Snkrsnaker1** 2 years, 2 months ago

Answer is B. The question is asking the best way to protect the company's data. The arguments for B or C are pretty good but we have to look at it from the scope of this course. CASB for the sake of this course is there to manage access to the cloud, where DLP's purpose is for protecting data. The best way to protect the data is to manage those laptops and implement DLP on all of them. CASB won't protect the data, think of them as security at the front door. It's a deterrent vs a preventative measure. I hope this helps.

upvoted 1 times

🗳️ 👤 **Jacobmy98** 2 years, 2 months ago

Selected Answer: C

An advantage of using a CASB for enforcement in DLP policies is that it is built for cloud security. A CASB will examine the traffic to and from a cloud application and enforce DLP policies for those cloud services.

upvoted 2 times

🗳️ 👤 **Stiobhan** 2 years, 3 months ago

Selected Answer: B

CASB and DLP are both very viable but because of its wider reach I am going to go with DLP - <https://www.nextdlp.com/resources/blog/casb-vs-dlp-whats-the-difference#:~:text=The%20main%20difference%20between%20a,premises%2C%20or%20stored%20in%20endpoints.>

upvoted 1 times

🗳️ 👤 **tatianna** 2 years, 3 months ago

Chat gpt

The BEST method to protect the company's data in this scenario would be to implement UEM (Unified Endpoint Management) on all systems and deploy security software. By doing so, the security team can enforce policies, manage software, and secure endpoints to protect against potential data breaches. Additionally, implementing DLP (Data Loss Prevention) and a CASB (Cloud Access Security Broker) can provide additional layers of security, but those would be secondary to deploying UEM and security software to protect the unmanaged laptops. Centralized monitoring and logging is also an essential practice to identify potential security incidents, but it is not a solution to secure the environment.

upvoted 3 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. Originally I kinda thought DLP maybe, but B is the best answer for this question. One of CASB functionality is to mitigate Data exfiltration.

upvoted 2 times

🗳️ 👤 **boletri** 2 years, 3 months ago

Selected Answer: C

Cloud Access Security Broker (CASB)

A cloud access security broker (CASB) is enterprise management software designed to mediate access to cloud services by users across all types of devices.

Some of the functions of a CASB are:

- Enable single sign-on authentication and enforce access controls and authorizations from the enterprise network to the cloud provider.
- Scan for malware and rogue or non-compliant device access.
- Monitor and audit user and resource activity.
- Mitigate data exfiltration by preventing access to unauthorized cloud services from managed devices.

upvoted 2 times

A security analyst is reviewing a vulnerability scan report and notes the following finding:

Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/tcp

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?

- A. Patch or reimage the device to complete the recovery.
- B. Restart the antiviruses running processes.
- C. Isolate the host from the network to prevent exposure.
- D. Confirm the workstation's signatures against the most current signatures.

Suggested Answer: C

Community vote distribution

D (63%)

C (37%)

  **midouban86** Highly Voted 2 years, 9 months ago

"As part of the detection and analysis procedures", means still under detection & analysis phase. So, D.
upvoted 23 times

  **2Fish** Highly Voted 2 years, 3 months ago

Selected Answer: D

D. Even though having out of date signatures is detected here. I would confirm first and then move on. This could be a false positive, the device may not be compromised so why jump to isolation until we know what is going on.
upvoted 10 times

  **2Fish** 2 years, 3 months ago

Additionally, remember the question says this is still part of the "detection and analysis" stage.
upvoted 2 times

  **AhmedSameer** Most Recent 1 year, 8 months ago

Selected Answer: C



Dears .. As cyber security analyst, I can tell you the FIRST STEP I will take after finding vulnaravity with 10 as CVSS Score, to Isolate the reason first then do any other steps..
upvoted 4 times

  **grelaman** 1 year, 9 months ago

Selected Answer: C



Given the high Quality of Detection (QoD) of 97%, it's reasonable to assume that the signature is indeed out of date. In such a case, the most appropriate next step for the security analyst should be Isolating the host from the network. It is a prudent step to prevent potential threats from exploiting the vulnerability caused by the outdated antivirus signature. Once isolated, the analyst can then work on updating the antivirus signatures to address the root cause of the issue.

The analyst is clearly at the step "Detection and analysis" in a Incident Response procedure, the next step in an IR procedure is "Containment".
upvoted 5 times

  **Aliyan** 1 year, 10 months ago

Selected Answer: D

I was thinking C also but Its a Vulnerability not a Compromise so you might not need to Isolate right away and as midouban86 stated "As part of the detection and analysis procedures"
upvoted 1 times

  **attesco** 1 year, 10 months ago

Selected Answer: D

This question looks so confusing, but it is clear now. The questions says " As part of the detection and analysis procedures" - That means , we should analyses those step under IR - detection and Analysis step . Then answer D coming to be the right answer.

Note - that answer " C" is part of the next step of IR - Eradication and Containment
upvoted 1 times

🗨️ 👤 **Stiobhan** 2 years, 3 months ago

Selected Answer: C

The answer is defo C. When you find a host on the network that has little or no AV protection your first action is to isolate and then next resolve, so D would be the second action.

upvoted 2 times

🗨️ 👤 **JoInn** 2 years, 3 months ago

Selected Answer: C

C is correct, because next step after detection is containment.

upvoted 2 times

🗨️ 👤 **josephconer1** 2 years, 2 months ago

the question says this is still part of the "detection and analysis" stage. We haven't moved into containment yet.

upvoted 2 times

🗨️ 👤 **PhillyCheese** 2 years, 4 months ago

Selected Answer: D

As part of the detection and analysis procedures, which of the following should the analyst do NEXT? Detection and analysis procedures, means verifying the threat.

D. Confirm the workstation's signatures against the most current signatures.

upvoted 3 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: C

C for the reasons i previously stated

upvoted 1 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

I agree you are still in the "detection and analysis" phase, but for me it's still C.

Why? Because the Severity is 10.0 and a QoD score is 97%!!!! for those unaware 10 is as high as severity goes and i won't patronize you with how high the % can go

Do you really think you're taking chances with that? Not for me. Get that laptop isolated ASAP

upvoted 3 times

🗨️ 👤 **lordguck** 2 years, 6 months ago

D: if you isolate a system every time (C:) just because the antivirus data is out of date, which is not even 100% certain, you have nothing else to do on your job. Confirm the problem and then restart the update procedure.

upvoted 3 times

🗨️ 👤 **gwanedm** 2 years, 7 months ago

You have to confirm the scan results to see if this is a true positive or a false positive.

upvoted 2 times

🗨️ 👤 **david124** 2 years, 7 months ago

Selected Answer: D

guys look up NIST Frame work of Incident response plan

step 2 is analysis and detection, means verifying the threat

step 3 is eradication and CONTAMINATION which would be C if we are talking about isolation

this is D

upvoted 2 times

🗨️ 👤 **saintallerdyce** 2 years, 7 months ago

Selected Answer: D

Detection and analysis

The detection and analysis phase is where the action begins to happen in our incident response process. In this phase, we will detect the occurrence of an issue and decide whether or not it is actually an incident so that we can respond to it appropriately.

[https://www.sciencedirect.com/topics/computer-science/incident-response-](https://www.sciencedirect.com/topics/computer-science/incident-response-process#:~:text=The%20detection%20and%20analysis%20phase%20is%20where%20the,so%20that%20we%20can%20respond%20to%20it%20appropriately.)

[process#:~:text=The%20detection%20and%20analysis%20phase%20is%20where%20the,so%20that%20we%20can%20respond%20to%20it%20appropriately.](https://www.sciencedirect.com/topics/computer-science/incident-response-process#:~:text=The%20detection%20and%20analysis%20phase%20is%20where%20the,so%20that%20we%20can%20respond%20to%20it%20appropriately.)

upvoted 1 times

🗨️ 👤 **TeyMe** 2 years, 8 months ago

Selected Answer: C

D states Workstation signature and not Antivirus Signature!

upvoted 1 times

  **Average_Joe** 2 years, 7 months ago

WTF. ESLs need some reading comprehension.

"Confirm the workstation's signatures against the most current signatures." This is heavily implied as "confirming the workstation's (anti-virus) database of signatures against the most current database of (anti-virus) signatures"

upvoted 3 times

  **david124** 2 years, 8 months ago

Selected Answer: D

d it is

upvoted 1 times

After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>
<userInfo>
```

Which of the following is the BEST solution to mitigate this type of attack?

- A. Implement a better level of user input filters and content sanitization.
- B. Properly configure XML handlers so they do not process &ent parameters coming from user inputs.
- C. Use parameterized queries to avoid user inputs from being processed by the server.
- D. Escape user inputs using character encoding conjoined with whitelisting.

Suggested Answer: A

Community vote distribution

B (78%)

A (22%)

🗳️ 👤 **2Fish** Highly Voted 2 years, 3 months ago

Selected Answer: B

B. Agree with everyone here. Credit to absabs for the link: <https://portswigger.net/web-security/xxe>
upvoted 5 times

🗳️ 👤 **skibby16** Most Recent 1 year, 6 months ago

Selected Answer: A

The piece of code in the XML file is an example of a command injection attack, which is a type of attack that exploits insufficient input validation or output encoding to execute arbitrary commands on a server or system² The attacker can inject malicious commands into an XML element that is processed by an XML handler on the server, and cause the server to execute those commands. The best solution to mitigate this type of attack is to implement a better level of user input filters and content sanitization, which means checking and validating any user input before processing it, and removing or encoding any potentially harmful characters or commands.
upvoted 2 times

🗳️ 👤 **buchhe** 1 year, 10 months ago

Selected Answer: A

To prevent XML vulnerabilities from being exploited, we need to use proper Input validation. Hence A is the right answer.
upvoted 2 times

🗳️ 👤 **mraval** 2 years, 3 months ago

Selected Answer: B

B is the correct Answer
upvoted 1 times

🗳️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: B

It is XEE vulnerability. You can research below link; <https://portswigger.net/web-security/xxe>
upvoted 4 times

🗳️ 👤 **Average_Joe** 2 years, 8 months ago

Selected Answer: B

parameterized queries is to mitigate SQLi
upvoted 2 times

🗳️ 👤 **david124** 2 years, 8 months ago

Selected Answer: B

B it is
upvoted 1 times

🗳️ 👤 **Adrian831** 2 years, 8 months ago

Selected Answer: B



B it's correct.

upvoted 1 times

  **rv438360** 2 years, 8 months ago



B is the right answer

upvoted 1 times

  **R00ted** 2 years, 9 months ago

B is the answer

upvoted 3 times

  **Ushouldkno** 2 years, 9 months ago

Isnt this B?

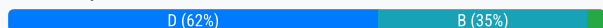
upvoted 4 times

A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation recommendation?

- A. Use TLS for all data exchanges.
- B. Use effective authentication and authorization methods.
- C. Implement parameterized queries.
- D. Validate all incoming data.

Suggested Answer: B

Community vote distribution



encxorblood Highly Voted 2 years, 4 months ago

Selected Answer: D

Answer is D - Using effective authentication and authorization methods (option B) is important for ensuring that only authorized users can access the API, but it does not specifically address the issue of insecure API parameters.

upvoted 12 times

2Fish 2 years, 3 months ago

I am leaning on D as well. As you mentioned; this question specifically asks for best 'parameter mitigation'.

upvoted 5 times

db97 Highly Voted 2 years, 4 months ago

Selected Answer: B

I think all of them are good recommendations, but B is more important for me due to with a proper authorization and authentication mechanism you are ensuring that only trusted sources/destinations get involved with the exchange of information. After this, you can set other security controls such as validate the incoming data and establish a secure channel with TLS.

Reference: <https://www.techtarget.com/searchapparchitecture/tip/10-API-security-guidelines-and-best-practices>

upvoted 6 times

edro Most Recent 1 year, 7 months ago

Access related attack would require authentication as a mitigation measure

Parameter attacks like an injection requires code validation as a security measure

Answer is D

upvoted 1 times

kumax 1 year, 9 months ago

Selected Answer: D

ChatGPT:

1. Implement Input Validation
2. Implement Output Encoding

upvoted 1 times

Kaynem 1 year, 9 months ago

Selected Answer: D

Jason dion says whenever you see input validation, it's the answer.

Can't say no to Jason.

upvoted 3 times

kmordalv 1 year, 9 months ago

Selected Answer: B

<https://blog.hubspot.com/website/api-security#best-practices>

upvoted 1 times

SimonR2 2 years, 1 month ago

If you actually look at the owasp top 10, the number one security issue is "Broken object property level authorization" my vote is for B

upvoted 1 times

🗨️ **kiduuu** 2 years, 2 months ago

Selected Answer: D

Validating all incoming data would be the BEST parameter mitigation recommendation for an insecure API. This is because validating incoming data helps to prevent injection attacks, such as SQL injection or cross-site scripting (XSS), by ensuring that the data is in the expected format and does not contain malicious code or unexpected characters. While TLS, authentication and authorization methods, and parameterized queries are also important security measures, they do not specifically address parameter validation and would not be the BEST parameter mitigation recommendation in this case.

upvoted 4 times

🗨️ **10cccordrazine** 2 years, 4 months ago

Selected Answer: D

The question says "parameter mitigation", which I admit is not very clear, but makes me want to choose D instead of B.

Of course B is always required when building an API, but I don't think that is what the question is asking for.

Also: <https://www.esecurityplanet.com/applications/how-to-control-api-security-risks/>

upvoted 5 times

🗨️ **absabs** 2 years, 4 months ago

Answer is B other question sites.

upvoted 1 times

🗨️ **Stiobhan** 2 years, 4 months ago

Enough said!!! <https://blog.hubspot.com/website/api-security#:~:text=API%20Security%20Best%20Practices%201%201.%20Implement%20authentication,activity.%20...%208%208.%20Conduct%20security%20te>

upvoted 2 times

🗨️ **TeyMe** 2 years, 7 months ago

Selected Answer: B

I would have gone for A if the question referenced REST API but B seems correct

upvoted 1 times

🗨️ **MortG7** 2 years, 8 months ago

Selected Answer: B

API Security Top 10 2019

Here is a sneak peek of the 2019 version:

API1:2019 Broken Object Level Authorization

APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorization checks should be considered in every function that accesses a data source using an input from the user. Read more.

API2:2019 Broken User Authentication

Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall. Read more.

upvoted 2 times

🗨️ **Adrian831** 2 years, 8 months ago

Selected Answer: B

Authentication and Authorization

Both authentication and authorization are core to the security of APIs. They play different roles but together they ensure that the right legitimate consumer has the right permissions to access an API.

upvoted 3 times

🗨️ **db97** 2 years, 4 months ago

A reasonable and simple answer. I support this.

I also found this other reference: <https://www.techtarget.com/searchapparchitecture/tip/10-API-security-guidelines-and-best-practices>

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: A

Use TLS for data exchanges

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Changing my answer to B

upvoted 2 times

🗨️ 👤 **EVE12** 2 years, 9 months ago

One common reason is that access to the APIs is often uncontrolled; insufficient permissions or authentication may be involved in accessing the API by unauthorized personnel.

Broken object-level authorization Failure to authorize access on an object basis

- Broken user authentication Failure to account for all the different ways a user could authenticate to the API, such as through other applications

<https://learning.oreilly.com/library/view/comptia-cysa>

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Why does it seem like C should be the answer?

upvoted 4 times

🗨️ 👤 **f3lix** 2 years, 5 months ago

I also would honestly want to believe C is the answer as the question is "BEST parameter mitigation recommendation", wouldn't that be implementing parameterized queries?

upvoted 3 times

A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions. Which of the following roles would be BEST suited to determine the breach notification requirements?

- A. Legal counsel
- B. Chief Security Officer
- C. Human resources
- D. Law enforcement

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **PatrickC_IT** Highly Voted 2 years, 9 months ago

Let the lawyers deal with it.

upvoted 7 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Yup.. agree, legal can assist with this.

upvoted 1 times

🗳️ 👤 **josephconer1** Most Recent 2 years, 2 months ago

All legal.

upvoted 1 times

🗳️ 👤 **EVE12** 2 years, 9 months ago

Legal counsel responsible for ensuring that the team's actions comply with legal, policy, and regulatory requirements and can advise team leaders on compliance issues and communication with regulatory bodies.

upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

Legal counsel is the best answer.

upvoted 2 times

🗳️ 👤 **Laudy** 2 years, 9 months ago

A is correct. HR will get involved, but this is definitely more of a legal issue.

upvoted 2 times

A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further investigation?

- A. Data carving
- B. Timeline construction
- C. File cloning
- D. Reverse engineering

Suggested Answer: D

Community vote distribution



🗳️ 👤 **Aliyan** Highly Voted 1 year, 11 months ago

Selected Answer: B

I studied Dion's course and I'm pretty sure this is B !!! I'm surprised no one says B! :o

Reverse Engineering is to understand how a CODE works. Here we identified some "malicious processes" you dont Reverse Engineer a process! to further investigate the MALICIOUS PROCESSES you must build a Timeline.

Timeline

Tool that shows the sequence of file system events within a source image

- How was access to the system obtain?
- What tools have been installed?
- What changes to files were made?
- What data has been retrieved?
- Was data exfiltrated?

upvoted 16 times

🗳️ 👤 **zecomeia_007** Most Recent 9 months, 2 weeks ago

Selected Answer: D

Correct is D.

upvoted 1 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

B. Timeline construction

upvoted 1 times

🗳️ 👤 **32d799a** 1 year, 7 months ago

Selected Answer: B

The NEXT step for further investigation after identifying potentially malicious processes in memory during incident response would typically be:

B. Timeline construction

upvoted 1 times

🗳️ 👤 **Chilaqui1es** 1 year, 7 months ago

Quizlet has the same question and says reverse engineering is the answer.

upvoted 1 times

🗳️ 👤 **AbdallaAM** 1 year, 8 months ago

Selected Answer: B

B. Timeline construction

In incident response, especially after capturing the contents of memory (also known as a memory dump) and identifying potentially malicious processes, constructing a timeline is typically a crucial next step.

upvoted 1 times

🗨️ 👤 **kumax** 1 year, 9 months ago

Selected Answer: B

ChatGPT:

1. Isolation and Containment
 2. Memory Analysis
 3. Process Identification and Investigation
 4. IOC and TTP Analysis:
 5. Malware Analysis (if applicable):
 - *** 6. Timeline and Event Reconstruction ***
 7. Affected System Examination
 8. User and Credential Investigation
 9. Network Traffic Analysis (if applicable)
 10. Incident Documentation:
 11. Incident Response Coordination
 12. Reporting and Escalation
 13. Remediation and Mitigation
 14. Lessons Learned
- upvoted 1 times

🗨️ 👤 **Big_Dre** 1 year, 9 months ago

Selected Answer: B

i don't think we can reverse Engineer a process. the best thing here to do will be time construct

upvoted 1 times

🗨️ 👤 **Pavel019846457** 1 year, 10 months ago

Selected Answer: C

I think it's C. It's wise to firstly create a copy of the file not to affect it during further investigation

upvoted 3 times

🗨️ 👤 **khrid4** 2 years, 3 months ago

Selected Answer: D

File (Data) carving is the process of extracting data from an image (from a computer) when that data has no associated file system metadata. A file-carving tool analyzes the disk at sector/page level and attempts to piece together data fragments from unallocated and slack space to reconstruct deleted files, or at least bits of information from deleted files.

In real world, once you identified a malicious file/process, security analysts will first check for other artifacts associated to it through reverse engineering. At later stages, once all IOCs were analyzed, timeline construction will be part of the reporting to get a view of the whole picture.

File cloning is of course not an option.

upvoted 2 times

🗨️ 👤 **tatianna** 2 years, 3 months ago

Data carving is a technique used to extract specific file types from a larger data set or volume. While it can be useful in certain investigations, it may not be the most appropriate next step for further investigation if the security analyst has already identified potentially malicious processes. In this case, the next step for further investigation could be to construct a timeline of events or to perform file cloning to further analyze the suspicious processes. Reverse engineering could also be a potential option if the security analyst has the necessary skills and resources.

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: D

D... if I had to choose from this mess. If reverse engineering means analyzing the captured processes, then D it is. Timeline construction would be a part over the overall reporting process of IR. Data carving is carving (putting together) files from a HD or SSD.

upvoted 3 times

🗨️ 👤 **db97** 2 years, 4 months ago

Selected Answer: D

Data carving is for hard disks...

upvoted 1 times

🗨️ 👤 **encxorblood** 2 years, 4 months ago

Selected Answer: B

Therefore, option B is the correct answer. Timeline construction involves identifying and documenting the sequence of events and actions that occurred on the system leading up to the incident. This process provides a clear picture of the actions taken by the attacker and the steps they took to achieve their goals. By reconstructing the timeline of events, the security analyst can identify patterns of activity that may help to identify the root cause of the incident and the extent of the compromise.

upvoted 1 times

🗨️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: D

In book glossary;

reverse engineering: The process of analyzing the structure of hardware or software to reveal more about how it functions.

Analyst already identified some malicious process, i think next step perform reverse engineering this process.

Data carving already performed.

upvoted 3 times

🗨️ 👤 **Eric1234** 2 years, 4 months ago

Selected Answer: D

Answer is D = Reverse Engineering, Carving is related to Storage, not memory.

upvoted 3 times

🗨️ 👤 **kmanb** 2 years, 5 months ago

Selected Answer: D

A. Data carving is a process used to extract files from unallocated space on a hard drive, which can be useful for discovering deleted files or hidden data. However, in this scenario, the security analyst has already captured the contents of memory from the machine, so data carving would not be the next step. Data carving would be useful in cases where the analyst is trying to recover data that was deleted or hidden by an attacker, but in this scenario, the focus is on analyzing the potentially malicious processes that were identified in memory, which would be best accomplished through reverse engineering.

upvoted 1 times

Understanding attack vectors and integrating intelligence sources are important components of:

- A. a vulnerability management plan.
- B. proactive threat hunting.
- C. risk management compliance.
- D. an incident response plan.

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Morph71** Highly Voted 3 years, 5 months ago

B proactive threat hunting

threat hunting activities.

1. Establishing a hypothesis,
2. Profile threat actors/activities,
3. Threat hunting tactics,
4. Reducing attack surface,
5. Bundle critical systems/assets into groups/protected zones,
6. Attack vectors understood, assessed and addressed
7. Integrated intelligence
8. Improving detection capabilities.

upvoted 24 times

🗳️ 👤 **f3lix** Highly Voted 3 years, 1 month ago

Exam Topics, what exactly is going on with questions 200+, the answers have degraded to skechiness now, resulting to have the forum jointly pointing out correct answers of late. Please could you do more to ensure correct options/answers are selected just as the earlier ones?? This will be very helpful

upvoted 8 times

🗳️ 👤 **HappyG** 2 years, 11 months ago

It's to prevent just straight memorization of tests. Other dumps are exactly the same as this without the conversation so if you use any dump outside of this one, you will fail.

upvoted 13 times

🗳️ 👤 **2Fish** Most Recent 2 years, 3 months ago

Selected Answer: B

B. Agree with everyone here. Understanding attack vectors and integrating intelligence sources can help identify potential threats and vulnerabilities that may otherwise go unnoticed, allowing organizations to take proactive measures in risk mitigations.

upvoted 1 times

🗳️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: B

looks good to me

upvoted 1 times

🗳️ 👤 **thegreatnivram** 3 years, 2 months ago

Selected Answer: B

the mentioned activities fit perfectly into proactive threat hunting.

upvoted 2 times

🗳️ 👤 **wazowski1321** 3 years, 3 months ago

B is right

upvoted 1 times

🗳️ 👤 **Xyz_40** 3 years, 4 months ago

B is the correct answer here....

upvoted 3 times

  **awad1997** 3 years, 4 months ago

Selected Answer: B

It's B thanks @Morph71

upvoted 3 times

  **Charlieb123** 3 years, 5 months ago

Agreed!

upvoted 2 times

  **Charlieb123** 3 years, 5 months ago

Agreed B.

upvoted 2 times

  **Pongpisit** 3 years, 5 months ago

B. proactive threat hunting.

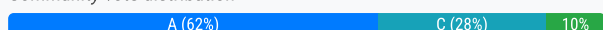
upvoted 5 times

A business recently acquired a software company. The software company's security posture is unknown. However, based on an initial assessment, there are limited security controls. No significant security monitoring exists. Which of the following is the NEXT step that should be completed to obtain information about the software company's security posture?

- A. Develop an asset inventory to determine the systems within the software company.
- B. Review relevant network drawings, diagrams, and documentation.
- C. Perform penetration tests against the software company's internal and external networks.
- D. Baseline the software company's network to determine the ports and protocols in use.

Suggested Answer: A

Community vote distribution



catastrophie 2 years, 5 months ago

Why in the world would you just jump straight into a pentest? Some of you really just want to throw a black hoodie on and sit in a dark room and look cool. What are you looking for in your pentest? Whats your scope? You just gonna test everything in the entire company?

An initial assessment was done and found the company was lacking security controls. You already know the posture is bad, there is no reason to test anything further at this point.

At this point you need to start with a BIA and determine your critical assets that need the protection. A complete inventory must be completed. You do this to firstly ensure you know critical assets but another reason is to ensure you're not spending more money on the protection of an asset than its worth. Once you complete A, then you move to B, review this and it with the outcome from the BIA you can move to D and decide what ports and protocols are needed. Finally you can do the pentest, at this point you'll know the scope of the test and what you need to ensure is properly secured.

upvoted 28 times

Joshey 2 years, 3 months ago

The question says an initial assessment has already been done though

upvoted 1 times

AC6280 2 years, 4 months ago

Just wanted to strongly echo this sentiment because this is very important. Guys, if you have ever seen or performed a pentest, you know that it can knock over services in production. I've seen it and had to fix it numerous times. So what you're saying when you pick C is "Hey, let's immediately go super invasive and possibly disrupt production even though we have zero idea what normal even is."

Pump the brakes and due the homework first. It's not sexy, but security rarely is.

upvoted 5 times

TheSkyMan 2 years, 9 months ago

Here are my thoughts:

A - this is asset management and won't help with determining a companies security posture.

B - a good thing to do, but won't reveal the security information needed for this scenario.

C - the only answer that could provide needed security information.

D - this sounds good, but performing a new baseline while an unknown security breach is occurring would be useless. Should verify the security posture, fix any issues/vulnerabilities, than perform a new baseline.

upvoted 7 times

uday1985 1 year, 10 months ago

YOu cannot perform a pentest while you don't know whats in your environment!

upvoted 2 times

PTcruiser 2 years, 8 months ago

I dont think C is the answer because it says NEXT in bold meaning you cant just skip straight to the pentest if you dont even know how the network is mapped out. You also have to know whats in scope for a pentest so you wont break a legacy system or violate any agreements if one of your servers are from a MSP, it would be out of scope so you need to map out your network first. Im stuck between A & B but im going with B

upvoted 6 times

Mr_BuCh3th34D 2 years, 6 months ago

I totally agree with you, it seems more logic to review network topology > asset inventory to only afterwards perform pentest, that's the last thing you'll do in order to check a company's security posture.

upvoted 2 times

  **AaronS1990** 2 years, 4 months ago

TheSkyMan how on earth do you figure that knowing what assets you have WON'T help you determine the security posture? Sorry but that's a baffling statement

upvoted 4 times

  **skibby16** Most Recent 1 year, 7 months ago



Selected Answer: B

I say this because the next step to obtain information about the software company's security posture is to review relevant network drawings, diagrams, and documentation. This step helps in understanding the existing network architecture, identifying critical assets, and assessing the overall network design.

By reviewing documentation, you can gather insights into the network topology, the placement of security controls, and potentially identify areas of concern. This step is essential for building an initial understanding of the environment before diving into more invasive activities like penetration testing.



Developing an asset inventory (Option A) is also crucial, but reviewing network drawings and documentation should precede it. Option C (performing penetration tests) may be premature without a clear understanding of the network, and Option D (baselining the network) can come later in the process after initial documentation review and asset identification.

upvoted 1 times

  **Gwatto** 1 year, 8 months ago

"After initial assessment" Why would your NEXT step be to do do inventory assessment to see what systems the company has? How did you know security controls are weak, there must have been an assessment of the current systems

upvoted 1 times

  **Aliyan** 1 year, 10 months ago

Selected Answer: B

Question says "Obtaining information about the software company's security posture" which refers to the process of assessing and understanding the current state of the software company's security measures, practices, and controls. It involves gathering insights into how well the company is protecting its information, systems, and assets from potential threats, vulnerabilities, and attacks.

So



A is wrong because its purpose is to form the basis for future security assessments and controls. (they are not asking to build a secure architecture and prepare and write down all the assets. they simply ask identify what this company has right now)

where

B will help identify existing security controls, even if limited. (plain and simple) you can see whats segmented, is there a firewall in between servers, is there a VPN server and much more.

I know the question also say "based on an initial assessment" but this initial assessment may have involved a cursory review, observation, or examination of the company's security practices, systems, or controls and not the network topology

upvoted 1 times

  **naleenh** 1 year, 10 months ago

Selected Answer: B

Even though the network drawings, diagrams, and documentation are not accurate. Better review the available details. I think immediate next step would be to Review relevant network drawings, diagrams, and documentation.

upvoted 1 times

  **josephconer1** 2 years, 2 months ago

without knowing your ASSETS , you cannot have a baseline, and without a baseline you cannot have security in general.

Start with the basics first especially since you don't know much about the software company. "Initial assessment" is too vague to not go with A. That's my thought at least.

upvoted 2 times

  **tatianna** 2 years, 3 months ago

Developing an asset inventory to determine the systems within the software company would be a logical next step to obtain information about the software company's security posture. This would provide a baseline of the company's hardware and software assets, allowing for a better

understanding of the scope of the security environment and the potential attack surface. From there, more targeted assessments and testing could be conducted to identify vulnerabilities and improve the security posture.

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. This is if Initial assessment = reviewing diagrams, drawings, docs, etc. You absolutely must have asset inventory before you can scope a pentest.

upvoted 2 times

🗳️ 👤 **encxorblood** 2 years, 4 months ago

Selected Answer: A

Answer A - Performing penetration tests against the software company's internal and external networks (option C) is a more aggressive and invasive approach to understanding the security posture of the software company, and should only be done after other less invasive measures have been taken.

upvoted 3 times

🗳️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: A

When perform pentest before have not information about asset is not logical for me. i going with A.

upvoted 3 times

🗳️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: A

Has to be A. You aren't going to be able to perform an effective pentest until you know what the system is

upvoted 2 times

🗳️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: A

Agreeing with the A.'s

upvoted 2 times

🗳️ 👤 **moonash** 2 years, 5 months ago

Selected Answer: A

I would go with A. What would I be pentesting if I don't know the assets. First I need to know what I have i.e. we have cisco switches, fortigate firewall, XYZ servers running on XYZ etc.. then I scan/ pentest the assets.. I can't use pentest to know what I have in the organization. I am going with A all the way

upvoted 3 times

🗳️ 👤 **trainingsmits** 2 years, 5 months ago

Selected Answer: A

They need to establish all of their assets to know what to protect/what is most valuable. A is the first step to take.

upvoted 3 times

🗳️ 👤 **f3lix** 2 years, 5 months ago

Selected Answer: A

Guys, C is the correct answer, the question is "what is the NEXT step that should be completed to OBTAIN INFORMATION ABOUT the software company's security posture", - You'll have to obtain an asset inventory to determine the systems within the software company, since its a newly acquired business - A!

upvoted 1 times

🗳️ 👤 **f3lix** 2 years, 5 months ago

Damn! I mean A is the correct answer**

upvoted 3 times

🗳️ 👤 **roman1000** 2 years, 6 months ago

Selected Answer: A

What are you going to pen test if you don't know your asset?

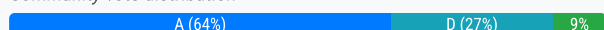
upvoted 3 times

A security analyst identified one server that was compromised and used as a data mining machine, and a clone of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

- A. System timeline reconstruction
- B. System registry extraction
- C. Data carving
- D. Volatile memory analysis

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Ryukendo** Highly Voted 2 years, 8 months ago
My Answer is A

They are asking "provide information about when and how", How does Volatile Memory Analysis Will help here, Cause it only gives us information about how malware works it can't say when or how. On the other hand, TIMELINE RECONSTRUCTION gives us

How was access to the system obtained?

What tools have been installed?

What changes to system files or applications have been made?

What data has been retrieved?

Is there evidence data was exfiltrated over the network or via attached storage?

upvoted 22 times

🗳️ 👤 **2Fish** Most Recent 2 years, 3 months ago

Selected Answer: A

A. A timeline will show the sequence of file system events within a source image and give you the ability to create a graphical representation of the events.

upvoted 1 times

🗳️ 👤 **boletri** 2 years, 3 months ago

Selected Answer: A

Timeline Generation and Analysis

When you have secured a copy of a forensic image, validated from the source by a cryptographic hash, you can start to analyze the information you have captured.

The visual representation of events happening in chronological order is called a timeline, and it can be a powerful tool in your forensics toolkit. Being able to analyze a timeline will give you a holistic perspective of the incident that wouldn't otherwise be possible.

For example, you can list files you find in a computer's web browser cache by their file name, date/time created, date/time last accessed, and date/time last modified.

Comptia Cysa+ Course Material

upvoted 1 times

🗳️ 👤 **encxorblood** 2 years, 4 months ago

Selected Answer: A

herefore, option A is the correct answer. System timeline reconstruction is the process of analyzing system logs, file system metadata, and other sources of information to create a timeline of events that occurred on the compromised machine. By reconstructing the timeline of events, the security analyst can identify the point of compromise, the actions taken by the attacker, and the extent of the compromise. This process can also help identify the location of any malware that may be present on the machine.

upvoted 1 times

🗨️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: A

I am confusing with A and D. Volatile memory analysis is not about with hard drive.... I am going with A.

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: A

By the time a clone of the hard drive would be completed, volatile memory would have already been lost. To provide information about when and how the machine was compromised and where the malware is located using the CLONED HARD DRIVE, you would have to perform a system timeline reconstruction. You cannot do that with volatile memory that was never captured. Answer is A.

upvoted 3 times

🗨️ 👤 **Jeend** 2 years, 5 months ago

Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data

So D Correct

upvoted 1 times

🗨️ 👤 **IT_Master_Tech** 2 years, 6 months ago

I don't even find what system timeline reconstruction is...so I go with D.

upvoted 2 times

🗨️ 👤 **trojan123** 2 years, 6 months ago

Selected Answer: A

⌚ Timeline Generation- Timeline- a tool that shows the sequence of file system events within a source image in a graphical format. Timelines can help the analyst understanding how access to the system was obtained, what tools were installed, what changes to files were made, what data was exfiltrated (if it was exfiltrated) and more. Many forensic tools generate a timeline.

upvoted 4 times

🗨️ 👤 **lordguck** 2 years, 6 months ago

C: As far as I remember, securing evidence it done from most fleeting media (memory) to the more stable ones. As a disk clone was created, a memory dump was saved before that. So the next step is to use data carving (memory dump & clone data).

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: A

After some search on timeline reconstruction, the answer seems A. Also, I agree with Ryukendo's claim.

upvoted 2 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

From my understanding, volatile memory analysis is to gain knowledge about any malicious processes currently running and what it's doing. From the question it seems the company already understands that the server was used for data mining. and I don't believe volatile memory analysis is done on clones of the drive but the drive itself once confiscated. Could be wrong, but I think A is the right answer here

upvoted 1 times

🗨️ 👤 **gwanedm** 2 years, 8 months ago

Because the question says "a clone of the hard drive was created" is excludes B and D. I would go with A because it gives date and time details

upvoted 1 times

🗨️ 👤 **Adrian831** 2 years, 8 months ago

but how about "how the machine was compromised and where the malware is located?" The A gives that too? I don't think so.

D is still valid here.

upvoted 1 times

🗨️ 👤 **ExamTopicsDiscussor** 2 years, 8 months ago

Adrian, how would you find that IN VOLATILE MEMORY? You can MAYBE find the malware in memory, but do you think the malware has historical logs stored in its executable code? No, it doesn't.

upvoted 3 times

🗨️ 👤 **jchutch2** 2 years, 8 months ago

Selected Answer: C

Definitely data carving

upvoted 2 times

🗨️ 👤 **Adrian831** 2 years, 8 months ago

Definitely not C.

D seems correct to me.

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 9 months ago

Selected Answer: D

pulled from chegg

Option D is correct

Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

upvoted 4 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: D

I would have to say D. I looked through 3 different CySa books and only memory analysis makes sense. <https://www.varonis.com/blog/memory-forensics>

upvoted 2 times

🗨️ 👤 **nonjabusiness** 2 years, 9 months ago

Not sure, but I think B is correct

upvoted 1 times

A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?

- A. A TXT record on the name server for SPF
- B. DNSSEC keys to secure replication
- C. Domain Keys Identified Mail
- D. A sandbox to check incoming mail

Suggested Answer: C

Community vote distribution

C (82%)

A (18%)

🗳️ 👤 **ThisGuyStillLearning** Highly Voted 👍 2 years, 9 months ago

In a nutshell, SPF allows email senders to define which IP addresses are allowed to send mail for a particular domain. DKIM on the other hand, provides an encryption key and digital signature that verifies that an email message was not forged or altered.

upvoted 11 times

🗳️ 👤 **RobV** Most Recent 🕒 1 year, 6 months ago

Selected Answer: C

C. Domain Keys Identified Mail

upvoted 1 times

🗳️ 👤 **buchhe** 1 year, 10 months ago

Selected Answer: C

DMARC (domain-based message authentication, reporting, and conformance) and DKIM (domain keys identified mail) are configurations that are performed on a DNS server to verify whether email being sent by a third-party is verified to send it on behalf of the organization.

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. If an attacker tries to impersonate an email address from a domain that has implemented DKIM, the digital signature will not match the public key in the DNS records, and the email will be flagged as suspicious or rejected by the recipient's email server.

upvoted 2 times

🗳️ 👤 **absabs** 2 years, 4 months ago

If SPF record set correctly, everybody sends mail. first thing is DKIM, when about impersonating. SPF more related about whether mail sending

upvoted 3 times

🗳️ 👤 **TeyMe** 2 years, 7 months ago

Selected Answer: A

Sender Policy Framework (SPF) uses a DNS record published by an organization hosting email service. The SPF record—there must be only one per domain—identifies the hosts authorized to send email from that domain.

VS

DomainKeys Identified Mail (DKIM) provides a cryptographic authentication mechanism. This can replace or supplement SPF.

upvoted 2 times

🗳️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: C

C is the best answer

upvoted 3 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C



C should be the correct answer

upvoted 1 times

🗳️ 👤 **Laudy** 2 years, 9 months ago



definitely DKIM

upvoted 3 times

  **Laudy** 2 years, 9 months ago

SPF lets you authorize senders that are allowed to send email on behalf of your domain. DKIM signs every outgoing message with your unique signature, so receiving servers can verify the message came from you. SPF and DKIM let receiving servers verify that messages that appear to be from your domain are legitimate.

upvoted 2 times

  **Laudy** 2 years, 9 months ago

[https://netcorecloud.com/tutorials/spf-dkim-](https://netcorecloud.com/tutorials/spf-dkim-dmarc/#:~:text=SPF%20DKIM%20and%20DMARC%20are,sending%20emails%20through%20your%20domain.)

[dmarc/#:~:text=SPF%20DKIM%20and%20DMARC%20are,sending%20emails%20through%20your%20domain.](https://netcorecloud.com/tutorials/spf-dkim-dmarc/#:~:text=SPF%20DKIM%20and%20DMARC%20are,sending%20emails%20through%20your%20domain.)

upvoted 1 times

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website. Which of the following would be the MOST appropriate recommendation to prevent similar activity from happening in the future?

- A. An IPS signature modification for the specific IP addresses
- B. An IDS signature modification for the specific IP addresses
- C. A firewall rule that will block port 80 traffic
- D. Implement a web proxy to restrict malicious web content

Suggested Answer: C

Community vote distribution

D (84%)

A (16%)

PatrickC_IT **Highly Voted** 2 years, 9 months ago

Selected Answer: D

I chose D:

A - IPS could prevent an intrusion, but this shows that it's going from internal to external.

B - IDS does nothing to prevent intrusions, only detects.

C - Overkill. You don't want to block ALL http traffic.

D - The web proxy can make a more intelligent decision on if a site is malicious or not and can block accordingly. Proxies often can update automatically as well, so they can keep on top of potentially malicious locations.

upvoted 20 times

Laudy **Highly Voted** 2 years, 9 months ago

Blocking all port 80 seems detrimental. There's many other ports too....

I feel you should add an IPS signature modification for the specific IP addresses/domains that the host is trying to beacon to.

Any other takes? Am I missing something?

upvoted 5 times

ProNerd 1 year, 11 months ago

Blocking 80 isn't an option. IDS and IPS are for inbound traffic, not outbound. Only a web proxy can be the solution.

upvoted 1 times

Junior24 **Most Recent** 1 year, 9 months ago

D is correct

upvoted 1 times

2Fish 2 years, 3 months ago

Selected Answer: D

D. This is the Best answer here, IPS and IDS are ingress and reactive, not a proactive approach.

upvoted 3 times

encorblood 2 years, 4 months ago

Selected Answer: A

Therefore, option D is the correct answer. A web proxy can be used to inspect and filter all web traffic, allowing the security team to block access to known malicious websites and to detect and block attempts to exfiltrate data from the organization. By implementing a web proxy, the organization can prevent similar suspicious activity from occurring in the future, and better protect its sensitive data.

upvoted 1 times

forest111 2 years, 7 months ago

Selected Answer: D

there wasn't mention port 80

upvoted 1 times

MortG7 2 years, 8 months ago

Selected Answer: D

I agree with D.

IPS - Intrusion (Ingress traffic)

IDS - Intrusion (ingress traffic)

The direction of this traffic is from an internal IP outbound. So it cannot be either of the above. Blocking port 80 blocks everyone and at all times (not just off hours and weekends)

upvoted 1 times

🗨️ 👤 **Ryukendo** 2 years, 8 months ago

Selected Answer: D

I chose D

It says internal IP to an external website, not external IP.

I could just use a web proxy to restrict access

upvoted 1 times

🗨️ 👤 **gwanedm** 2 years, 8 months ago

D makes more sense

upvoted 3 times

🗨️ 👤 **Fastyt0p** 2 years, 9 months ago

Selected Answer: A

A- An IPS signature modification for the specific IP addresses.

upvoted 1 times

🗨️ 👤 **A_Shadows_Soul** 2 years, 8 months ago

Problem is its internal going to external. IPS doesn't stop that.

Process of elimination says D

upvoted 2 times

🗨️ 👤 **cyberseckid** 2 years, 9 months ago

Im feeling D , you don't want to block only a specific website but all malicious websites , not sure though.

upvoted 2 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

A is the BEST choice.

upvoted 3 times

🗨️ 👤 **Treymb6** 2 years, 9 months ago

What type of intrusion are you preventing when it was internal to external??

upvoted 7 times

🗨️ 👤 **maxi99** 2 years, 9 months ago

Blocking Port 80 makes no sense. Adding an IPS signature for that IP makes more sense.

upvoted 3 times

A company frequently experiences issues with credential stuffing attacks. Which of the following is the BEST control to help prevent these attacks from being successful?

- A. SIEM
- B. IDS
- C. MFA
- D. TLS

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. None of the other answers are even close.
upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

C is the right answer.
upvoted 1 times

🗳️ 👤 **maxi99** 2 years, 9 months ago

ANS - C | Credential stuffing is testing username/password pairs obtained from the breach of another site and it is an authentication-related attack. Hence MFA is correct.
upvoted 2 times

🗳️ 👤 **Laudy** 2 years, 9 months ago

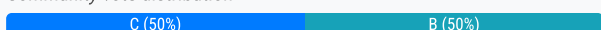
C. Multi Factor Authentication (MFA)
upvoted 3 times

Company A is in the process of merging with Company B. As part of the merger, connectivity between the ERP systems must be established so pertinent financial information can be shared between the two entities. Which of the following will establish a more automated approach to secure data transfers between the two entities?

- A. Set up an FTP server that both companies can access and export the required financial data to a folder.
- B. Set up a VPN between Company A and Company B, granting access only to the ERPs within the connection.
- C. Set up a PKI between Company A and Company B and intermediate shared certificates between the two entities.
- D. Create static NATs on each entity's firewalls that map to the ERP systems and use native ERP authentication to allow access.

Suggested Answer: B

Community vote distribution



🗳️ 👤 **zecomeia_007** 11 months ago

Selected Answer: B

Given the context of secure data transfers between ERPs during a merger, I recommend Option B: Set up a VPN. It provides a secure, automated connection between the two entities' systems while limiting access to authorized ERPs.

upvoted 1 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: C

C. Set up a PKI between Company A and Company B and intermediate shared certificates between the two entities.

upvoted 1 times

🗳️ 👤 **edro** 1 year, 7 months ago

They can both be automated when setup well.

VPN focuses on securing a tunnel, a communication path

Keys and certificates primary use case is the protection of data itself

upvoted 1 times

🗳️ 👤 **kyw5** 1 year, 7 months ago

B. I think B and C both work but the question is asking for a more 'AUTOMATED' approach. VPN is more automated and easier to set up

upvoted 1 times

🗳️ 👤 **AhmedSameer** 1 year, 8 months ago

I donno both A or B are correct ! what a stupid question..

upvoted 3 times

🗳️ 👤 **AbdallaAM** 1 year, 8 months ago

Selected Answer: B

B. Set up a VPN between Company A and Company B, granting access only to the ERPs within the connection.

Establishing a Virtual Private Network (VPN) between Company A and Company B would create a secure, encrypted communication channel between the two entities. Restricting access only to the Enterprise Resource Planning (ERP) systems within this secure connection minimizes the risk of unauthorized access and provides a relatively automated,

upvoted 1 times

🗳️ 👤 **kumax** 1 year, 9 months ago

Selected Answer: C

ChatGPT:

Implementing a Public Key Infrastructure (PKI) between Company A and Company B, along with intermediate shared certificates, is an excellent approach to ensure secure and authenticated communication and data exchange between the two entities. Here's how this setup works and the benefits it provides:

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 8 months ago

Where a few days ago CHATGPT said C, today it says B. Please, look for other sources

upvoted 4 times

🗨️ **dhdrms** 1 year, 7 months ago

ChatGPT is unreliable.

upvoted 2 times

🗨️ **Junior24** 1 year, 9 months ago

Keyword is secure data transfer, why would you not implement a VPN?!!

upvoted 3 times

🗨️ **naleenh** 1 year, 10 months ago

Selected Answer: C

"Automated Approach" is the keyword for the answer.

upvoted 2 times

🗨️ **sudoptgoaway** 1 year, 9 months ago

Key exchanges happen behind the scenes and typically do not involve users interaction. It's C.

upvoted 1 times

🗨️ **Aliyan** 1 year, 11 months ago

Selected Answer: C

This gotta be C bro what ???

upvoted 3 times

🗨️ **ksr933** 2 years, 2 months ago

How about the wording "more automated approach"? Isn't the VPN require manual transfer?

upvoted 2 times

🗨️ **TAC45** 1 year, 7 months ago

A site to site VPN connection differs from a Host to Site VPN where the user would have to manually connect.

upvoted 1 times

🗨️ **2Fish** 2 years, 3 months ago

Selected Answer: B

Obviously B. This the preferred method to connect in this situation.

upvoted 1 times

🗨️ **MrRobotJ** 2 years, 7 months ago

Selected Answer: B

Indeed B

upvoted 1 times

🗨️ **TheStudiosPeepz** 2 years, 8 months ago

Selected Answer: B

Secure Data transfer = VPN = B

upvoted 1 times

🗨️ **amateurguy** 2 years, 9 months ago

Selected Answer: B

Go with B

upvoted 2 times

🗨️ **Laudy** 2 years, 9 months ago

Agreed. B

upvoted 2 times

After an incident involving a phishing email, a security analyst reviews the following email access log:

DATE	TIME	USER	IP	LOCATION	ACTION
08262020	09:25:03	CARLB	93.12.56.200	USA	PERMIT
08262020	09:25:03	CINDYP	102.45.97.212	ITALY	DENY
08262020	09:25:04	CINDYP	54.90.11.65	CHINA	DENY
08262020	09:25:05	GILLIANO	42.176.23.77	GERMANY	PERMIT
08262020	09:26:30	ANDREAD	12.45.87.2	USA	PERMIT
08262020	10:30:12	CINDYP	54.56.32.12	CHINA	DENY
08262020	10:31:54	ANDREAD	102.45.97.212	ITALY	PERMIT
08262020	11:02:01	LAURAB	231.2.45.21	ENGLAND	PERMIT
08262020	11:02:45	LAURAB	102.43.77.43	USA	DENY

Based on this information, which of the following accounts was MOST likely compromised?

- A. CARLB
- B. CINDYP
- C. GILLIANO
- D. ANDREAD
- E. LAURAB

Suggested Answer: D

Community vote distribution

D (83%)

B (17%)

TKW36 Highly Voted 2 years, 5 months ago

Selected Answer: D

D. ANDREAD. The reason she was most likely compromised is because of her impossible travel time from Italy to USA and she was PERMITTED access both times. LauraB is not compromised because yes, while she did travel from England to USA in 45 seconds, one login attempt was DENIED! So it's safe to assume one was the REAL Laura and one was a bad actor logging in at about the same time.

upvoted 12 times

Lilik Most Recent 10 months, 3 weeks ago

D is the correct answer due to the fact that the access was permitted 2 times from different locations.

upvoted 1 times

RobV 1 year, 6 months ago

Selected Answer: D

D. ANDREAD

upvoted 1 times

JimmyJams 1 year, 11 months ago

Selected Answer: B

If these are email 'access' logs from O365 I might expect to see users appear to connect from different regions depending on the resources that they are accessing but I would not expect access attempts from CHINA if I was based in the west, which I am.

CINDYP is seen accessing email from USA which is permitted then a second later seen logging in from CHINA for which the access is DENIED.

As a security analyst this would be the FIRST log entry I would query. Why are we seeing failed login attempts into CINDYP's account from CHINA?

upvoted 3 times

2Fish 2 years, 3 months ago

Selected Answer: D

D. For reasons already stated here.

upvoted 1 times

🗨️ 👤 **kabhatti** 2 years, 6 months ago

I guess the chance Andrea connecting to a corporate IP or a VPN is not part of the information provided in the question eh
upvoted 2 times

🗨️ 👤 **maxi99** 2 years, 9 months ago

1hr:05mins difference in time for Andread is an impossible travel time, hence the user is compromised.
upvoted 1 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

what about the 45 seconds it took LauraB to get from England to the U.S.? she was also denied her second attempt, what am I missing here?
upvoted 1 times

🗨️ 👤 **TheStudiosPeepz** 2 years, 8 months ago

Laura was Denied on "her" second attempt. Real Laura was permitted, Fake Laura got denied.
upvoted 4 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

I see, makes sense. dumb mistake on my part, thanks
upvoted 1 times

🗨️ 👤 **TheStudiosPeepz** 2 years, 8 months ago

Andrea was Permitted on her second attempt, she wasn't denied.
upvoted 3 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: D

andread - D is the answer.
upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

1hr travel time to Italy? lol. Definitely D, ANDREAD.
upvoted 2 times

An organization wants to ensure the privacy of the data that is on its systems. Full disk encryption and DLP are already in use. Which of the following is the BEST option?

- A. Require all remote employees to sign an NDA.
- B. Enforce geofencing to limit data accessibility.
- C. Require users to change their passwords more frequently.
- D. Update the AUP to restrict data sharing.

Suggested Answer: A

Community vote distribution



Henry88 Highly Voted 2 years, 4 months ago

Why do so many of these questions have such conflicting answers? I am more confused now than ever before since I started studying for CYSA 5 months ago. Maybe I shouldn't even bother.

upvoted 13 times

kill_chain 2 years ago

did you end up writing?

upvoted 3 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: B

B. Enforce geofencing to limit data accessibility.

Reasoning:

Geofencing allows the organization to define geographical boundaries where data can be accessed, adding an extra layer of control.

It complements existing security measures by restricting access based on the physical location of the user or device.

This measure is particularly effective for remote employees or devices accessing sensitive data.

upvoted 1 times

dickchappy 1 year, 7 months ago

Selected Answer: B

It's crazy to me that people are saying NDA and AUP when those are DETERRENTS, they do not actually prevent anything. Geofencing is the correct answer.

upvoted 1 times

AbdallaAM 1 year, 8 months ago

Selected Answer: D

D. Update the AUP (Acceptable Use Policy) to restrict data sharing.

Modifying the AUP to clearly define and restrict data sharing practices, coupled with ongoing user training and awareness programs, helps in establishing organizational norms and expectations regarding data privacy. It can regulate how data should be handled, shared, and processed by the employees, providing a policy framework that supports the technical measures (like DLP and encryption) in place.

upvoted 1 times

kumax 1 year, 9 months ago

Selected Answer: D

ChatGPT: go for Acceptable Use Policy

AUP covers more than geofencing.

upvoted 1 times

5H4K1R 1 year, 7 months ago

ChatGPT: B. Enforce geofencing to limit data accessibility.

Explanation: Geofencing is a technology that uses GPS or RFID to create a virtual geographic boundary. By implementing geofencing, an organization can restrict access to sensitive data based on the physical location of the user or device. This additional layer of security

complements full disk encryption and DLP (Data Loss Prevention) measures. It helps ensure that data can only be accessed from specific geographical locations, adding an extra dimension to data protection.

upvoted 1 times

🗳️ 👤 **Big_Dre** 1 year, 10 months ago

Selected Answer: B

perimeter security or geo fencing is the only possible next step.

upvoted 1 times

🗳️ 👤 **kyky** 2 years ago

Selected Answer: D

D. Update the AUP to restrict data sharing.

upvoted 2 times

🗳️ 👤 **kyky** 2 years ago

While full disk encryption and DLP (Data Loss Prevention) are already in use, they provide protection against data loss or leakage. However, updating the AUP adds an additional layer of policy-based control specifically targeting data sharing, thus enhancing the organization's data privacy measures

upvoted 2 times

🗳️ 👤 **nedeajob12** 2 years, 2 months ago

Selected Answer: D

the BEST option to ensure the privacy of data on an organization's systems that already have full disk encryption and DLP in use is to update the Acceptable Use Policy (AUP) to restrict data sharing.

upvoted 3 times

🗳️ 👤 **AI75diablo** 2 years, 3 months ago

DLP and Encryption are sound technical controls that ensure data protection (which would include the Privacy). As mentioned below they are looking for a Managerial control, which would point to "Company Policy" - AUP: This would cover the organisation with sharing of information due to the consequences that will be imposed (even legal).

Answer should be D in my opinion

upvoted 1 times

🗳️ 👤 **tatianna** 2 years, 3 months ago

B. Enforce geofencing to limit data accessibility would be the BEST option to ensure the privacy of the data that is on the organization's systems. Geofencing technology can help restrict access to sensitive data from outside certain geographic locations, which can help prevent unauthorized access to the data. This is a strong control that can help prevent both accidental and intentional unauthorized access to sensitive data, and it is often used in combination with other security measures like full disk encryption and DLP. While NDAs, password policies, and AUPs can help protect data privacy in certain circumstances, they are not as effective at preventing unauthorized access as geofencing.

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. geofencing can restrict access to data based on the geographic location of the user or device, helping to prevent unauthorized access or data leakage. It is the best option to complement the existing security measures and ensure data privacy.

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Changing my answer to D. After more research and reading the comments, D does seem to be what this question is looking for.

upvoted 2 times

🗳️ 👤 **Jolnn** 2 years, 3 months ago

Selected Answer: A

This question is making it pretty clear that they are after managerial controls, since technicals are in place and seems to be working fine. A is clearly the correct answer.

upvoted 2 times

🗳️ 👤 **jleonard_ddc** 2 years, 3 months ago

Selected Answer: B

Privacy of data is a concern of who is accessing it. NDA's are more of a legal protection against the data itself being exposed by people who already have access.

Geofencing would further help limit who can access it.

upvoted 1 times

🗨️ 👤 **talosDevbot** 2 years, 4 months ago

Selected Answer: D

I would go with D, because of the keyword "privacy" in the question.

If it asked how to ensure the SECURITY, then I would pick B

upvoted 2 times

🗨️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: D

A and C not necessarily. i am confusing B and D, but D is most correct i think.

upvoted 2 times

🗨️ 👤 **10cccordrazine** 2 years, 4 months ago

Selected Answer: D

I think it's D. Exam guide book, privacy is about the control the user has over who their data is shared with.

A is weird because only references remote workers. B could help, but you already have DLP, and doesn't relate as much to privacy as D, I feel.

upvoted 3 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: B

B is the only one that will actually ensure that people can't do it. Signing an NDA for example is simply them saying they won't disclose information, it doesn't actually seal their lips

upvoted 2 times

An organization has specific technical risk mitigation configurations that must be implemented before a new server can be approved for production. Several critical servers were recently deployed with the antivirus missing, unnecessary ports disabled, and insufficient password complexity. Which of the following should the analyst recommend to prevent a recurrence of this risk exposure?

- A. Perform password-cracking attempts on all devices going into production
- B. Perform an Nmap scan on all devices before they are released to production
- C. Perform antivirus scans on all devices before they are approved for production
- D. Perform automated security controls testing of expected configurations prior to production

Suggested Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: D

D. Some questions make sense.. others... not so much.
upvoted 3 times

🗲️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: D

Pretty straightforward The issues are:
Antivirus missing
Unnecessary ports disabled
Insufficient password complexity

- A- Addresses Insufficient password complexity
- B- Addresses Unnecessary ports disabled
- C- Addresses Antivirus missing

D- Create a baseline and test for the lot. Answer, D
upvoted 3 times

🗲️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: D

D seems like the most intelligent option.
upvoted 2 times

🗲️ 👤 **Laudy** 2 years, 9 months ago

D is correct
upvoted 3 times

Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?

- A. Remote code execution
- B. Buffer overflow
- C. Unauthenticated commands
- D. Certificate spoofing

Suggested Answer: A

Community vote distribution

C (100%)

🗳️ **david124** Highly Voted 2 years, 8 months ago

c it is, coming from someone who works in automotive cybersecurity
upvoted 5 times

🗳️ **nomad421** Most Recent 2 years, 1 month ago

This is a horrible question. Almost all could be the answer:

Another vulnerability is due to lack of sufficient security checks in the MODBUS/TCP protocol implementation. The protocol specification does not include an authentication mechanism for validating communication between MODBUS master and slave devices. This flaw could allow an unauthenticated, remote attacker to issue arbitrary commands to any slave device via a MODBUS master.

An attacker creates a specially crafted packet longer than 260 bytes and sends it to a MODBUS client and server. If the client or server were programmed incorrectly, this could lead to a successful buffer overflow or denial-of-service attack.

The easiest attack to use against Modbus is to simply sniff the traffic on a network, find the Modbus devices and then issue harmful commands to the Modbus devices.

<https://www.radiflow.com/blog/hack-the-modbus/>

upvoted 2 times

🗳️ **2Fish** 2 years, 3 months ago

Selected Answer: C

C. Remote code execution, buffer overflow, and certificate spoofing attacks require more expertise and time to carry out successfully. However, unauthenticated commands pose the greatest likelihood of quick success against Modbus assets.
upvoted 2 times

🗳️ **Stiobhan** 2 years, 4 months ago

I am going to sway for A here. To be honest all of them are plausible
<https://resources.infosecinstitute.com/topic/ics-scada-threats-and-threat-actors/>
upvoted 2 times

🗳️ **Joshgip95** 2 years, 4 months ago

100% C and you choose A? Stop throwing people off.
upvoted 4 times

🗳️ **Stiobhan** 2 years, 3 months ago

At least I have some backup to what is only my opinion so don't nail me to the cross so easily my friend. On reflection, reading through TheSkyMan's resource it also stands a good chance of being C. Too many sheep on here mate that want to memorize answers and pass an exam, I am old school and need to know the why!! So if you are going to swear by an answer, have something to back it up with because other than that your statement is on subjective.
upvoted 4 times

🗳️ **HNICA** 2 years, 6 months ago

Modbus messages can also be sent over Ethernet or TCP/IP. Remote code execution (RCE) attacks allow an attacker to remotely execute malicious code on a computer. The impact of an RCE vulnerability can range from malware execution to an attacker gaining full control over a compromised

machine.

upvoted 2 times

  **haykaybam** 2 years, 8 months ago

Selected Answer: C

I go with Option C has it tends more towards one of the vulnerabilities of Modbus systems - authentication.

There is no authentication method for the Modbus TCP protocol to verify communication between MODBUS master and slave devices. A remote, unauthenticated attacker might take advantage of this exploit to send arbitrary commands through a MODBUS master to any slave device.

upvoted 2 times

  **Adrian831** 2 years, 9 months ago

Selected Answer: C

C should be the correct one.

upvoted 2 times

  **TheSkyMan** 2 years, 9 months ago

I'm leaning toward C. The Modbus protocol lacks security and heavily relies on command input (i.e. diagnostic commands).

<https://www.radiflow.com/blog/hack-the-modbus/>

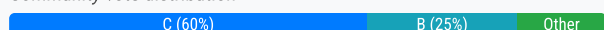
upvoted 4 times

A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

- A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.
- B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.
- C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.
- D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

Suggested Answer: C

Community vote distribution



🗳️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: C

C: the best approach is to utilize the CASB to enforce DLP (Data Loss Prevention) data-in-motion protection for financial information moving to the cloud.

upvoted 1 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

The company has decided not to store financial information in the cloud, so the risk of financial data leakage into the cloud is specifically related to data in motion

upvoted 1 times

🗳️ 👤 **OnA_Mule** 2 years, 3 months ago

Selected Answer: C

It's data in motion, so A+D are obviously out. I initially thought that it would be B, since the data doesn't reside in the cloud, but after doing more research, it appears that CASB can also scan data in transit to identify sensitive information and apply policy controls to prevent it from being stored in unapproved cloud services or locations.

upvoted 2 times

🗳️ 👤 **[Removed]** 2 years, 3 months ago

Selected Answer: C

Certainly C. We are still using a DLP, but ensuring that data-in-motion protection is being reinforced during any transactions between on-site and cloud.

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. I really wanted to say B, but CASB can be used to protect Data in motion from on-prem to cloud. CASB can also apply DLP policies to encrypted traffic, which is important as more and more cloud applications are using encrypted traffic by default.

upvoted 1 times

🗳️ 👤 **jleonard_ddc** 2 years, 3 months ago

Selected Answer: B

We need to protect data in motion ("leakage into the cloud"). This eliminates options A and D. The company does not store data in the cloud, so we need to use DLP to ensure it never reaches there.

WRONG ANSWERS

- A – The company is looking to protect data from moving to the cloud, not data at rest. Furthermore, data is not in the cloud at all so a CASB is not appropriate.
- C – CASBs can leverage DLP for protection, but the company is not storing data in the cloud so it's not likely a CASB would help.
- D – DLP would help their cause since data is not in the cloud, but they want to stop data in motion (not at rest)

upvoted 2 times

🗳️ 👤 **Jolnn** 2 years, 3 months ago

I think CASB would help in this case, by blocking the data-in-motion from trying to enter the cloud. I think C is correct.

upvoted 2 times

🗳️ 👤 **knister** 2 years, 5 months ago

Selected Answer: B

I am going for B here. The reason is that CASB is useless since you have this data on premises. The DLP solution will avoid the data to be uploaded to the cloud. CASB will not help avoid this.

upvoted 2 times

🗳️ 👤 **OnA_Mule** 2 years, 3 months ago

Actually, a CASB DLP solution can also scan data in transit to identify sensitive information and apply policy controls preventing it from being stored in the cloud. So CASB does in fact help here too.

upvoted 1 times

🗳️ 👤 **prntscrn23** 2 years, 6 months ago

Selected Answer: C

Voting for C as the concern is data leakage while data in motion not at rest. Also, the company does not like to store data in the cloud.

upvoted 1 times

🗳️ 👤 **Cizzla7049** 2 years, 7 months ago

Selected Answer: B

Should be B. DLP will monitor and stop data in motion if there is financial info going to the cloud.

upvoted 1 times

🗳️ 👤 **TheStudiosPeepz** 2 years, 7 months ago

Selected Answer: C

You need CASB and the problem is only concerned with data in motion. Hence C

upvoted 1 times

🗳️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: C

Answer C is correct. Financial info is not stored in the cloud, but their concern the financial infos leakage into the cloud. This is not the data at rest, but data in motion. To mitigate financial infos leakage into cloud, company needs to utilize CASB to enforce/implement DLP for data-in-motion. So, the answer C is right.

upvoted 4 times

🗳️ 👤 **david124** 2 years, 8 months ago

Selected Answer: A

A it is

upvoted 1 times

🗳️ 👤 **gingham_gansta** 2 years, 7 months ago

You need to provide some more justifications for your answers - you're often contrary to the consensus and *wrong*.

upvoted 1 times

🗳️ 👤 **david124** 2 years, 7 months ago

My Apologies, i answered this for the wrong question

upvoted 1 times

🗳️ 👤 **buchhe** 2 years, 8 months ago

A! is the answer in my understanding of the question. The question is not for the data in motion but about storing company's sensitive data in the cloud and mitigating leakage.

upvoted 1 times

🗳️ 👤 **forklord72** 2 years, 8 months ago

But the question is concerning data leaking into the cloud, meaning the financial data not being stored there at all.

upvoted 2 times

🗳️ 👤 **forklord72** 2 years, 8 months ago

Selected Answer: D

My thought process: I don't think it can be A or C since this issue concerns data in motion. CASB does implement DLP but I have no idea if that concerns data moving from the cloud only or from company premises as well. I think D is the safest answer here.

upvoted 2 times

🗳️ 👤 **forklord72** 2 years, 8 months ago

Correction: Can't be A or D. Meant to vote for B.

upvoted 1 times

  **rv438360** 2 years, 8 months ago

answer should be A

upvoted 4 times

  **TheSkyMan** 2 years, 9 months ago

Answer looks right.

"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."

<https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solution/>

upvoted 4 times

  **MacherNewSrCyberSecAnal** 2 years, 2 months ago

The answer to the question is base64

"RIVDSyBGVUNLIEZVQ0sgRIVDSyBGVUNLIEZVQ0sgRIVDSyBGVUNLIEZVQ0sgRIVDSyA="

upvoted 1 times

A security administrator needs to provide access from partners to an isolated laboratory network inside an organization that meets the following requirements:

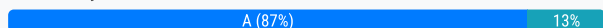
- * The partners' PCs must not connect directly to the laboratory network
- * The tools the partners need to access while on the laboratory network must be available to all partners
- * The partners must be able to run analyses on the laboratory network, which may take hours to complete

Which of the following capabilities will MOST likely meet the security objectives of the request?

- A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
- B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis
- C. Deployment of a firewall to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
- D. Deployment of a jump box to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis

Suggested Answer: A

Community vote distribution



🗳️ 👤 **2Fish** Highly Voted 2 years, 3 months ago

Selected Answer: A

A. Option A meets the requirement that partners' PCs must not connect directly to the laboratory network by using a jump box as an intermediary. Using a VDI in persistent mode provides partners with access to the necessary tools for analysis, while also allowing for the long-running analyses to continue uninterrupted. This option also meets the requirement that the tools must be available to all partners.

upvoted 5 times

🗳️ 👤 **skibby16** Most Recent 1 year, 6 months ago

Selected Answer: D

A VDI can operate in two modes: persistent and non-persistent. In persistent mode, each user has a dedicated virtual desktop that retains its settings and data across sessions. In non-persistent mode, each user has a temporary virtual desktop that is deleted or reset after each session³. In this scenario, deploying a jump box to allow access to the laboratory network and using VDI in non-persistent mode can meet the security objectives of the request. The jump box can prevent the partners' PCs from connecting directly to the laboratory network and reduce the risk of unauthorized access or compromise. The VDI in non-persistent mode can provide the necessary tools for analysis without storing any data on the partners' PCs or the virtual desktops. The VDI in non-persistent mode can also allow the partners to run long analyses without losing their progress or results.

upvoted 1 times

🗳️ 👤 **skibby16** 1 year, 8 months ago

Selected Answer: D

Non-Persistent VDI: Non-persistent VDI means that the virtual desktops are temporary and reset to a known clean state after each use. This is ideal for security because it ensures that no changes or potential compromises persist between sessions. Any malware or unwanted changes are discarded upon logoff, maintaining a clean environment.

upvoted 1 times

🗳️ 👤 **kyky** 2 years ago

Selected Answer: A

definitely A, Yes

upvoted 1 times

🗳️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: A

Persistent means; all data keep on system when you dont delete it. 3th sentence adress this point.

upvoted 3 times

🗳️ 👤 **BABrendan** 2 years, 6 months ago

Why persistent over non?

upvoted 1 times

🗨️ 👤 **f3lix** 2 years, 5 months ago

+1 - T'will be nice to have answer to this

upvoted 1 times

🗨️ 👤 **f3lix** 2 years, 5 months ago

Review this link:

[https://www.parallels.com/blogs/ras/persistent-vdi-vs-non-](https://www.parallels.com/blogs/ras/persistent-vdi-vs-non-persistent/#:~:text=Persistent%20VDIs%20are%20full%2Dsize,at%20will%20on%20the%20VMs)

[persistent/#:~:text=Persistent%20VDIs%20are%20full%2Dsize,at%20will%20on%20the%20VMs](https://www.parallels.com/blogs/ras/persistent-vdi-vs-non-persistent/#:~:text=Persistent%20VDIs%20are%20full%2Dsize,at%20will%20on%20the%20VMs).

upvoted 1 times

🗨️ 👤 **MrRobotJ** 2 years, 7 months ago

Selected Answer: A

Going with A

upvoted 1 times

🗨️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: A

[https://www.parallels.com/blogs/ras/persistent-vdi-vs-non-](https://www.parallels.com/blogs/ras/persistent-vdi-vs-non-persistent/#:~:text=Persistent%20VDIs%20are%20full%2Dsize,at%20will%20on%20the%20VMs)

[persistent/#:~:text=Persistent%20VDIs%20are%20full%2Dsize,at%20will%20on%20the%20VMs](https://www.parallels.com/blogs/ras/persistent-vdi-vs-non-persistent/#:~:text=Persistent%20VDIs%20are%20full%2Dsize,at%20will%20on%20the%20VMs).

upvoted 1 times

🗨️ 👤 **EVE12** 2 years, 9 months ago

Selected Answer: A

<https://www.techtarget.com/searchvirtualdesktop/feature/Understanding-nonpersistent-vs-persistent-VDI>

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

Agree. A is correct.

upvoted 2 times

The incident response team is working with a third-party forensic specialist to investigate the root cause of a recent intrusion. An analyst was asked to submit sensitive network design details for review. The forensic specialist recommended electronic delivery for efficiency, but email was not an approved communication channel to send network details. Which of the following BEST explains the importance of using a secure method of communication during incident response?

- A. To prevent adversaries from intercepting response and recovery details
- B. To ensure intellectual property remains on company servers
- C. To have a backup plan in case email access is disabled
- D. To ensure the management team has access to all the details that are being exchanged

Suggested Answer: B

Community vote distribution

A (88%)

13%

🗳️ 👤 **Laudy** Highly Voted 🏆 2 years, 9 months ago

Disagree. I think this is "A. To prevent adversaries from intercepting response and recovery details"
upvoted 14 times

🗳️ 👤 **TheSkyMan** 2 years, 9 months ago

I'm with you on that. A is the best answer.
upvoted 2 times

🗳️ 👤 **FEITH** Most Recent 🕒 10 months ago

Definetly A !
upvoted 1 times

🗳️ 👤 **Gwatto** 1 year, 8 months ago

Selected Answer: A

Option B isn't completely ruled out but in the case of "Secure method of communication" b has nothing to do with that.
upvoted 1 times

🗳️ 👤 **Big_Dre** 1 year, 10 months ago

Selected Answer: A

i think A is the bet option
upvoted 1 times

🗳️ 👤 **Jolnn** 2 years, 2 months ago

Selected Answer: B

The reason why B is the correct one in this case is because we are not referring to general best practice. It specifically mentions that the data they have been asked to submit is sensitive network design details, so it has nothing to do with the way they are conducting incident response. The end of this question should have said BEST in this scenario, but it only implies it without specifying. So it's B.
upvoted 1 times

🗳️ 👤 **alayeluwa** 2 years, 2 months ago

Nah foo
upvoted 4 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. Absolutely, credit to boletri, A secure method of communication between the members of the CSIRT is essential for managing incidents successfully. The team may require "out-of-band" or "off-band" channels that cannot be intercepted. In a major intrusion incident, using corporate email or VoIP runs the risk that the adversary will be able to intercept communications.

Official Compitia Cysa+ Course Material
upvoted 3 times

🗳️ 👤 **boletri** 2 years, 3 months ago

Selected Answer: A

A secure method of communication between the members of the CSIRT is essential for managing incidents successfully. The team may require "out-of-band" or "off-band" channels that cannot be intercepted. In a major intrusion incident, using corporate email or VoIP runs the risk that the adversary will be able to intercept communications.

Official CompTia Cysa+ Course Material

upvoted 3 times



  **Cock** 2 years, 4 months ago

It's important to use a secure method of communication during incident response to prevent adversaries from intercepting response and recovery details. In this case, email is not an approved communication channel, which means that it may not be secure and could potentially be intercepted by malicious actors.

Using a secure method of communication, such as an encrypted file transfer protocol or a virtual private network (VPN), will help to ensure that sensitive information, such as network design details, remains confidential and is not intercepted by unauthorized individuals.

The other options listed are not the primary reasons for using a secure method of communication during incident response. However, ensuring intellectual property remains on company servers and having a backup plan in case email access is disabled are important considerations for protecting sensitive information. Having management access to all details being exchanged is also important, but is not directly related to the security of the communication itself.

upvoted 2 times

  **absabs** 2 years, 4 months ago

Selected Answer: A

Guys focus on "during incident response", so i going with A.



upvoted 1 times

  **CatoFong** 2 years, 5 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

  **Abyad** 2 years, 7 months ago

Selected Answer: A

A is explaining the importance to use secure methods

upvoted 2 times

  **KingDeeko** 2 years, 8 months ago

Selected Answer: B

Industrial designs can be protected through various forms of intellectual property (IP), including patents, trademarks, copyrights, and/or standalone design systems.

if that email gets intercepted then the threat now has the design of the network at their disposal.

upvoted 1 times

  **bigerblue2002** 2 years, 9 months ago

Any rational as every other place that has, has the given answer as correct?



upvoted 1 times

  **TheSkyMan** 2 years, 9 months ago

"It is important to remember that in the event of a network compromise, unauthorized parties are likely to be monitoring—and attempting to counteract—your efforts. Encrypted, out-of-band communications can protect your IR activities from prying eyes"

<https://wickr.com/using-out-of-band-communication-to-bolster-incident-response/>

upvoted 1 times

  **Abyad** 2 years, 9 months ago

Selected Answer: A

I think the correct answer is A

upvoted 1 times

  **shocker111** 2 years, 9 months ago

Selected Answer: A

I think it is A, sounds correct

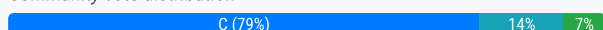
upvoted 1 times

According to a static analysis report for a web application, a dynamic code evaluation script injection vulnerability was found. Which of the following actions is the BEST option to fix the vulnerability in the source code?

- A. Delete the vulnerable section of the code immediately.
- B. Create a custom rule on the web application firewall.
- C. Validate user input before execution and interpretation.
- D. Use parameterized queries.

Suggested Answer: C

Community vote distribution



🗳️ 👤 **david124** Highly Voted 👍 2 years, 9 months ago

Script = Java = Validate user input
if it was SQL then it would have been D
upvoted 11 times

🗳️ 👤 **R00ted** Highly Voted 👍 2 years, 8 months ago

Selected Answer: C

The correct answer is C. This is a XSS issue

D = Using parameterized queries, which are precompiled SQL that takes input variables before it is executed. This helps prevent SQL injection attacks. -- This is for a SQL vulnerability
upvoted 9 times

🗳️ 👤 **skibby16** Most Recent 🕒 1 year, 6 months ago

Selected Answer: C

The best option to fix a dynamic code evaluation script injection vulnerability in the source code is to validate user input before execution and interpretation. This involves implementing proper input validation and sanitization mechanisms to ensure that user-supplied data is free from malicious code or characters that could lead to code injection vulnerabilities.
upvoted 1 times

🗳️ 👤 **Hershey2025** 1 year, 10 months ago

It says in the source code answer is D
upvoted 1 times

🗳️ 👤 **tatianna** 2 years, 3 months ago

CHAT GPT

Dynamic code evaluation or script injection vulnerabilities can be fixed by ensuring that user input is validated before it is executed or interpreted. Input validation can include sanitizing the input, restricting input characters, and ensuring that the input is in the expected format. This approach will help prevent malicious code from being executed on the server or client side. Deleting the vulnerable section of the code is not an ideal solution, as it can cause the web application to malfunction. Creating a custom rule on the web application firewall or using parameterized queries can help protect against known attack patterns but may not fully address the root cause of the vulnerability.
upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago



Selected Answer: C

C. The BEST option is to validate user input before execution and interpretation, which means that input received from users should be checked and filtered before being executed or interpreted by the application.
upvoted 1 times

🗳️ 👤 **ikedias** 2 years, 2 months ago

Hey 2Fish I see that you have been commenting with a lot of valid answers and you've been helping give me some clarity. By chance did you take the CYSA exam yet?

upvoted 1 times

  **boletri** 2 years, 3 months ago

Selected Answer: D

Parameterized Queries

Most secure websites with an SQL backend will incorporate a technique called parameterized queries to defend against code injection attacks and insecure object references.

Official CompTia Cysa+ Course Material

upvoted 1 times

  **Stiobhan** 2 years, 4 months ago

Selected Answer: C

This article will explain why it is C - <https://securityboulevard.com/2019/09/what-is-code-injection-and-how-to-avoid-it/#:~:text=Regardless%20of%20language%2C%20you%20can%20avoid%20code%20injection,functions%20on%20raw%20user%20inputs.%20...%20More%20i>

upvoted 1 times

  **Mr_BuCh3th34D** 2 years, 6 months ago

Explaining the wrong answers:

A. Delete the vulnerable section of the code immediately: if you do it you have chances to inutilize the software, hence, not the BEST option.

B. Create a custom rule on the web application firewall: also not the BEST option, this is a workaround.

D. Use parameterized queries: it talks about a web server, not a database, for that reason i don't see how it can be associated to SQLi.

C is the correct answer.

upvoted 2 times

  **moonash** 2 years, 6 months ago

Selected Answer: A

I would go with A. This is static code that was reviewed. Meaning it is not yet in prod. Developers might reuse code and the code might be having that vulnerability. I would suggest deleting that piece of vulnerable code section.

upvoted 1 times

  **Fastyt0p** 2 years, 9 months ago

Selected Answer: D

We have here tow things:

A parameterized query is a query in which placeholders are used for parameters and the parameter values are supplied at execution time. The most important reason to use parameterized queries is to avoid SQL injection attacks.

and

Goals of Input Validation¶

Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components. Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the external party.



So I thing D is the correct

upvoted 1 times

  **amateurguy** 2 years, 9 months ago

C is correct.

upvoted 1 times

  **Laudy** 2 years, 9 months ago

Agree. C is correct

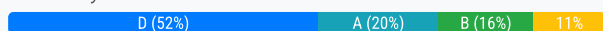
upvoted 2 times

A security analyst has discovered malware is spreading across multiple critical systems and is originating from a single workstation, which belongs to a member of the cyberinfrastructure team who has legitimate administrator credentials. An analysis of the traffic indicates the workstation swept the network looking for vulnerable hosts to infect. Which of the following would have worked BEST to prevent the spread of this infection?

- A. Vulnerability scans of the network and proper patching
- B. A properly configured and updated EDR solution
- C. A honeynet used to catalog the anomalous behavior and update the IPS
- D. Logical network segmentation and the use of jump boxes

Suggested Answer: C

Community vote distribution



Remilia Highly Voted 3 years, 6 months ago

Surprised it isn't D?

upvoted 14 times

usoldier 3 years, 5 months ago

lol right.. but segmenting a single workstation won't prevent it from happening again.. nor would it be feasible to segment a workstation every time it has a vulnerability. Understanding the what, why and how is important.

upvoted 4 times

MAGON Highly Voted 3 years, 5 months ago

The answer is B I thought it was A at first, However after reading the following insert from Malwarebytes on the functions of a Endpoint Detection and Response, it definitely makes sense to go with B.

EDR SUMMARY:

This refers to EDR's ability to capture images of an endpoint at various times and re-image or rollback to a previous good state in the event of an attack. EDR also gives administrators the option to isolate endpoints and prevent further spread across the network. Remediation and rollback can be automated, manual, or a combination of the two.

upvoted 10 times

mmm55555 3 years, 4 months ago

<https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html#~capabilities>

upvoted 4 times

haykaybam 2 years, 8 months ago

Endpoint detection and response (EDR) focuses on logging and alerting functions rather than prevention per se. The aim is to alert administrators to an intrusion and allow them to respond quickly. B can never be an option.

upvoted 1 times

NerdAlert 2 years, 2 months ago

bruh. it's Endpoint Detection and RESPONSE. not Endpoint Detection and notification

upvoted 5 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: D

D. Logical network segmentation and the use of jump boxes

upvoted 1 times

grelaman 1 year, 9 months ago

Selected Answer: A

Always Patch your system, Is the first and most important rule and It is mandatory if you have to protect CRITICAL assets. That would have prevented any kind of spreaded infections.

upvoted 1 times

NerdAlert 2 years, 1 month ago

Selected Answer: B

I choose B because EDR could stop the infection at the host level, rather than allowing it to spread throughout the network segment before stopping the spread. I think D is good, but B is better especially the bigger the network segment gets.

upvoted 2 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

In this scenario, the malware is originating from a single workstation with legitimate administrator credentials. By implementing logical network segmentation and the use of jump boxes, the spread of the malware could be contained to the segment of the network where the infected workstation is located, rather than allowing it to spread to critical systems across multiple segments.

While vulnerability scans and proper patching (A), properly configured and updated EDR solutions (B), and honeynets used to catalog anomalous behavior and update IPS (C) are all important security measures, they would not be as effective in preventing the spread of the malware in this specific scenario as logical network segmentation and the use of jump boxes.

upvoted 4 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. implementing logical network segmentation, critical systems can be isolated from other less critical systems and users, limiting the potential spread of malware.

upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Mistake, this should be D.

upvoted 4 times

🗨️ 👤 **AC6280** 2 years, 4 months ago

I initially was leaning towards B because why wouldn't an EDR be able to detect and prevent infection? Microsoft Defender for Endpoint, for example, can perform Automated Investigation and Response (AIR) which includes isolating a device, quarantining files, etc. Also, it's mentioned the analyst who owns that workstation has valid admin creds, so has the malware escalated privileges and is it operating under that account? If so, would they just be able to connect to the jump host anyways?

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automated-investigations?view=o365-worldwide>

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-auto-investigation?view=o365-worldwide#remediation-actions>

Given the details/context that this is more network based, however, I think the answer they want you to give is D (definitely a valid answer and should be part of the overall security posture regardless of the question).

upvoted 1 times

🗨️ 👤 **Cock** 2 years, 4 months ago

chatGPT told me it's D

upvoted 3 times

🗨️ 👤 **attesco** 1 year, 10 months ago

Never use chatGPT for this questions; because it does not make you think. Put on your thinking cap and don't rely on ready made answer. It will not help you in life

upvoted 1 times

🗨️ 👤 **sudoptgoaway** 1 year, 9 months ago

You're on a test bank site mr. noble

upvoted 7 times

🗨️ 👤 **Eric1234** 2 years, 4 months ago

Selected Answer: D

Going with D

upvoted 2 times

🗨️ 👤 **mhop321** 2 years, 5 months ago

Selected Answer: A

I believe the answer to be A. This is my reasoning:

"the workstation swept the network looking for vulnerable hosts to infect" - so we know that this is the trigger for this attack.

"Which of the following would have worked BEST to prevent the spread of this infection?" - So which answer would be best to prevent this infection?

A. Vulnerability scans of the network and proper patching - patching the vulnerable hosts would stop/prevent this from happening again.

upvoted 3 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

Selected Answer: D

Please read the question everyone. B will not stop the spread, it will prevent it from happening in the first place. Administrator credentials were exploited, the only option that prevents the SPREAD is D.

upvoted 6 times

  **SolventCourseisSCAM** 2 years, 8 months ago


agree w u

upvoted 1 times

  **saspurstx21** 2 years, 4 months ago

The question states "What WOULD have stopped the spread" meaning, what would have prevented it to happening in the first place.. It does not ask "What can stop further spreading?"

upvoted 2 times

  **Felix010** 2 years, 8 months ago

Selected Answer: B

I think deploying and configuring the endpoint security is the best option

upvoted 1 times



  **KingDeeko** 2 years, 8 months ago

Selected Answer: C

A honeynet is a network set up with intentional vulnerabilities hosted on a decoy server to attract hackers. They are expressly set up to attract and trap interlopers who attempt to penetrate other people's computer systems...

If that machine was compromised with malware that scanned for targets that were vulnerable it would hit that honeynet and become trapped and that's that.. it would be stuck in there for the SOC to study and analyze for further review.

upvoted 4 times

  **MortG7** 2 years, 8 months ago

Selected Answer: B

I selecting B for the following reasons:

How EDR Works

EDR security solutions use advanced techniques to proactively detect and respond to threats.

Data Collection

EDR tools install software agents on all devices and collect telemetry data from communications, queries, processes, and user logins which get stored in central logs.

Data Analysis

Behavioral analysis establishes a baseline of normal activity over time to help identify anomalies that represent malicious behavior.

Response

In case of a suspected breach, EDRs quarantine malware while isolating and testing the malicious file in a safe sandboxed environment.

upvoted 1 times

  **haykaybam** 2 years, 8 months ago

Selected Answer: D

The keyword here is to prevent the spread of the infection - can only be best achieved by use of network segmentation and use of jump boxes. Answer is D.

upvoted 2 times

  **PTcruiser** 2 years, 8 months ago

Selected Answer: B

Using EDR, the threat hunters work proactively to hunt, investigate and advise on threat activity in your environment. When they find a threat, they work alongside your team to triage, investigate and remediate the incident, before it has the chance to become a full-blown breach

<https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/#:~:text=Using%20EDR%2C%20the%20threat%20hunters,become%20a%20full%2Dblo%20wn%20breach.>

upvoted 1 times

Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

- A. To identify weaknesses in an organization's security posture
- B. To identify likely attack scenarios within an organization
- C. To build a business continuity plan for an organization
- D. To build a network segmentation strategy

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **I_Faisal** 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

🗳️ 👤 **NIKTES** 1 year, 10 months ago

B is the right answer

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. Threat intelligence can be used to identify potential threats and attack scenarios that an organization may face, allowing for the development of more effective detection and response strategies. This includes identifying TTPs used by threat actors and understanding the motivations and goals behind attacks.

upvoted 2 times

🗳️ 👤 **EVE12** 2 years, 9 months ago

Threat intelligence comprises information gathered that does one of the following things:

Educates and warns you about potential dangers not yet seen in the environment

Identifies behavior that accompanies malicious activity

Threat intelligence comprises information gathered that does one of the following things:

Educates and warns you about potential dangers not yet seen in the environment

Identifies behavior that accompanies malicious activity

Alerts you of ongoing malicious activity

upvoted 2 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is the right one

upvoted 1 times

🗳️ 👤 **Laudy** 2 years, 9 months ago

agreed. B is correct

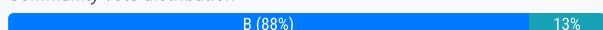
upvoted 2 times

A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization. Which of the following BEST describes the security analyst's goal?

- A. To create a system baseline
- B. To reduce the attack surface
- C. To optimize system performance
- D. To improve malware detection

Suggested Answer: B

Community vote distribution



🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. by removing unnecessary stuff, you reduce the attack surface.

upvoted 1 times

🗳️ 👤 **Cock** 2 years, 4 months ago

Selected Answer: B

The security analyst's goal is to reduce the attack surface by disabling unneeded, benign services that are currently running as part of the standard OS deployment for workstations. Attack surfaces refer to the various entry points that an attacker can use to exploit a system or network. By reducing the number of services that are running, the analyst is reducing the number of potential entry points for an attacker, thus making the system or network more secure.

A system baseline refers to the standard configuration of a system or network, which is used as a reference for identifying deviations from normal behavior. Improving malware detection refers to taking steps to increase the ability to detect malware infections. Optimizing system performance refers to improving the efficiency and speed of a system or network. These are not the primary goals of disabling unneeded services in this scenario.

upvoted 1 times

🗳️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: A

the list of unneeded, benign services are part of standard "that are currently running as part of the standard OS deployment for workstations." and he wants to create policy (The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.)

upvoted 1 times

🗳️ 👤 **Abyad** 2 years, 7 months ago

A baseline configuration is a group of settings placed on a system before it is approved for production. Using baselines is a technique that evolved from administration checklists to ensure systems were set up correctly for their intended purpose.

upvoted 1 times

🗳️ 👤 **edudarl** 2 years, 8 months ago

Selected Answer: B

certainly B

upvoted 1 times

🗳️ 👤 **Fastyt0p** 2 years, 9 months ago

Selected Answer: B

To reduce the attack surface is the best answer.

upvoted 2 times

🗳️ 👤 **EVE12** 2 years, 9 months ago

Reducing the Attack Surface Area

Reducing the attack surface area means limiting the features and functions that are available to an attacker. For example, if I lock all doors to the

facility with the exception of one, I have reduced the attack surface. Another term for reducing the attack surface area is system hardening because it involves ensuring that all systems have been hardened to the extent that is possible and still provide functionality

upvoted 2 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is correct.

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

agreed. B

upvoted 3 times

A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

Suggested Answer: D

Community vote distribution

D (79%)

A (21%)

🗳️ 👤 **Obi_Wan_Jacoby** Highly Voted 4 years, 5 months ago

Gather intelligence on threats is always part of the preparation phase which includes requirements analysis etc. Answer A looks correct.

<https://digitalguardian.com/blog/five-steps-incident-response>

upvoted 14 times

🗳️ 👤 **Obi_Wan_Jacoby** 4 years, 5 months ago

Threat feeds/sources (like plug-ins for IDS/IPS etc) give you the threat data you need to make sure you are up to date on your defense. This is always at the beginning as you want it in place and as updated as possible.

upvoted 3 times

🗳️ 👤 **SrGhost** 3 years, 9 months ago

The issue is that we have an ongoing incident, at which point we have to do post-incident recovery and review.

correct answer: C

If there was no incident, then the answer would be A.

upvoted 5 times

🗳️ 👤 **forest111** 2 years, 6 months ago

but there isn't any incident, question says "incident response effort", it could mean whole incident response generally. Am I correct?

upvoted 3 times

🗳️ 👤 **SniipZ** Highly Voted 4 years ago

A -> This is the first phase of intelligence life cycle not incident response life cycle

B -> Does not make sense

C -> This sounds correct but I feel like recovery and threat intelligence does not fit so well together

D -> These terms are not common in cybersec

Final Answer: C

upvoted 9 times

🗳️ 👤 **hloq015** 3 years, 11 months ago

the question stated via threat intelligence. So, it makes sense with the answer A

upvoted 1 times

🗳️ 👤 **VinciTheTechnic1an** 3 years, 8 months ago

If you have access to CompTia Self pace Reader. You will find the Threat Intelligence is supporting Collection, in particular.

upvoted 1 times

🗳️ 👤 **yanyan20** Most Recent 2 years, 1 month ago

Selected Answer: D

The cybersecurity analyst is MOST likely executing indicator enrichment and research pivoting during the incident response effort via threat intelligence. This involves gathering additional information and context on identified indicators of compromise (IOCs), such as IP addresses, domains, hashes, and other artifacts, to gain insight into the threat actor's tactics, techniques, and procedures (TTPs) and possible attribution. By enriching IOCs with open-source and proprietary intelligence sources and pivoting across different data sets, the analyst can generate new leads, prioritize the investigation, and improve the detection and prevention capabilities. The other options listed (requirements analysis and collection

planning, containment and eradication, and recovery and post-incident review) are also part of the incident response process, but they are not specifically related to the use of threat intelligence.

upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Me thinks the most likely is D. It's asking what the analyst is 'executing'

Indicator enrichment = gathering IOCs to better understand its relevance to the IR and its impact.

research pivoting - using information gained from one area of research and pivot to another area for more investigation.

upvoted 1 times

🗨️ 👤 **Cock** 2 years, 4 months ago

In the context of incident response, threat intelligence refers to the collection and analysis of information about potential security threats. The analyst is likely executing indicator enrichment and research pivoting, which involves collecting and analyzing information about potential security threats and using that information to identify other related threats.

This may involve using tools such as threat intelligence platforms, malware sandboxes, and open-source intelligence (OSINT) sources to gather and analyze data. The goal is to improve the understanding of the threat and identify any potential indicators of compromise that can be used to contain and eradicate the threat.

Requirements analysis and collection planning involve identifying the information that is needed to support an incident response effort. Containment and eradication involve taking steps to prevent the threat from spreading and remove it from the system or network. Recovery and post-incident review involve restoring normal operations and conducting a review of the incident to identify lessons learned and areas for improvement.

upvoted 1 times

🗨️ 👤 **jleonard_ddc** 2 years, 5 months ago

Selected Answer: D

It's definitely D but it seems like many of you are confused over why. Remember the question asks what the analyst is doing (or, in other words - how is threat intelligence benefiting the IR effort?)

A -> These are the first phases of the Intelligence lifecycle, not an incident response effort

B -> These phases come after we've identified the threat; it's this identification which threat intelligence supports

C -> Post-incident activities are where we identify what can be improved based on what happened during the incident

D -> This is the answer, because it's what the threat intelligence is actually benefiting us. It is going to give us better indicators of compromise to narrow on that could help us pivot our research (think the OODA loop) in the right direction.

For those who mentioned the preparation phase of IR, this is where we develop hardening, carry out training / exercises, establish procedures - essentially do everything we can to be ready for the big moment.

upvoted 5 times

🗨️ 👤 **kmanb** 2 years, 5 months ago

Selected Answer: D

During an incident response effort, threat intelligence is used to gather information about the incident and the attackers involved. The cybersecurity analyst's role in this process would involve gathering and analyzing data, such as IP addresses, domain names, and malware samples, in order to identify and track the attackers. This process is known as indicator enrichment and research pivoting. It falls under the category of information gathering and analysis, as opposed to implementing security controls, incident containment, and incident recovery.

upvoted 3 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: A

Going with A because I've never heard of D.

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: D

supporting incident response with threat intelligence actually provides enrichment on incident and pivoting on research.

upvoted 3 times

🗨️ 👤 **TheStudiosPeepz** 2 years, 7 months ago

Selected Answer: A

The others don't make sense, thus it's A

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 8 months ago

I'm thinking that it is A. I did some research on indicator enrichment and to me it sounds like part of the requirements analysis and collection(IoC threat intelligence gathering).

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 8 months ago

Wouldn't D be incorporated as part of A? .

upvoted 1 times

🗨️ 👤 **EVE12** 2 years, 9 months ago

Key Objectives at Each Phase of the Threat Intelligence Lifecycle

Planning and direction: Set the scope and objectives for core intel roles and processes.

Collection: Deploy data gathering and processing techniques and sources.

Analysis: Translate raw intel into meaningful and taxonomized actors, events, and attributes.

Production: Assess intel significance and severity based on business and environmental context.

Dissemination and feedback: Report on finished intel, considering urgency and confidentiality.

upvoted 1 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

I personally think it's D. but every other test dump site says A.... idk...

upvoted 1 times

🗨️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: A

looks good to me

upvoted 1 times

🗨️ 👤 **MacherGaming** 3 years ago

The question states this is part of an incident response. There's only one phase of the Threat Intelligence Lifecycle that occurs post-event, phase 6 - Feedback. This is where we reanalyze our intelligence and decide if our alerts (indicators) are working effectively and if we should redirect (pivot) our assets/research.

I've voting D.

upvoted 3 times

🗨️ 👤 **Xyz_40** 3 years, 3 months ago

A goes to explain better

upvoted 1 times

A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -l
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ?    Ss  0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp  0  0  0.0.0.0:22          172.168.0.4:8394 ESTABLISHED 1204/sshd
tcp  0  0  127.0.0.1:631      0.0.0.0:*        LISTEN      1214/cupsd
tcp  0  0  0.0.0.0:443        0.0.0.0:*        LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

- A. Run `crontab -r; rm -rf /tmp/.t` to remove and disable the malware on the system.
- B. Examine the server logs for further indicators of compromise of a web application.
- C. Run `kill -9 1325` to bring the load average down so the server is usable again.
- D. Perform a binary analysis on the `/tmp/.t/t` file, as it is likely to be a rogue SSHD server.

Suggested Answer: B

Community vote distribution

B (75%)

D (25%)

🗳️ 👤 **Obi_Wan_Jacoby** Highly Voted 4 years, 5 months ago

Well, the question states "which of the following should the analyst do NEXT to further the investigation?" Answers A and C are actions to kill 1325 or remove the malware, but the question says what to do next to further the "investigation". I'm going with answer B
upvoted 28 times

🗳️ 👤 **ufovictim** 4 years, 5 months ago

Seconded, while A would kill the possible malware it might hamper further investigation. The wording of the question suggests B is correct
upvoted 4 times

🗳️ 👤 **comptia23** 3 years, 9 months ago

I do also agree with B.

Even when comptia tries to let "t" look suspicious, it has no cputime (ps ax) and is not the reason for our high resources exhaustion.
upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree.

upvoted 1 times

🗳️ 👤 **I_heart_shuffle_girls** Highly Voted 4 years, 5 months ago

- A. We dont know what that is yet.
 - B. Examine the server logs for further indicators of compromise of a web application.
 - C. We dont know the amount of resources being used.
 - D. None of the netstat pids match.
- upvoted 7 times

🗳️ 👤 **grelaman** Most Recent 1 year, 9 months ago

Selected Answer: D

Here's the breakdown of why this is the most appropriate next step:

1. The uptime command shows a very high load average, indicating that the server is under significant stress. A high load average can be a sign of a rogue process consuming system resources.
 2. The crontab -l command reveals a suspicious cron job running every minute, executing the `/tmp/.t/t` file. This is unusual and could indicate malicious activity.
 3. The ps command shows a process with the ID 1325 running `/tmp/.t/t`. This process appears suspicious and may be the source of the high load average.
- upvoted 1 times

🗨️ **grelaman** 1 year, 9 months ago

4. The netstat output indicates an SSH connection on port 8394, which could be related to the suspicious process.

Given these findings, it's essential to investigate the /tmp/.t/t file to determine its nature and whether it is indeed a rogue SSHD server or a potentially malicious program. Analyzing the binary will provide insights into its functionality and whether it poses a security threat.

upvoted 1 times

🗨️ **Xoomalla** 1 year, 10 months ago

I will go for D, below is my reasoning

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.

--> This is more like mitigating the problem not INVESTIGATING it.

B. Examine the server logs for further indicators of compromise of a web application.

--> Could be possible answer

C. Run kill -9 1325 to bring the load average down so the server is usable again.

--> Again this will mitigate the problem. However, the malware will run again since the cron job scheduled to run each minute.

D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

--> I will go to this option, since you have a malicious file next step is to decide if it's malicious or not and figure out what it does in the system

upvoted 2 times

🗨️ **tatianna** 2 years, 3 months ago

CHAT GPT

Based on the output from the commands, the analyst has identified a suspicious file, /tmp/.t/t, which is running as a process with the PID 1325. The file command shows that it is a binary file. Therefore, the NEXT step the analyst should take to further the investigation is to perform a binary analysis on the file. This may involve examining the file's behavior, determining its origin, and identifying any associated threats or malware. It is important to do this analysis carefully, as malware can be designed to evade detection and removal attempts. Once the analyst has identified the nature of the threat, they can take appropriate action to contain and remediate the issue.

upvoted 2 times

🗨️ **khrid4** 2 years, 3 months ago

my first answer is also D, but after I saw l_heart_shuffle_girls answer, D shows that netstat did not match any result for 1325. By "acting" as a server, then it must show artifacts as PID 1325 listening to traffic from clients. But this is not the case.

upvoted 1 times

🗨️ **CatoFong** 2 years, 4 months ago

Selected Answer: B

B. is correct as we are advancing the investigation

upvoted 1 times

🗨️ **Eric1234** 2 years, 4 months ago

Selected Answer: B

B seems the most likely

upvoted 1 times

🗨️ **miabe** 2 years, 11 months ago

Selected Answer: B

looks good to me

upvoted 1 times

🗨️ **JenG59** 3 years ago

Public facing and SSH to private, check the logs

upvoted 1 times

🗨️ **BlackdaRipper** 3 years, 4 months ago

B is correct.

upvoted 2 times

🗨️ **Ham_Solo** 3 years, 11 months ago

It clearly states public facing, and SSH to a private 172.168.*.* address is internal LAN traffic. I'm going to check logs for further IOC.

upvoted 1 times

🗨️ 👤 **Alizadeh** 4 years, 3 months ago

B is correct

upvoted 3 times

🗨️ 👤 **Alizadeh** 4 years, 3 months ago

B is correct

upvoted 1 times

🗨️ 👤 **Umer24** 4 years, 5 months ago

send me a mail ryan23680 at yahoo for new Cysa+ cs0-002 questions and we can find the correct answers together.

upvoted 1 times

🗨️ 👤 **Berlus** 4 years ago

If you can't share your thoughts here, then we don't need you on this platform

upvoted 15 times

🗨️ 👤 **RokzyBalboa** 4 years, 5 months ago

I would do A first. The cronjob is running every minute, and every minute that goes by, is another minute of suspected malicious activity. I would stop the malicious activity first before attempting to examine server logs. Note also the .t folder is a hidden folder, which would add to the suspicion of why a cronjob would be running something that is in a hidden folder. And note the established ssh session, which likely means a backdoor exists to the system, and the cronjob likely ensures the persistent connection for the malicious entity.

upvoted 1 times

🗨️ 👤 **lollo1234** 4 years ago

Fair point, however notice you can't just remove the cronjob, the option also includes permanently deleting the suspicious file. The best answer is remove the cronjob, kill the process, and review the logs, but that is not an option, so I go with B.

upvoted 1 times

An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages.

Which of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?

- A. Change the passwords on the devices.
- B. Implement BIOS passwords.
- C. Remove the assets from the production network for analysis.
- D. Report the findings to the threat intel community.

Suggested Answer: B

Community vote distribution

C (54%)

B (46%)

🗳️ 👤 **Laudy** Highly Voted 2 years, 9 months ago

I think this is C.

If were referring to other devices, yes - Implement BIOS passwords before they are compromised.

But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.

upvoted 20 times

🗳️ 👤 **Abz1999** 1 year, 9 months ago

this makes the most sense, idk why people are confused

upvoted 1 times

🗳️ 👤 **RobV** Most Recent 1 year, 6 months ago

Selected Answer: C

C. Remove the assets from the production network for analysis.

upvoted 2 times

🗳️ 👤 **sirpetey** 1 year, 7 months ago

SO. From my understanding.... just googling... Field devices are "Equipment that is connected to the field side on an ICS. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications." which doesn't have BIOS? so it would have to be C?

upvoted 1 times

🗳️ 👤 **Big_Dre** 1 year, 10 months ago

Selected Answer: B

i will go with B because the key statement is ; To secure the devices from further exploitation; device not system. so i think B fits perfectly.

upvoted 1 times

🗳️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: C

Among the options provided, the best action to recommend is to remove the assets from the production network for analysis

upvoted 4 times

🗳️ 👤 **heinzelrumpel** 1 year, 11 months ago

Selected Answer: C

The other answers don't fit

upvoted 3 times

🗳️ 👤 **heinzelrumpel** 1 year, 11 months ago

The question is mentioning "devices". That could be tablets and phones which don't have BIOS

upvoted 3 times

🗳️ 👤 **Noragretz** 1 year, 11 months ago

I was looking for "contain" as the key word and not "remove from production" good to see it in different wording.

upvoted 1 times

🗨️ 👤 **JimmyJams** 1 year, 11 months ago

Selected Answer: C

In the real world you would remove those devices in the first instance and this fits the question as removing them would be securing them and removing them from further exploitation. Then you would examine them in your lab setup.

upvoted 3 times

🗨️ 👤 **tutita** 2 years ago

Selected Answer: B

the best step for securing the devices is to implement password BIOS...

upvoted 3 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Unauthorized changes to firmware versions on field devices indicate that the devices have likely been compromised by an attacker. By removing the compromised devices from the production network for analysis, the organization can better understand the extent of the compromise and take steps to remediate the issue. Changing the passwords on the devices (A) or implementing BIOS passwords (B) may provide some additional security, but these measures are unlikely to fully address the compromise of the devices.

upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. it is essential to isolate the devices and analyze them in a controlled environment to identify the root cause of the issue, assess the scope of the compromise, and implement appropriate remediation measures.

upvoted 2 times

🗨️ 👤 **Jacobmy98** 2 years, 2 months ago

I've been following most of your answers lol. It has to be B: it's asking for the BEST way to secure the devices. Not the next step

upvoted 1 times

🗨️ 👤 **IanRogerStewart** 2 years, 4 months ago

Selected Answer: C

Next step is Containment. Remove devices

upvoted 1 times

🗨️ 👤 **Jacobmy98** 2 years, 2 months ago

It's not asking for the next step. It's asking what is the BEST way to secure the devices

upvoted 3 times

🗨️ 👤 **JoInn** 2 years, 1 month ago

yes, to avoid FURTHER exploitation. Same thing is what comes next lol

upvoted 1 times

🗨️ 👤 **Cock** 2 years, 4 months ago

In this scenario, the unauthorized changes to the firmware versions of the field devices indicate a potential security breach. To secure the devices from further exploitation, the best course of action is to remove them from the production network for analysis. This will help to prevent any potential harm to the network and reduce the risk of further compromise. The analysis will also provide important information for determining the source and extent of the breach, as well as any necessary steps to remediate it. Other recommended actions may include changing passwords, implementing BIOS passwords, and reporting the findings to the threat intel community, but removing the assets from the production network should be the first priority

upvoted 1 times

🗨️ 👤 **Stiobhan** 2 years, 4 months ago

Removing the devices from the production network?? What will you replace them with?? For sure some analysis will need to be completed but the key in the question is "Secure devices from FURTHER EXPLOITATION. Changing the BIOS passwords would be the best fit.

upvoted 3 times

🗨️ 👤 **knister** 2 years, 5 months ago

Selected Answer: B

B, the only one that secures the devices.

upvoted 3 times

🗨️ 👤 **lordguck** 2 years, 6 months ago

I go for C: in order to investigate. B: can't be right, as the question talks about "field devices" which may or may not have an accessible bios.

upvoted 1 times

An organization has not had an incident for several months. The Chief Information Security Officer wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

- A. Root-cause analysis
- B. Active response
- C. Advanced antivirus
- D. Information-sharing community
- E. Threat hunting

Suggested Answer: E

Community vote distribution

E (100%)

🗳️ 👤 **I_heart_shuffle_girls** Highly Voted 👍 4 years, 5 months ago

E is a proactive approach.
upvoted 18 times

🗳️ 👤 **Obi_Wan_Jacoby** 4 years, 5 months ago

I concur with E
upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree, Threat Hunting is very proactive.
upvoted 1 times

🗳️ 👤 **heinzelrumpel** Most Recent ⌚ 1 year, 11 months ago

Selected Answer: E

E is proactive
upvoted 1 times

🗳️ 👤 **Eric1234** 2 years, 4 months ago

Selected Answer: E

Threat Hunting
upvoted 1 times

🗳️ 👤 **Average_Joe** 2 years, 8 months ago

- Threat Hunting is Proactive.
- Incident Response is Reactive.
upvoted 4 times

🗳️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: E

looks good to me
upvoted 3 times

🗳️ 👤 **Sameeh** 3 years, 7 months ago

The answer is 'E'
upvoted 2 times

🗳️ 👤 **Panda156423** 4 years, 1 month ago

100% E
upvoted 3 times

🗳️ 👤 **americaman80** 4 years, 4 months ago

I concur with E as well.
upvoted 4 times

Massivelog.log has grown to 40GB on a Windows server. At this size, local tools are unable to read the file, and it cannot be moved off the virtual server where it is located. Which of the following lines of PowerShell script will allow a user to extract the last 10,000 lines of the log for review?

- A. `tail -10000 Massivelog.log > extract.txt`
- B. `info tail n -10000 Massivelog.log | extract.txt;`
- C. `get content './Massivelog.log' -Last 10000 | extract.txt`
- D. `get-content './Massivelog.log' -Last 10000 > extract.txt;`

Suggested Answer: C

Community vote distribution

D (86%)

14%

🗳️ **VinciTheTechnic1an** Highly Voted 3 years, 5 months ago

I use powershell, so this is 100% sure. D. is the answer.

upvoted 11 times

🗳️ **2Fish** 2 years, 3 months ago

Agree, > is sending that output to a file.

upvoted 1 times

🗳️ **Lilik** Most Recent 10 months, 3 weeks ago

D.Use redirection operators (>, >>, 2>, 2>>, and 2>&1) to send the output of a command or expression to a text file.

upvoted 1 times

🗳️ **AbdallaAM** 1 year, 8 months ago

Selected Answer: D

Options A, B, and C are incorrect for the following reasons:

A. tail is not a PowerShell command (it's a Unix/Linux command).

B. info is not a recognized command or parameter and the syntax is incorrect.

C. The syntax is incorrect because it uses | (pipe) followed by extract.txt, which is not a command. Also, get content should be get-content.

upvoted 1 times

🗳️ **Lorello2023** 1 year, 10 months ago

Selected Answer: D

D I mean get content is wrong

get-content is correct

upvoted 1 times

🗳️ **heinzlumpel** 1 year, 11 months ago

Selected Answer: D

Why do people destroy this site with useless answers? C is crap . Cmdlets are always noun-verb so D is the only correct answer

upvoted 3 times

🗳️ **OK97** 1 year, 11 months ago

how have people learnt to interpret these commands, i am struggling to understand. Where can i learn this commands and make it easier to understand?

upvoted 3 times

🗳️ **kill_chain** 2 years ago

Selected Answer: C

Doesn't powershell use a pipeline to the the output file instead of a > ?

upvoted 2 times

🗳️ **cbrow** 1 year, 8 months ago

Using the pipe '|' is to send an object through to the next command (i.e., "Get-Content myfile.txt -Last 10000 | Select -First 1" would first get the last 10,000 lines of the file, and then you are selecting the first object of the 10,000 with "Select -First 1"). Using '>' sends text to a file (overwrites current file if the name already exists). If you use '>>', it appends the text you are sending to the file instead of overwrites.

upvoted 1 times

🗨️ 👤 **NerdAlert** 2 years, 2 months ago

Selected Answer: D

well "tail" is linux, and Powershell hyphenates commands like get-content. So, not knowing the right command, the bottom one is the only one that looks like a real Powershell command anyway

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

This script uses the get-content cmdlet to read the contents of the Massivelog.log file and then selects the last 10,000 lines using the -Last parameter. The output is then redirected to a new file called extract.txt using the > operator.

upvoted 1 times

🗨️ 👤 **tatianna** 2 years, 3 months ago

D. get-content './Massivelog.log' -Last 10000 > extract.txt;

upvoted 2 times

🗨️ 👤 **Stiobhan** 2 years, 3 months ago

Selected Answer: D

The closest answer is D. The actual command should be:

get-content './Massivelog.log' -Last 10000 > extract.txt

upvoted 1 times

🗨️ 👤 **diomastik88** 2 years, 5 months ago

The answer is C

upvoted 1 times

🗨️ 👤 **mhop321** 2 years, 5 months ago

Why? Least someone else has said "I use powershell so know it is D".....

upvoted 1 times

🗨️ 👤 **HouseOfMouse** 2 years, 6 months ago

The cmdlet feels like a giveaway to me. I thought tails was exclusive to Linux.

upvoted 1 times

🗨️ 👤 **MrRobotJ** 2 years, 7 months ago

what is the with (;) at the end of C?

upvoted 1 times

🗨️ 👤 **diomastik88** 2 years, 5 months ago

There's no (;) at the end of C but at the end of D

So the right answer for this question is C

upvoted 1 times

🗨️ 👤 **Average_Joe** 2 years, 8 months ago

PowerShell uses Verb-Noun syntax for cmdlets. D (Get-Content) is correcto.

<https://learn.microsoft.com/en-us/powershell/scripting/developer/cmdlet/approved-verbs-for-windows-powershell-commands?view=powershell-7.2>

upvoted 2 times

🗨️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: D

D is the answer

upvoted 2 times

🗨️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: D

looks good to me

upvoted 3 times

A cybersecurity analyst is establishing a threat-hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

- A. IoC feeds
- B. CVSS scores
- C. Scrum
- D. ISAC

Suggested Answer: A

Community vote distribution

D (100%)

🗳️ 👤 **AbdallaAM** 1 year, 8 months ago

Selected Answer: D

Considering the collaborative nature of threat-hunting and intelligence group activities, ISACs (Option D) would most likely be the most beneficial resource among the listed options. ISACs offer a collaborative platform for sharing threat intelligence, experiences, and effective security practices, which are fundamental for establishing a robust threat-hunting and intelligence group at a growing organization.

upvoted 1 times

🗳️ 👤 **Pavel019846457** 1 year, 10 months ago

Selected Answer: D

Definitely D

upvoted 2 times

🗳️ 👤 **jade290** 1 year, 10 months ago

Selected Answer: D

I plugged this into an AI and this is the explanation it gave me:

The collaborative resource that would MOST likely be used for threat-hunting and intelligence is ISAC (Information Sharing and Analysis Center).

IoC feeds are a good source of threat intelligence, but they are not as collaborative as ISACs. IoC feeds are typically one-way, meaning that organizations can only receive information from them. ISACs, on the other hand, are two-way, meaning that organizations can both receive and share information. This makes ISACs more valuable for threat-hunting and intelligence, as organizations can get real-time information from other organizations that are facing similar threats.

ISACs are also more specialized than IoC feeds. IoC feeds typically cover a wide range of threats, while ISACs focus on specific industries or sectors. This makes ISACs more relevant to the organizations that they serve, as they can provide more targeted threat intelligence.

upvoted 2 times

🗳️ 👤 **heinzeltumpel** 1 year, 11 months ago

Selected Answer: D

Can't believe the correct Answer is marked A.

upvoted 2 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

ISAC (Information Sharing and Analysis Center)

upvoted 2 times

🗳️ 👤 **DrVoIP** 2 years, 4 months ago

D. ISAC (Information Sharing and Analysis Center) is the most likely collaborative resource that would be used for establishing a threat-hunting and intelligence group at a growing organization. ISACs are industry-specific organizations that facilitate the sharing of threat intelligence, best practices, and other security-related information among member organizations.

upvoted 3 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree, any ISAC is going to provide a wealth of information.

upvoted 1 times

  **encxorblood** 2 years, 4 months ago

Selected Answer: D

D. ISAC (Information Sharing and Analysis Center) is a collaborative resource that would MOST likely be used for establishing a threat-hunting and intelligence group at a growing organization.

ISACs are industry-specific organizations that gather, analyze, and disseminate information on cyber threats, vulnerabilities, and incidents to their members. ISACs facilitate the sharing of threat intelligence, best practices, and mitigation strategies, enabling their members to be better prepared and protected against cyber threats.

By joining an ISAC, a cybersecurity analyst can gain access to a broad range of threat intelligence resources and collaborate with other members of the organization to share information and insights about emerging threats and vulnerabilities. This can help the analyst to better understand the evolving threat landscape and proactively identify and respond to potential threats.

upvoted 2 times

  **Cock** 2 years, 4 months ago

Indicators of Compromise (IoC) feeds are a collaborative resource that would most likely be used by a threat-hunting and intelligence group. IoC feeds provide a centralized repository of threat intelligence data, including information about known malicious IP addresses, domains, and hashes of malware. This information can be used to detect and respond to potential security threats in a timely manner. IoCs can be generated from internal sources, such as a security operations center (SOC), or from external sources, such as threat intelligence platforms or community-driven threat intelligence initiatives. By subscribing to and utilizing these feeds, organizations can enhance their threat-hunting capabilities and improve their overall security posture.

upvoted 1 times

  **Mouhammad1** 2 years, 5 months ago

ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes



upvoted 1 times

  **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: D

It needs collaborative resource, so ISAC is the most collaborative resource you can find.



upvoted 1 times

  **arctanx** 2 years, 8 months ago

Selected Answer: D

collaborative resource.

upvoted 1 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: D

So based on my research, there are threat feeds and ioc management, I don't see anything named "ioc feeds".

D looks to be the most correct answer as it deals directly with collaborative work and information sharing. Im going with D but hey, let me know if im wrong.



upvoted 4 times

  **TheSkyMan** 2 years, 9 months ago

Selected Answer: D

I know cyber threat feeds are a thing, but I'm not sure if IOC feeds are a thing. Looking at previous company IOC's is helpful, but not collaborative. ISAC seems like the only collaborative resource here.

upvoted 1 times

  **Laudy** 2 years, 9 months ago

Is A and C not almost synonymous?

C feels like a more formal A

Does anyone know the nuance differences?

I can tell the answers are different, but this question alludes to either one. How can I tell the difference, is what I'm asking...

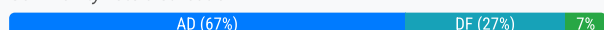
upvoted 1 times

Which of the following are considered PII by themselves? (Choose two.)

- A. Government ID
- B. Job title
- C. Employment start date
- D. Birth certificate
- E. Employer address
- F. Mother's maiden name

Suggested Answer: DE

Community vote distribution



AbdallaAM 1 year, 8 months ago

Selected Answer: AD

A. Government ID:

This is considered PII as it is unique to an individual and can be used to identify them.

D. Birth Certificate:

A birth certificate is also considered PII as it contains unique information such as name, date of birth, and place of birth which can be used to identify an individual.

The other options, like job title, employment start date, employer address, and mother's maiden name, are not considered PII by themselves as they cannot singularly identify an individual. However, when combined with other pieces of information, they could contribute to identifying an individual.

upvoted 1 times

Awaleh 1 year, 9 months ago

A and D are the correct answers

upvoted 1 times

Blooit 1 year, 11 months ago

Selected Answer: AD

A and D are the correct answers.

upvoted 1 times

[Removed] 2 years, 1 month ago

The employer address might not even be the same as where you actually work! I know some use the main HQ as the address if they work from home. That could be 1000s of miles away on the other side of the state. I am picking A&D.

upvoted 1 times

kiduuu 2 years, 2 months ago

Selected Answer: AD

Government ID and Birth certificate are considered PI because they contain unique and identifiable information about an individual.

Job title, employment start date, employer address, and mother's maiden name may be considered personal information but they are not considered PI on their own as they do not uniquely identify an individual.

upvoted 1 times

[Removed] 2 years, 3 months ago

Selected Answer: AD

A & D

Literally PII

upvoted 2 times

2Fish 2 years, 3 months ago

Agree, absolutely A & D.

upvoted 2 times

🗨️ 👤 **davidma** 2 years, 4 months ago

E EmployER address could not be the right answer...
upvoted 1 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: AD

It's definitely A and D they're the only two things that alone are PII
upvoted 1 times

🗨️ 👤 **Stiobhan** 2 years, 4 months ago

OMG it is A&D, how can Employer address be PII ☹️Come on ET, that is embarrassing.
upvoted 1 times

🗨️ 👤 **catastrophie** 2 years, 5 months ago

A and D are correct. You can determine an individuals personal identity with a government issues identification number. You license number, DoD ID, and similar can be entered into a system by itself and it will populate your information. You can enter the last name "Smith" all day and see if that leads directly back to you as a one-to-one relationship.
upvoted 1 times

🗨️ 👤 **CertKid** 2 years, 5 months ago

I think because it says BY ITSELF, the answer is Government ID and Birth Cert. Maiden name is PII but it's useless without context/other information. Rest are not PII
upvoted 1 times

🗨️ 👤 **jleonard_ddc** 2 years, 5 months ago

Selected Answer: AD

Be careful on this as the question says which items are PII by themselves. I guarantee if you have my birth certificate or my ID, however - you know exactly who I am without needing any supplemental data. All the rest may be forms of PII, but would require some sort of supplemental research or documents to link directly to you. (your mother's maiden name doesn't link to your given name, but that given name could be determined second-hand, etc.)
upvoted 1 times

🗨️ 👤 **simsbow1098** 2 years, 5 months ago

Selected Answer: AD

What's annoying about this is A D and F are all PII. If you google all three (ex. is A D or F PII) google will say it is. There's alot of confusion on what a Government ID is, Google it. A government ID can be a state ID or passport. To me a state ID is more revealing than a mother's maiden name. So I would have to say A and D
upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: DF

A simple Google Search reveals the following information:

PII can include unique individual identifiers or combinations of identifiers, such as an individual's name, Social Security number, date and place of birth, mother's maiden name, biometric data, etc.

upvoted 2 times

🗨️ 👤 **jleonard_ddc** 2 years, 5 months ago

Good point, but the question says "by themselves". Mother's maiden name doesn't, by itself - link you to her. It needs supplemented with other data. This is why I also think employer address isn't the answer. I guarantee if you have my birth certificate or my ID, however - you know exactly who I am without needing any supplemental data.
upvoted 1 times

🗨️ 👤 **TKW36** 2 years, 5 months ago

Selected Answer: DF

D. Birth certificate and F. Mother's maiden name.

PII, or personally identifiable information, is any data that can be used to identify an individual. Birth certificates and mother's maiden names are considered PII because they can both be used to uniquely identify an individual. Government ID, job title, employment start date, and employer address are not considered PII by themselves, as they are not unique identifiers. However, these pieces of information can be combined with other information to create PII.

upvoted 2 times

🗨️ 👤 **marc4354345** 2 years, 6 months ago

Selected Answer: AD

With AD you can identify a specific person. With the other options not so much.

upvoted 2 times

  **Ruby2021** 2 years, 6 months ago

I have to go with AD. My reasoning for A is I am retired from the US Army and my retiree ID card (Government) as my Social Security number right on the front of the card, all 9 digits.

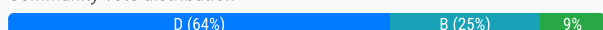
upvoted 1 times

A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

- A. CASB
- B. VPC
- C. Federation
- D. VPN

Suggested Answer: B

Community vote distribution



🗳️ **kiduuu** Highly Voted 2 years, 2 months ago

Selected Answer: D

A VPN is a technology that provides secure and encrypted communication between two networks over an unsecured network such as the internet. It can be used to connect remote users or networks to the corporate network securely. In this case, the development team needs access to servers in all three tiers of the cloud environment, and a VPN can provide secure transport for the team to access these servers.

Option B, VPC (Virtual Private Cloud), is a cloud computing technology that enables users to create a private cloud within a public cloud environment. While VPCs can be used to create secure networks within a cloud environment, they do not provide secure transport for accessing servers in a cloud environment from a corporate network.

upvoted 5 times

🗳️ **RobV** Most Recent 1 year, 6 months ago

Selected Answer: D

D. VPN

upvoted 1 times

🗳️ **Junior24** 1 year, 9 months ago

Selected Answer: D

secure transport is VPN. VPC is basically your data centers in the cloud

upvoted 2 times

🗳️ **Big_Dre** 1 year, 10 months ago

Selected Answer: D

VPCs create a private network within a public cloud environment, VPNs offer secure access to those resources remotely,

upvoted 2 times

🗳️ **heinzlumpel** 1 year, 11 months ago

Selected Answer: D

VPC is just a term to describe, that you can set up virtual switches, PCs, NICs etc, which are separated from the rest of a public cloud. VPC does not define the meaning of how one is connection to it. So D is the only correct answer.

upvoted 3 times

🗳️ **JoInn** 2 years, 3 months ago

Selected Answer: B

A Virtual Private Cloud (VPC) allows you to virtually create a private and isolated network in the cloud. Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.

upvoted 2 times

🗳️ **db97** 2 years, 4 months ago

Selected Answer: D

If you want to connect an on-premise network with a cloud environment then you will need a VPN first. A VPC is to move between one tier to another one.

Check this reference: <https://docs.aws.amazon.com/whitepapers/latest/security-best-practices-for-manufacturing-ot/secure-network-connection-to-the-cloud.html>

upvoted 4 times

🗨️ **2Fish** 2 years, 3 months ago

Agree. You have to have a VPN to get access from on-prem to Cloud. If not a VPN, then some type of direct connect or express connect.

upvoted 1 times

🗨️ **absabs** 2 years, 4 months ago

Selected Answer: B

I taked from book;

A virtual private cloud (VPC) is an example of infrastructure as a service (IaaS). VPC lets you provision virtual servers and appliances within a virtual network hosted on a public cloud.

It allows to create subnet. I going with VPC. I think; people use to VPN for more general reasons. If i am wrong, can you discuss me?

upvoted 3 times

🗨️ **Cock** 2 years, 4 months ago

openAI spent a lot of time considering this question. A Virtual Private Network (VPN) would be the best technology for the security analyst to implement to provide secure transport for the development team. A VPN creates an encrypted connection between the corporate network and the cloud environment, allowing the developers to access servers in all three tiers securely. This protects the sensitive data and network traffic from unauthorized access or eavesdropping. The VPN uses tunneling protocols, such as IPsec or SSL, to encrypt the traffic and authenticate the users. The analyst can configure the VPN to enforce access controls and restrict the developers to only the resources they need, providing an additional layer of security. By using a VPN, the analyst can ensure that the development team has secure and controlled access to the cloud environment, protecting both the corporate network and the cloud environment from potential threats.

upvoted 2 times

🗨️ **Stiobhan** 2 years, 4 months ago

Wee bit tricky this one but from the wording of the question it suggests connecting from an on-prem environment "secure connectivity from the corporate network to a three-tier cloud environment. " If you were pivoting around in the Cloud then VPC. Here is a good link and the reason I'd go with VPN <https://docs.aws.amazon.com/whitepapers/latest/security-best-practices-for-manufacturing-ot/secure-network-connection-to-the-cloud.html>

upvoted 1 times

🗨️ **10cccordrazine** 2 years, 4 months ago

Selected Answer: D

As someone with a Google Cloud Professional Architect Certification, the answer should be D, as the question is about providing "the development team with secure connectivity from the corporate network to a three-tier cloud environment".

If we want to connect on-prem to the cloud we should use a VPN connection, not a VPC. In this scenario, a VPC would be used for the connection between the different cloud components and between the three tiers, but as I read it the question is asking for secure transport between on-prem and cloud.

upvoted 3 times

🗨️ **absabs** 2 years, 4 months ago

Selected Answer: B

Answer is C. You pass in Azure with VPN, but VPC is logical divisions. You set rule to access in VPC.

upvoted 1 times

🗨️ **iraidesc** 2 years, 5 months ago

Selected Answer: C

Answer is C:

A Virtual Private Cloud (VPC) allows you to virtually create a private and isolated network in the cloud. Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider. This ensures that each customer's data remains isolated from other customer's data, both in transit and inside the cloud provider's network. This isolation can be accomplished using security policies that require some – or all – of the following elements: private IP addressing, tunneling, encryption, or allocating a unique VLAN to each customer.

upvoted 4 times

🗨️ **CyberNoob404** 2 years, 5 months ago

Selected Answer: D

Answer is D. Google Cloud VPN.

upvoted 1 times

  **jleonard_ddc** 2 years, 5 months ago

A cloud VPN is not the same thing as a standalone VPN. It's more of a VPC.

upvoted 1 times

  **Freddy90** 2 years, 5 months ago

Selected Answer: B



A VPC typically exists on a private subnet and may have additional security to ensure that intersystem communications remain secure.

upvoted 1 times

  **Freddy90** 2 years, 5 months ago

B - VPC typically exists on a private subnet and may have additional security to ensure that intersystem communications remain secure.

upvoted 1 times

  **f3lix** 2 years, 5 months ago

Selected Answer: B

Emerging answer, VPC is correct! - B

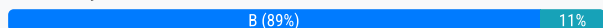
upvoted 1 times

A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

- A. The server is configured to communicate on the secure database standard listener port.
- B. Someone has configured an unauthorized SMTP application over SSL.
- C. A connection from the database to the web front end is communicating on the port.
- D. The server is receiving a secure connection using the new TLS 1.3 standard.

Suggested Answer: B

Community vote distribution



Cock Highly Voted 2 years, 4 months ago

TCP port 465 is commonly used for Secure SMTP (SMTPS) traffic, which is an encrypted version of Simple Mail Transfer Protocol (SMTP). SMTPS is used for secure communication between mail servers and other mail clients. If the security analyst is noticing encrypted inbound traffic on TCP port 465 from a database server, it is most likely that someone has configured an unauthorized SMTP application over SSL. This could pose a security risk if the encrypted traffic is carrying sensitive information, as it could potentially be intercepted and decrypted by an attacker. The security analyst should investigate the cause of the traffic and determine if the SMTP application is authorized and properly secured, and take necessary action to remediate any security risks identified.

upvoted 5 times

kyky Most Recent 2 years ago

Selected Answer: B

B: "Someone has configured an unauthorized SMTP application over SSL" as the reason for the traffic on TCP port 465.

SMTP (Simple Mail Transfer Protocol) is commonly used for sending email messages, and port 465 is typically associated with SMTP over SSL (Secure Sockets Layer) or SMTPS. The use of encryption on this port suggests that the traffic is related to email communication, and the fact that it is inbound traffic from a database server indicates that an unauthorized SMTP application over SSL may have been configured.

upvoted 3 times

2Fish 2 years, 3 months ago

Selected Answer: B

B. Although, this port has been deprecated, A&D could also use this port, but it is not "Most Likely" those would use port 465.

<https://www.mailgun.com/blog/email/which-smtp-port-understanding-ports-25-465-587/>

upvoted 2 times

david124 2 years, 4 months ago

Selected Answer: B

chat GBT says B

upvoted 2 times

AaronS1990 2 years, 4 months ago

That doesn't mean it's the answer though does it?

How about a meaningful contribution for a change rather than posting what chat GBT says, which I would add.... no one asked.

upvoted 7 times

Olaswolla 2 years, 5 months ago

Selected Answer: D

Port 465 is used for implicit TLS and can be used to facilitate secure communications for mail services.

upvoted 1 times

MrRobotJ 2 years, 10 months ago

Can someone please tell me why we chose B?



Thanks in advance.

upvoted 2 times

amateurguy 2 years, 10 months ago

if you google port 465, it shows smtp over implicit ssl.



upvoted 2 times

  **miabe** 2 years, 11 months ago

Selected Answer: B

looks good to me

upvoted 1 times

  **Xyz_40** 3 years, 3 months ago

correct answer

upvoted 3 times

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

Firewall ACL

```

10 permit tcp from:any to:server1:www
15 permit udp from:lan-net to:any:dns
16 permit udp from:any to:server2:dns
20 permit tcp from:any to server1:ssl
25 permit tcp from:lan-net to:any www
26 permit tcp from:lan-net to:any:ssl
27 permit tcp from:any to pc2:mssql
30 permit tcp from:any to server1:ssh
100 deny ip any any

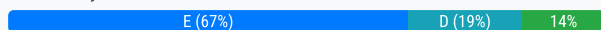
```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

Suggested Answer: B

Community vote distribution



dymson 1 year, 8 months ago

Why option B is marked as correct ?

upvoted 1 times

boxv4 1 year, 10 months ago

Selected Answer: E

agreed, answer E is correct.

upvoted 1 times

boxv4 1 year, 10 months ago

Considering the options and the goal of reducing organizational risk while maintaining functionality, the best choice would be:

E. Firewall: The security analyst should reconfigure the firewall ACL to carefully define and restrict outbound access, particularly regarding rules that allow traffic from the internal LAN network to external destinations. This can help prevent unintended data leakage, unauthorized access, and exposure to potential threats.

upvoted 3 times

Dutch012 2 years ago

The only issue here is that the firewall has "from:any" a lot in all of it's ACL lines, and it needs to be reviewed again.

regarding port 3389 in Server2 it's not an issue because Implicit deny will deny any connection coming to it.

So I think it's E

upvoted 1 times

kiduuu 2 years, 2 months ago

Selected Answer: E

It say "reconfigure to best reduce organizational risk while maintaining current functionality"

So, it's firewall

upvoted 1 times

🗨️ 👤 **Snkrsnaker1** 2 years, 2 months ago

Answer is B.

As an analyst, you're definitely not reconfiguring the firewall, and reconfiguring it would not maintain its "current functionality". As in, this is the way we want it set so don't change too much of it. The easiest way to maintain this is to make a rule change to PC2 because its allowing anyone to access it.

upvoted 2 times

🗨️ 👤 **slcc99** 2 years, 3 months ago

This question was put on the exam

upvoted 4 times

🗨️ 👤 **khrid4** 2 years, 3 months ago

Selected Answer: E

keyword here is "reconfigure to best reduce organizational risk while maintaining current functionality". Assuming to maintain current functionality as is of each asset, inbound connection especially for port 3389 should not be allowed or atleast controlled if not fully closed. Hence, E. Firewall.

upvoted 1 times

🗨️ 👤 **OnA_Mule** 2 years, 3 months ago

Selected Answer: E

For those pointing at PC2, if they need to change this, then they would also need to update the firewall. Since it's a firewall rule, I would make the assumption that it is supposed to be there.

I would lean towards Firewall just because RDP isn't getting through, or I could see reconfiguring the Server2 to get rid of RDP. Another poorly worded question either way.

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: E

E. This one seems a bit tricky. While Server 2 does have 3389 (probably should close it) open, there does not appear to be any rules allowing access to that port. However, SQL does have a permit rule from Any and that is an issue. So I would adjust the firewall rule for that device.

upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

More discussions here - <https://www.examtopycs.com/discussions/comptia/view/42438-exam-cs0-002-topic-1-question-16-discussion/>

upvoted 2 times

🗨️ 👤 **NerdAlert** 2 years, 2 months ago

a lot of them recommend firewall because we need are reducing risk while "maintaining current functionality" - some devices on the LAN might need those ports open that are normally closed. Great point!

upvoted 1 times

🗨️ 👤 **aisling** 2 years, 4 months ago

Selected Answer: D

RDP Port 3389 is a Risk and should be turned off if not absolutely needed

upvoted 1 times

🗨️ 👤 **db97** 2 years, 4 months ago

There isn't any permit rule going to that port and in case that someone attempts to connect through it will be denied by the implicit deny ACL at the end.

upvoted 2 times

🗨️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: D

I going with D. Because any rules about 3389 is not in ACL. It is vulnerable. PAY ATTENTION!!

upvoted 3 times

🗨️ 👤 **catastrophie** 2 years, 5 months ago

I believe B is the correct answer. Why would a PC be running as an SQL server? All the firewall rules are fine with the exception of 27, there is no reason that needs to be opened up to the world. Shutting the port down on the PC is the safest option. If someone were to gain access to the network through another channel they'd be able to exploit 1433 without having to pass the firewall.

10- Allow anyone to connect to svr1 via 80/443 depends on default.

15- Local net can connect to any DNS (DNS is 53)

16- Any to svr2 via DNS - Needs outside connection to advertise.

20- any ssl to svr1 - Generally secure, no issues

25- local net access to the outside world internet via 80/443

26- local net ssl access to outside world

27- any to connect to pc2 via 1433 - bad, shouldn't use 1433 on pc2

30- any to connect to svr1 via ssh - generally extremely secure with proper password implementation.

100 - deny anything else that doesn't meet the rules above.

upvoted 4 times

  **Treymb6** 2 years, 9 months ago

Selected Answer: B

I believe B is right.

https://www.grc.com/port_1433.htm



upvoted 2 times

  **Treymb6** 2 years, 8 months ago

I think I recant my original answer.

Mostly because "while maintaining current functionality" is holding me up. Seeing that port 1433 is open on the server and firewall, I assume that is a database server. Changing my answer to E as well.



upvoted 1 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: E

Firewall is the correct answer.



upvoted 3 times

  **Adonist** 2 years, 9 months ago

Selected Answer: E

I'd go for E for multiple reasons, but mostly because allows traffic from any to database



upvoted 3 times

  **Abyad** 2 years, 9 months ago

Selected Answer: E

Firewall is the answer

upvoted 1 times

  **shocker111** 2 years, 9 months ago

Selected Answer: B

Sounds about right

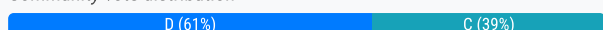
upvoted 1 times

The help desk is having difficulty keeping up with all onboarding and offboarding requests. Managers often submit requests for new users at the last minute, causing the help desk to scramble to create accounts across many different interconnected systems. Which of the following solutions would work BEST to assist the help desk with the onboarding and offboarding process while protecting the company's assets?

- A. MFA
- B. CASB
- C. SSO
- D. RBAC

Suggested Answer: C

Community vote distribution



amateurguy Highly Voted 2 years, 9 months ago

Selected Answer: D

OK so here is my theory: They do mention that the help desk has to scramble to create different accounts for across many systems and sso would solve that but that is not what the final question is asking, the actual question is what will be assist the help desk with the onboarding and offboarding process while protecting company assets. RBAC (Role based access control) would be best because the employees who leave the job would be removed of their role and no longer be able to access the assets. When a new employee is onboarded, they would be assigned a role and would be able to access certain assets / accounts based on their role. It would simplify the onboarding and offboarding process and protect assets because the person who doesnt have the right role cant access assets that they are not allowed to .

Im going with D.

What do the experts think?

upvoted 18 times

bigerblue2002 2 years, 9 months ago

I amateurguy has the correct explanation here. Very thorough, thank you sir. Going with D, but I did pick C the first time around but that was due to me not knowing what RBAC was. RBAC seems like the answer to THE actual question.

upvoted 1 times

Treymb6 2 years, 9 months ago

I understand your thought process, but offboarding is not in this equation at all. I believe you are over thinking it.

SSO means less account creation = less work for help desk. I believe C is correct.

upvoted 7 times

Treymb6 2 years, 9 months ago

Oh wait. I see the offboarding part. I still stand with C for the main goal of relieving extra work off of help desk. RBAC helps with certain access but not with accounts themselves.

upvoted 3 times

db97 2 years, 4 months ago

With SSO you can disable the access once and it doesn't matter what roles were assigned, it won't have access to anything.

upvoted 3 times

heinzelrumpel 1 year, 11 months ago

Well, offboarding does not neccesarly mean the employee leaving the company. He could just switch to a different devision, right? Then disbaling account would not help.

upvoted 3 times

Merc16 Highly Voted 2 years, 2 months ago

This was in my exam. But SSO was not one of the choices. the obvious answer was RBAC

upvoted 16 times

Merc16 2 years, 2 months ago

the choices are

A. Casb,

- B. MFA
- C. RBAC
- D. CTI

upvoted 14 times

🗳️ 👤 **RobV** Most Recent 1 year, 6 months ago

Selected Answer: D

D: RBAC

Here's why RBAC is particularly relevant for asset protection:

Granular Access Control: RBAC allows for granular control over access rights. By defining roles and associated permissions, you can restrict access to sensitive assets, reducing the risk of unauthorized access or data breaches.

Least Privilege Principle: RBAC follows the principle of least privilege, meaning that users are granted the minimum level of access needed to perform their job functions. This minimizes the potential damage that can occur in the event of a security incident or if a user account is compromised.

Ease of Management: RBAC simplifies access management by grouping users based on their roles. This makes it easier to handle onboarding and offboarding processes because administrators can assign or revoke access by modifying a user's role rather than dealing with individual permissions across multiple systems.

upvoted 1 times

🗳️ 👤 **skibby16** 1 year, 6 months ago

Selected Answer: D

Which method would work best? RBAC (Role-Based Access Control) is a solution that would work best to assist the help desk with the onboarding and offboarding process while protecting the company's assets. RBAC is a method of granting access to resources based on the roles of users within an organization. RBAC simplifies the management of user permissions by assigning predefined roles to users based on their job functions, rather than granting individual permissions to each user. RBAC can help automate the onboarding and offboarding process by enabling the help desk to quickly create or delete user accounts and assign or revoke access rights based on the roles of the users¹. RBAC can also help protect the company's assets by enforcing the principle of least privilege, which means that users only have access to the resources they need to perform their duties and nothing more².

upvoted 1 times

🗳️ 👤 **32d799a** 1 year, 7 months ago

Selected Answer: C

The most effective solution for streamlining the onboarding and offboarding process while protecting company assets is C. Single Sign-On (SSO).

Single Sign-On (SSO) allows users to log in once and gain access to multiple systems without having to log in separately to each one

upvoted 1 times

🗳️ 👤 **novolyus** 1 year, 7 months ago

Key point is "protecting company assets". You cannot accomplish this with the SSO but with a RBAC

upvoted 1 times

🗳️ 👤 **greatsparta** 1 year, 7 months ago

Selected Answer: C

if SSO is an option, i would go for it because SSO allows users to log in once and access multiple systems and applications without the need to re-enter credentials. It can streamline the on-boarding and off-boarding process by providing centralized control over user access. When an employee joins or leaves the organization, their access can be easily managed through a single point, reducing the workload on the help desk.

RBAC makes the most sense if SSO is not an option

upvoted 1 times

🗳️ 👤 **sirpetey** 1 year, 7 months ago

Selected Answer: D

SSO won't protect company's asset, while RBAC will assign the user appropriate authorization/permissions to the user.

upvoted 1 times

🗳️ 👤 **skibby16** 1 year, 8 months ago

Selected Answer: D

RBAC (Role-Based Access Control) is a solution that would work best to assist the help desk with the onboarding and offboarding process while protecting the company's assets. RBAC is a method of granting access to resources based on the roles of users within an organization. RBAC simplifies the management of user permissions by assigning redefined roles to users based on their job functions, rather than granting individual permissions to each user. RBAC can help automate the onboarding and offboarding process by enabling the help desk to quickly create or delete user accounts and assign or revoke access rights based on the roles of the users¹. RBAC can also help protect the company's assets by enforcing the principle of least privilege, which means that users only have access to the resources they need to perform their duties and nothing more².

upvoted 1 times

🗳️ 👤 **JakeH** 1 year, 8 months ago

Selected Answer: D

Saw this question in the exam. I don't believe SSO was an option, went with RBAC here

upvoted 2 times

🗳️ 👤 **Saphi** 1 year, 9 months ago

Selected Answer: D

While SSO would provide a single login across multiple systems it doesn't provide access to systems in and of itself. Roles would still need assigning to the user across each system in order for access to be provided. I work in an org with a lot of SSO and it is frankly still a nightmare onboarding people onto multiple systems.

upvoted 1 times

🗳️ 👤 **grelaman** 1 year, 9 months ago

Selected Answer: C

SSO is a security solution that allows users to access multiple applications and systems with a single set of credentials. This can help the help desk by automating the account creation process and reducing the number of requests they receive. Additionally, SSO can help protect the company's assets by ensuring that only authorized users have access to sensitive data.

upvoted 1 times

🗳️ 👤 **grelaman** 1 year, 9 months ago

RBAC (Role-Based Access Control) is a security model that defines who has access to what resources. It can help protect sensitive data, but it does not address the issue of automating the account creation process.

upvoted 1 times

🗳️ 👤 **skibby16** 1 year, 10 months ago

SSO is the correct answer. One account and password used across multiple systems.

upvoted 1 times

🗳️ 👤 **kill_chain** 1 year, 10 months ago

Selected Answer: D

Role based access control.... once your role is confirmed you are good to go.

upvoted 1 times

🗳️ 👤 **kyky** 2 years ago

Selected Answer: C

I agree with C

upvoted 1 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

SSO is a technology that allows users to authenticate once and then access multiple systems or services without having to re-authenticate. SSO can simplify the onboarding and offboarding process by allowing the help desk to manage user access to multiple interconnected systems from a single location. When a user is onboarded or offboarded, their access to all systems and services can be managed from a central location.

RBAC (Role-Based Access Control), is a security model that assigns permissions and access rights based on a user's role in the organization. While RBAC can help with managing user access to systems and services, it does not simplify the onboarding and offboarding process across multiple interconnected systems.

upvoted 1 times

🗳️ 👤 **josephconer1** 2 years, 2 months ago

I initially thought it was C, but after reading the discussion and re-reading the question RBAC makes the most sense. When it mentions protecting the company's assets only RBAC would allow that, SSO would not. RBAC provides the principle of least privilege which will add that factor of protection.

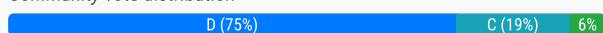
upvoted 2 times

Which of the following is MOST important when developing a threat hunting program?

- A. Understanding penetration testing techniques
- B. Understanding how to build correlation rules within a SIEM
- C. Understanding security software technologies
- D. Understanding assets and categories of assets

Suggested Answer: D

Community vote distribution



🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

Before a threat hunting program can be developed, it is essential to have a complete understanding of the organization's assets, including the types of assets, where they are located, and their value to the organization. Without this understanding, it is difficult to know what to hunt for, where to look, and what data sources to use.

upvoted 4 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: D

D. Remember we are talking about "developing the program". Understanding the categories of assets, such as financial, intellectual property, or customer data, helps to prioritize the focus of the threat hunting program and allocate resources effectively. The others are skills that are refined as part of the overall program.

upvoted 3 times

🗳️ 👤 **Cock** 2 years, 4 months ago

Threat hunting is a proactive process of identifying and neutralizing threats that have already infiltrated an organization's systems. In order to effectively hunt for threats, it is essential to have a comprehensive understanding of the organization's assets and the categories of assets that are present within the network. This includes understanding the types of systems, data, and information that are most valuable to the organization, as well as the different attack scenarios that could be used to target these assets. By having a thorough understanding of the organization's assets, the threat hunting team can more effectively prioritize their efforts, focus on the most critical assets, and develop strategies to protect them from potential threats. Additionally, this understanding can inform the development of correlation rules within a SIEM and help the team to better understand the types of security software technologies that are best suited for their needs.

upvoted 2 times

🗳️ 👤 **catastrophie** 2 years, 5 months ago

D is the correct answer. You need to know what the threat is trying to access and how they may go about it to profile them properly. Just like a bank robber, you're not going to search for them in the park. You can have the greatest detectives in the world with the best equipment but if you're looking in the wrong place what good does it do? Why would they be in the park? Is that where the money is kept? Understand what they want and where they will look, then you can work on building the proper security measures tailored to your specific hunt. Plus you are developing a program here not actively hunting a threat yet.

upvoted 3 times

🗳️ 👤 **CertKid** 2 years, 5 months ago

It should be B - correlating logs in SIEM. You're threat hunting, aka looking for threats within logs to catch what was missed by tools.

upvoted 1 times

🗳️ 👤 **Jeend** 2 years, 5 months ago

Answer C 100%

When creating a threat hunting program it is important to start by developing standardized processes to guide threat hunting efforts. Security teams should outline when and how hunting takes place (whether at scheduled intervals, in response to specific triggering actions, or continuously with the help of automated tools), what techniques are to be used, and which people and TOOLS will be responsible for performing specific threat hunting tasks.

upvoted 1 times

🗨️ 👤 **albano23412415** 2 years, 6 months ago

Selected Answer: D

Threat hunters need to have a good understanding of the company's profile, employee behavior, company valuable data, as well as business activities that could be of interest to attackers so they can baseline what is "normal"

upvoted 1 times

🗨️ 👤 **TeyMe** 2 years, 7 months ago

Selected Answer: D

Purpose of a threat is aiming to archive access to systems that hosts data or main goal. Systems = Assets. That's all!

upvoted 1 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

When threat hunting the goal is to seek out anything malicious. I suppose when you are developing a threat hunting program, knowing everything you can about the assets is great but is that going to do you any good for finding threats? If one were to learn about every single component and mechanic of a refrigerator, what good is that going to do someone when a thief is stealing your yogurt while you're sleeping? I think understanding the security software that you would use to seek out threats is more important.

upvoted 1 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

To add on, when you learn about assets you will also have an understanding of what motives a person might have for intruding your asset, such as some random hungry dude stealing your yogurt. But to seek him out in the night while you're sleeping, a security camera is the perfect tool to find the threat and determine the risk solution you want to implement afterwards. Assets will teach you about the threat actors, not the threats themselves.

upvoted 1 times

🗨️ 👤 **RoVasq3** 2 years, 8 months ago

Selected Answer: D

Threat hunters need to have a good understanding of the company's profile, employee behavior, company valuable data, as well as business activities that could be of interest to attackers so they can baseline what is "normal".

upvoted 2 times

🗨️ 👤 **jagoichi** 2 years, 8 months ago

Selected Answer: D

Answer D

It is important first to prioritize the assets I'm going to protect . Whether they are tangible or intangible. This answer encompasses the other options

upvoted 2 times

🗨️ 👤 **rubali** 2 years, 8 months ago

confused

upvoted 1 times

🗨️ 👤 **Adrian831** 2 years, 8 months ago

Selected Answer: C

When creating a threat hunting program it is important to start by developing standardized processes to guide threat hunting efforts. Security teams should outline when and how hunting takes place (whether at scheduled intervals, in response to specific triggering actions, or continuously with the help of automated tools), what techniques are to be used, and which people and TOOLS will be responsible for performing specific threat hunting tasks.

I choose C for that word "TOOLS".

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 8 months ago

Why wouldn't it be D?

I've read many articles on this and most talking about knowing the risks within the environment and knowing what the key assets/information is needed for threat hunting. Once this information is determined a hypothesis on the type/kind of threat actor/hacker can be better determined imo.

This to me sounds like D would be the answer.

upvoted 2 times

🗨️ 👤 **cyberseckid** 2 years, 9 months ago

its talking about the program , not the threat hunter him self , you need to know what is in the environment to build hypothesis and scenarios , going with D

upvoted 2 times

🗨️ 👤 **Treymb6** 2 years, 9 months ago

I second this.

upvoted 1 times

  **TheSkyMan** 2 years, 9 months ago

Selected Answer: C

My gut says A, but research says C. All the sites I've come across say it's vital for threat hunters to fully understand security tools to be an effective threat hunter. While understanding pentesting would be beneficial, the execution of threat hunting is different. I'll go with C.

<https://www.stickmancyber.com/cybersecurity-blog/7-threat-hunting-misconceptions>

<https://www.simplilearn.com/skills-to-become-threat-hunter-article>

upvoted 2 times

  **shocker111** 2 years, 9 months ago

Selected Answer: A

avid124 is right

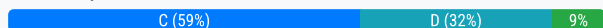
upvoted 1 times

A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security. To BEST complete this task, the analyst should place the:

- A. firewall behind the VPN server.
- B. VPN server parallel to the firewall
- C. VPN server behind the firewall.
- D. VPN on the firewall.

Suggested Answer: D

Community vote distribution



🗳️ 👤 **I_heart_shuffle_girls** Highly Voted 4 years, 5 months ago

I believe C is the correct answer.

upvoted 21 times

🗳️ 👤 **Obi_Wan_Jacoby** 4 years, 5 months ago

I concur with C

upvoted 9 times

🗳️ 👤 **Adonist** Highly Voted 2 years, 9 months ago

Selected Answer: D

D is correct. If you ever set up a firewall and VPN in any company you would know the Firewall is usually the VPN server and it relays the authentication.

upvoted 6 times

🗳️ 👤 **RobV** Most Recent 1 year, 6 months ago

Selected Answer: C

C. VPN server behind the firewall.

upvoted 1 times

🗳️ 👤 **Pavel019846457** 1 year, 8 months ago

Selected Answer: C

C looks the most reasonable.

upvoted 1 times

🗳️ 👤 **chaddman** 1 year, 8 months ago

Selected Answer: C

This is the most secure configuration among the provided options. The firewall will filter incoming and outgoing traffic, allowing only legitimate traffic to reach the VPN server. This setup provides an additional layer of security to the VPN server and the internal network.

upvoted 1 times

🗳️ 👤 **asdDD12** 2 years, 2 months ago

Selected Answer: D

The provided answer is correct.

When the VPN server is on the firewall the firewall itself works before the VPN and after the VPN, which provides highest level of security.

upvoted 3 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

By placing the VPN server behind the firewall, all incoming and outgoing traffic is inspected by the firewall before it reaches the VPN server. This setup provides an additional layer of security, as the firewall can block any unauthorized traffic before it reaches the VPN server, and the VPN server only allows authenticated users to connect to the network.

upvoted 2 times

🗳️ 👤 **heinzelrumpel** 1 year, 11 months ago

The same is achieved with answer D. Every Packet reaching the FW will be inspected, so is every outgoing packet. There is no extra layer of security when placing the VPN behind the FW. I am going with D

upvoted 3 times

🗨️ **2Fish** 2 years, 3 months ago

Agree. C provides the most security. Even though many firewalls contain VPN features these days, this may submit the firewall to more attacks.

upvoted 1 times

🗨️ **CatoFong** 2 years, 4 months ago

Selected Answer: C

C. is for correct

upvoted 1 times

🗨️ **CyberNoob404** 2 years, 5 months ago

Selected Answer: C

C is correct

upvoted 1 times

🗨️ **Mr_BuCh3th34D** 2 years, 6 months ago

I will go with C, VPN server behind FW, and for a simple reason: it is talking about a VPN Server to establish the remote connectivity, if the FW itself was supposed to be the gateway one could argue that VPN at the firewall would be the correct answer, but I agree this is outdated since companies rarely use specific purpose-built VPN servers nowadays.

upvoted 1 times

🗨️ **lordguck** 2 years, 6 months ago

C: The traditional answer is "VPN server behind FW". Personally I think this is outdated for some time now. A VPN Server on a FW offers severe advantages (solution by one provider, central management, packet inspection of VPN connections, FW rules applied to VPN connections, geofencing ...) which outweigh the drawbacks at least in small and medium sized companies.

upvoted 2 times

🗨️ **Weezyfbaby** 2 years, 9 months ago

Selected Answer: C

The most common place for a VPN Server is behind the firewall, often in a DMZ with mail servers, Web servers, database servers, and so on. The advantage of this placement is that it fits cleanly into the network's current security infrastructure. Also, the administrator is already familiar with how to route traffic through the firewall and only has to become familiar with the ports needed by the VPN server.

<https://www.techrepublic.com/article/configuring-vpn-connections-with-firewalls/#:~:text=As%20I%20mentioned%20above%2C%20the,database%20servers%2C%20and%20so%20on.>

upvoted 1 times

🗨️ **Laudy** 2 years, 10 months ago

Selected Answer: C

VPN Servers are almost exclusively internal to the Firewall.

upvoted 1 times

🗨️ **sn30** 2 years, 10 months ago

Selected Answer: C

Best to achieve the highest security, has to be C

upvoted 1 times

🗨️ **Adonist** 2 years, 10 months ago

I would go with D here. I've configured many firewalls and VPN and usually the VPN is on the firewall itself. Unless your VPN server will be on a host (like OpenVPN, Strongswan or even Windows VPN).

upvoted 4 times

🗨️ **FrancisBakon** 2 years, 11 months ago

I have never seen a VPN in front of firewall. At most you have a FW->vpn->fw

If you have an exposed public open vpn, chances of getting compromised are higher than behind the FW

upvoted 1 times

An executive assistant wants to onboard a new cloud-based product to help with business analytics and dashboarding. Which of the following would be the BEST integration option for this service?

- A. Manually log in to the service and upload data files on a regular basis.
- B. Have the internal development team script connectivity and file transfers to the new service.
- C. Create a dedicated SFTP site and schedule transfers to ensure file transport security.
- D. Utilize the cloud product's API for supported and ongoing integrations.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Practice_all** Highly Voted 3 years, 11 months ago
cant believe it, are the options for real?

btw answer is D
upvoted 7 times

🗳️ 👤 **2Fish** 2 years, 3 months ago
Bahahah right, Also, I agree.. this is D
upvoted 3 times

🗳️ 👤 **CyberNoob404** Most Recent 2 years, 5 months ago
Selected Answer: D
D is correct
upvoted 2 times

🗳️ 👤 **f3lix** 2 years, 5 months ago
Selected Answer: D
Newly implemented this at work - Defo D!
upvoted 3 times

🗳️ 👤 **miabe** 2 years, 11 months ago
Selected Answer: D
looks good to me
upvoted 2 times

🗳️ 👤 **SniipZ** 4 years ago
D is correct
upvoted 2 times

🗳️ 👤 **Yeweja** 4 years ago
D is the answer. APIs are best for cloud integrations
upvoted 2 times

🗳️ 👤 **Ty_tyy** 3 years, 10 months ago
agreed and the only one that makes any sense what so ever.
upvoted 1 times

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST steps to confirm and respond to the incident? (Choose two.)

- A. Pause the virtual machine.
- B. Shut down the virtual machine.
- C. Take a snapshot of the virtual machine.
- D. Remove the NIC from the virtual machine.
- E. Review host hypervisor log of the virtual machine.
- F. Execute a migration of the virtual machine.

Suggested Answer: CD

Community vote distribution



forklord72 Highly Voted 2 years, 8 months ago

I guess I'm the only one who thinks it's A and E huh....

upvoted 15 times

Cock 2 years, 4 months ago

I use openAI for this question. It also shows A & E

upvoted 2 times

CatoFong 2 years, 4 months ago

chatgpt did too...

upvoted 2 times

uday1985 1 year, 10 months ago

They said its compromised ! what do you want to review?

upvoted 1 times

Big_Dre 1 year, 9 months ago

they also said confirm which aligned with reviewing to confirm.

upvoted 3 times

2Fish 2 years, 3 months ago

agree... kinda, most of my research was torn between Pause and Shutdown, most recommendations was to shutdown, but I can see pausing would work as well. As it would keep running memory.

upvoted 1 times

2Fish 2 years, 3 months ago

Now that I am rethinking, I agree with catastrophe. DE. Confirm = review logs, Respond = remove the NIC (that would contain the VM) and you could analyze it from VShpere console.

upvoted 1 times

kiduuu Highly Voted 2 years, 2 months ago

Selected Answer: BE

E. Review host hypervisor log of the virtual machine: The first step is to review the host hypervisor log of the virtual machine to determine the extent of the compromise, identify the attacker's methods and tools, and determine what data or systems may have been accessed or compromised. This step can help determine the best course of action to mitigate the incident.

B. Shut down the virtual machine: The second step is to shut down the virtual machine to prevent further damage to the system and the data it contains. Shutting down the virtual machine can prevent the attacker from continuing to access or modify data on the compromised system and limit the spread of the compromise to other systems in the network.

upvoted 5 times

edro Most Recent 1 year, 7 months ago

In the incident response plan, the analyst's initial step is identification, but it necessitates analysis for confirmation, a process facilitated by reviewing the logs. In a corporate setting, it's prudent not to hastily disconnect the system without verification; instead, a thorough examination of logs is recommended. Subsequently, the containment of the incident becomes crucial, presenting a choice among various valid responses. Personally, I lean towards opting for shutting down the system over removing the NIC. The rationale behind this choice lies in the preservation of artifacts essential for further investigation. While removing the NIC may be a more forceful option, it comes at the cost of potentially losing critical evidence. Therefore, my preference is to proceed with reviewing logs and initiating a shutdown for a comprehensive and cautious incident response.

upvoted 1 times

🗳️ 👤 **heinzelrumpel** 1 year, 11 months ago

"which of the following should be the FIRST steps to confirm and respond to the incident? (Choose two.)" If I am conducting an action, as pausing the VM, or as taking a snapshot etc. I am not confirming anything as it is mentioned in the question. So reading the logs would be the best to confirm

upvoted 1 times

🗳️ 👤 **Nixon333** 1 year, 11 months ago

I would say B,E. B: Shutting down the compromised virtual machine is an essential response step to prevent further damage and mitigate the risk of the attacker's continued presence.

E: Reviewing the host hypervisor log is crucial as it can provide valuable information about the activities and events related to the virtual machine.

upvoted 1 times

🗳️ 👤 **Sleezyglizzy** 1 year, 11 months ago

A and C most of the old dumps refers to A and everyone is choosing C.

upvoted 1 times

🗳️ 👤 **alayeluwa** 2 years, 2 months ago

Selected Answer: AC

Don't you have to pause a VM to take a snapshot?

upvoted 2 times

🗳️ 👤 **Dree_Dogg** 1 year, 9 months ago

yep, you gotta pause for a few seconds.

upvoted 1 times

🗳️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: CE

Pausing the virtual machine may allow the attacker to continue operating because the attacker may have already gained persistent access to the system or may have left behind a backdoor or other means of maintaining access. If the attacker still has access to the system, they may be able to continue their activities even if the virtual machine is paused. Additionally, pausing the virtual machine does not provide any additional information to the analyst and may only serve to alert the attacker that their activities have been discovered. Therefore, taking a snapshot of the virtual machine and reviewing the hypervisor logs are more effective first steps to confirm and respond to a compromised virtual machine

upvoted 1 times

🗳️ 👤 **HereToStudy** 2 years, 2 months ago

Removing the NIC (network interface card) from the virtual machine may be a useful step to prevent the attacker from communicating with the outside world. However, removing the NIC may not necessarily stop the attacker from continuing to operate within the virtual machine. The attacker may have already gained access to the system and may have multiple methods of communication, such as an internal network or other communication channels. Removing the NIC may also prevent the analyst from collecting important information about the attacker's activities

upvoted 1 times

🗳️ 👤 **Gaven** 2 years, 3 months ago

Selected Answer: CD

C Dez nutz

No but really contain the machine by removing the NIC and then take a snapshot.

upvoted 2 times

🗳️ 👤 **encxorblood** 2 years, 4 months ago

Selected Answer: AC

A. Pause the virtual machine and C. Take a snapshot of the virtual machine should be the FIRST steps to confirm and respond to the incident.

Pausing the virtual machine will isolate the compromised system and prevent it from further communicating with other systems on the network. This can help to contain the incident and reduce the risk of further damage.

Taking a snapshot of the virtual machine is important for preserving the state of the system at the time of compromise. The snapshot can be used for analysis and forensic purposes to determine the cause of the incident, identify the extent of the damage, and develop a response plan.

upvoted 4 times

🗨️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: CD

preserve evidence; take away ability to spread

upvoted 1 times

🗨️ 👤 **david124** 2 years, 4 months ago

Selected Answer: AC

A. Pause the virtual machine.

C. Take a snapshot of the virtual machine.

The first step in responding to a suspected compromise of a virtual machine should be to pause the virtual machine to prevent any further activity or data exfiltration, and take a snapshot of the virtual machine for later analysis. This will allow the information security analyst to preserve the state of the virtual machine, including all files, system settings, and configurations, for a comprehensive analysis and investigation of the incident. By taking a snapshot, the analyst can revert back to a known good state in case the investigation reveals that the virtual machine is indeed compromised and needs to be rebuilt.

upvoted 2 times

🗨️ 👤 **catastrophie** 2 years, 5 months ago

I would go with D,E. If the VM server (assuming they are using VM server in terms of type one hypervisors - VMWare, Hyper-V, etc.) was compromised then they have access to the hypervisor, this would allow for the potential of a host escape, allowing them to access other physical hosts. By removing the NIC you restrict the attack to that one physical host. With the NIC removed, you've cut off access to the attacker and since the host was compromised, all VM's on that host are considered compromised. Pausing a VM in this situation would seem like it would be as effective as rolling up the window of a convertible with the top down during a rain storm. With the host system isolated you'd be able to review the logs to attempt to find the VM point of entry. Then you can proceed with pausing, creating snapshots of the VMs and proceeding with the investigation.

All this goes out the window if I'm overthinking this and in fact they are talking about a single virtual machine setup as a server such as RHEL... In that case A,D would be what I chose.....

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

I think DE would also work for both. If its a VM on a ESXI Host, then you could still disco the NIC or put into a Deadnet then analyze further.

upvoted 1 times

🗨️ 👤 **mhop321** 2 years, 5 months ago

Selected Answer: CD

A. Pause the virtual machine. - I was leaning towards this but you can achieve what you need with C & D.

B. Shut down the virtual machine. - This is a no, you would lose the evidence and CompTIA always state not to shut the VM down.

C. Take a snapshot of the virtual machine. -This allows you to preserve and analyse the issue. (Confirm)

D. Remove the NIC from the virtual machine. - Stops the spread (contain)

E. Review host hypervisor log of the virtual machine.- You can do this but the analysis can be done through the snapshot.

F. Execute a migration of the virtual machine.- I don't need to explain this one surely.

upvoted 1 times

🗨️ 👤 **mhop321** 2 years, 4 months ago

Or maybe it is A & C - To pause the VM to stop any further exploitation, and take a snapshot to analyse the issue. States "first steps" in the question - so you would pause and analyse the VM before containing the issue. So A&C and then D would come after.

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: AC

Going with A & C.

upvoted 3 times

🗨️ 👤 **roman1000** 2 years, 6 months ago

Selected Answer: AC

This is always discussed from comptia reviewers: turning off/shutting down a compromised VM is a NO. Logical thing to do is to first suspend, then take the snapshot of the VM

upvoted 2 times

🗨️ 👤 **iking** 2 years, 6 months ago

Selected Answer: BE

B. Shutdown the virtual machine - It will stop the other files manipulation and spreading. It also preserves the server for investigation and no other changes will happen anymore. You don't want to do snapshots(aka BACKUP) on that server coz it will take a lot of time especially if this is a big server and has lots of files. If you want to back it up, you can clone it while it is shut down. If it happens that the compromise is a worm, then it will change the files while the server is still on, the time that the snapshots is done, you cant even recover any files coz the whole thing is encrypted. This applies also in removing the NIC. Compromise always needs immediate action not another problem.

Secondly, which of the following should be the FIRST steps to confirm?

E. Check the logs in the hypervisor on that specific VM to investigate. Even if the server is shut down, checking the logs of the hypervisor will still work since this is the host logs, this is your first step to confirm.

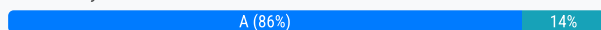
upvoted 5 times

The security team decides to meet informally to discuss and test their response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?

- A. Tabletop exercise
- B. Red-team attack
- C. System assessment implementation
- D. Blue-team training
- E. White-team engagement

Suggested Answer: A

Community vote distribution



josephconer1 2 years, 2 months ago

A.

CySA+ CS0-002 book:

A tabletop exercise is a facilitator-led training event where staff practice responses to a particular risk scenario. The facilitator's role is to describe the scenario as it starts and unfolds, and to prompt participants for their responses. As well as a facilitator and the participants, there may be other observers and evaluators who witness and record the exercise and assist with follow-up analysis. A single event may use multiple scenarios, but it is important to use practical and realistic examples, and to focus on each scenario in turn.

These are simple to set up but do not provide any practical evidence of things that could go wrong, time to complete, and so on.

Tabletop is the only right answer.

upvoted 1 times

wnecrow 2 years, 3 months ago

Selected Answer: D

Informal meeting to discuss and evaluate the incident response plan. therefore, they are not conducting a tabletop exercise since there is no mention of the presence of a red team, which is usually external to the organization. The correct answer should be blue team training. The confusing word here is "test", but i think this is not sufficient to assume there is a tabletop exercise going on.

upvoted 1 times

2Fish 2 years, 3 months ago

Hmmm... Blue team training is typically a process of training individuals or teams in defensive cybersecurity techniques to protect against cyber attacks.

upvoted 2 times

ra774ra7 2 years, 5 months ago

Selected Answer: A

informally

DISCUSS and test their response plan

upvoted 3 times

2Fish 2 years, 3 months ago

100% table top exercise.

upvoted 2 times

RoBery 2 years, 5 months ago

informally= not A

upvoted 1 times

🗨️ 👤 **Orean** 2 years, 4 months ago

What's the correct answer in your opinion, then? Not sure what other option would be centered around discussions.

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: A

I vote A too

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

It is a tabletop exercise.

upvoted 2 times

🗨️ 👤 **david124** 2 years, 9 months ago

A, True

upvoted 1 times

Which of the following BEST explains the function of TPM?

- A. To provide hardware-based security features using unique keys
- B. To ensure platform confidentiality by storing security measurements
- C. To improve management of the OS Installations
- D. To implement encryption algorithms for hard drives

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

TPM provides hardware-based security features using unique keys to enhance the security of computing systems and protect sensitive data.
upvoted 1 times

🗳️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: A

A. is correct
upvoted 1 times

🗳️ 👤 **Freddy90** 2 years, 5 months ago

D - TPM chips are frequently used to provide built-in encryption...
upvoted 1 times

🗳️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: A

I like A too
upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

A is the right answer.
upvoted 1 times

🗳️ 👤 **david124** 2 years, 9 months ago

Trusted Platform Module - A True
upvoted 1 times

A security analyst is investigating an incident related to an alert from the threat detection platform on a host (10.0.1.25) in a staging environment that could be running a cryptomining tool because it is sending traffic to an IP address that is related to Bitcoin.

The network rules for the instance are the following:

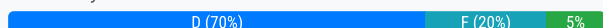
Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

Which of the following is the BEST way to isolate and triage the host?

- A. Remove rules 1, 2, and 3.
- B. Remove rules 1, 2, 4, and 5.
- C. Remove rules 1, 2, 3, 4, and 5.
- D. Remove rules 1, 2, and 5.
- E. Remove rules 1, 4, and 5.
- F. Remove rules 4 and 5.

Suggested Answer: E

Community vote distribution



TheSkyMan Highly Voted 2 years, 9 months ago

Selected Answer: D

I'll go with D. For a staging server, I'd want to deny all external connections; which are rules 1, 2, and 5. Lines 3 and 4 allow SSH and DNS connectivity from only the internal network.

upvoted 10 times

2Fish 2 years, 3 months ago

Agree. I am thinking stop those inbound and outbound "any" connections. Those that are saying it says "sending" is the key word. You can still send both ways using a tcp shell and tcp reverse shell.

upvoted 1 times

Laudy Highly Voted 2 years, 9 months ago

This question is dumb...

upvoted 9 times

cyberseckid 2 years, 9 months ago

yes , it docent even say allow or deny , imo don't waste your time

upvoted 1 times

skibby16 Most Recent 1 year, 6 months ago

Selected Answer: C

The best way to isolate and triage the host is to remove rules 1, 2, 3, 4, and 5. These rules allow inbound and outbound traffic on ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) from any source or destination. By removing these rules, the security analyst can block any network communication to or from the host, preventing any further data exfiltration or malware infection. This will also allow the security analyst to perform a forensic analysis on the host without any interference from external sources.

upvoted 1 times

skibby16 1 year, 9 months ago

What is DNS crypto mining?

While many threats were analyzed, the report found cryptomining generated the most malicious DNS traffic out of any individual category. When placed inside victims' environments, cryptomining malware abuses computing resources to mine for digital currencies like bitcoin, which can be profitable to threat actors.

upvoted 1 times

🗋️ 👤 **nomad421** 2 years ago

Selected Answer: D

D is the best answer. Honestly, I would have only removed the last rule if possible.

upvoted 1 times

🗋️ 👤 **Dutch012** 2 years ago

What ?

upvoted 1 times

🗋️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: F

Read the question. 10.0.1.25 is SENDING traffic to a BTC related ip...

Correct ans is F.

upvoted 1 times

🗋️ 👤 **AaronS1990** 2 years, 4 months ago

How do you suppose it was sending in the first place, an inbound connection too

upvoted 2 times

🗋️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: D

This will block incoming/outgoing.

upvoted 1 times

🗋️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: D

It says isolating staging environment from external network. You need to remove http and https, but you need to keep ssh and dns because it is used in internal network for the staging environment.

upvoted 2 times

🗋️ 👤 **ThisGuyStillLearning** 2 years, 9 months ago

Correct me if I'm wrong, doesn't isolate means "completely alone"? So, how about C?

upvoted 1 times

🗋️ 👤 **Mr_BuCh3th34D** 2 years, 6 months ago

You will definitely isolate the machine if you choose to remove all rules, but that includes yourself. In order to isolate the machine from the rest of the network, but still allows you, as an administrator, to triage/analyze the machine, you still need SSH connectivity. Not sure about DNS though, I think only SSH would be enough for isolation and analysis.

upvoted 1 times

🗋️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: E

You dont want 4 and 5 but you also dont want insecure http traffic in any direction.

Im going with E.

upvoted 1 times

🗋️ 👤 **piotr3439** 2 years, 9 months ago

Selected Answer: F

Block dns and any outbound TCP. I now understnad the question

upvoted 3 times

Which of the following BEST describes what an organization's incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

- A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
- B. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.
- C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution.
- D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening in the future.

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

B. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.

An organization's incident response plan should address how the organization handles public or private disclosures of an incident in accordance with legal and regulatory requirements. This involves considering the appropriate channels and methods for communication, as well as the information that can be shared without violating any laws or regulations. This approach ensures that the organization complies with legal obligations and minimizes potential legal consequences related to the incident.

upvoted 1 times

🗳️ 👤 **f3lix** 2 years, 5 months ago

Selected Answer: B

Even though D sounds fair, B is the correct answer.

upvoted 3 times

🗳️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: B

B is the answer

upvoted 3 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree.

upvoted 1 times

🗳️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: B

B is correct.

upvoted 2 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is the most reasonable answer.

upvoted 2 times

An organization has the following policy statements:

- ⇒ All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized content.
- ⇒ All network activity will be logged and monitored.
- ⇒ Confidential data will be tagged and tracked.
- ⇒ Confidential data must never be transmitted in an unencrypted form.
- ⇒ Confidential data must never be stored on an unencrypted mobile device.

Which of the following is the organization enforcing?

- A. Acceptable use policy
- B. Data privacy policy
- C. Encryption policy
- D. Data management policy

Suggested Answer: D

Community vote distribution



kyky 2 years ago

Selected Answer: C

C. Encryption policy - The statements related to inspecting emails for malware, policy violations, and unauthorized coolant, as well as the prohibition of transmitting confidential data in an unencrypted form and storing it on unencrypted mobile devices, indicate a focus on enforcing encryption policies to protect sensitive information.

Therefore, the organization is primarily enforcing an Encryption polic
upvoted 1 times

heinzelrumpel 1 year, 11 months ago

There is no thing like an encryption policy in the real world. It's all about privacy and data handling
upvoted 2 times

kiduuu 2 years, 2 months ago

Selected Answer: C

The policy statement "Confidential data must never be transmitted in an unencrypted form" and "Confidential data must never be stored on an unencrypted mobile device" suggest that the organization is enforcing an Encryption policy.

The policy statements in the question do include aspects related to data management, such as tagging and tracking of confidential data. However, the primary focus of the policy statements seems to be on the security of data and the prevention of unauthorized access or data breaches.

Therefore, while the organization may have elements of a Data management policy in place, the primary policy being enforced in this case appears to be an Encryption policy.

upvoted 1 times

Cyber_Guru 2 years, 4 months ago

Selected Answer: A

I will go with A (AUP).

AUP is set of rules which are set by an organization and it can be enforced.

upvoted 1 times

AaronS1990 2 years, 4 months ago

That is an absolutely terrible explanation of AUP.

An acceptable use policy is a document the rules which employees follow when using company user must agree to. It can relate to networks but is mostly used as a ruleset for hardware devices such as laptops, company owned smartphones

upvoted 3 times

R00ted 2 years, 8 months ago

Selected Answer: D

D is the correct answer

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Absolutely D. Data Management covers all the requirements here.
upvoted 2 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: D

D is correct
upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: D

Data management police - D is the correct answer .

Comptia has a whole article on data management and it closely relates to the listed points: <https://www.comptia.org/newsroom/2020/02/25/data-management-fundamentals-are-the-first-step-towards-advanced-data-practices-new-comptia-report-reveals>

Also a simple definition for data management is this: The practice of ensuring that data, no matter its form, is protected while in your possession and use from unauthorized access or corruption.

upvoted 3 times

An organization has the following risk mitigation policies:

- ⇒ Risks without compensating controls will be mitigated first if the risk value is greater than \$50,000.
- ⇒ Other risk mitigation will be prioritized based on risk value.

The following risks have been identified:

Risk	Probability	Impact	Compensating control?
A	80%	\$100,000	Y
B	20%	\$500,000	Y
C	50%	\$120,000	N
D	40%	\$80,000	N

Which of the following is the order of priority for risk mitigation from highest to lowest?


- A. A, C, D, B
- B. B, C, D, A
- C. C, B, A, D
- D. C, D, A, B
- E. D, C, B, A

Suggested Answer: C

Community vote distribution

C (81%)

D (19%)

 **trainingsmits** Highly Voted 2 years, 5 months ago

Selected Answer: C

Risk value = Impact x Probability

C (120,000 x .5 = 60,000)-with NO compensating control (and above \$50,000)

B (500,000 x .2 = 100,000)

A (100,000 x .8 = 80,000)

D (80,000 x .4 = 32,000)- NO compensating control (but under \$50,000)

upvoted 22 times

 **2Fish** 2 years, 3 months ago

Agree... of course I forgot to calculate at first like a few others.

upvoted 4 times

 **mrodmy** Highly Voted 2 years, 6 months ago

Selected Answer: D

Risks without compensating controls will be mitigated first if the risk value is greater than \$50,000.

C and D on the table go first.

upvoted 6 times

 **smudder** 2 years, 2 months ago

40% of \$80,000 is not greater than \$50,000.

Only 'C' has priority as it is above the \$50,000.

upvoted 1 times

 **Nouuv** Most Recent 2 years ago

1. find the risk value, which equals impact x probability

so A=80,000 / B= 100,000 / C=60,000/ D=32,000.

2. the first statement says if the compensating control is greater than 50,000 it's mitigated first and the last row of the table says that the only two options with compensating controls are C/D. C (only) is greater than 50,000 so it comes first.

then the risk is mitigated by the order of the risk value - B= 100,000 then A=80,000, and lastly D = 32,000.

so C - B - A - D which is option C.

upvoted 1 times

🗨️ 👤 **Nouuv** 2 years ago

sorry I mean risk *without* mitigation controls grater than 50,000 will be first

upvoted 1 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: C

It's C.

As it is i can see why people would say D but remember that you have to calculate the risk value first

upvoted 1 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: C

After reading Risk Value = Impact x Probability, C now makes sense and is correct.

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 7 months ago

Shouldnt the answer be D? Since C and D is still under the no compensating controls is mitigated first and if over 50K, all their risk value is over 50K

upvoted 3 times

🗨️ 👤 **Mr_BuCh3th34D** 2 years, 6 months ago

No, because that's the impact not the risk value. You have to do probability x impact, for example if probability equals to 20% and impact is \$500k, it's $0.20 \times 500k = 100k$

upvoted 3 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: C

Risk value = impact x probability.

C is correct

upvoted 1 times

🗨️ 👤 **DaroKa** 2 years, 9 months ago

Selected Answer: C

80 k CC-Y

100 k CC-Y

60 k CC-N

32 k CC-N

C is first because of has no compensating control and the risk value is greater than \$50,000

D is last because of has no compensating control and the risk value is LESS than \$50,000

C, B, A, D

upvoted 1 times

🗨️ 👤 **Mr_BuCh3th34D** 2 years, 6 months ago

What? How can \$80k be less than \$50k?

upvoted 2 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

Make sure you properly read the question and know basic math - the answer is C: C,B,A,D

upvoted 1 times

🗨️ 👤 **SandyPanda** 2 years, 9 months ago



C D A B

upvoted 2 times

🗨️ 👤 **david124** 2 years, 9 months ago

i would say D .. cause its said if it exceeds 50.000 and risks without mitigation will be protrizd first.

upvoted 2 times

  **david124** 2 years, 9 months ago
sorry after calculation, C is the right answer.
upvoted 1 times

After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

- A. Header analysis
- B. File carving
- C. Metadata analysis
- D. Data recovery

Suggested Answer: D

Community vote distribution

B (100%)

🗳️ 👤 **sh4dali** Highly Voted 2 years, 9 months ago

Selected Answer: B

B is correct

Three common types of file carving methods are as follows:

Header- and footer-based carving, which focuses on headers like those found in JPEG files. For example, JPEGs can be found by looking for \xFF\xD8 in the header and \xFF\xD9 in the footer.

Content-based carving techniques look for information about the content of a file such as character counts and text recognition.

File structure-based carving techniques that use information about the structure of files.

upvoted 9 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree, this is File Carving for sure.

upvoted 1 times

🗳️ 👤 **dymson** Most Recent 1 year, 8 months ago

so , who and why marks incorrect answers here?

upvoted 3 times

🗳️ 👤 **buchhe** 1 year, 10 months ago

Selected Answer: B

File Carving

File carving is a technique used to fully recover partially recovered files or those discovered to be damaged. Because carving techniques don't depend on the file system in use, file carving is a common method for data recovery when all else fails. The basic concept of carving is that specified file types are searched for and extracted from raw binary data by looking at file structure and content without any matching file system metadata.

upvoted 1 times

🗳️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: B

B seems correct

upvoted 2 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

It looks like what they are describing is file carving.

upvoted 3 times

🗳️ 👤 **david124** 2 years, 9 months ago

B.

File carving is the process of reconstructing files by scanning the raw bytes of the disk and reassembling them.

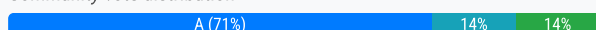
upvoted 2 times

In SIEM software, a security analyst detected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers. Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

- A. Fully segregate the affected servers physically in a network segment, apart from the production network.
- B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours.
- C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.
- D. Collect all the files that have changed and compare them with the previous baseline.

Suggested Answer: A

Community vote distribution



🗳️ 👤 **novolyus** 1 year, 7 months ago

Don't you realize that it is a nonsense to remove PHYSICALLY the servers in order to add to another network segment to isolate them?
upvoted 1 times

🗳️ 👤 **kyky** 2 years ago

Selected Answer: D

D. Collect all the files that have changed and compare them with the previous baseline.

By collecting the files that have changed and comparing them with the previous baseline, you can identify any unauthorized modifications or potential compromises. This step helps in understanding the nature of the changes and determining if they are malicious or not. It allows you to assess the scope and impact of the incident.

upvoted 1 times

🗳️ 👤 **kyky** 2 years ago

Once you have identified the modified files, you can analyze them for any signs of malware or suspicious activity. This may involve scanning the files using antivirus software, checking their hash signatures against known malware databases, or performing deeper analysis to detect any indicators of compromise.

upvoted 1 times

🗳️ 👤 **khrid4** 2 years, 3 months ago

Selected Answer: A

We are talking about a file server that have clients/end-users that may be connecting to it. Answer A, ensures that the users won't be able to access the possible maliciously altered files PREVENTING a more serious compromise.

upvoted 2 times

🗳️ 👤 **yolylight** 2 years, 3 months ago

Selected Answer: C

First confirm that an compromise has occurred

upvoted 1 times

🗳️ 👤 **josephconer1** 2 years, 2 months ago

They state it was brute force -- that's an IoC. Next step is to "prevent" any further damage AKA the answer can only be A.

upvoted 2 times

🗳️ 👤 **Mockento** 2 years, 6 months ago

A - First to prevent

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree, First to prevent = contain the treat and segment/separate.

upvoted 1 times

🗳️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: A

"FIRST to prevent"

I would say A too.

upvoted 1 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: A

A. should be done first to prevent more serious compromise.

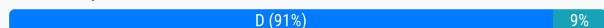
upvoted 2 times

While monitoring the information security notification mailbox, a security analyst notices several emails were reported as spam. Which of the following should the analyst do FIRST?

- A. Block the sender in the email gateway.
- B. Delete the email from the company's email servers.
- C. Ask the sender to stop sending messages.
- D. Review the message in a secure environment.

Suggested Answer: D

Community vote distribution



🗳️ 👤 **uday1985** 1 year, 9 months ago

I wonder how effective this answer if you have hundred email spam reported every day!
upvoted 1 times

🗳️ 👤 **josephconer1** 2 years, 2 months ago

Could be a false positive -- I'd go with D first then take necessary action after if it's a malicious actor.
upvoted 1 times

🗳️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: D

D. You're not just going to block someone without safely checking first
upvoted 3 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree, we need to make sure this is a true positive, before taking action.
upvoted 2 times

🗳️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: D

You dont block without analyze them. Answer is D.
upvoted 2 times

🗳️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: D

D. is correct
upvoted 1 times

🗳️ 👤 **Mattmaxx** 2 years, 5 months ago

Selected Answer: A

I would go with A, if SEVERAL people reported it's already a SPAM, now the next step would be check if is there anything malicious.
upvoted 1 times

🗳️ 👤 **Mattmaxx** 2 years, 5 months ago

My bad! its D!
upvoted 2 times

🗳️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: D

Agree. D
upvoted 2 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: D

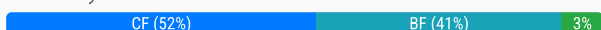
D first, review them first to make sure they are actually spam.
upvoted 2 times

While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certificate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Choose two.)

- A. On a private VLAN
- B. Full disk encrypted
- C. Powered off
- D. Backed up hourly
- E. VPN accessible only
- F. Air gapped

Suggested Answer: CF

Community vote distribution



robullo Highly Voted 2 years, 9 months ago

Selected Answer: BF

Without encryption, an insider threat can steal the server's HD.

upvoted 6 times

RoVasq3 2 years, 8 months ago

I concur with B and F

upvoted 2 times

TeyMe 2 years, 7 months ago

Air gapped is tightly security control for both technical and physical. Check that out.. CYSA study guide

upvoted 1 times

roman1000 2 years, 6 months ago

Air gapped is already secured. Refer to wikipedia, Should root CA be offline?

A common method to ensure the security and integrity of a root CA is to keep it in an offline state. It is only brought online when needed for specific, infrequent tasks, typically limited to the issuance or re-issuance of certificates authorizing intermediate CAs.

upvoted 2 times

amateurguy Highly Voted 2 years, 9 months ago

Selected Answer: CF

I would first say Air Gapped and backed up hourly because in the workplace, it is very common to take backups at minimum on a daily basis (hourly is even better) but i dont think backed up hourly falls under the definition of "secure state" so i have to go with air gapped and powered off.

So i have to go with C and F.

upvoted 5 times

zecomeia_007 Most Recent 11 months ago

Selected Answer: BF

Full disk encrypted: This ensures that even if the physical server is compromised, the data on the disk remains protected.

Air gapped: This isolates the CA server from any network connection, preventing unauthorized access and potential malware infections.

upvoted 1 times

Big_Dre 1 year, 10 months ago

Selected Answer: CF

rule number 1. a powered down system is a secured system because it cant be compromise

2, an air gap is a pretty secure security measure. if they asked for 3 then we can talk encryption now.

upvoted 3 times

heinzlumpel 1 year, 11 months ago

Selected Answer: BF

Airgapped, because Root CA never goes online
Encrypted in case the HDD or server will be stolen
upvoted 1 times

🗨️ 👤 **heinzelrumpel** 1 year, 11 months ago

Our tutor was telling us about a certificate signing ceremony
<https://www.keyfactor.com/blog/top-5-root-ca-key-signing-ceremony-mistakes/>

Please read Mistake #1 - Never bring a root CA online
upvoted 1 times

🗨️ 👤 **heinzelrumpel** 1 year, 11 months ago

A root CA is only signing Certificates for intermediate CAs. This can be done offline. The CSR will be presented to the Root Ca eg. via USB Stick and given back the same way.
upvoted 1 times

🗨️ 👤 **Justian** 1 year, 12 months ago

Selected Answer: CF

Because I'm confident with this answer
upvoted 2 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: AF

By placing the certificate authority server on a private VLAN, it is isolated from other networks and can only be accessed by authorized users. This helps to reduce the risk of unauthorized access and potential attacks.

Options A and F are the most secure states for the certificate authority server when it is not in use. Full disk encryption, backing up hourly, and VPN accessibility can provide additional security measures but do not guarantee the server's complete isolation and protection from unauthorized access or attacks. Powering off the server is also a secure state, but it would not allow the server to be used when it is needed.
upvoted 1 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: BC

Encryption will help with physical attacks. And powered off will prevent remote attacks
upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 2 months ago

Selected Answer: CF

CF
Powered Off is the Most secure state.
Don't think of it too hard. I work in a field that yells this all the time.
upvoted 3 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

the certificate authority server needs to be accessible to issue certificates. So power off would not be the answer
upvoted 1 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

My bad it is when it is not in use. In which case I agree with you
upvoted 1 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

I'm curious what good airgapping is once it's powered off? Maybe powered off and encrypted incase anyone gets physical access
upvoted 1 times

🗨️ 👤 **101martin101** 2 years, 3 months ago

The most secure states for the certificate authority server when it is not in use are:

B. Full disk encrypted: This would prevent unauthorized access to the server's data in case the server is stolen or misplaced. This is especially important for a server that holds sensitive data like a certificate authority.

F. Air gapped: An air-gapped system is physically isolated from other networks, which can prevent it from being accessed or compromised remotely. This can be an effective way to protect the certificate authority server from attacks, particularly those that may be launched over a network.

While the other options, such as on a private VLAN, powered off, backed up hourly, or VPN accessible only, may provide some degree of security, they may not be sufficient to protect the certificate authority server from advanced attacks that may target the server's data and resources.

upvoted 1 times

🗨️ 👤 **aleXplicitly** 2 years, 4 months ago

Selected Answer: CF

root certificate authority is a certificate authority which has been isolated from network access, and is often kept in a powered-down state.

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Agree, "when not in use" is key. That means you can shut it down. All Root CA's should be shutdown when not in use. Of course we can call agree on Air Gap.

upvoted 2 times

🗨️ 👤 **db97** 2 years, 4 months ago

Selected Answer: CF

CA should be off and completely isolated based on the good practices. Going for C&F here.

upvoted 2 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: BF

I think we all agree F for the purposes of physical security, but what about a technical control.

I see the argument for powered off, however those choosing powered off seem to be concerning data at rest only and that's because the question says when the server is not in use. I'll still go with encryption being better than simply turning it off.

upvoted 2 times

🗨️ 👤 **Lukers** 2 years, 3 months ago

Full disk encryption is not a state, but rather a security measure. The question is specifically asking about MOST secure states for the certificate authority server. Considering this I'm going with C and F.

upvoted 1 times

🗨️ 👤 **Cock** 2 years, 4 months ago

The two most secure states for the certificate authority server when it is not in use would likely be "Powered off" and "Air gapped".

Powered off: This minimizes the attack surface of the server and reduces the risk of unauthorized access or manipulation.

Air gapped: By physically separating the server from other networks, it makes it significantly more difficult for attackers to penetrate the network and access sensitive data. Additionally, air gapping ensures that malware cannot spread from one network to another.

upvoted 1 times

🗨️ 👤 **j0n45** 2 years, 5 months ago

Selected Answer: CF

Your root CA should be standalone, and offline.

That is to say, it should not be connected to a forest, and in fact, it should not ever be connected to any network.

A Root CA's only purpose is to sign and revoke subordinate CAs certificate requests, and create a periodic Certificate Revocation List file.

That's it.

Other than that, there is no reason for this CA to even be powered on. Your root CA should be immune from online threats, as it's not online, and should be physically and logically protected.

Your root CA should never be put online for any reason ever. The moment you put this server online, your claim of "offline root" is no longer completely legitimate.

<https://social.technet.microsoft.com/Forums/en-US/342b2de5-0496-4b0c-aeb7-83069a545712/root-ca-offline?forum=winserversecurity>

upvoted 1 times

🗨️ 👤 **bdub16** 2 years, 5 months ago

Selected Answer: BF

Specifically for FDE. "When not in use" makes me think of data at rest.

upvoted 2 times

While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

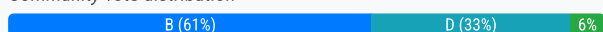
```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?

- A. Delete CloudDev access key 1.
- B. Delete BusinessUsr access key 1.
- C. Delete access key 1.
- D. Delete access key 2.

Suggested Answer: B

Community vote distribution



skibby16 1 year, 6 months ago

Selected Answer: C

Prowler is a tool that can scan AWS environments for security issues and compliance violations. The Prowler report shows that there are two access keys for CloudDev user: access key 1 and access key 2. Access key 1 has not been used in more than 90 days, which violates the AWS CIS benchmark 1.4 (Ensure access keys are rotated every 90 days or less). Therefore, the best recommendation is to delete access key 1 and use access key 2 instead. Deleting CloudDev access key 1, deleting BusinessUsr access key 1, or deleting access key 2 are not appropriate recommendations based on the Prowler report. Reference: <https://github.com/toniblyx/prowler>
upvoted 2 times

[Removed] 1 year, 10 months ago

Selected Answer: D

This is a D account because no one is using it.
upvoted 1 times

kyky 2 years ago

Selected Answer: B

I agree on B
upvoted 1 times

Fibonacci_i 2 years, 1 month ago

Selected Answer: B

I choose B because BusinessUser "FAIL" based on Prowler report
upvoted 1 times

IAlonsoAck 2 years, 2 months ago

I would go with C.
Why 2 different users would be using the same Key?
upvoted 2 times

khrid4 2 years, 3 months ago

Selected Answer: B

I initially thought that it is D but after seeing everyone's points, I'm changing it to B.

Correct me if im wrong but the pass/fail criteria depends on the first line: "Ensure credentials unused for 30 days or great are disabled"

Due to this, I understand that "no users found with access key 2 enabled" passed because the credentials/access key 2 is disabled. Hence, the only option that we need to take action is B.
upvoted 2 times

2Fish 2 years, 3 months ago

Selected Answer: B

B. This is a Fail and should be corrected as it presents the most significant security issues.

upvoted 2 times

  **AaronS1990** 2 years, 4 months ago



absabs, you're misinterpreting what Pass and Fail mean (somehow)

These are Pass or Fail checks that the system is passing or failing if you will on a security basis. The businessUsr key isn't being used or rotated.

That is the security concern and that is what needs to be fixed.

CloudDev hasn't been used since creation but there's no saying when the key was created but it could've been less than 30 days ago

upvoted 1 times

  **absabs** 2 years, 4 months ago



Selected Answer: D

businessur has never used access key 1 (FAIL) -> he/she used it. Why you want delete the used key?

No users found with access key 2 enabled? (PASS) -> so nobody using them. for reduce attack surface, i delete them.



If i am wrong, discuss with me? i going with D

upvoted 2 times

  **db97** 2 years, 4 months ago

Those seem to be pre-written rules to audit things they expect. If they set "businessuser" should not be accessing using key 1 it's because they probably expect to have a "pass" in this point, but surpriseee it failed. So they need to disable that one asap. Maybe I'm wrong but I'm using that logic.



upvoted 1 times

  **knister** 2 years, 5 months ago

Selected Answer: D

I am going to go for D as first thing to disable.



upvoted 1 times

  **R00ted** 2 years, 8 months ago

Selected Answer: B

B is the answer


upvoted 1 times

  **sh4dali** 2 years, 9 months ago

Selected Answer: B

I would say B also.


upvoted 1 times

  **TheSkyMan** 2 years, 9 months ago

Selected Answer: B


The only "FAIL!" in this report is BusinessUsr. I'll go with B.

upvoted 3 times

  **cyberseckid** 2 years, 9 months ago

going with B , it say key 2 is not even enabled

upvoted 3 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: D

D seems correct.

upvoted 2 times



  **david124** 2 years, 9 months ago

i think D, why ?

cause you have remove unused keys first then go to used keys and investigate them.

it's like closing the unused ports first then invisitage the used ports if they should be closed or still opened

upvoted 4 times

  **sh4dali** 2 years, 9 months ago

No your reasoning does not make sense. It states Key 2 is not enabled/ not being used.

upvoted 2 times

After receiving reports of high latency, a security analyst performs an Nmap scan and observes the following output:

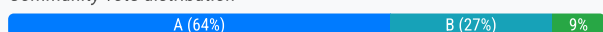
Port	State	Service	Version
80/tcp	open	http	Apache httpd 2.2.14
111/udp	open	rpcbind	
443/tcp	filtered	https	Apache httpd 2.2.14
2222/tcp	open	ssh	OpenSSH 5.3pl Debian
3306/tcp	open	mysql	5.5.40-0ubuntu0.14.1

Which of the following suggests the system that produced this output was compromised?

- A. Secure shell is operating on a non-standard port.
- B. There are no indicators of compromise on this system.
- C. MySQL service is identified on a standard PostgreSQL port.
- D. Standard HTTP is open on the system and should be closed.

Suggested Answer: D

Community vote distribution



TheSkyMan Highly Voted 2 years, 9 months ago

Selected Answer: A

Looks like a SQL database with a web front-end. All ports are necessary except port 2222 which is making an outbound SSH connection. This is indicative of a reverse shell exploit.

upvoted 12 times

2Fish 2 years, 3 months ago

Agree, reports of high latency and a service using a non-standard port.

upvoted 1 times

2Fish 2 years, 3 months ago

However, to also add, sometimes port 2222 is used for SSH to help avoid potential attacks on the default port. Sooo.. yeah..

upvoted 2 times

uday1985 1 year, 9 months ago

Hacker use it to trick you and you use it to trick hacker :D

upvoted 1 times

sudoptgoaway 1 year, 9 months ago

Why do you think its making an outbound ssh connection? It says its open and listening on 2222 which is standard security hardening practice.

upvoted 1 times

amateurguy Highly Voted 2 years, 9 months ago

Selected Answer: B

There arent any indicators of compromise as far as i can tell.

upvoted 6 times

Bihari Most Recent 1 year, 6 months ago

Selected Answer: B

In the provided Nmap scan output, there is no clear evidence suggesting that the system has been compromised. The services mentioned, such as HTTP, HTTPS, SSH, and MySQL, seem to be running on expected ports. There are no unusual or unexpected services or ports mentioned in the scan.

Therefore, the correct answer is:

- B. There are no indicators of compromise on this system.

It's essential to note that the presence of open ports or services alone does not necessarily indicate a compromise. However, further analysis, such as reviewing logs, monitoring network traffic, and conducting a thorough investigation, would be necessary to assess the security of the system.

upvoted 1 times

🗄️ 👤 **novolyus** 1 year, 7 months ago

Selected Answer: A

CVE-2007-0655 : The MicroWorld Agent service (MWAGENT.EXE) in MicroWorld Technologies eScan 8.0.671.1, and possibly other versions, allows remote or local attackers to gain privileges and execute arbitrary commands by connecting directly to TCP port 2222.

upvoted 1 times

🗄️ 👤 **JakeH** 1 year, 8 months ago

Selected Answer: A

This was on the exam. Went with A on this

upvoted 1 times

🗄️ 👤 **sudoptgoaway** 1 year, 9 months ago

Answer is B. ssh listening on port 2222 is a standard security practice.

upvoted 1 times

🗄️ 👤 **grelaman** 1 year, 9 months ago

Selected Answer: A

<https://resources.infosecinstitute.com/topics/threat-hunting/threat-hunting-for-mismatched-port-application-traffic/>

if an application is using an unusual port which pretends to be a normal application port, then it indicates a sign of compromise. Therefore, this indication of compromise is said to be a "Mismatch Port / Application Traffic".

upvoted 1 times

🗄️ 👤 **kmordalv** 1 year, 10 months ago

Selected Answer: D

I believe the correct answer is D

If we look at the output we see that while port 443 is filtered, port 80 is not. This doesn't make much sense and I could think that the attacker opened it.

In a default configuration for the SSH service port 22 is used. If you want to harden the system you will open the service on another port (2222).

Complicated question

upvoted 2 times

🗄️ 👤 **cyberrae** 2 years, 2 months ago

Selected Answer: D

I'm going with D - HTTP and HTTPS both of them doesn't need to be opened at the same time

upvoted 1 times

🗄️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: A

As others have rightly said, this has reverse shell written all over it

upvoted 2 times

🗄️ 👤 **Lis3yve** 2 years, 6 months ago

Selected Answer: A

SSH shell is 22. So this is a reverse shell exploit.

Port 2222 Details

The MicroWorld Agent service (MWAGENT. EXE) in MicroWorld Technologies eScan, allows remote or local attackers to gain privileges and execute arbitrary commands by connecting directly to TCP port 2222.

upvoted 1 times

🗄️ 👤 **White_T_10** 2 years, 7 months ago

I also go with B as there is no indication of compromise. Nmap is just a port scanner.

upvoted 2 times

🗄️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

Selected Answer: A

SSH is working on a non-standard port 2222. looks like reverse shell

upvoted 3 times

🗄️ 👤 **Riwon** 2 years, 3 months ago

And ofcourse, nmap was able to check the version of reverse shell - 5.3 ssh.

upvoted 1 times

🗄️ 👤 **SAAVYTECH** 2 years, 9 months ago

the reason why the analyst conducted the SCAN in the first place is a report of high Latency. High Latency usually occur because of

1- high download volume

2- many application an browser tabs

3- malware

4- streaming services.

i would say that SSH operating on port 2222 is definitely doing some funky shit, i would close that.

upvoted 6 times

🗨️ 👤 **Adonist** 2 years, 9 months ago

Selected Answer: B

I'd go with B. There's no indication it got compromised. Just that it has open ports.

upvoted 2 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Your explanation isn't even what answering B would state.

The questions is effectively asking "something here suggests it was compromised. What?"

Your answer: The fact it says nothing was compromised is what makes me think it was compromised

upvoted 1 times

🗨️ 👤 **david124** 2 years, 9 months ago

Is port 3306 necessary?

In general, you should not open port 3306 as it can make your server vulnerable to attack. If you need to connect to your database remotely, there are more secure options than opening port 3306, such as using an SSH tunnel.

upvoted 1 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

While, yes, you should close plain text http... That's not what was asked. There's no indications that the box was compromised...

upvoted 3 times

An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions, the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:

- ⇒ Successful administrator login reporting priority `` high
- ⇒ Failed administrator login reporting priority `` medium
- ⇒ Failed temporary elevated permissions `` low
- ⇒ Successful temporary elevated permissions `` non-reportable

A security analyst is reviewing server syslogs and sees the following:

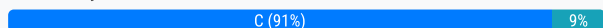
```
<100>2 2020-01-10T19:33:41.002Z webserver sudo 201 32001 - BOM 'sudo vi httpd.conf' failed for Joe
<100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success
<100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
<100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success
<100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe
```

Which of the following events is the HIGHEST reporting priority?

- A. <100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success
- B. <100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success
- C. <100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success
- D. <100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe

Suggested Answer: B

Community vote distribution



🗳️ 👤 **Laudy** Highly Voted 2 years, 9 months ago

B is non-reportable.

C is the correct answer

upvoted 12 times

🗳️ 👤 **cyberseckid** 2 years, 9 months ago

I agree

upvoted 1 times

🗳️ 👤 **ThisGuyStillLearning** 2 years, 9 months ago

Pls help, how do you read the syslog?

upvoted 1 times

🗳️ 👤 **R00ted** 2 years, 8 months ago

Google "su"

upvoted 4 times

🗳️ 👤 **DerekM** 2 years ago

su stands for super user aka admin so doing the command 'su' would be logging in as a administrator account. Whereas 'sudo' is super user do would be doing a command with the admin credentials. sudo is non-reportable and su is a high status. Correct me if I'm wrong please.

upvoted 6 times

🗳️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

how do you understand on the syslog that B is temporary elevated permissions, so it is non-reportable?

upvoted 1 times

🗳️ 👤 **cbrow** 1 year, 8 months ago

The only way of knowing is the differences between the 'su' and 'sudo' commands.

upvoted 1 times

🗳️ 👤 **th3man** 2 years, 7 months ago

su provides temp acces (non-reportable), but you chose C, and stated B is non-reportable (uses sudo). ???

upvoted 1 times

🗄️ 👤 **cbrow** 1 year, 8 months ago

Su allows users to switch to the root account and perform administrative tasks, while sudo allows users to execute specific commands with elevated privileges

upvoted 2 times

🗄️ 👤 **2Fish** 2 years, 3 months ago

Agree. This is C, this is a successful login from su.

upvoted 1 times

🗄️ 👤 **anhod1578** Most Recent 1 year, 3 months ago

Selected Answer: D

The provided line "su vi syslog.conf failed" indicates an unsuccessful attempt to gain elevated privileges and edit the system log file on a server named "financeserver" by a user named "joe".

This event suggests a potential security concern, as a regular user attempted to gain administrator privileges and modify a critical system file. It's important to investigate this event further to understand the context and potential motivations behind the attempt.

upvoted 1 times

🗄️ 👤 **Gwatto** 1 year, 7 months ago

Selected Answer: C

Answer has to be C. "SU" meaning switch user to the root account which is a successful login with admin privilege .

upvoted 1 times

🗄️ 👤 **Leonidasss** 2 years, 3 months ago

Selected Answer: C

su switches permanently

upvoted 3 times

🗄️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: C

Sudo is the command for elevated admin privileges and C doesn't have this command and was successful.

upvoted 1 times

🗄️ 👤 **TKW36** 2 years, 5 months ago

Selected Answer: C

The event that is the highest reporting priority is C.

According to the organization's reporting priorities, a successful administrator login is a high priority, and a failed administrator login is a medium priority. In this log message, the user is attempting to log in to the administrator account using the "su" command, which suggests that the user is attempting to gain elevated privileges. Therefore, this event is a failed administrator login, which is a medium reporting priority.

In comparison, the other log messages in the choices provided involve the use of the "sudo" command, which indicates that the user is attempting to temporarily escalate permissions rather than logging in to the administrator account. As such, these events would not be considered administrator login events and would not be considered high or medium reporting priorities. Instead, they would be considered temporary elevated permissions events, which have a low or non-reportable reporting priority according to the organization's reporting priorities.

upvoted 3 times

🗄️ 👤 **White_T_10** 2 years, 7 months ago

This is a tricky question. However, the main difference between the two is that su requires the password of the target account, while sudo requires the password of the current user. So, I would go with C.

upvoted 3 times

🗄️ 👤 **Ouma** 2 years, 8 months ago

Selected Answer: C

Definitely C

upvoted 1 times

🗄️ 👤 **cfrazzy** 2 years, 9 months ago

Selected Answer: C

C indicates root access and using root privileges

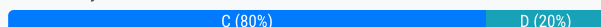
upvoted 1 times

An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place, which of the following should be notified for lessons learned?

- A. The human resources department
- B. Customers
- C. Company leadership
- D. The legal team

Suggested Answer: C

Community vote distribution



🗳️ 👤 **talosDevbot** Highly Voted 2 years, 4 months ago

Selected Answer: C

Keyword here is Lessons Learned.

This phase of IR is used to improve security measures and IR handling. Company leadership should be involved in that
upvoted 5 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree. 100% leadership team. Legal does not really care about lessons learned.
upvoted 2 times

🗳️ 👤 **AaronS1990** Most Recent 2 years, 4 months ago

Selected Answer: C

Lessons learned will be pushed up to company leadership
upvoted 4 times

🗳️ 👤 **Cock** 2 years, 4 months ago

Selected Answer: D

D. The legal team. It is important to notify the legal team in the event of a security breach, as they may need to handle legal implications and ensure compliance with relevant laws and regulations. The incident response team should also inform company leadership, as they will need to be aware of the situation and any potential impact on the company's reputation. Depending on the severity and scope of the breach, customers may also need to be notified. The human resources department may also be involved in the aftermath of a security breach, but is not typically the first group to be notified in this type of situation.
upvoted 2 times

🗳️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: C

just need to read the scenario fully. it is a lessons learned exercise. kick it up to leadership
upvoted 1 times

🗳️ 👤 **f3lix** 2 years, 5 months ago

Selected Answer: D

D. The legal team. Pure use of English here, could have gained access (not did not), mitigate significant damage (meaning theres likely damage but insignificant), I believe the legal team should be notified.
upvoted 1 times

🗳️ 👤 **Cyril_the_Squirrel** 2 years, 7 months ago

C is correct, there was no actual breach. Lessons learnt is an internal exercise.
upvoted 2 times


🗳️ 👤 **Cizzla7049** 2 years, 7 months ago

answer should be customers. This involves credit card
upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

i see what you are saying, but is states "could have gained access". We are not sure at this point. However, if there was a data leak of breach, customers would need to be notified for sure.



upvoted 1 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: C

C - company leadership

upvoted 3 times

  **Laudy** 2 years, 9 months ago

agreed. C

upvoted 3 times

When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

```
Jun 25 10:40:34 localhost pexec[19962]: comptia: Executing command [USERroot] [TTY=unknown] [CWD=/home/comptia] [COMMAND=/usr/libexec/gsd-backlight-helper --set-brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xroot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

Which of the following can the analyst conclude from viewing the log file?

- A. The comptia user knows the sudo password.
- B. The comptia user executed the sudo su command.
- C. The comptia user knows the root password.
- D. The comptia user added himself or herself to the /etc/sudoers file.

Suggested Answer: D

Community vote distribution

C (100%)

Laudy Highly Voted 2 years, 9 months ago

Wrong. C is correct.

the user is not in the sudoers file. you use your own password for that. the user used the su command to switch user accounts. when no user is specified, the su command defaults to the root account. the user is now logged into the root account. you need to know the root password to log into the root account.

upvoted 15 times

cyberseckid 2 years, 9 months ago

but that means b is also right ?

upvoted 1 times

Tag 2 years, 8 months ago

no, B states that they used the "sudo su" command, they only used "su"

C is correct

upvoted 3 times

2Fish Most Recent 2 years, 3 months ago

Selected Answer: C

Agree with Laudy. C is correct.

upvoted 1 times

CatoFong 2 years, 4 months ago

Selected Answer: C

Laudy is correct

upvoted 1 times

Sethwlch98 2 years, 5 months ago

Selected Answer: C

C is the correct answer

upvoted 1 times

Learner_77 2 years, 8 months ago

Comptia user used su command to login as root user

su requires the password of the target account, while sudo requires the password of the current user.



upvoted 1 times

ryanzou 2 years, 8 months ago

Selected Answer: C

C is correct

upvoted 2 times

  **Weezyfbaby** 2 years, 9 months ago

Selected Answer: C

Agree w/ Laudy

upvoted 1 times

A security analyst is reviewing the following server statistics:

% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following is MOST likely occurring?

- A. Race condition
- B. Privilege escalation
- C. Resource exhaustion
- D. VM escape

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **david124** Highly Voted 2 years, 9 months ago

C right answer, as you can see CPU usage is +95% all the time
upvoted 5 times

🗳️ 👤 **Kmz7** Most Recent 2 years, 8 months ago

Definitely C.
upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree, this is resource exhaustion.
upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

Looks like resource exhaustion.
upvoted 4 times

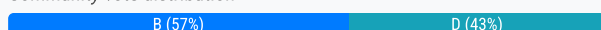
A company has started planning the implementation of a vulnerability management procedure. However, its security maturity level is low. So there are some prerequisites to complete before risk calculation and prioritization.

Which of the following should be completed FIRST?

- A. A business impact analysis
- B. A system assessment
- C. Communication of the risk factors
- D. A risk identification process

Suggested Answer: D

Community vote distribution



Whoah Highly Voted 2 years, 7 months ago

Selected Answer: B

Step 1. Assess

Step 2. Prioritize

Step 3. Act

Step 4. Reassess

Step 5. Improve

upvoted 18 times

khrid4 Highly Voted 2 years, 3 months ago

Selected Answer: D

Before risk calculation and prioritization, a risk "identification" process should first be created, given that the security level is low, it is possible that the company doesn't have this in the first place.

I. Once the process is established, the process may include the conducting of a system assessment or other means as part of the identification.

As per COMPTIA Cysa Official Study Guide:

Under Risk Identification Process (NIST SP 800-39):

Assess, Respond, Monitor, Frame.

upvoted 10 times

Dutch012 2 years ago

Logic!, I 100% agree

upvoted 1 times

Xoomalla 1 year, 10 months ago

The option "D. A risk identification process" refers to the process of recognizing potential threats and vulnerabilities that could negatively impact an organization. While it's a crucial part of risk management, risk identification is somewhat ahead of the game if the organization's security maturity level is low.

upvoted 1 times

Xoomalla 1 year, 10 months ago

CHATGPT, and it make sense...

upvoted 1 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: D

D. A risk identification process

Before conducting a business impact analysis, system assessment, or communication of risk factors, it's crucial to identify and understand the risks associated with the systems and processes in the organization. The risk identification process helps in identifying potential vulnerabilities, threats,

and weaknesses that may exist in the current environment. Once risks are identified, the organization can then proceed to assess their impact on the business (business impact analysis), evaluate the current state of systems (system assessment), and communicate the relevant risk factors.

upvoted 1 times

🗳️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: D

In the context of implementing a vulnerability management procedure, the first step should be to identify and assess the risks associated with the organization's systems and assets.

upvoted 1 times

🗳️ 👤 **Nixon333** 1 year, 11 months ago

Its B.A system assessment is the foundational step in vulnerability management. Before calculating and prioritizing risks, it is essential to have a comprehensive understanding of the organization's systems, assets, and their associated vulnerabilities.

D. A risk identification process is part of the vulnerability management procedure, but it comes after the system assessment.

upvoted 2 times

🗳️ 👤 **Sleezyglizzy** 1 year, 11 months ago

D

It has to be identified first, look it up.

upvoted 1 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

Since the security maturity level of the company is low, it is important to complete some prerequisites before risk calculation and prioritization. The first step should be to identify the risks that the organization is facing. Therefore, option D, which suggests completing a risk identification process, should be completed first.

Once the risks have been identified, the organization can then move on to perform a system assessment to understand the current state of their security posture. After that, they can conduct a business impact analysis to understand the potential impact of these risks on their business operations. Finally, the organization can communicate the risk factors to the relevant stakeholders to ensure that everyone is aware of the potential risks

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: B

B. A system assessment will typically involve identifying risks. This is a funky question because I can see B or D being ok. But I would lean towards an assessment FIRST.

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Hmmm ..khrid makes a good point.. This could very well be D.

upvoted 1 times

🗳️ 👤 **i_Alfie** 1 year, 7 months ago

Why not A?

upvoted 1 times

🗳️ 👤 **AaronS1990** 2 years, 4 months ago

"prerequisites to complete before risk calculation and prioritization"

This steers me to risk identification being the most feasible, though I think a few of these answers make sense

upvoted 1 times

🗳️ 👤 **Cock** 2 years, 4 months ago

A. A business impact analysis should be completed first. Before starting the implementation of a vulnerability management procedure, it is important to understand the potential impact of a security breach on the company's operations, reputation, and finances. A business impact analysis can help identify critical systems, data, and processes and determine the consequences of a security breach on these areas. This information is crucial in determining the priority and resources needed for the vulnerability management process.

upvoted 2 times

🗳️ 👤 **i_Alfie** 1 year, 7 months ago

i agree. you do BIA first before anything else especially your maturity level is low

upvoted 1 times

🗳️ 👤 **CatoFong** 2 years, 4 months ago



Selected Answer: B

assess your systems so you know what vulnerabilities you are potentially managing
upvoted 3 times

  **Stiobhan** 2 years, 4 months ago

Selected Answer: D

I am going to go with D. My rationale is a system assessment would be part of the risk identification process - <https://www.cyberwatching.eu/cyber-risk-identification#:~:text=As%20mentioned%20in%20the%20section%20on%20the%20cyber,Decide%20what%20to%20do%20about%20the%20residual%20risk>
upvoted 2 times



  **absabs** 2 years, 4 months ago

"to complete before risk calculation and prioritization." --> before risk calculation, we must check system. We don't assess system that we don't know about
upvoted 1 times

  **MrRobotJ** 2 years, 7 months ago

Selected Answer: B



The question literally says "risk calculation and prioritization."
upvoted 1 times

  **MrRobotJ** 2 years, 7 months ago
"before risk calculation and prioritization"
upvoted 3 times

  **Cizzla7049** 2 years, 7 months ago



Selected Answer: B

assess the system to know what all you're protecting
upvoted 2 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: D

D is the most reasonable first choice.
upvoted 3 times

  **Laudy** 2 years, 9 months ago

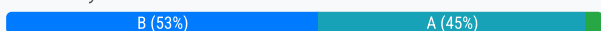
agreed D
upvoted 2 times

An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts. A security analyst has created a script to snapshot the system configuration each day. Following is one of the scripts: `cat /etc/passwd > daily_$(date +%m_%d_%Y)`
This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?

- A. `diff daily_11_03_2019 daily_11_04_2019`
- B. `ps -ef | grep admin > daily_process_$(date +%m_%d_%Y)`
- C. `more /etc/passwd > daily_$(date +%m_%d_%Y_%H:%M:%S)`
- D. `ls -lai /usr/sbin > daily_applications`

Suggested Answer: B

Community vote distribution



f3lix Highly Voted 2 years, 5 months ago

Selected Answer: B

Guys dont make a mistake, B is the answer to this question. The question is asking to see more information about the running script. it'll be `ps -ef | grep "the script, i.e python"` ... with this, you can see how long the script has been running for, the storage location of the capture, size and the time the script started etc. I do this on daily basis so I know. Answer is affirmative B!!

upvoted 8 times

aleXplicitly 2 years, 4 months ago

My guy, the script is bash not python... all the analyst is doing is outputting the `/etc/passwd` file to different files differentiated by each day. So the only logical thing he would do is to view the diff of 2 files to see which users are created each day.

Why would viewing processes help the analyst in solving the problem with sysadmins creating unnecessary accounts.

upvoted 10 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: B

Answer is B.

upvoted 1 times

32d799a 1 year, 7 months ago

Selected Answer: A

Option B is focused on monitoring processes containing the term "admin" but is not directly related to changes in user accounts.

To address the security incidents where unauthorized user accounts are being created, you would want to compare the snapshots of the `/etc/passwd` file on different days to identify any changes. Therefore, the most relevant command is:

A. `diff daily_11_03_2019 daily_11_04_2019`

upvoted 2 times

chaddman 1 year, 8 months ago

Command A: `diff daily_11_03_2019 daily_11_04_2019`

This command compares the snapshots of the `/etc/passwd` file on two different days to find any differences. This could potentially highlight unauthorized user account creation by showing what changed between these two snapshots.

upvoted 1 times

Xoomalla 1 year, 10 months ago

My Guy (Just kidding), Your answer would convince me if the word admin is not there. Why greping for admin? administrator can be root or Xoomalla or F3lix.

upvoted 1 times

naleenh 1 year, 10 months ago

Selected Answer: B

The command in option B (`ps -ef | grep admin > daily_process_$(date +%m_%d_%Y)`) would provide the analyst with additional useful information relevant to the script. This command uses the `ps` command to list all running processes (`-ef` flag) and then pipes the output to `grep` to search for processes containing the keyword "admin." The results are then redirected to a file named with the current date in the filename.

upvoted 1 times

🗳️ 👤 **Sleezyglizzy** 1 year, 11 months ago

B

most logical to me

upvoted 1 times

🗳️ 👤 **tutita** 2 years ago

Selected Answer: B

A doesn't seem right, you are comparing 2 dates which are not stated above in the questions, and also what about the other days? I think running the command `ps` to see the processes make more sense and adds additional information

upvoted 2 times

🗳️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: B

A compares two different snapshots of the `/etc/passwd` file, which could be useful for identifying changes to the user account database over time but would not provide any information about specific processes or user activity.

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 3 months ago

Selected Answer: A

Diff Daily duh

upvoted 1 times

🗳️ 👤 **101martin101** 2 years, 3 months ago

Selected Answer: A

The script `cat /etc/passwd > daily_$(date +%m_%d_%Y)` creates a daily snapshot of the `/etc/passwd` file, which contains information about user accounts on the system. The script captures this information and saves it in a file named `daily_<date>`.

To gather additional useful information relevant to the above script, the security analyst could run the following command:

A. `diff daily_11_03_2019 daily_11_04_2019`

This command would compare the contents of the `daily_11_03_2019` and `daily_11_04_2019` files and show any differences. This would help the analyst identify any unauthorized changes to user accounts that may have been made between those two days.

upvoted 2 times

🗳️ 👤 **AC6280** 2 years, 4 months ago

Selected Answer: B

So the question is presented as, the analyst is doing something each day (over some period of time) to gather information. I initially thought A, but that command only works for a single day as others have pointed out. I think this is CompTIA trying to trick you by giving a command that seems very useful (and honestly I would do A in real life but) but only works in that one instance (why not use the variables for that day in the script?).

B allows you to output the running processes each day running under the security context of admin. Maybe there's a rogue process that has elevated its permissions. But by reviewing the processes each day, you can see what 'admin' is doing, so if there's a funny process or port that sticks out, you can investigate further.

upvoted 1 times

🗳️ 👤 **khrid4** 2 years, 3 months ago

"additional useful information relevant to the above script"

I am not sure if I can comprehend the keyword above directly but I think only A makes the most relevance for the existing script. While others is more relevant to conducting further investigation.

upvoted 1 times

🗳️ 👤 **aleExplicitly** 2 years, 4 months ago

Selected Answer: A

Viewing the diff of each day will help the analyst figure out which accounts were created by the sysadmins...

upvoted 1 times

🗳️ 👤 **db97** 2 years, 4 months ago

Selected Answer: A

I tested this on my home lab and the "A" seems to be most logic/useful one.



The diff command will show you the output of why file1.txt is different of file2.txt. For example:

```
echo "test" >> file1.txt
echo "test" >> file2.txt
echo "something else" >> file1.txt
```

diff file1.txt file2.txt --> output will be: "something else"

And that would be useful for the security analyst and figure out if new accounts were added from one day to another.

upvoted 3 times

  **Cock** 2 years, 4 months ago

Selected Answer: A

The command "diff daily_11_03_2019 daily_11_04_2019" would be useful in this scenario because it compares two files and outputs the differences between them. By comparing the /etc/passwd file snapshots taken on different dates, the analyst could identify any unauthorized user accounts that were added or removed over time, which would help with their investigation into the security incidents.

upvoted 3 times

  **sudoptgoaway** 1 year, 9 months ago

Good point cock.



upvoted 2 times

  **IanRogerStewart** 2 years, 5 months ago

Selected Answer: A

While it would require changing each day, A is the only one that makes sense. B is only going to pull out processes with the word "admin" in them (why would that be useful?). C & D are nonsense.

upvoted 1 times

  **knister** 2 years, 5 months ago

Selected Answer: B

f3lix all the way

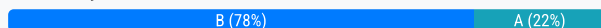
upvoted 3 times

A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

- A. Submit a change request to have the system patched.
- B. Evaluate the risk and criticality to determine if further action is necessary.
- C. Notify a manager of the breach and initiate emergency procedures.
- D. Remove the application from production and inform the users.

Suggested Answer: A

Community vote distribution



🗳️ 👤 **skibby16** 1 year, 6 months ago

Selected Answer: B

Before taking any immediate actions, it's essential to evaluate the risk and criticality of the known vulnerability. This involves assessing the potential impact on the organization, understanding the exploitability of the vulnerability, and considering the business context. Based on this evaluation, the organization can make informed decisions about the urgency and appropriate response, whether it involves immediate patching, implementing compensating controls, or planning a more comprehensive remediation strategy. Simply patching without understanding the risk may lead to unintended consequences or unnecessary disruptions.

upvoted 1 times

🗳️ 👤 **uday1985** 1 year, 9 months ago

Known Vuln = Known impact, risk and consequences ! So patch it!

Again dumb question!

However, in real life! there is always testing the patch ! it might break things in the site

upvoted 2 times

🗳️ 👤 **Chilaqui1es** 1 year, 8 months ago

Known = There is a patch for it / missing patch

Critical System means act asap

upvoted 2 times

🗳️ 👤 **buchhe** 1 year, 10 months ago

Selected Answer: A

It is a known vulnerability on the company's web application.... which implies the possible accessible to and from the world. I think some of you voted for B are overthinking of the issue. It needs to initiate change management....

upvoted 1 times

🗳️ 👤 **SimonR2** 2 years, 1 month ago

A "vulnerability" was found in a "critical system". From that information we have no way of knowing if the vulnerability is even relevant or how serious it is. This is why the analyst must determine the severity of the vulnerability and it's relevance.

Like for example in my company we have an internal load balancer which is currently outdated and running on an old software version. We can see the vulnerabilities but since the load balancer is only internally accessible it's not necessary for us to patch it. Therefore we ignore those particular vulnerabilities it finds.

Definitely B

upvoted 3 times

🗳️ 👤 **novolyus** 1 year, 7 months ago

"Critical enterprise web application" remove all that you have explained in the second part of your comment.

Web access and critical. You should patch it through change management procedure.

upvoted 1 times

🗳️ 👤 **cyberrae** 2 years, 2 months ago

Selected Answer: A

From the study guide practice questions and this exam dump - whenever compita has an question about an critical vulnerability - the answer is always to remove the critical vulnerability (I know in the real world - we verify beforehand)

upvoted 1 times

🗨️ **AaronS1990** 2 years, 4 months ago

I have to agree with J0n45.

I too thought B but question 215 makes me think A

upvoted 2 times

🗨️ **absabs** 2 years, 4 months ago

Selected Answer: B

You must verify that web application accessible for wild life. I going with B. My opinion; concept of A is more narrow than B

upvoted 1 times

🗨️ **j0n45** 2 years, 5 months ago

Hello everyone, I see all comments are choosing B and everything that's written makes sense.

However I have a question;

QUESTION 215 in this dump says: The analyst immediately deploys a critical

security patch. and the ANSWER to that question was: A Known exploit was discovered.

Then given the above, why would choose B over A, if we use the same logic in the 2 questions? I mean both are mentioning a known vulnerability/exploit was discovered..

I will monitor that question for an answer until the next 7 days (day of the exam), appreciate your feedback profs.

upvoted 3 times

🗨️ **2Fish** 2 years, 3 months ago

I think the difference here was or is, in this question, it mentions it is a "known vulnerability" in a Critical system. In question 215 from you

description, is mentions a critical security patch. This question does not mention there was a critical exploit found. I see what your saying though

upvoted 3 times

🗨️ **gwanedm** 2 years, 7 months ago

Selected Answer: B

Any time you have a vulnerability show up on a scan result it has to be verified

upvoted 1 times

🗨️ **jchutch2** 2 years, 8 months ago

Selected Answer: B

B

You don't just blindly have a critical system patched without evaluating the risk, not only of the vulnerability but also of installing the patch. Patches ROUTINELY bring down critical services.

upvoted 2 times

🗨️ **Treymb6** 2 years, 8 months ago

Selected Answer: B

There is such a thing as risk acceptance. Since it is a critical application, you definitely want to make sure even NEED to mess with it first.

upvoted 3 times

🗨️ **tehge** 2 years, 9 months ago

Selected Answer: B

the keyword is "a known vulnerability" which mean you need to re evaluate the vulnerability to know if there would be any impact

upvoted 3 times

🗨️ **Adrian831** 2 years, 9 months ago

Selected Answer: B

Going with B also

upvoted 1 times

🗨️ **sh4dali** 2 years, 9 months ago

Selected Answer: A

A is correct.



upvoted 2 times

🗨️ **marc4354345** 2 years, 9 months ago

Selected Answer: B

B makes more sense. Always start by understanding what is the risk and possible impact.

upvoted 2 times

  **sh4dali** 2 years, 9 months ago



Not really. It already said critical patch is missing.

upvoted 1 times

  **Maverick713** 2 years, 9 months ago

Actually it doesn't. It says a critical system, not a critical vulnerability. I thought A at first also but re-reading the question I am leaning with B.

upvoted 2 times

  **Big_Dre** 1 year, 10 months ago

it also says a known vulnerability. if its know, there is no need to investigate more move on to patching. i stand with A

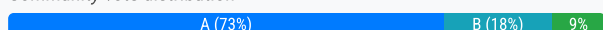
upvoted 2 times

A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

- A. Implement a secure supply chain program with governance.
- B. Implement blacklisting for IP addresses from outside the country
- C. Implement strong authentication controls for all contractors.
- D. Implement user behavior analytics for key staff members.

Suggested Answer: A

Community vote distribution



🗳️ 👤 **huehuehello** Highly Voted 1 year, 8 months ago

this questions are just fo fckin dumb that it hurst my eyes to read
upvoted 7 times

🗳️ 👤 **skibby16** Most Recent 1 year, 6 months ago

Selected Answer: A

Implementing a secure supply chain program with governance would be the most appropriate option to ensure that the third-party service provider complies with the requirement of only sourcing talent from its own country. This program would involve establishing policies, procedures, and contractual agreements that explicitly outline the expectations regarding the sourcing of talent and ensure compliance with geopolitical and national security interests. It provides a framework for managing and overseeing the supply chain, including the sourcing of personnel, to meet the company's specific requirements.

upvoted 1 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: A

Implementing a secure supply chain program with governance can help the manufacturing company ensure that the third-party service provider is meeting the requirement of sourcing talent only from its own country. This program can include measures such as conducting background checks on all contractors, verifying the location of the contractors' offices, and requiring the third-party service provider to provide regular reports on the location of their talent.

upvoted 3 times

🗳️ 👤 **AC6280** 2 years, 4 months ago

Selected Answer: C

I guess I'm playing Devil's advocate here.

A- I don't understand what supply chain programs with governance have to do with Tier 1 support. It doesn't say they're manufacturing the product which, to me, would be the tip off that we need to look at supply chain.

B- Kind of? But easily circumvented.

C- Authentication platforms can allow/block access based on location (conditional access).

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#locations>

<https://today.uic.edu/duo-to-block-authentication-in-countries-or-regions-subject-to-ofac-sanctions/>

D- Throwaway answer. What would analytics do to prevent anything? While there are products that use behavior analytics to apply policy, I don't think that's what we're talking about here. Also, you would have to train the software for a bit to understand what's anomalous.

upvoted 1 times

🗳️ 👤 **AC6280** 2 years, 3 months ago

Reading more on supply chain, changing answer to A. From the all-in-one Exam guide:

This is a key part of performing supply chain risk assessments: to determine your risk that results from what your vendors and suppliers are or are not doing to protect themselves. Let's look at some things an organization may look at to determine whether its vendors are practicing due diligence and, if not, what the level of risk might be:

(...)

- Ensure that contracts/agreements include requirements for adequate security controls.
- Ensure that service level agreements are in place if appropriate.
- Review the vendor's security program before signing an agreement, and periodically thereafter.
- Review internal and external audit reports and third-party reviews.
- Conduct onsite inspection and interviews after signing the agreement.
- Ensure that the vendor has a business continuity plan (BCP) in place.
- Implement a nondisclosure agreement (NDA).

upvoted 6 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Agree, this right here^[^]. I was about to type all this out, thanks for doing it already. This is basically a 3rd party risk assessment which would include all the things you mentioned and more.

upvoted 3 times

🗨️ 👤 **knister** 2 years, 5 months ago

Does anyone have a source of information for this response? Because I am still with amateurguy.

upvoted 1 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

third-party service so bolstering the supply chain is good

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: A

IP blacklisting can be bypass with VPN, so it does not help the require situation. In this case, it needs to have secure supply chain vector. The answer should be A.

upvoted 2 times

🗨️ 👤 **Adrian831** 2 years, 9 months ago

Selected Answer: A

I agree with A

upvoted 1 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: A

A is correct. It said tier 1, which is physical security.

upvoted 1 times

🗨️ 👤 **bigerblue2002** 2 years, 9 months ago

Plus, could one note just use a VPN app to appear to be in country? Asking for a friend.

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

what does supply chain have to do with security support? I would say ip blacklisting is better. Im going with B.

upvoted 2 times

🗨️ 👤 **cyberseckid** 2 years, 9 months ago

read more about supply chain , going with a

upvoted 5 times

🗨️ 👤 **Treymb6** 2 years, 9 months ago

Not B. Blacklisting a country's IP is easily bypassed with a VPN.

A is correct.

upvoted 3 times

🗨️ 👤 **Big_Dre** 1 year, 9 months ago

ohh boy thought i was the only one thinking that. been wondering too. don't know if its the English in the question or just the construct hahah

upvoted 1 times

A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

- A. Nessus
- B. Nikto
- C. Fuzzer
- D. Wireshark
- E. Prowler

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **MetaHack** 1 year, 10 months ago

The answer is AAAAAA
upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: A

A is the right answer
upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

A. Absolutely
upvoted 1 times

🗨️ 👤 **Adrian831** 2 years, 9 months ago

Selected Answer: A

Agree with A
upvoted 1 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: A

A is correct. Vulnerability scanner
upvoted 2 times

A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

- A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
- B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
- C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
- D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Suggested Answer: C

Community vote distribution

D (89%)

11%

🗳️ 👤 **I_heart_shuffle_girls** Highly Voted 4 years, 5 months ago

D looks correct.

upvoted 17 times

🗳️ 👤 **RokzyBalboa** 4 years, 5 months ago

Yes D looks the best since the question references what to do next in the detection phase.

upvoted 11 times

🗳️ 👤 **DrChats** Highly Voted 4 years ago

detect is to identify.....D

upvoted 9 times

🗳️ 👤 **heinzelrumpel** Most Recent 1 year, 11 months ago

Selected Answer: D

D because they are stil in thh Identification Phase

upvoted 2 times

🗳️ 👤 **SimonR2** 1 year, 11 months ago

A little tip i've found with questions like this is to look for a keyword in each of the answers and then match that with the IR life cycle.

- Escalate

- Remove

- Block

- Identify

In the Detection & Analysis phase we are looking into "potential" malware activity we are going to want to "Identify" before we Escalate, Block or Remove.

upvoted 4 times

🗳️ 👤 **NIKTES** 1 year, 10 months ago

Great logic

upvoted 1 times

🗳️ 👤 **kill_chain** 2 years ago

Selected Answer: D

I don't think C is a detection phase. as the question states.

upvoted 1 times

🗳️ 👤 **Dutch012** 2 years ago

NEXT step during the "detection phase"

upvoted 2 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

Creating a correlation search in the Security Information and Event Management (SIEM) system based on the network traffic can help the team identify potentially affected systems and gather more information on the behavior of the malware. This step will also help the team to determine the

scope of the incident and prioritize their response efforts accordingly.

Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses, is not the immediate next step as the team needs to gather more information before engaging other teams and blocking traffic.

upvoted 1 times

🗨️ 👤 **ksr933** 2 years, 2 months ago

I'm going for D. The question mentioned "potential malware". We don't know yet if it's really malware. Next step is finding out the behavior if it's malicious. If the question states that malware is detected then we would immediately do the C.

upvoted 1 times

🗨️ 👤 **Snkrsnaker1** 2 years, 2 months ago

Selected Answer: C

Answer is C:

Based on this by CompTIA: "Detection and Analysis—Determine whether an incident has taken place and assess how severe it might be (triage), followed by notification of the incident to stakeholders." We already did an initial assessment and based on the findings, it needs to be "triaged", which is still in the detection phase. Which is why C is the best answer. This thing is actively beaconing out, you need to take action on this first, then go to D. So that is my reasoning for choosing C.

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: D

D. It specifically mentions "detection" phase.

upvoted 1 times

🗨️ 👤 **shivas** 2 years, 7 months ago

Selected Answer: D

Going with D. "NEXT step during the detection phase"

upvoted 2 times

🗨️ 👤 **Maniact165** 2 years, 7 months ago

Selected Answer: D

D due to the wording of the question

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: D

"during the detection phase of this response process", so it needs to take action D. After that option C can be taken with the process completed through SIEM.

upvoted 1 times

🗨️ 👤 **Abyad** 2 years, 9 months ago

Selected Answer: D

What is asked here is the detection phase not the solution. so D is the best choice according to me

upvoted 3 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

"during the detection phase".... Definitely D.

upvoted 1 times

🗨️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: D

looks good to me

upvoted 2 times

🗨️ 👤 **cysa_1127** 3 years, 4 months ago

Selected Answer: D

going with D

upvoted 2 times

An organization is developing software to match customers' expectations. Before the software goes into production, it must meet the following quality assurance guidelines:

Uncover all the software vulnerabilities.

▪

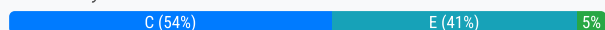
- ⇒ Safeguard the interest of the software's end users.
- ⇒ Reduce the likelihood that a defective program will enter production.
- ⇒ Preserve the interests of the software producer.

Which of the following should be performed FIRST?

- A. Run source code against the latest OWASP vulnerabilities.
- B. Document the life-cycle changes that took place.
- C. Ensure verification and validation took place during each phase.
- D. Store the source code in a software escrow.
- E. Conduct a static analysis of the code.

Suggested Answer: E

Community vote distribution



🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: C

C. Ensure verification and validation took place during each phase.

The FIRST step in ensuring software quality and addressing the specified guidelines is typically related to the software development process and verification/validation. Among the given options, option C, "Ensure verification and validation took place during each phase," is the most appropriate initial step.

upvoted 1 times

🗳️ 👤 **skibby16** 1 year, 6 months ago

Selected Answer: C

Ensuring verification and validation take place during each phase of the software development life cycle is a fundamental step in meeting quality assurance guidelines. Verification involves checking whether the product design and implementation align with the specified requirements, while validation ensures that the final product meets the intended use and satisfies customer needs. By incorporating these practices throughout the development process, the organization can uncover vulnerabilities, safeguard end-users' interests, reduce the likelihood of defects, and preserve the interests of the software producer. This approach helps maintain the overall quality and reliability of the software.

upvoted 1 times

🗳️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: E

It asks what to perform first. Since C is to be performed at each phase, E would be the valid answer.

upvoted 2 times

🗳️ 👤 **Big_Dre** 1 year, 10 months ago

Selected Answer: C

i believe c because even E can be done in C meaning E is a child of C

upvoted 1 times

🗳️ 👤 **salmonIsDecent** 1 year, 10 months ago

Selected Answer: C

The answer is: C. Ensure verification and validation took place during each phase.

Verification and validation are essential steps in the software development life cycle to ensure that the software meets the specified requirements and is free from defects. By conducting verification and validation during each phase of the development process, the organization can identify and address issues early on, reducing the likelihood of defective code entering production.

upvoted 2 times

🗨️ 👤 **Aliyan** 1 year, 11 months ago

Selected Answer: C

"must meet the following quality assurance guidelines"

searching COMPTIA CYSA Guide for Quality Control (QC) and Quality Assurance (QA) first big title came across was "Verification and Validation (V&V)"

the whole QA Unit doesnt talk about static code analysis at all.

Im %100 sure this is C

upvoted 3 times

🗨️ 👤 **heinzeltumpel** 1 year, 11 months ago

Selected Answer: C

E is just one step in the chain of maintaining a secure coding environment. C covers more

upvoted 1 times

🗨️ 👤 **Rori791** 1 year, 11 months ago

Selected Answer: E

Answer is E.

It is better to perform a static analysis of the code before ensuring verification and validation took place during each phase. The reason for this is that a static analysis of the code can help you identify potential issues such as security vulnerabilities, coding errors, and other defects, which can then be addressed before proceeding with further testing and validation. This can help reduce the likelihood of defective code entering production, which is one of the guidelines listed. After conducting a static analysis, it is then important to ensure that verification and validation took place during each phase of the software development life cycle. This can help ensure that the software meets the desired requirements and that any defects or issues are identified and addressed before the software is released to end-users.

E then C

upvoted 1 times

🗨️ 👤 **HotWings8** 1 year, 11 months ago

I vote C:

Verification - A compliance-testing process to ensure that the security system meets the requirements of a framework or regulatory environment, or that a product or system meets its design goals

Validation - The process of determining whether the security system is fit for purpose. Fit for purpose, in the ITIL framework, is known as utility (meets the designed needs of the software or service

Jason Dion

upvoted 1 times

🗨️ 👤 **justauser** 2 years ago

Selected Answer: E

GPT-4 calibrated to CS0-002 with community votes included in the prompt: Answer: E. Explanation: The FIRST task that should be done, according to the guidelines provided, is to uncover all the software vulnerabilities. Static code analysis (Option E) allows you to inspect the code without executing it, providing a mechanism for detecting vulnerabilities, bugs, and other issues. This method is a key practice in secure development lifecycle processes and directly meets the first guideline. [Option C, while important in every phase of software development, does not directly uncover vulnerabilities. It's rather a process-oriented task which ensures the requirements are met and the product satisfies users' needs. While Option A can help identify vulnerabilities, it wouldn't uncover ALL vulnerabilities as it's specifically targeted towards OWASP classified vulnerabilities. Options B and D don't directly address the need to uncover vulnerabilities.]

upvoted 1 times

🗨️ 👤 **tutita** 2 years ago

Selected Answer: E

Its a tricky question, I have read couple of times back and forward C sounds good but "ensure" that it took place sounds not right, they asking for what action to take first, for me answer is E perform an static code review, that's the best action you can take.

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

Ensuring verification and validation took place during each phase of the software development life cycle will help identify and address any defects or vulnerabilities in the software before it goes into production. This step will help meet guidelines 1 and 2 and reduce the likelihood of defective software entering production.

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 2 months ago

Selected Answer: C

At first I thought it was E, but when looking back at the requirements:

- safeguard interests of end users
- preserve interests of software producer

I decided C is more correct in alignment with yanyan20's and Sam_0735's answers

upvoted 1 times

🗨️ 👤 **yanyan20** 2 years, 2 months ago

Selected Answer: C

Before anything else, it is important to ensure that verification and validation took place during each phase of the software development life cycle.

This is because the earlier a vulnerability is detected, the easier and cheaper it is to fix. By verifying and validating the software at every phase, any vulnerabilities can be identified and addressed before the software enters production, reducing the likelihood that a defective program will be released. Running the source code against the latest OWASP vulnerabilities and conducting a static analysis of the code are important steps in identifying vulnerabilities, but they should be done after verification and validation have taken place. Documenting life-cycle changes and storing the source code in a software escrow are also important, but they are not directly related to ensuring the quality of the software.

upvoted 1 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: C

Conducting a static analysis of the code is an important step in ensuring software quality, but it should not be the first step. Before conducting a static analysis, it is crucial to ensure that verification and validation have taken place during each phase of software development to identify and address any defects or issues.

upvoted 1 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

After reviewing my answer I think E is actually correct. My apologies

upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. It meets all requirements, but "safe guarding ... end users" interests is the key.

upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 2 months ago

after reviewing again.. I think I will need to go with E.

upvoted 1 times

🗨️ 👤 **talosDevbot** 2 years, 3 months ago

Selected Answer: C

Before developing code, you should ensure security is integrated into the CI/CD pipeline. This is part of DevSecOps. With this implemented, security checks will take places in between stages of the SDLC.

C is a better answer since you would typically set a CI/CD pipeline before performing static analysis of code

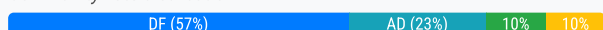
upvoted 1 times

Which of the following APT adversary archetypes represent non-nation-state threat actors? (Choose two.)

- A. Kitten
- B. Panda
- C. Tiger
- D. Jackal
- E. Bear
- F. Spider

Suggested Answer: CD

Community vote distribution



TheSkyMan Highly Voted 2 years, 9 months ago

Looks like Spider and Jackal are not associated with a specific nation-state APT.

<https://warnerchad.medium.com/why-apt-group-names-include-animals-bear-panda-etc-6bdcadedf82b>

upvoted 20 times

101martin101 2 years, 3 months ago

Thanks for the link

upvoted 2 times

heinzelrumpel Highly Voted 1 year, 11 months ago

This is one of the dumbest CompTia Question. Why on earth is this important to know in a test?

upvoted 16 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: DF

Non-state-affiliated suffixes include Spider for criminal gangs and Jackal for hacktivist groups.

upvoted 2 times

Gwatto 1 year, 7 months ago

Now why would you ask a question like this

upvoted 1 times

sudoptgoaway 1 year, 9 months ago

Imagine failing because you got this question wrong..

Ridiculous of CompTIA to ask this, and it's why I love these dumps.

upvoted 3 times

buchhe 1 year, 10 months ago

Selected Answer: A

Kitten=Iran

Panda=china

Bear=Russia

Tiger=India

Spider=Ecrime

Jackal=Hacktivist

upvoted 3 times

Nouuv 2 years ago

Panda is China, Bear is Russia, Chollima is North Korea, Kitten is Iran, Buffalo is Vietnam, and so on.

Non-state-affiliated suffixes include Spider for criminal gangs and Jackal for hacktivist groups.

upvoted 2 times

Sepu 2 years, 2 months ago

Selected Answer: DF

Crowdstrike is linked in the official CompTIA eLearn, so it has to be their source:
<https://www.crowdstrike.com/adversaries/>

Spider - eCrime

Jackal - Hacktivism

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: AB

Kitten and Panda are both examples of APT groups that are associated with non-nation-state actors such as hacktivists, cybercriminals, or mercenaries.

Tiger, is an example of an APT group that is associated WITH A nation-state actor, not non-nation-state
Jackal and Bear, are not commonly used APT adversary archetypes !

Spider, is a commonly used APT adversary archetype, but it can be used by both nation-state and non-nation-state actors.

upvoted 3 times

🗨️ 👤 **JoshuaXIV** 2 years, 2 months ago

Selected Answer: DF

Guys, Spider and Jackal are the answers.

Spider are related to criminal gangs and Jackal are for hacktivist groups.

upvoted 1 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: DF

D&F for all previously mentioned reasons. Also Kitten could likely be state sponsored, maybe not typically, but they have been known to be state sponsored.

upvoted 3 times

🗨️ 👤 **doyona** 2 years, 2 months ago

Charming Kitten is Iranian state sponsored.

<https://explore.avertium.com/resource/in-depth-look-at-apt35-aka-charming-kitten>

upvoted 1 times

🗨️ 👤 **Lunarr** 2 years, 3 months ago

Selected Answer: AD

encxorblood is correct

upvoted 1 times

🗨️ 👤 **encxorblood** 2 years, 4 months ago

Selected Answer: AD

Two APT adversary archetypes that represent non-nation-state threat actors are Kitten and Jackal. Therefore, the correct answers are A and D.

Kitten is a term used to describe Iranian-based threat actors that are typically not backed by the Iranian government.

Jackal is a term used to describe smaller, less sophisticated groups or individuals who use APT techniques to achieve their goals.

Panda, Tiger, and Bear are all nation-state threat actors associated with China, North Korea, and Russia, respectively.

Spider is not an APT adversary archetype, but rather a term used to describe the automated tools used by threat actors to crawl websites and collect information.

Therefore, the two APT adversary archetypes that represent non-nation-state threat actors are Kitten (Option A) and Jackal (Option D).

upvoted 6 times

🗨️ 👤 **doyona** 2 years, 2 months ago

Charming Kitten is Iranian state sponsored.

<https://explore.avertium.com/resource/in-depth-look-at-apt35-aka-charming-kitten>

upvoted 3 times

🗨️ 👤 **Cock** 2 years, 4 months ago

Jackals are typically motivated by financial gain and they often work alone or in small groups. They often target smaller organizations that lack robust security systems, using tactics like phishing, malware, and other forms of social engineering to compromise their targets.

Spiders are criminal organizations or individuals who use the Internet to carry out their attacks. They often target e-commerce sites, banks, and other organizations that hold valuable information, such as credit card numbers and other sensitive financial data. They are motivated by financial gain and use a variety of hacking tools and techniques to achieve their objectives.

upvoted 1 times

🗨️ 👤 **Maniact165** 2 years, 7 months ago

Selected Answer: DF

It defo DF

upvoted 1 times

🗨️ 👤 **TheStudiosPeepz** 2 years, 7 months ago

Selected Answer: DF

Look at TheSkyMan's link.

upvoted 1 times

🗨️ 👤 **Weezyfbaby** 2 years, 9 months ago

Selected Answer: DF

Definitely Jackal and Spider

<https://outlookseries.com/A0781/Security/3511.htm>

upvoted 5 times

A cybersecurity analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

- A. Implement port security with one MAC address per network port of the switch.
- B. Deploy network address protection with DHCP and dynamic VLANs
- C. Configure 802.1X and EAPOL across the network.
- D. Implement software-defined networking and security groups for isolation.

Suggested Answer: A

Community vote distribution



🗨️ **RobV** 1 year, 6 months ago

Selected Answer: A

A. Implement port security with one MAC address per network port of the switch:

Port security restricts access to a specific MAC address on a network port.

This solution is relatively straightforward to implement and manage.

It provides a level of security by ensuring that only devices with approved MAC addresses can connect to the network through a specific port.

It is less likely to cause issues during the deployment phase compared to more complex solutions.

upvoted 1 times

🗨️ **novolyus** 1 year, 7 months ago

Port security with only 1 MAC does not mean this address would be licit. I can connect a bogus device in a switch port and this device will be allowed as far as my device uses this 1 MAC.

For those who say that static mac is easy to configure, just think about a 48 port switch in a DC with 100 switches.

upvoted 1 times

🗨️ **Pavel019846457** 1 year, 7 months ago

Selected Answer: A

ChatGPT

The best solution for implementing a new network configuration on an existing network access layer to prevent possible physical attacks while causing fewer issues during the deployment phase would be:

A. Implement port security with one MAC address per network port of the switch.

This option is a straightforward and effective way to enhance network security by allowing only specific devices (based on their MAC addresses) to connect to network ports. It's relatively easy to implement and manage, and it doesn't introduce complex network changes that might cause issues during deployment. Additionally, it's a good measure against physical attacks, as it ensures that only authorized devices can connect to the network.

upvoted 1 times

🗨️ **uday1985** 1 year, 9 months ago

Can't the attacker spoof the MAC address?

upvoted 2 times

🗨️ **Dutch012** 2 years ago

"to prevent possible physical attacks"

upvoted 3 times

🗨️ **kiduuu** 2 years, 2 months ago

Selected Answer: A

Implementing port security will help prevent unauthorized access to the network by limiting the number of MAC addresses that can be associated with each network port. This solution is easy to deploy and does not require significant changes to the network topology. It is also less likely to cause issues during the deployment phase compared to other options.

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: A

A. Only because it mentions "cause fewer issues to implement". With that being said. Port security is easier to implement with less issues. 802.1x and EAPOL fits the bill as well, to only allow authenticated devices/users access to the network. They device will be in a state of restriction until it passes, however, it will be a bit more difficult to implement which may cause some issues.

upvoted 1 times

🗨️ 👤 **talosDevbot** 2 years, 3 months ago

Selected Answer: C

802.1X and EAPOL will prevent a device from connecting to the network (via Ethernet) until user is successfully authenticated.

Port security feature can be set to only allow one specific MAC address and/or limit the number of devices/MAC address through the port.

Option A is suggesting to just limit the number of machines connected to each port to just one, which really isn't a strong security measure against malicious users accessing the network.

upvoted 1 times

🗨️ 👤 **heinzeltumpel** 1 year, 11 months ago

MAC addresses could easily be spoofed.

upvoted 1 times

🗨️ 👤 **Cyber_Guru** 2 years, 4 months ago

Selected Answer: A

Use of authentication and security features such as IEEE 802.1x and access control lists, while an integral part of an organization's threat defense policies, cannot prevent the Layer 2 security attacks. Port Security is a dynamic feature that can be used to limit and identify the MAC addresses of the stations that allow access to the same physical port. When an administrator assigns secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

<https://www.techtarget.com/searchnetworking/tip/Preventing-Layer-2-security-threats>

upvoted 1 times

🗨️ 👤 **Cock** 2 years, 4 months ago

Selected Answer: C

Implementing 802.1X and EAPOL (Extensible Authentication Protocol over LAN) can help to secure the network by requiring authentication before granting network access. This can prevent unauthorized access to the network and protect it from physical attacks, as only authorized devices will be able to connect to the network. Additionally, 802.1X is a widely used and well-established solution, which means that it is likely to have fewer issues during the deployment phase compared to other, more complex solutions.

upvoted 2 times

🗨️ 👤 **cmllsu** 2 years, 6 months ago

Selected Answer: A

Because of "fewer issues during the deployment phase"

upvoted 2 times

🗨️ 👤 **gwanedm** 2 years, 7 months ago

Selected Answer: A

both A and C will do the job but the question says prevent possible physical attacks so I have to go with A

upvoted 2 times

🗨️ 👤 **MrRobotJ** 2 years, 7 months ago

Selected Answer: C

After researching this it has to be C

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: A

to prevent possible physical attacks, you need to assign one mac address to each physical port on the switch.

upvoted 2 times

🗨️ 👤 **franbarpro** 2 years, 7 months ago

Mac filtering is not security. Attackers can easily clone that.

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 8 months ago

The question requires "prevent possible physical attacks.", so why the answer not A?

upvoted 1 times

  **TheStudiosPeepz** 2 years, 8 months ago

Selected Answer: C



It can't be A so it's C.

upvoted 1 times

  **TheStudiosPeepz** 2 years, 3 months ago

Ignore my previous comment...

upvoted 1 times

  **Merc16** 2 years, 8 months ago

Selected Answer: C

I don't think A is a good solution. That is, considering that MAC addresses can be spoofed. The secure solution would be C.

upvoted 2 times

Which of the following types of controls defines placing an ACL on a file folder?

- A. Technical control
- B. Confidentiality control
- C. Managerial control
- D. Operational control

Suggested Answer: A

Community vote distribution

A (87%)

13%

  **R00ted**  2 years, 8 months ago

Selected Answer: A

A: "Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption."

upvoted 6 times

  **MrRobotJ**  2 years, 7 months ago

Selected Answer: A



Indeed A

upvoted 2 times

  **2Fish** 2 years, 3 months ago

Agree, absolutely A.

upvoted 1 times

  **Abyad** 2 years, 7 months ago

Selected Answer: A

B confidentiality is not part of security controls

upvoted 3 times

  **tnqi12** 2 years, 9 months ago

Selected Answer: A

Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption.

CompTIA CySA Study Guide Exam Exam CSO-002 - Mike Chapple (P. 709)

upvoted 1 times

  **Adrian831** 2 years, 9 months ago

Selected Answer: B

B make more sense to me.

upvoted 2 times

  **Treymb6** 2 years, 8 months ago



That isn't a thing.

upvoted 3 times

  **Adrian831** 2 years, 8 months ago

you are right, I re-read the question again and the I'm also agree with the A.

upvoted 2 times

  **sh4dali** 2 years, 9 months ago

Selected Answer: A

Agree A.

upvoted 1 times

Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

- A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.
- B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom tools for embedded devices.
- C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices.
- D. Trusted firmware updates provide organizations with secure code signing, distribution, installation, and attestation for embedded devices.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: D

D:"The CySA+ exam outline calls out "trusted firmware updates," but trusted firmware itself is more commonly described as part of trusted execution environments (TEEs). Trusted firmware is signed by a chip vendor or other trusted party, and then used to access keys to help control access to hardware. TEEs like those used by ARM processors leverage these technologies to protect the hardware by preventing unsigned code from using privileged features."

upvoted 4 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree - Trusted firmware updates are also distributed using secure channels to prevent interception or modification by attackers. Once the update is installed, the firmware attestation process checks to ensure that the updated firmware has been successfully installed and is running correctly.

upvoted 1 times

🗳️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: D

D is correct. Trusted firmware updates can help, with validation done using methods like checksum validation, cryptographic signing, and similar techniques.

upvoted 2 times

After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

- A. Make a backup of the server and update the JBoss server that is running on it.
- B. Contact the vendor for the legacy application and request an updated version.
- C. Create a proper DMZ for outdated components and segregate the JBoss server.
- D. Apply virtualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

Suggested Answer: C

Community vote distribution

C (71%)

A (29%)

 **R00ted**  2 years, 8 months ago

Selected Answer: C



C is the best answer. I still don't like it. What is that application for? "The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy"

upvoted 6 times

 **2Fish** 2 years, 3 months ago

Agree. Typically in these situations, you would have to have a compensatory control. In this case, segmenting it away may be the best solution and not be less disruptive to business.

upvoted 2 times

 **skibby16**  1 year, 6 months ago

Selected Answer: C

Creating a proper DMZ for outdated components and segregating the JBoss server is the best action to take first to prevent server compromise and business disruption at the same time. A DMZ (demilitarized zone) is a network segment that separates internal networks from external networks, such as the internet, and provides an additional layer of security³. Creating a proper DMZ for outdated components and segregating the JBoss server can isolate and protect the critical server from external attacks that may exploit its vulnerability.

upvoted 1 times

 **grelaman** 1 year, 9 months ago

Selected Answer: A


This is because updating the JBoss server is the most direct way to address the security vulnerability. Making a backup of the server first will help to protect the data in case something goes wrong during the update process

upvoted 1 times

 **grelaman** 1 year, 9 months ago

creating a DMZ for outdated components, would help to protect the server from external attacks, but it would not address the underlying security vulnerability.

upvoted 1 times

 **mraval** 2 years, 3 months ago

Selected Answer: A

I think If any application is outdated it is more Vulnerable, it doesn't matter u put behind firewall of in DMZ by usend that vulnerability attacker can exploit system. So the first step is to update JBoss.

upvoted 3 times

 **Henry88** 2 years, 3 months ago

Updating JBoss in this scenario would make the legacy application unusable which is what you are trying to avoid because it would disrupt business operations.

upvoted 2 times

🗨️ 👤 **whoami_808** 2 years, 3 months ago

I agree, the FIRST action to take to prevent server compromise and business disruption would be to make a backup of the server and update the JBoss server that is running on it. This action will ensure that the server is running the latest version of JBoss, which will reduce the risk of exploitation from external attackers. It will also ensure that the legacy application running on the server can continue to function without any disruptions.

upvoted 2 times

🗨️ 👤 **heinzelrumpel** 1 year, 11 months ago

No way. Update ist definently not possible in this scenario. The legacy app is not getting updates, because it's legacy and JBOss need to stay in the specific version because the app needs it that way.

upvoted 3 times

🗨️ 👤 **Adrian831** 2 years, 9 months ago

Selected Answer: C

C seems correct.

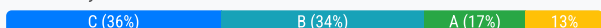
upvoted 3 times

A company's application development has been outsourced to a third-party development team. Based on the SLA, the development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

- A. Input validation
- B. Security regression testing
- C. Application fuzzing
- D. User acceptance testing
- E. Stress testing

Suggested Answer: D

Community vote distribution



TIM0088 Highly Voted 2 years, 6 months ago

Selected Answer: B

Security regression testing is a type of testing that is designed to ensure that changes to an application or system do not introduce new security vulnerabilities. It involves rerunning security tests that were previously performed on the application or system to verify that the security controls are still effective and that no new vulnerabilities have been introduced.

upvoted 13 times

trojan123 2 years, 5 months ago

100% agree <https://www.we45.com/post/why-regression-testing-is-so-important-for-appsec-automation>

upvoted 2 times

TheSkyMan Highly Voted 2 years, 9 months ago

Selected Answer: C

Here are my thoughts:

- A. Input validation is just a one of many secure coding practices.
- B. Security regression happens AFTER a change has been made to test the apps function.
- C. Application fuzzing automates the discovery of security and coding mistakes.
- D. User acceptance is more about functionality and fit for purpose.
- E. Stress testing won't necessarily test for secure coding.

I'll go with C.

"Threat actors use fuzzing to find zero-day exploits – this is known as a fuzzing attack. Security professionals, on the other hand, leverage fuzzing techniques to assess the security and stability of applications."

<https://brightsec.com/blog/fuzzing/>

upvoted 11 times

HereToStudy 2 years, 2 months ago

I'm going to assume the applications already existed and they are outsourcing further development and go with B

upvoted 2 times

Treymb6 2 years, 8 months ago

Second all the above. This was my thought process as well.

upvoted 1 times

SolventCourseisSCAM 2 years, 8 months ago

I agree almost for all in your statement.

upvoted 1 times

2Fish 2 years, 3 months ago

This is the best answer if you are trying to verify security.

upvoted 1 times

zecomeia_007 Most Recent 11 months ago

Selected Answer: B

Security regression testing is designed to ensure that new code or updates do not introduce new vulnerabilities and that existing security features remain effective. This type of testing helps verify that the development team is adhering to secure coding practices, as outlined in the SLA, by checking for security flaws consistently throughout the development process.

upvoted 1 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

B. Security regression testing

Explanation:

Security regression testing involves systematically retesting a software application to ensure that new code changes have not introduced security vulnerabilities or weaknesses. This type of testing helps identify any unintended security issues that may arise as a result of modifications to the code.

upvoted 1 times

🗳️ 👤 **32d799a** 1 year, 7 months ago

Selected Answer: B

B. Security regression testing

Security regression testing involves systematically retesting a software application to ensure that any recent changes or updates have not introduced new security vulnerabilities or negatively impacted existing security measures.

upvoted 2 times

🗳️ 👤 **Saphi** 1 year, 9 months ago

Selected Answer: C

Got to go with C for this one.

At the end of the day while it's an awkwardly worded question user acceptance testing is not a code review technique. Security regression testing is out since this is a new application, not one having changes made, input validation is too specific and stress testing is just irrelevant to the question.

upvoted 1 times

🗳️ 👤 **Xoomalla** 1 year, 10 months ago

Selected Answer: B

CHATGPT assumed the same... the company is outsourcing an existing application hence, security regression

upvoted 1 times

🗳️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: B

Security regression testing is a type of testing that is performed to ensure that changes to an application do not introduce new security vulnerabilities. This is done by re-testing the application for security vulnerabilities after each change is made.

upvoted 1 times

🗳️ 👤 **Aliyan** 1 year, 11 months ago

Selected Answer: B

The company started the code with industry best practices for secure coding in mind and its outsourcing it wanting to make sure the third party follows the original secure coding practices and nothing is changed on security just work on the code and finish it because the original company don't have the time to do the trivia work that takes long time. They will insure you the best practices and you follow their steps and they make sure you didn't change anything so original company should do B. Security regression testing

upvoted 1 times

🗳️ 👤 **kyky** 2 years ago

Selected Answer: B

The best way to verify if the third-party development team is following industry best practices for secure coding, based on the SLA, would be to conduct security regression testing (option B).

Security regression testing involves retesting the application to ensure that any security vulnerabilities or weaknesses that were previously identified have been resolved and that new vulnerabilities have not been introduced during the development process. It helps to verify that the secure coding practices and measures are being implemented effectively.

upvoted 1 times

🗳️ 👤 **tutita** 2 years ago

Selected Answer: C

I'm choosing c, User acceptance doesn't have nothing to do with the SLA and best code practice, this is "testing the application by its intended audience, option B security regression you do it after you patch it, no make sure there is not vulnerabilities and everything has been solved (last step), and input validation is not even an option

upvoted 1 times

🗳️ 👤 **HereToStudy** 2 years, 2 months ago

Tough security regression if they are making changes to the application. And fuzzing if it's the first version of the application. I cant tell what the question is asking for unfortunately

upvoted 1 times

🗳️ 👤 **bradseth** 2 years, 2 months ago

Selected Answer: B

come on guys

upvoted 1 times

🗳️ 👤 **aisling** 2 years, 3 months ago

Selected Answer: C

From a security point of view Fuzzing seems to make the most sense

upvoted 1 times

🗳️ 👤 **prntscrn23** 2 years, 6 months ago

Selected Answer: A

Input validation is included in secure coding best practices.

upvoted 2 times

🗳️ 👤 **trojan123** 2 years, 6 months ago

Selected Answer: B

The best way to verify that the third-party development team is following industry best practices for secure coding is to conduct security regression testing. This type of testing involves retesting a previously tested application after modifying or updating it to ensure that the changes have not introduced any new vulnerabilities or security issues. By conducting security regression testing, the company can verify that the development team is following industry best practices for secure coding and that the application is secure. Other testing methods, such as input validation, application fuzzing, user acceptance testing, and stress testing, may also be useful in ensuring the security of the application, but are not specifically focused on verifying that the development team is following industry best practices for secure coding.

upvoted 1 times

🗳️ 👤 **Tag** 2 years, 8 months ago

Selected Answer: C

Answer is C

the question states that according to the SLA, the 3rd party must comply with industry standard rules , so after that, we can forget about the SLA itself, industry standard is across the board for everyone. If it had stated specifically in the SLA that the company requires x,y,z , then you could consider user acceptance testing.

What Is Fuzzing? Fuzzing or fuzz testing is a dynamic application security testing technique for negative testing. Fuzzing aims to detect known, unknown, and zero-day vulnerabilities

upvoted 5 times

🗳️ 👤 **Tag** 2 years, 8 months ago

industry "best practices" for "secure coding"

upvoted 1 times

🗳️ 👤 **Tag** 2 years, 8 months ago

on the topic of "secure" coding, fuzzing would be directly related to that.

whilst user acceptance testing doesnt necessarily have anything to do with coding,.



User Acceptance Testing (UAT) is a type of testing performed by the end user or the client to verify/accept the software system before moving the software application to the production environment. UAT is done in the final phase of testing after functional, integration and system testing is done.

upvoted 3 times

🗳️ 👤 **Tag** 2 years, 8 months ago



you can even go so far as to do the user acceptance testing but that wont prove that the code is secure. the application can run just as intended and somewhere down the line, all hell breaks loose

upvoted 1 times

  **2Fish** 2 years, 3 months ago

I see what you are saying, however, it did not mention any security updates to the application code, which would warrant Security Regression testing.

upvoted 1 times

  **2Fish** 2 years, 3 months ago

apologies, I responded to the wrong thread.

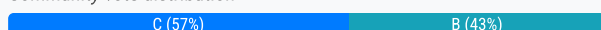
upvoted 1 times

During the security assessment of a new application, a tester attempts to log in to the application but receives the following message: incorrect password for given username. Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?

- A. Set the web page to redirect to an application support page when a bad password is entered.
- B. Disable error messaging for authentication.
- C. Recognize that error messaging does not provide confirmation of the correct element of authentication.
- D. Avoid using password-based authentication for the application.

Suggested Answer: C

Community vote distribution



🗳️ 👤 **Tag** Highly Voted 2 years, 8 months ago

Selected Answer: C

its C

how would you feel if you kept entering your username and password and nothing happened, but after a few click you get locked out of your account thinking that the people who designed the application were total idiots for atleast warning me that something i was typing was wrong.

"decrease likelihood" of attacker gaining "helpful info" . as it is, the application is already telling you that the username is correct, so if he were brute forcing in a sense, he has already attained half of the needed info.

he wouldnt know this if it were stating "username or password is incorrect" as do the majority of other sites on the internet have.

upvoted 20 times

🗳️ 👤 **Xoomalla** 1 year, 10 months ago

Loved the way you explained it :D

upvoted 1 times

🗳️ 👤 **RobV** Most Recent 1 year, 6 months ago

Selected Answer: B

B. Disable error messaging for authentication.

Disable error messaging for authentication (Option B):

This is a good practice to prevent attackers from gaining information about the correctness of the entered username or password.

By disabling detailed error messages, the system avoids providing attackers with specific feedback, making it more difficult for them to determine valid usernames.

Recognize that error messaging does not provide confirmation of the correct element of authentication (Option C):

While recognizing this fact is important, it doesn't directly address the issue of preventing potentially revealing error messages.

upvoted 1 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Key is "decrease the likelihood that a malicious attacker will receive helpful information?"

upvoted 1 times

🗳️ 👤 **Xoomalla** 1 year, 10 months ago

Selected Answer: C

Can't vote without comment, so I will quote his comment

""

how would you feel if you kept entering your username and password and nothing happened, but after a few click you get locked out of your account thinking that the people who designed the application were total idiots for atleast warning me that something i was typing was wrong.

""

upvoted 1 times

🗨️ 👤 **Xoomalla** 1 year, 10 months ago

Tag comment, I mean

upvoted 1 times

🗨️ 👤 **Dany_Suarez** 1 year, 11 months ago

Selected Answer: C

I think the correct answer is C.

upvoted 1 times

🗨️ 👤 **tutita** 2 years ago

Selected Answer: B

quote "Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?"

should be B that's the recommendation, my first choice was C but then I re read the question and I'm going for B

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: B

Disabling error messaging for authentication is a recommended approach to decreasing the likelihood that a malicious attacker will receive helpful information. By disabling error messaging, an attacker will not receive specific information about what went wrong during authentication, such as whether the username or password was incorrect.

upvoted 1 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: C

After rethinking this I dont think the error message tells you anything. It is basically only saying that the username and password dont go together. It doesnt say anything about whether or not the username exists

upvoted 1 times

🗨️ 👤 **HereToStudy** 2 years, 2 months ago

Wow these questions are terrible... I'm changing my mind back to B and here is why. The question is "Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?" unfortunately C does nothing to decrease the likelihood.

upvoted 3 times

🗨️ 👤 **[Removed]** 2 years, 2 months ago

The error message confirms to the attacker/tester that the username is correct while the password is not. This means the attacker/tester only has to work on password now and not both, so I think its B

upvoted 2 times

🗨️ 👤 **[Removed]** 2 years, 3 months ago

Selected Answer: B

If C said Incorrect password/username please try again. Then I would certainly go with that option, however, the error message tells me I found the correct username just not the correct password.

So the only reasonable answer is B. Disabling error messages for auth.

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Completely agree. Good explanation.

upvoted 1 times

🗨️ 👤 **aleExplicitly** 2 years, 4 months ago

Selected Answer: B

Going with B on this.

upvoted 1 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Which of the following can the tester recommend to decrease the likelihood that a malicious attacker will receive helpful information?

I understand people saying how disablign the notification wouldn't help regular users but from what the question gives us, that is of no concern. It's gotta be B

upvoted 2 times

🗨️ 👤 **Eric1234** 2 years, 4 months ago

Selected Answer: B

I think the answer is B, while it doesn't make sense to fully disable messaging the question is asking how to prevent information from being provided to the adversary. It doesn't ask for the solution to make it easier to solve future issues. Terrible question
upvoted 3 times

🗨️ 👤 **absabs** 2 years, 4 months ago

It is also C. When you enter wrong pass/user, what do you do without authentication error messaging?
upvoted 1 times

🗨️ 👤 **kmanb** 2 years, 4 months ago

Selected Answer: C

If you disable error messaging completely it will make it alot harder to solve issues
upvoted 2 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

Disable error messaging then no information can be provided.
upvoted 1 times

🗨️ 👤 **trainingsmits** 2 years, 5 months ago

Selected Answer: B

The only valid answer I see is B.

A - Setting the web page to redirect can give the attacker insight they don't need.

C - Recognizing the error message doesn't provide confirmation just isn't true - the error message reads "incorrect password for a given username", so they know the username is correct, but the password is incorrect.

D - just unrealistic.

B - disabling the error message for authentication doesn't seem like a great option, but it will avoid giving the attacker unnecessary/helpful information, which is what the question is asking for.

upvoted 3 times

🗨️ 👤 **TKW36** 2 years, 5 months ago

Selected Answer: B

This is a horribly worded question. The only correct answer by the parameters set by the question is realistically B, if we assume that the message did in fact give information. I don't think it did but if CompTIA's autists do then.. I would choose C but I'm almost forced to choose B..
upvoted 3 times

🗨️ 👤 **TIM0088** 2 years, 6 months ago

Selected Answer: B

Error messaging is a type of feedback that is provided to users when something goes wrong, such as when they enter an incorrect password. In some cases, error messaging can provide helpful information to attackers, such as confirming that they have correctly guessed the username or that they are using the correct password format.

By disabling error messaging for authentication, the tester can reduce the amount of information that is provided to attackers and make it more difficult for them to guess the correct username and password.

The correct answer is B: Disable error messaging for authentication.

upvoted 1 times

A security analyst is reviewing the following Internet usage trend report:

Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb


Which of the following usernames should the security analyst investigate further?

- A. User 1
- B. User 2
- C. User 3
- D. User 4


Suggested Answer: B

Community vote distribution

B (100%)

  **AaronS1990** Highly Voted 2 years, 4 months ago

Probably 2 as it has the biggest single change in traffic in week 10. What a shit question though
upvoted 6 times


  **2Fish** 2 years, 3 months ago

Fo real, and answer is B (user 2).
upvoted 2 times

  **TheSkyMan** Highly Voted 2 years, 9 months ago

Selected Answer: B

Looks like we're looking for trends here and User 2 is the odd one out.
upvoted 5 times

  **alayeluwa** Most Recent 2 years, 2 months ago

Selected Answer: B

Pay attention to the descending table type question.
upvoted 3 times

  **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is correct.
upvoted 4 times

  **david124** 2 years, 9 months ago

Right.
upvoted 1 times

An analyst is responding to an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the field. Malware was loaded on the device via the installation of a third-party software package. The analyst has baselined the device. Which of the following should the analyst do to BEST mitigate future attacks?

- A. Implement MDM.
- B. Update the malware catalog.
- C. Patch the mobile device's OS.
- D. Block third-party applications.

Suggested Answer: A

Community vote distribution

A (82%)

D (18%)

🗳️ 👤 **sh4dali** Highly Voted 👍 2 years, 9 months ago

Selected Answer: A

Correct A.

MDM) solution to manage the configuration of those devices, automatically installing patches, requiring the use of encryption, and providing remote wiping functionality. MDM solutions may also restrict the applications that can be run on a mobile device to those that appear on an approved list.

upvoted 5 times

🗳️ 👤 **skibby16** Most Recent 🕒 1 year, 8 months ago

Selected Answer: D

Blocking third-party applications would be the best way to mitigate future attacks on company-owned mobile devices that are used by employees to collect data from clients in the field. Third-party applications are applications that are not developed or authorized by the device manufacturer or operating system provider 1. Third-party applications can pose a security risk for mobile devices, as they may contain malware, spyware, or other malicious code that can compromise the device or its data 2. Blocking third-party applications can help prevent employees from installing unauthorized or untrusted applications on company-owned mobile devices and reduce the attack surface.

upvoted 2 times

🗳️ 👤 **Trick509_111** 1 year, 11 months ago

C. Patch the mobile device's OS.

Patching the mobile device's operating system is a crucial step in improving the device's security. It involves applying updates and security patches provided by the device's manufacturer or operating system vendor. These updates often include bug fixes and security enhancements that address known vulnerabilities, including vulnerabilities that could be exploited by malware.

upvoted 1 times

🗳️ 👤 **skibby16** 1 year, 8 months ago

The device was already baselined

upvoted 1 times

🗳️ 👤 **MrRobotJ** 2 years, 7 months ago

A can provide all the other options

upvoted 4 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree, answer is A.

upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

A is correct.

upvoted 4 times

A security analyst at example.com receives SIEM alert for an IDS signature and reviews the associated packet capture and TCP stream:

Packet capture:

Source	Destination	Protocol	Length	Info
203.0.113.15	192.168.100.56	TCP	1016	60100 > 80 [PSH, ACK] Seq=1 Ack=1 Win=229 Len=946 TSval=419499016 TSecr=668384771 [TCP segment of a reassembled PDU]

TCP stream:

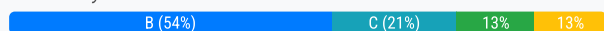
```
GET /admin/auth/Register.do HTTP/1.1
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
connection: close
content-type: %({#test='multipart/form-data'}).(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?{#_memberAccess=#dm}):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).(#ros=
(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(#ros.println(31337*31337)).(#ros.flush()))}
host: connect.example.local
iv-user: Unauthenticated
user-agent: Security Operations Center; X-SOC-Scan (soc@example.com);
via: HTTP/1.1 revproxy.dmz.example.local:443
iv_server_name: connect-webseald-revproxy.dmz.example.local
x-
```

Which of the following actions should the security analyst take NEXT?

- A. Review the known Apache vulnerabilities to determine if a compromise actually occurred.
- B. Contact the application owner for connect.example.local for additional information.
- C. Mark the alert as a false positive scan coming from an approved source.
- D. Raise a request to the firewall team to block 203.0.113.15.

Suggested Answer: B

Community vote distribution



talosDevbot Highly Voted 2 years, 4 months ago

Selected Answer: B

I currently work in a SOC.

Anytime we receive alerts/offenses that appears to be a potential scan (interna/external), we already verify with the app owner/client if this was expected activity.

We never close a ticket without confirmation, even its from an approved source

upvoted 12 times

2Fish 2 years, 3 months ago

Agree. We need to confirm.

upvoted 1 times

m025 Most Recent 1 year, 3 months ago

Selected Answer: A

skibby16 answer

upvoted 1 times

skibby16 1 year, 6 months ago

Selected Answer: A

The security analyst should review the known Apache vulnerabilities to determine if a compromise actually occurred. The SIEM alert indicates that an IDS signature detected an attempt to exploit a vulnerability in Apache Struts 2 (CVE-2017-5638), which allows remote code execution via a crafted Content-Type header⁴. The packet capture and TCP stream show that the attacker sent a malicious request with a Content-Type header containing an OGNL expression that executes the command “whoami” on the target server. However, this does not necessarily mean that the attack was successful, as it depends on whether the target server was running a vulnerable version of Apache Struts 2 or not. Therefore, the security analyst should review the known Apache vulnerabilities and compare them with the version of Apache Struts 2 running on the server to confirm if a compromise actually occurred or not.

upvoted 2 times

🗨️ 👤 **Xoomalla** 1 year, 10 months ago

Selected Answer: A

Should be A. user agent can be manipulated easily
upvoted 2 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: B

I agree with Ian pretty much word for word. It looks like this is coming from the SOC but it has still triggered the IDS and so it is worth confirming before either blocking or dismissing.
upvoted 3 times

🗨️ 👤 **IanRogerStewart** 2 years, 4 months ago

Selected Answer: B

While it might *look* like this is coming from the SOC, you haven't done your due diligence until you've confirmed with the source that this is legit.
upvoted 4 times

🗨️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: C

C. should be the unanimous answer. Read the TPC stream and you'll see that the SOC team is running an unauthenticated scan.
upvoted 1 times

🗨️ 👤 **ra774ra7** 2 years, 5 months ago

can someone please explain how they got the answer?

I am going to be honest, I have no clue!

upvoted 4 times

🗨️ 👤 **hanybee** 2 years, 5 months ago

Selected Answer: B

An authenticated scan reports weaknesses exposed to the authenticated users of the system, as all the hosted services can be accessed with a right set of credentials. An -unauthenticated scan reports weaknesses from a public viewpoint (this is what the system looks like to the unauthenticated users) of the system.

So the scan may be valid but instead of concluding asking for additional information from the application owner doesn't hurt and confirms if this activity is done internally.

upvoted 2 times

🗨️ 👤 **TKW36** 2 years, 5 months ago

From the TCP stream, starting at the bottom, lines 4 and 5 give the answer. SOC team running an unauthenticated scan. Answer is C.

upvoted 4 times

🗨️ 👤 **Xoomalla** 1 year, 10 months ago

User agent can be spoofed easily

upvoted 1 times

🗨️ 👤 **TIM0088** 2 years, 6 months ago

Selected Answer: C

SOC team doing scan. MY ans. is C

upvoted 4 times

🗨️ 👤 **cmllsu** 2 years, 6 months ago

Selected Answer: D

Tricky questions, not sure either but knowing the one that investigating this is SOC from exampledotcom, looks like it wants us to pick C. Later part of the suspicious code is related to Apache Struts vulnerability. but IV info in the TCP stream indicate that it is coming from example.local. There should be a choice to validate the activity if it is part of pentest or vulscan but regardless if it is unauthorized scanning I would go with D.

it is close for me with C & D but would choose D for this scenario.

upvoted 2 times

🗨️ 👤 **cmllsu** 2 years, 6 months ago

check CVE-2017-5638 and for some reason the source IP in the question is tagged as internal in VT. so this is leaning more on the scanning that choice C is saying. I change my answer to C.

upvoted 1 times

🗨️ 👤 **Whoah** 2 years, 7 months ago

Selected Answer: C

This appears to be an unauthenticated connection from SoC, the reverse proxy line shows the source as being from the same domain along with more containers showing SoC attributes. I'm calling this a false positive

upvoted 3 times

🗨️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: D

D makes sense for me

upvoted 1 times

🗨️ 👤 **[Removed]** 2 years, 8 months ago

Selected Answer: D

This looks like an OGNL Injection attack to me. From what I've read seems like a WAF is best protection/mitigation for it so I'm going with D.

upvoted 1 times

🗨️ 👤 **Adrian831** 2 years, 9 months ago

Selected Answer: D

D seems the right answer here.

upvoted 1 times

🗨️ 👤 **adamhoms** 2 years, 9 months ago

I think D is the answer, I tried to understand the TCP stream and found out that the user is not authenticated, and this user trying to do many things seems unusual. so we must block it on the firewall.

upvoted 2 times

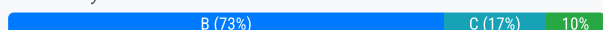
A company's domain has been spoofed in numerous phishing campaigns. An analyst needs to determine why the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC. Upon review of the record, the analyst finds the following: v=DMARC1; p=none; fo=0; rua=mailto:security@company.com; ruf=mailto:security@company.com; adkim=r; rf=afrf; ri=86400;

Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?

- A. The DMARC record's DKIM alignment tag is incorrectly configured.
- B. The DMARC record's policy tag is incorrectly configured.
- C. The DMARC record does not have an SPF alignment tag.
- D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.

Suggested Answer: B

Community vote distribution



DaroKa Highly Voted 2 years, 9 months ago

Selected Answer: B

I agree with B

p=none - Take no action on the message and deliver it to the intended recipient.

should be p=reject or p=quarantine

upvoted 10 times

sh4dali 2 years, 9 months ago

Correct

upvoted 1 times

PTcruiser 2 years, 8 months ago

<https://mxtoolbox.com/dmarc/details/how-to-setup-dmarc>

For the "p" tag pair "p=" can be paired with none, quarantine, or reject. As tag-value pairs they would look like: p=none or p=quarantine or p=reject. MxToolbox recommends all new DMARC records should start with p=none, as this policy value allows you to identify email delivery problems due to the domain's SPF or DKIM so that mail isn't accidentally quarantined or rejected.

upvoted 3 times

Adrian831 2 years, 8 months ago

After a closer look I think you are right, so the correct answer here should be C

upvoted 3 times

AC6280 Highly Voted 2 years, 4 months ago

Selected Answer: B

To add more clarity here (I worked specifically in email security).

It is not required to have an SPF alignment tag (ASPF tag).

<https://easydmarc.com/blog/what-are-dmarc-tags-dmarc-tags-explained/>

Even if you did have it, DMARC policy is in monitor only mode (p=none), so it wouldn't matter. The policy is never going to be enforced until you move it to p=quarantine at the minimum (very few orgs actually hit a p=reject stage, it's incredibly difficult).

upvoted 8 times

2Fish 2 years, 3 months ago

Agree. Thank you for the explanation.

upvoted 1 times

MacheenZero Most Recent 1 year, 10 months ago

Selected Answer: C

This is an example of a DMARC policy record. The v and p tags must be listed first, other tags can be in any order:

Example:

v=DMARC1; p=reject; rua=mailto:postmaster@solarbora.com, mailto:dmarc@solarbora.com; pct=100; adkim=s; aspf=s

You can choose from two alignment modes: strict and relaxed. Set the alignment mode for SPF and DKIM in the DMARC record. The aspf and adkim DMARC record tags set the alignment mode.

In the following cases, we recommend you consider changing to strict alignment for increased protection against spoofing:

Mail is sent for your domain from a subdomain outside your control
You have subdomains that are managed by another entity

To pass DMARC, a message must pass at least one of these checks:

SPF authentication and SPF alignment
DKIM authentication and DKIM alignment

A message fails the DMARC check if the message fails both:

SPF (or SPF alignment)
DKIM (or DKIM alignment)

Important: Relaxed alignment typically provides sufficient spoofing protection. Strict alignment can result in messages from associated subdomains to be rejected or sent to spam.

<https://support.google.com/a/answer/10032169?hl=en>
upvoted 1 times

🗨️ **[Removed]** 2 years, 2 months ago

Selected Answer: B

I would go with B as well.. Here is what I found about setting up Policies and email spoofing. Take a look at the Final Notes towards the bottom.
<https://4sysops.com/archives/set-up-dmarc-for-spf-and-dkim/>
upvoted 1 times

🗨️ **Cyber_Guru** 2 years, 4 months ago

Selected Answer: A

"adkim="

This sets the DKIM portion of DMARC authentication to either "s" for strict or "r" for relaxed. The strict setting ensures DKIM will only pass if the "d=" field in the signature precisely matches the "from" domain. When set to relaxed, messages will pass DKIM only if the "d=" field matches the root domain of the "from" address.
upvoted 1 times

🗨️ **IanRogerStewart** 2 years, 5 months ago

Selected Answer: C

Actually must be C. It must have an aspf tag which is missing
upvoted 1 times

🗨️ **IanRogerStewart** 2 years, 5 months ago

Selected Answer: A

The alignment tag is set to 'R' meaning relaxed. Any valid subdomain of d=domain in the DKIM mail headers is accepted. Should be set to 'S' strict.
upvoted 2 times

🗨️ **TIM0088** 2 years, 6 months ago

Selected Answer: B

the policy tag is set to "none," which means that mailbox providers should not take any action on email that fails DMARC. This is likely the reason why the company's domain is being spoofed in numerous phishing campaigns, as mailbox providers are not blocking or quarantining the suspicious emails.

To fix this issue, the analyst should change the value of the policy tag to "quarantine" or "reject" to instruct mailbox providers to take appropriate

action on email that fails DMARC.

B is the correct ans

upvoted 2 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

Selected Answer: C

I did research on DMARC and to pass DMARC, you must pass SPF authentication and alignment. I see nothing about SPF alignment in the code so I think it should be C.

upvoted 1 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

I was wrong here, answer is B. The emails were not failing DMARC which is the problem making the answer B.

upvoted 2 times

🗨️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: B

B p=none

upvoted 1 times

🗨️ 👤 **TheSkyMan** 2 years, 9 months ago

Selected Answer: C

I'm feeling C.

"The way it works is to help email receivers determine if the purported message "aligns" with what the receiver knows about the sender."

<https://dmarc.org/overview/>

upvoted 2 times

🗨️ 👤 **piotr3439** 2 years, 9 months ago

Selected Answer: B

I agree B

upvoted 2 times

🗨️ 👤 **Laudy** 2 years, 9 months ago

Literally no idea...

Hope B is right....

upvoted 2 times

A company experienced a security compromise due to the inappropriate disposal of one of its hardware appliances. Sensitive information stored on the hardware appliance was not removed prior to disposal. Which of the following is the BEST manner in which to dispose of the hardware appliance?

- A. Ensure the hardware appliance has the ability to encrypt the data before disposing of it.
- B. Dispose of all hardware appliances securely, thoroughly, and in compliance with company policies.
- C. Return the hardware appliance to the vendor, as the vendor is responsible for disposal.
- D. Establish guidelines for the handling of sensitive information.

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **FT000** 1 year, 4 months ago

Selected Answer: B

None other makes sense and would help in this particular scenario.

upvoted 1 times

🗳️ 👤 **ryanzou** 2 years, 8 months ago

Selected Answer: B

b with no doubts

upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree. Nice to have a question this simple.

upvoted 2 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: B

B is so obvious.

upvoted 2 times

During a review of the vulnerability scan results on a server, an information security analyst notices the following:
 'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
 'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
 'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
 TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

- A. it only accepts TLSv1 .2.
- B. it only accepts cipher suites using AES and SHA.
- C. it no longer accepts the vulnerable cipher suites.
- D. SSL/TLS is offloaded to a WAF and load balancer.

Suggested Answer: C

Community vote distribution



C (71%)

B (29%)

  **bootleg** Highly Voted 2 years, 6 months ago

I passed today, chose "C".

upvoted 9 times

  **skibby16** Most Recent 1 year, 6 months ago

Selected Answer: C

A cipher suite is a set of algorithms that defines how the encryption, authentication, and integrity of data are performed during a secure communication session. Some cipher suites are considered vulnerable or weak because they use outdated or insecure algorithms that can be easily broken or compromised by attackers. The vulnerability scan results show that the web server accepts several vulnerable cipher suites, such as RC4, MD5, or DES. The best action for the analyst to recommend to developers is to change the web server so it no longer accepts the vulnerable cipher suites and only accepts the secure ones.

upvoted 1 times

  **2Fish** 2 years, 3 months ago

Selected Answer: C

C. There are still vulnerable cipher suites with AES and SHA.

upvoted 1 times

  **SylFlo** 2 years, 5 months ago

i passed today and had this one on there, i chose C

upvoted 4 times

  **Cizzla7049** 2 years, 7 months ago

Selected Answer: B


DES is a weaker hashing algorithm than AES

upvoted 2 times

  **Comptia_Secret_Service** 2 years, 6 months ago

Wrong, read the result from the vulnerable tests, it is C, TLS 1.2, and below are no longer secure.

upvoted 1 times

  **sh4dali** 2 years, 9 months ago

Selected Answer: C

C is correct. They should implement TLS version 1.3

upvoted 3 times

  **Average_Joe** 2 years, 8 months ago

and 3des is a non-issue?

upvoted 1 times

A threat hunting team received a new IoC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

- A. The whitelist
- B. The DNS
- C. The blocklist
- D. The IDS signature

Suggested Answer: D

Community vote distribution

D (63%)

C (37%)

  **db97**  2 years, 4 months ago

Selected Answer: D

Our alerts sources must be updated first (going with D here).




I do work for a SOC and when we receive feeds for IOCs we update our bunch of rules in order to detect potential activity related, and sometimes an alert triggers but the traffic is automatically blocked by the firewall so we don't need to blacklist first.

upvoted 5 times

  **2Fish** 2 years, 3 months ago

Agree. IDS first, then blacklist.

upvoted 1 times

  **skibby16**  1 year, 6 months ago

Selected Answer: D

When a threat hunting team receives a new Indicator of Compromise (IoC) that follows a threat actor's profile and activities, the next action should be to update the relevant security controls to detect and mitigate the identified threat. In this context, the most appropriate update would be to: D. The IDS signature

Updating the Intrusion Detection System (IDS) signature will help the security system recognize and alert on the specific indicators associated with the threat actor's activities. This ensures that the organization's security infrastructure is better prepared to detect and respond to potential threats.

upvoted 1 times

  **edro** 1 year, 7 months ago

Blocking the malicious entities for immediate damage control is the primary step, followed by updating the IDS signatures. These two actions are equally vital, embodying both due diligence and due care in fortifying cybersecurity measures.


C is the most crucial here

upvoted 1 times

  **Chilaqui1es** 1 year, 8 months ago

I think its C you "update" a block list but you "add" signatures. Its a close call.

upvoted 1 times

  **grelaman** 1 year, 9 months ago

Selected Answer: D

When a threat hunting team receives a new Indicator of Compromise (IoC) from an Information Sharing and Analysis Center (ISAC) that follows a threat actor's profile and activities, the next step should typically involve updating the relevant security controls to enhance detection and protection against the threat. In this context, the most appropriate next action would be:

Updating the IDS signature allows the security team to proactively detect and respond to the specific threat associated with the new IoC. By incorporating this IoC into the IDS signature, the system can better identify and alert on potential threats related to the threat actor's profile and activities.

upvoted 2 times

  **Xoomalla** 1 year, 10 months ago

Selected Answer: C

Block list... That's threat actor IOC... I sure would like to block PREVENT them.. IDS wouldn't prevent but detect. I believe I will go for Block list.

upvoted 2 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

the threat hunting team has received a new IoC from an ISAC (Information Sharing and Analysis Center) that follows a threat actor's profile and activities. The team needs to take immediate action to prevent any potential damage. The first step is to update the IDS (Intrusion Detection System) signature. IDS systems are network security appliances that monitor network traffic for signs of suspicious behavior. Updating the IDS signature allows it to recognize and alert the team of any network traffic that matches the IoC.

Once the IDS signature has been updated, the team can move on to other tasks, such as updating the blocklist, DNS, or whitelist, depending on the specific circumstances of the IoC

upvoted 2 times

🗨️ 👤 **josbornx** 2 years, 2 months ago

D. The IDS signature should be updated next.

A threat hunting team typically uses Indicators of Compromise (IoCs) to identify potential threats or malicious activity in their network. In this scenario, the team has received a new IoC from an Information Sharing and Analysis Center (ISAC) that is related to a known threat actor's profile and activities.

To leverage this new information, the team should update their Intrusion Detection System (IDS) signature to include this IoC. This allows the IDS to identify and alert on any traffic that matches the IoC, providing an early warning of potential threats in the network.

While updating the whitelist, DNS, and blocklist are also important steps in securing the network, they are not the most immediate and critical next step in response to a new IoC.

ChatGPT

upvoted 1 times

🗨️ 👤 **josephconer1** 2 years, 2 months ago

"An indicator of compromise (IoC) is a residual sign that an asset or network has been successfully attacked or is continuing to be attacked."

Prevent THEN update the detection signature. ANSWER C.

upvoted 1 times

🗨️ 👤 **khrid4** 2 years, 3 months ago

Selected Answer: C

IDS = only detects and log

Blocklist = Prevent and also log

Why not block known IOC from a trusted source such as ISAC? Why choose to only detect?. It may be too late for your IR teams to respond if you wasted the intelligence in advance and do not configure any action to be taken against the known IOC.

Also, when doing blocklist, there's this thing called "retroactive alert" whereas even if you have delayed the input of the IOC into blocklist, "some" products may be able to catch it from the available historical data, if it has already affected your environment.

upvoted 2 times

🗨️ 👤 **10cccordrazine** 2 years, 4 months ago

Selected Answer: D

Agree on D.

The question says that they received an IoC from the ISAC -- this does not mean that their organization is compromised, only that there is a new threat to be aware of in the wider world. As others have mentioned, an IoC is not necessarily a blockable IP address, but rather behaviour patterns and other indicators, so updating the IDS to detect these indicators is the only thing that makes sense.

upvoted 3 times

🗨️ 👤 **david124** 2 years, 4 months ago

Selected Answer: D

D. The IDS signature

The next step after receiving a new Indicator of Compromise (IoC) from an Information Sharing and Analysis Center (ISAC) should be to update the Intrusion Detection System (IDS) signature. The IDS is a key component of an organization's security infrastructure that is designed to detect and alert on malicious activity on the network. By updating the IDS signature with the new IoC, the threat hunting team can be better prepared to detect

and respond to the activities of the identified threat actor. Other updates, such as to the whitelist, blocklist, or DNS, may also be necessary depending on the specific threat and the organization's security posture, but updating the IDS signature should be the first step to ensure that the organization is prepared to detect and respond to the identified threat.

upvoted 2 times

🗨️ **BRIGADIER** 2 years, 4 months ago

i found this link below. answer is D

<https://accedian.com/blog/what-is-the-difference-between-signature-based-and-behavior-based-ids/>

upvoted 1 times

🗨️ **IanRogerStewart** 2 years, 5 months ago

Selected Answer: C

assuming you have an IP address, block it, then worry about your IDS. Remember the IDS only detects doesn't prevent.

upvoted 2 times

🗨️ **trainingsmits** 2 years, 5 months ago

D should be the answer. The IoC could be a number of things, not necessarily a "blockable" IP address. Updating the IDS signature helps the IDS to catch the indicator, from whatever source it originates from.

upvoted 2 times

🗨️ **TIM0088** 2 years, 6 months ago

Selected Answer: C

After receiving a new IoC (Indicator of Compromise) from an ISAC (Information Sharing and Analysis Center) that follows a threat actor's profile and activities, the next step for the threat hunting team should be to update the blocklist.

A blocklist is a list of known malicious IP addresses, domains, or other indicators of compromise that are used to block or filter out potentially harmful traffic. By updating the blocklist with the new IoC, the threat hunting team can prevent the threat actor from accessing the network or other resources.

The correct answer is C: The blocklist.

upvoted 2 times

🗨️ **forest111** 2 years, 6 months ago

Selected Answer: C

CORRECTION, answer C. the fact is, given IOC are definitely examples of malicious communication, files, etc. So it has to be blocked, not only detect.

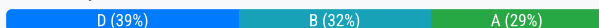
upvoted 1 times

A security analyst discovers a standard user has unauthorized access to the command prompt, PowerShell, and other system utilities. Which of the following is the BEST action for the security analyst to take?

- A. Disable the appropriate settings in the administrative template of the Group Policy.
- B. Use AppLocker to create a set of whitelist and blacklist rules specific to group membership.
- C. Modify the registry keys that correlate with the access settings for the System32 directory.
- D. Remove the user's permissions from the various system executables.

Suggested Answer: A

Community vote distribution



encxorblood Highly Voted 2 years, 4 months ago

Selected Answer: B

The BEST action for the security analyst to take when a standard user has unauthorized access to the command prompt, PowerShell, and other system utilities is to use AppLocker to create a set of whitelist and blacklist rules specific to group membership. Therefore, the correct answer is B.

AppLocker is a Windows feature that enables organizations to specify which applications are allowed to run on a computer system. By creating a set of whitelist and blacklist rules specific to group membership, the security analyst can restrict access to command prompt, PowerShell, and other system utilities for the standard user. This will help to prevent unauthorized access and misuse of these tools.

upvoted 7 times

tutita 2 years ago

the question is talking about an (just one) standard user with "extra" access to system assets, so by disabling that will do, so its D

upvoted 2 times

uday1985 1 year, 9 months ago

How about new users? isn't this involve manually configuring for each alert generated? rather than automating the process?

upvoted 2 times

RobV 1 year, 6 months ago

It did not specify ONE standard user. Standard user is also a group.

upvoted 1 times

Yerfez Highly Voted 2 years, 9 months ago

Selected Answer: A

A is correct

upvoted 6 times

zecomeia_007 Most Recent 11 months ago

Selected Answer: B

AppLocker is a powerful tool designed to control which applications users and groups can run on a system. By creating specific rules based on group membership, the analyst can effectively restrict access to command prompt, PowerShell, and other system utilities for standard users while allowing authorized users to continue using them.

upvoted 1 times

Ha89 12 months ago

Selected Answer: D

D it is.

upvoted 1 times

FT000 1 year, 4 months ago

Selected Answer: D

For me, the keyword here is 'unauthorised access'. If we are to use GPO or whitelist/blacklist, it means currently he is authorised albeit by mistake only, but authorised. So I am going with D as that removes the user's access to executables and brings reinstates his account to authorised accesses only.

upvoted 1 times

🗨️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

B. Use AppLocker to create a set of whitelist and blacklist rules specific to group membership.

AppLocker is a security feature in Windows that allows you to create policies to control which applications are allowed to run on a system. In this scenario, using AppLocker to create a set of whitelist rules specific to group membership would be the best action. This approach would allow the security analyst to specify which applications (such as the command prompt, PowerShell, and other system utilities) are allowed to run based on the user's group membership.

upvoted 1 times

🗨️ 👤 **32d799a** 1 year, 7 months ago

Selected Answer: B

AppLocker is a Microsoft Windows feature that allows administrators to create policies to control which applications are allowed to run on a system. In this scenario, using AppLocker to create a set of rules specific to group membership would be an effective way to control and restrict the unauthorized access to command prompt, PowerShell, and other system utilities.

upvoted 1 times

🗨️ 👤 **novolyus** 1 year, 7 months ago

Applocker? who mentioned anything about using Windows?

upvoted 1 times

🗨️ 👤 **skibby16** 1 year, 6 months ago

Powershell is windows native scripting tool

upvoted 1 times

🗨️ 👤 **grelaman** 1 year, 9 months ago

Selected Answer: A

This will prevent the standard user from accessing the command prompt, PowerShell, and other system utilities, regardless of their permissions to the individual executables.

Group Policy can be used to enforce a wide variety of administrative rules. It's the best administrative option from my perspective.

upvoted 1 times

🗨️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: A

Disabling the appropriate settings in the administrative template of the Group Policy can help restrict access to command prompt, PowerShell, and other system utilities for standard users.

upvoted 1 times

🗨️ 👤 **tutita** 2 years ago

Selected Answer: D

the question is talking about an (just one) standard user with "extra" access to system assets, so by disabling that will do, so its D

upvoted 3 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: D

Remove the user's permissions from the various system executables is the BEST action for the security analyst to take.

upvoted 1 times

🗨️ 👤 **JoshuaXIV** 2 years, 2 months ago

Selected Answer: D

Based on the scenario, there is a malicious event happened to a standard user which has access to system utilities beyond the set permission.

Ofcourse, first we will isolate it.

Why not A? because it may affect other legitimate users as well.

Just my thoughts on the question.

upvoted 1 times

🗨️ 👤 **trainingsmits** 2 years, 5 months ago

Selected Answer: D

The question states that the user is a "standard user", not an administrator account, with extra permissions. Disabling the settings in the administrative template (A) will not affect a standard user unless they are part of the administrative group.

D is the only answer that makes sense.

upvoted 2 times

  **trojan123** 2 years, 5 months ago

Standard user permissions can also be set using administrative templates in Group Policy Objects (GPOs). These templates can be used to configure settings for standard users just like they can be used to configure settings for privileged users. For example, an organization can use administrative templates to configure security settings, software installation and maintenance settings, and settings for specific applications for standard users.

It's important to note that while standard users may not have the ability to modify GPO settings themselves, the administrative templates can be used by a privileged user, such as an administrator, to configure settings for standard users. These templates can be used to restrict access to certain features or applications for standard users, or to configure settings that will enforce specific policies for standard users.

It's important to review and test the changes made by GPO for standard users, to ensure that the changes do not negatively impact their daily work.

upvoted 2 times

  **Comptia_Secret_Service** 2 years, 6 months ago

Selected Answer: D

This should be D. The problem states the user has been given excessive permissions violating the principle of least privilege, removing the user's access to stated executables will correct the user's permission. Changing settings in the group policy is excessive and is actually needed for admin roles, the question also didn't state the use of Group Policies to apply user permissions.

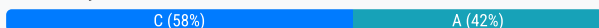
upvoted 2 times

The Chief Information Officer of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue?

- A. Include digital signatures on messages originating within the company.
- B. Require users to authenticate to the SMTP server.
- C. Implement DKIM to perform authentication that will prevent the issue.
- D. Set up an email analysis solution that looks for known malicious links within the email.

Suggested Answer: C

Community vote distribution



🗳️ **AC6280** Highly Voted 2 years, 4 months ago

Selected Answer: A

Drawing from my email security experience...

A- The most likely answer. Digital signatures are just that, signatures that should apply to only you. It provides non-repudiation (you can't deny that you sent it, or at the very least that your machine sent it, or that someone who has the crypto keys sent it)

B- This doesn't really stop anything. Sure you have to log in to use your email, but anyone can still spoof you (email is inherently and insanely insecure)

C- DKIM is nice as part of email authentication (use DMARC with SPF/DKIM), but DKIM doesn't care about 'friendly from' headers that users see in their mailbox. You can still very much spoof the 'from' field and still pass DKIM (I've had to explain this scenario to customers a gazillion times).

D- Doesn't stop the spoofing. Just checks links.

upvoted 11 times

🗳️ **saci_frosty** 2 years, 3 months ago

Answer A

I agree with you, DKIM won't stop "friendly from" headers, also D doesn't work as the scammer might be trying to trick the user to send them gift cards for instance. I had it happened to a user once. They made the email look like it was coming from the manager asking the employee to buy gift cards and I had to explain why the manager's email hadn't been hacked. Key word of the question is "Appear"

upvoted 1 times

🗳️ **DaroKa** Highly Voted 2 years, 9 months ago

Selected Answer: C

Following:

<https://www.examttopics.com/discussions/comptia/view/75177-exam-cs0-002-topic-1-question-239-discussion/>

upvoted 5 times

🗳️ **RobV** Most Recent 1 year, 6 months ago

Selected Answer: C

C. Implement DKIM to perform authentication that will prevent the issue.

Phishing attacks often involve spoofed emails that appear to come from legitimate sources within the organization. DKIM helps address this issue by providing a way to verify the integrity of the email's source. It won't prevent all phishing attacks, but it can significantly reduce the effectiveness of attacks that rely on impersonating internal senders.

Option A, including digital signatures on messages originating within the company, is related to DKIM, but DKIM is a more specific and widely adopted standard for email authentication.

upvoted 1 times

🗳️ **skibby16** 1 year, 6 months ago

Selected Answer: C

DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing. By signing outgoing emails with a private key and allowing the recipient to verify the signature using a public key published in the DNS, DKIM helps prevent email forging and ensures the integrity of the email content. Implementing DKIM can significantly reduce the effectiveness of phishing attacks that rely on spoofing the sender's address.

upvoted 1 times

🗄️ 👤 **32d799a** 1 year, 7 months ago

Selected Answer: C

DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing

upvoted 1 times

🗄️ 👤 **uday1985** 1 year, 9 months ago

This question is not clear! is the threat actor the employee? someone else spoofed them? if its a threat actor then DKIM. but if its an internal risk then its a different approach

upvoted 1 times

🗄️ 👤 **naleenh** 1 year, 10 months ago

Selected Answer: C

DKIM (DomainKeys Identified Mail) is an email authentication method that allows the sender to prove that they are who they say they are. This helps to prevent phishing emails, which are emails that appear to come from a legitimate source but are actually from a malicious actor.

upvoted 1 times

🗄️ 👤 **kill_chain** 1 year, 10 months ago

Selected Answer: C

DKIM allows organizations to add content to messages to identify them as being from their domain. DKIM signs both the body of the message and elements of the header, helping to ensure that the message is actually from the organization it claims to be from.

upvoted 2 times

🗄️ 👤 **Sleezyglizzy** 1 year, 11 months ago

C

from previous dump

upvoted 1 times

🗄️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

By implementing DKIM, an organization can ensure that emails appearing to come from within the company are legitimate and have not been spoofed by an attacker. This can help prevent employees from falling victim to phishing emails.

Option A, including digital signatures on messages originating within the company, is a possible solution. However, this would require all employees to have digital signatures, which may not be practical

upvoted 1 times

🗄️ 👤 **HereToStudy** 2 years, 2 months ago

Selected Answer: A

DKIM is also a valid solution for email authentication, it alone does not address the issue of email spoofing or impersonation in the "friendly from" header. Therefore, in this case, the BEST solution to prevent this issue would be to include digital signatures on messages originating within the company.

upvoted 2 times

🗄️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. I like both A and C, my thought process is that DKIM validates the sender on the server level. If I spoof a company username in the 'friendly from' field, DKIM should not allow it as it was sent from a mail server that is not validated.

upvoted 3 times

A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?

- A. `dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5, sha1 hashlog=/mnt/usb/evidence.bin.hashlog`
- B. `dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha512sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash`
- C. `tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt; sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash`
- D. `find / -type f -exec cp {} /mnt/usb/evidence/ \; sha1sum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash`

Suggested Answer: B

Community vote distribution

B (52%)

A (48%)

🗳️ 👤 **Tag** Highly Voted 2 years, 8 months ago

Selected Answer: B

B is correct

upvoted 7 times

🗳️ 👤 **2Fish** 2 years, 2 months ago

Agree - (A) would also work but I'm not so sure about /dev/one and the MD5. (B) also creates a sha512 hash.

upvoted 1 times

🗳️ 👤 **kyky** 2 years ago

Option B (dd command with sha512sum) is incorrect because sha512sum is not a valid command. It seems to be a typographical error, and the command should have been sha512sum.

upvoted 1 times

🗳️ 👤 **SAAVYTECH** Highly Voted 2 years, 9 months ago

Selected Answer: A

"dcfldd is an enhanced version of GNU dd with features useful for forensics and security. dcfldd has the following additional features
Hashing on the fly- dcfldd can hash the input data as it is being transferred helping to ensure data integrity.

<https://www.forensics-matters.com/2020/10/20/simple-forensics-imaging-with-dd-dc3dd-dcfldd/#:~:text=dcfldd%20is%20an%20enhanced%20version,helping%20to%20ensure%20data%20integrity.>

upvoted 7 times

🗳️ 👤 **Abyad** 2 years, 7 months ago

but it uses md5 and sha1, while B uses sha512

upvoted 1 times

🗳️ 👤 **abrilo** 2 years, 7 months ago

You may be wondering why MD5 is used for forensic imaging when most security practitioners recommend against using it. MD5 remains in use because it is fast and widely available, and the attacks against MD5 are primarily threats for reasons that don't apply to forensic images. As a practitioner, you are unlikely to encounter someone who can or would intentionally make two drives with different contents hash to the same value.....from CompTIA notebook

upvoted 3 times

🗳️ 👤 **Tag** 2 years, 8 months ago

however, the answers given, id say B is correct based on the syntax.

in A, the file or block copied is "one" .. /dev/one
idk what that is

in B, its /dev/sda which is the block itself "sda"

upvoted 10 times

🗳️ 👤 **fermins** 2 years, 4 months ago

this is most likely the key, one is not a valid partition...

upvoted 2 times

🗨️ 👤 **RobV** Most Recent 1 year, 6 months ago

Is sha512sum an error or intentional?

upvoted 1 times

🗨️ 👤 **RobV** 1 year, 6 months ago

B is right if it's a typo. If an intentional mistake then it would return an error making A correct.

upvoted 1 times

🗨️ 👤 **greatsparta** 1 year, 7 months ago

Selected Answer: A

This command uses dcfldd to copy the contents of the hard drive (if=/dev/one) to a file (of=/mnt/usb/evidence.bin). It also generates MD5 and SHA-1 hash values for the copied data, and the hash values are logged to /mnt/usb/evidence.bin.hashlog.

upvoted 1 times

🗨️ 👤 **Xoomalla** 1 year, 10 months ago

Selected Answer: B

Syntax error in A... this is why B was chosen.

/dev/one .. I don't know any device with the name "one".

upvoted 1 times

🗨️ 👤 **Aliyan** 1 year, 11 months ago

Selected Answer: B

Question is

"Which of the following would allow the analyst to perform the task?"

NOT

"Which of the following would allow BEST AND MORE DETAILED FOR the analyst to perform the task?"

I would not risk it for A because also /dev/one is not default hard drive name. Also dcfldd is more advanced and not everyone can read it

upvoted 1 times

🗨️ 👤 **heinzeltumpel** 1 year, 11 months ago

ther is no thing as /dev/one

upvoted 2 times

🗨️ 👤 **Sleezyglizzy** 1 year, 11 months ago

B

first part of command in A is wrong

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: A

A. dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5, sha1 hashlog=/mnt/usb/evidence.bin.hashlog.

Option A would allow the security analyst to perform the task of providing a copy of a hard drive for forensic analysis. The command dcfldd is a forensic version of the dd command and is commonly used for creating forensic disk images.

The command dcfldd if=/dev/one specifies the input file as /dev/one, representing the hard drive. The of=/mnt/usb/evidence.bin specifies the output file as /mnt/usb/evidence.bin, which is where the copy of the hard drive will be saved.

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Option B (dd command with sha512sum) is incorrect because sha512sum is not a valid command. It seems to be a typographical error, and the command should have been sha512sum.

upvoted 1 times

🗨️ 👤 **tutita** 2 years ago

Selected Answer: B

option B its the right one, option A has a wrong syntax its copying from dev/one and it doesn't exist such a thing dev/sda is where the partitions are located

upvoted 1 times

🗨️ 👤 **Jolnn** 2 years, 1 month ago

Selected Answer: B

Guys, this is B. For the people who are wondering about the misspelling in sha512sum command, it's just the way the questions were transcribed.

upvoted 2 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: A

The dcfldd command is a forensic version of the dd command that is used for low-level copying of data. The "if" parameter specifies the input file (in this case, the hard drive to be imaged), and the "of" parameter specifies the output file (in this case, the destination of the forensic image). The "hash" parameter allows the analyst to generate a hash of the forensic image to verify its integrity, and the "hashlog" parameter specifies the location of the hash log file.

Option B, `dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha5l2sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash`, is missing a digit in the command (it should be sha512sum instead of sha5l2sum) and it does not use a forensic version of the dd command like dcfldd.

upvoted 2 times

🗨️ 👤 **JoshuaXIV** 2 years, 2 months ago

For the guys who answer B, have you notice the sha5l2sum on the command? it should be sha512sum right?

upvoted 1 times

🗨️ 👤 **trojan123** 2 years, 5 months ago

Selected Answer: A

Option B is not suitable to provide a copy of a hard drive for forensic analysis as it does not include unused and slack space.

Unused and slack space are the areas on a hard drive that do not contain data and can contain hidden data that may be important for forensic analysis. By not including these areas in the copy, valuable data may be missed, and the integrity of the evidence can be compromised.

upvoted 3 times

🗨️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: B

B is the only answer that makes sense since it's a forensic tool.

upvoted 1 times

🗨️ 👤 **j0n45** 2 years, 5 months ago

Selected Answer: B

also B is correct because the syntax in A has a ";" in it, and not "," for properly executing the sha command.

upvoted 1 times

🗨️ 👤 **lordguck** 2 years, 6 months ago

B: A: is the better solution but the command line is wrong "if=/dev/one"

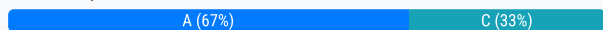
upvoted 2 times

A Chief Information Security Officer (CISO) is concerned developers have too much visibility into customer data. Which of the following controls should be implemented to BEST address these concerns?

- A. Data masking
- B. Data loss prevention
- C. Data minimization
- D. Data sovereignty

Suggested Answer: A

Community vote distribution



Ty_tty Highly Voted 3 years, 10 months ago

im surprised one of the choices wasnt Network Segmentation. Imao
upvoted 37 times

2Fish 2 years, 3 months ago

bahahah... yes! Also the given answer is correct.
upvoted 1 times

SniipZ Highly Voted 4 years ago

A is correct. Devs do not need real data to test their applications!
upvoted 9 times

Pavel019846457 Most Recent 1 year, 7 months ago

Selected Answer: A
Data masking
upvoted 1 times

kyky 2 years ago

Selected Answer: C
To address the Chief Information Security Officer's (CISO) concerns about developers having too much visibility into customer data, the control that should be implemented to BEST address these concerns is:

C. Data minimization.

Data minimization refers to the practice of reducing the amount of data collected, processed, and stored to only what is necessary for legitimate business purposes. By implementing data minimization controls, the organization can limit the exposure of customer data to developers and other personnel.
upvoted 2 times

miabe 2 years, 11 months ago

Selected Answer: A
looks good to me
upvoted 3 times

DrChats 4 years ago

A is Right
upvoted 3 times

mcNik 4 years ago

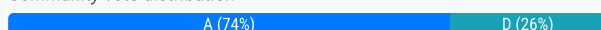
Data masking works .
upvoted 2 times

During a forensic investigation, a security analyst reviews some Session Initiation Protocol packets that came from a suspicious IP address. Law enforcement requires access to a VoIP call that originated from the suspicious IP address. Which of the following should the analyst use to accomplish this task?

- A. Wireshark
- B. iptables
- C. Tcp dump
- D. Net flow

Suggested Answer: A

Community vote distribution



🗳️ 👤 **jleonard_ddc** Highly Voted 2 years, 3 months ago

Selected Answer: A

Wireshark would allow us to quickly highlight and analyze the VOIP conversation from the packet capture. In fact it has built-in features specific to VOIP.

WRONG ANSWERS

- B – iptables is used in Linux for building firewall rules. It might be something we could use to direct / filter VOIP access but we already have packets captured.
- C – Packets have already been captured by the analyst, so we don't need to do more packet captures.
- D – Net flow can be used to capture and analyze packets, but is primarily designed to generate statistics from that data. We need a deep dive into the contents of the VOIP conversation instead.

upvoted 7 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree. The question does not state it needs access to the actual Voice call or just the packets, I think this is the best answer from the ones given.

upvoted 1 times

🗳️ 👤 **RobV** Most Recent 1 year, 6 months ago

Selected Answer: A

A. Wireshark

upvoted 1 times

🗳️ 👤 **Chilaqui1es** 1 year, 8 months ago

"The Wireshark program implements a convenient mechanism for diagnosing (analyzing) VoIP calls" - Google (Answer is definitely A)

upvoted 2 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: A

Option D, NetFlow, is a network protocol that provides traffic visibility and analysis, but it does not have the ability to extract audio from VoIP packets.

upvoted 3 times

🗳️ 👤 **CyberNoob404** 2 years, 5 months ago

Selected Answer: A

Google Wireshark VOIP

upvoted 1 times

🗳️ 👤 **trainingsmits** 2 years, 5 months ago

Selected Answer: A

WireShark is best for reassembling VoIP

upvoted 3 times

🗳️ 👤 **j0n45** 2 years, 5 months ago

Selected Answer: D

Basically, we use NetFlow format, for collecting SIP information that is commonly used for broadband traffic monitoring.

<https://silo.tips/download/analysis-of-sip-traffic-behavior-with-netflow-based-statistical-information>

upvoted 2 times

🗨️ 👤 **novolyus** 1 year, 7 months ago

But you cannot extract the voice conversation with the netflow. So no, the answer is Wireshark that has a convenient tool for this.

upvoted 1 times

🗨️ 👤 **mrodmv** 2 years, 6 months ago

Based on my knowledge i can't say which is correct, this maybe help to clarify this

<https://learningnetwork.cisco.com/s/question/0D53i00000KszWaCAJ/netflow-vs-packet-analyzer>

upvoted 1 times

🗨️ 👤 **iking** 2 years, 6 months ago

Selected Answer: A

A. Wireshark. Reviewing Session Initiation Protocol (SIP) packets or VOIP , you must use Wireshark. This is now an investigation and analysis and no chance of capturing it again. Wireshark can decode SIP over TLS and Decrypting SDES too. This is what they need for forensic investigation.

upvoted 3 times

🗨️ 👤 **Comptia_Secret_Service** 2 years, 6 months ago

Selected Answer: D

Agree with D, although it would be best to use a dedicated protocol analysis application like Wireshark or TCPdump, they aren't typically run passively on enterprise networks. Flows however are very commonly deployed on networks and would still provide you with connection details such as bytes transferred, ports, IPs, timestamps, etc.

upvoted 1 times

🗨️ 👤 **Frog_Man** 2 years, 7 months ago

It cannot be netflow as it captures traffic as it enters or leaves a router. The tech has already captured the packets. Answer is "A".

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: A

Answer is Wireshark, just download it try on VOIP traffic

upvoted 1 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

Not that I spent all day researching but from the research I have done it could be A or D. From CompTIA's POV I feel like they'd want A as the answer but I don't know anymore.

upvoted 1 times

🗨️ 👤 **KingDeeko** 2 years, 8 months ago

Selected Answer: A

Analysis of Telephony Protocols VoIP Analysis Tip: Wireshark has the ability to reconstruct not only VoIP conversations, but also other media streams

upvoted 3 times

🗨️ 👤 **jagoichi** 2 years, 8 months ago

Selected Answer: A

Answer is A

Wireshark is used to analyze VOIP traffic.

upvoted 1 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: D

Agree with TheSkyMan. D

upvoted 1 times

🗨️ 👤 **adamhoms** 2 years, 9 months ago

Wireshark allows you to capture and analyze VoIP network traffic and packet data from the NEC SL2100 and SL1100. This is a must-read for installers working with or troubleshooting VoIP issues.

upvoted 2 times

A security team has begun updating the risk management plan, incident response plan, and system security plan to ensure compliance with security review guidelines. Which of the following can be executed by internal managers to simulate and validate the proposed changes?

- A. Internal management review
- B. Control assessment
- C. Tabletop exercise
- D. Peer review

Suggested Answer: A

Community vote distribution

C (63%)

A (37%)

10cccordrazine Highly Voted 2 years, 4 months ago

Selected Answer: A

"Which of the following can be executed by internal managers"

Internal managers will never execute a tabletop exercise, they wouldn't have the required skills. That's for the security team to do.

Now, if by that sentence they mean that the internal managers plan the session, then it could be C, but I'm still banking on A.

As usual unfortunate wording which adds artificial difficulty to an otherwise simple question
upvoted 10 times

HereToStudy 2 years, 2 months ago

internal managers can execute tabletop exercises. Tabletop exercises are a common tool used by organizations to test and validate their incident response plans and security procedures. They typically involve a group of stakeholders, including internal managers and employees, who simulate a security incident or breach scenario and discuss the appropriate response actions.

upvoted 1 times

POWNED Highly Voted 1 year, 10 months ago

Selected Answer: C

Key word here in the question is SIMULATE answer is C
upvoted 6 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: C

C. Tabletop exercise - Key word is "SIMULATE"

A tabletop exercise is a type of simulation where key personnel gather to discuss and simulate a hypothetical scenario, often involving a cybersecurity incident. It is used to validate and test the effectiveness of plans, procedures, and communication channels. In this case, a tabletop exercise would be suitable for simulating and validating the proposed changes to the risk management plan, incident response plan, and system security plan.

While internal management review (Option A) and peer review (Option D) involve evaluations by internal stakeholders, they may not actively simulate scenarios and test the plans in the same way a tabletop exercise does.
upvoted 1 times

Pavel019846457 1 year, 7 months ago

Selected Answer: C

I would go with "C" because of word "simulate"
upvoted 2 times

Nixon333 1 year, 10 months ago

Internal management review could involve high-level overview and approval but may not simulate and validate the proposed changes in a practical manner like a tabletop exercise.
upvoted 1 times

kyky 2 years ago

Selected Answer: C

A tabletop exercise is a simulated scenario-based discussion that involves key stakeholders and decision-makers to evaluate the effectiveness and readiness of a proposed plan or process. In the context of security updates and compliance, a tabletop exercise can be used to simulate various security incidents and assess how the proposed changes in the risk management plan, incident response plan, and system security plan hold up in practice. It allows internal managers to test the effectiveness of the proposed changes, identify any gaps or weaknesses, and make necessary adjustments before implementing them in real-world situations.

upvoted 2 times

JoshuaXIV 2 years, 2 months ago

Selected Answer: C

Internal Managers can do Tabletop Exercise.

upvoted 1 times

HereToStudy 2 years, 2 months ago

Selected Answer: C

Internal management review is a process where internal managers review documents or processes to ensure that they comply with established policies, standards, and procedures. It is a general process that can be used for any document or process and may not be specific to validating security changes.

upvoted 1 times

AbusedInk 2 years, 3 months ago

Selected Answer: C

Tabletop exercises (TTXs) may or may not happen at a tabletop, but they do not involve a technical control infrastructure. TTXs can happen at the executive level (for example, CEO, CIO, or CFO), at the team level (for example, security operations center or SOC), or anywhere in between. The idea is usually to test out procedures and ensure that they actually do what they're intended to and that everyone knows their role in responding to an event. TTXs require relatively few resources apart from deliberate planning by qualified individuals and the undisturbed time and attention of the participants.

upvoted 1 times

Lukers 2 years, 3 months ago

Selected Answer: C

The question is asking which would simulate and validate the proposed changes. The only answer that includes a simulation is C. Tabletop exercise.

upvoted 2 times

2Fish 2 years, 3 months ago

Selected Answer: C

C. Mainly because the word simulate is mentioned. I would also say that there are managers in the table top discussions along with technical staff.

upvoted 3 times

jleonard_ddc 2 years, 3 months ago

Selected Answer: A

An internal management review is usually done for auditing purposes to check that plans are compliant with company policies.

WRONG ANSWERS

- B – We're not looking to assess if certain controls are in place or designed correctly. We're looking to see if the plans we've updated are still in compliance with guidelines.
- C – a tabletop exercise is verbally simulated and therefore doesn't require extensive technical skill. However, it does require very technical knowledge, and would be done by a cybersecurity expert.
- D – peers not only might not know if our policies are compliant, they may not be the best people to share security plans with.

upvoted 3 times

Study4America 2 years, 7 months ago

Selected Answer: C

the key word is simulate

upvoted 3 times

Maniact165 2 years, 7 months ago

Selected Answer: C

C right?

upvoted 1 times

SolventCourseisSCAM 2 years, 7 months ago

Selected Answer: A



Management review is the routine evaluation of whether management systems are performing as intended and producing the desired results as efficiently as possible. It is the ongoing "due diligence" review by management that fills the gap between day-to-day work activities and periodic formal audits.

upvoted 2 times

  **SolventCourseisSCAM** 2 years, 7 months ago

I changed my mind to answer C, made a search on it and compitua asking here tabletop by mentioning simulation

upvoted 2 times

  **R00ted** 2 years, 8 months ago

Selected Answer: C

C is the correct answer

upvoted 1 times

  **KingDeeko** 2 years, 8 months ago

Selected Answer: A

can be executed by internal managers to simulate and validate the proposed changes?

is literally has the answer in the question.. its a review.. who knows how they conduct the review. could be a simulated event

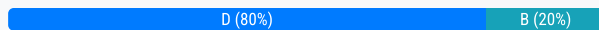
upvoted 1 times

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs. Which of the following is the main concern a security analyst should have with this arrangement?

- A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
- B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
- C. Development phases occurring at multiple sites may produce change management issues.
- D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Suggested Answer: D

Community vote distribution



Obi_Wan_Jacoby **Highly Voted** 4 years, 5 months ago

D is correct. There is a large two part series out there on the theft of intellectual property on FPGA's, so that is a real thing and big deal it seems "https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part-1/"
upvoted 13 times

who_cares123456789__ 4 years, 3 months ago

Agreed!!
upvoted 3 times

2Fish 2 years, 3 months ago

Agree. Good article!
upvoted 1 times

RobV **Most Recent** 1 year, 6 months ago

Selected Answer: D

D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

The main concern for a security analyst in this scenario is the potential for intellectual property theft. FPGAs (Field-Programmable Gate Arrays) are reprogrammable devices that can be configured for specific applications. If the development phases involve sharing FPGA designs or configurations between the small electronics company and the contractor's labs, there is a risk that the intellectual property associated with the FPGA-based device could be copied or stolen.
upvoted 1 times

novolyus 1 year, 7 months ago

Selected Answer: B

Concern of a security analyst. A security analyst concern should be doing his job properly, and option B is his concern. Intellectual property should be the concern of another department.
If the question was "Which should be the company's concern" then D. But the company accepted the risk of intellectual property leak and you have to do your task as a security analyst.
It is not your business intellectual property or health and safety conditions.
upvoted 1 times

CatoFong 2 years, 4 months ago

Selected Answer: D

D. is correct
upvoted 1 times

SylFlo 2 years, 5 months ago

i'm glad i guessed correctly, i couldn't remember this answer, but guessed D, passed today
upvoted 1 times

Mr_Robot69 2 years, 10 months ago

Below article is from CompTIA official guide
Anti-Tamper

If an attacker can steal the hardware, TPMs and HSMs are vulnerable to physical attacks against the chips to extract the keys. Anti-tamper solutions are designed to mitigate this risk. An anti-tamper mechanism makes use of a type of programmable controller called a field programmable gate array (FPGA) and a physically unclonable function (PUF). The PUF generates a digital fingerprint based on unique features of the device. This means that tampering, by removing the chip or adding an unknown input/output mechanism for instance, can be detected and a remedial action, such as zerofilling cryptographic keys, can be performed automatically.

upvoted 1 times

🗨️ 👤 **Mr_Robot69** 2 years, 10 months ago

Going with option B

upvoted 1 times

🗨️ 👤 **twobuckchuck** 2 years, 10 months ago

Is FPGA a new crypto coin? Fungible Payment in Gold Allowance?

upvoted 1 times

🗨️ 👤 **miabe** 2 years, 11 months ago

Selected Answer: D

looks good to me

upvoted 1 times

🗨️ 👤 **Davar39** 3 years, 3 months ago

Selected Answer: D

Only D directly concerns a security analyst.

upvoted 1 times

🗨️ 👤 **Action66** 3 years, 11 months ago

Several CYSA+ (002) test preps I used show the answer as B. Reference: <https://www.certification-questions.com/pdf-download/comptia/cs0-002-pdf.pdf>

upvoted 2 times

🗨️ 👤 **Sweetlulu** 3 years, 11 months ago

D is the correct answer. B is close 2nd.

Which is of the security issues are the worse for the company? Losing the Company's intellectual property or diminishing security viewing?

upvoted 2 times

🗨️ 👤 **Remilia** 3 years, 6 months ago

This is why I value the discussions in exam topics. Very insightful.

upvoted 3 times

🗨️ 👤 **Alizadeh** 4 years, 3 months ago

D is correct

upvoted 3 times

🗨️ 👤 **I_heart_shuffle_girls** 4 years, 5 months ago

D seems to be correct but B might also be a correct answer. Any other thoughts?

upvoted 4 times

🗨️ 👤 **who_cares123456789___** 4 years, 2 months ago

Yes. Another thought is that there is no time frame mentioned. No end date mentioned so no reason to assume security testing will be diminished. But deployment for testing at off-site locales put property out of any chain of custody and someone could easily steal the Intel Property...quite simple really.

upvoted 3 times

A security analyst needs to reduce the overall attack surface. Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

Suggested Answer: B

Community vote distribution

C (74%)

B (26%)

🗳️ 👤 **I_heart_shuffle_girls** Highly Voted 4 years, 5 months ago

I agree on C.

upvoted 12 times

🗳️ 👤 **Obi_Wan_Jacoby** 4 years, 5 months ago

I concur with C

upvoted 8 times

🗳️ 👤 **catastrophie** Highly Voted 2 years, 4 months ago

Selected Answer: C

Answer is C increasing network segmentation. There are many ways to reduce the network surface including air gapping. However this is asking for the reduction in the overall attack surface, not just for sensitive systems. Other broad strokes of reducing the attack surface would be things like enforcing zero trust on systems, strong authentication policy enforcement, strict access control processes, etc... anything that can be applied over a wide spread area to reduce potential points of entry.

upvoted 6 times

🗳️ 👤 **RobV** Most Recent 1 year, 6 months ago

Selected Answer: C

C. Increase the network segmentation.

upvoted 1 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Selected Answer: C

C. The key here is "overall" attack surface.

upvoted 3 times

🗳️ 👤 **Stiobhan** 2 years, 4 months ago

I need to go with Air Gap here. Reducing the attack surface is achieved by Air Gapping, well from logical attack anyway. If something is properly Air Gapped then it needs a physical interaction to breach it (usb etc... See Stuxnet) Segmentation is great and it should be high on the design agenda of a network but it doesn't make the attack surface smaller it just makes it harder to breach.

upvoted 2 times

🗳️ 👤 **jleonard_ddc** 2 years, 5 months ago

Selected Answer: B

Network segmentation doesn't reduce your attack surface, it just isolates the impact of any attack. Air gap is the only solution here that actually reduces attack surface.

upvoted 3 times

🗳️ 👤 **moonash** 2 years, 7 months ago

key word overall attack surface will go with C

upvoted 2 times

🗳️ 👤 **soska123** 2 years, 7 months ago

I think the segmentation is the best solution to isolated the infection or threat and make it smaller so can be handled easy and controlled it, I going with C.

upvoted 1 times

🗄️ 👤 **TeyMe** 2 years, 7 months ago

Selected Answer: B

The attack surface is all the points at which an adversary could interact with the system and potentially compromise it. To determine the attack surface, you must inventory the assets deployed on your network and the processes that those assets support.

upvoted 2 times

🗄️ 👤 **KingDeeko** 2 years, 8 months ago

Two proven techniques for reducing the attack surface on your backup data that often go hand in hand are data isolation and air gapping.

upvoted 1 times

🗄️ 👤 **Tag** 2 years, 8 months ago

Selected Answer: C

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.

Attack Surface Reduction in 5 Steps

1. Implement Zero-trust Policies
2. Eliminate Complexity
3. Scan for Vulnerabilities
4. Segment Network
5. Train Employees

<https://www.fortinet.com/resources/cyberglossary/attack-surface>

upvoted 2 times

🗄️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: C

"The number of systems that are exposed to attackers (commonly called the organization's attack surface) can be reduced by compartmentalizing systems and networks."

upvoted 1 times

🗄️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

i thought it was C

upvoted 2 times

🗄️ 👤 **Cizzla7049** 2 years, 9 months ago

Increase network segmentation per google

upvoted 1 times

🗄️ 👤 **kchugh** 4 years ago

Wouldn't segmenting the network create small pieces of the network but when you combine those pieces the total are of the network be the same? Wouldn't moving to cloud-based architecture better as you are transferring some of the risk to the vendor hence reducing the attack surface?

upvoted 1 times

🗄️ 👤 **SniipZ** 4 years ago

No. Segmentation means for example to split up the network into DMZ and internal network. The attack surface is now reduced, because only the DMZ is exposed to the internet.

upvoted 5 times

🗄️ 👤 **MinnesotaMike** 3 years, 11 months ago

You could do that but what company could afford that. Risk analysis man. Is the cost of moving your whole infrastructure feasible. What CIO would sign off on that. The risk would have to be huge and the cost of a breach would have to greatly exceed the price to move it all to the cloud.

upvoted 1 times


🗄️ 👤 **vorozco** 3 years, 6 months ago

I see your logic. That a segmented network is still the same size as the whole prior to segmentation, thus not reduced. However, the source provided states segmentation "helps to reduce the attack surface by increasing the number of barriers an attacker encounters when attempting to travel through the network."

Think of a big, flat network (one big surface). This usually isn't a good idea because if an attacker makes their way in, it's a free for all. BUT, if we segment that network (I guess you can think of it as multiple fragmented surfaces where each fragment is a REDUCED portion of the whole), it becomes harder for the attacker to maneuver throughout the network because there are more barriers. Thus, the overall attack surface is reduced.

Hope this helps clarify.

upvoted 3 times

  **somsom** 4 years, 3 months ago

Agree on C

upvoted 3 times

A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported, and patches are no longer available. The company is not prepared to cease its use of these workstations. Which of the following would be the BEST method to protect these workstations from threats?

- A. Deploy whitelisting to the identified workstations to limit the attack surface.
- B. Determine the system process criticality and document it.
- C. Isolate the workstations and air gap them when it is feasible.
- D. Increase security monitoring on the workstations.

Suggested Answer: C

Community vote distribution

C (89%)

11%

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: C

C. Isolate the workstations and air gap them when it is feasible.
upvoted 2 times

🗳️ 👤 **skibby16** 1 year, 6 months ago

Selected Answer: A

Deploying whitelisting to the identified workstations would be the best method to protect these workstations from threats. Whitelisting is a technique that allows only authorized applications, processes, or users to run or access a system or resource. Whitelisting can help limit the attack surface and prevent malware or unauthorized software from running on a system. Deploying whitelisting to the workstations that are at the end of life can help mitigate the risk of exploitation due to lack of patches or support from the vendor.
upvoted 1 times

🗳️ 👤 **Tag** 2 years, 8 months ago

Selected Answer: C

An air gap, air wall, air gapping or disconnected network is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.
upvoted 2 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree. C is the best option here.
upvoted 1 times

🗳️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: C

"Best method" It is hard to beat an Airgap
upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

C seems like the best answer to me, despite what Cizzla7049 says about google.
upvoted 2 times

🗳️ 👤 **marc4354345** 2 years, 9 months ago

Selected Answer: C

security monitoring does not protect from threats. isolation / air gapping does.
upvoted 2 times

🗳️ 👤 **Cizzla7049** 2 years, 9 months ago

Google says increase security monitoring
upvoted 1 times

A small business does not have enough staff in the accounting department to segregate duties. The comptroller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

- A. Deterrent
- B. Preventive
- C. Compensating
- D. Detective

Suggested Answer: C

Community vote distribution



msellers Highly Voted 3 years, 5 months ago

I think this falls under compensating controls.

<https://www.fa.ufl.edu/directives/compensating-controls/>

Here is an example of when a compensating control would be required:

A single employee has the duties of accepting cash payments, recording the deposit, and reconciling the monthly financial reports. To prevent errors and/or fraud, additional oversight is required. This means we need a compensating control, such as the leader performing a review of the reconciliation or another unit performing the reconciliation. In some cases, two small units have "swapped" reconciliation duties to provide the needed separation of duties that are not possible within the unit.

upvoted 29 times

Loveguitar 3 years, 1 month ago

Absolutely a compensating control. Yes it is an operational control that is detective in nature but in the situation where you can not apply the required control (PCI DSS allows you to apply compensating controls) While this does not relate to credit card environment (CDE) and PCI DSS most likely does not apply, in financial audit, where segregation of duties (the required control) cannot be applied, the company is allowed to adopt oversight (supervision) as a compensating control

upvoted 2 times

Threat_Analyst 3 years ago

It cannot be compensating because they are not applying another control similar or changing the scope, it's just reviewing if something looked suspicious on the revision. It is a detective control but the damage is done.

upvoted 3 times

appleness123 Highly Voted 3 years, 5 months ago

I saw this as being D. If the checks are cleared, it's not preventing anything. The other officer is checking to see if there's discrepancies

upvoted 14 times

Ha89 Most Recent 12 months ago

Selected Answer: D

Leaning more toward D since it's already happened. Compensating is usually for potential/future. According to CompTIA at least..

upvoted 1 times

Ree1234 1 year, 1 month ago

Selected Answer: D

It cannot be compensating because it is a measurement in place to detect any fraud that might have occurred. If it was a measurement in place to prevent any fraud, then it could have been compensating control.

upvoted 1 times

RobV 1 year, 6 months ago

Selected Answer: D

D. Detective

"Cleared checks" is the key. Compensating would stop it from happening, Once cleared we are detecting that it DID happen.

upvoted 3 times

🗳️ 👤 **greatsparta** 1 year, 7 months ago

Compensating controls are implemented to compensate for the absence or failure of other controls. The quarterly reviews serve as a detective control compensating for the lack of segregation of duties. So, who knows?

upvoted 2 times

🗳️ 👤 **d8viev** 1 year, 7 months ago

Selected Answer: C

this looks more like a compensating control for their segregation of duties issue. The root is they don't have enough people to have proper SoD. Therefore, they've implemented this process to mitigate the control gap.

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 7 months ago

Selected Answer: C

<https://pathlock.com/learn/what-are-compensating-controls-and-why-you-need-them/>

upvoted 1 times

🗳️ 👤 **ElDirec** 1 year, 7 months ago

changing my answer to compensating, after reading the full discussion

upvoted 1 times

🗳️ 👤 **ElDirec** 1 year, 7 months ago

Selected Answer: D

Detective. I use the cbt nuggets testing platform, and they have similar questions, where instead of the different officer, a guard watches a camera

upvoted 1 times

🗳️ 👤 **chaddman** 1 year, 8 months ago

Selected Answer: C

This scenario describes a compensating control. Compensating controls are alternative measures implemented to mitigate risk when primary controls are not feasible. In this case, due to the staff shortage, segregation of duties, which is a primary control, cannot be implemented. Instead, the business has put in place a quarterly review by a different officer as a compensating control to catch any discrepancies or potential fraud that might occur due to the lack of segregation of duties. This compensating control helps the business maintain a level of oversight and assurance over the financial processes despite the limitations in staffing. Therefore, the correct answer is:

upvoted 1 times

🗳️ 👤 **Big_Dre** 1 year, 9 months ago

Selected Answer: C

it is clearly C. the question clearly says due to lack of enough personals.

upvoted 1 times

🗳️ 👤 **Big_Dre** 1 year, 9 months ago

Selected Answer: C

The control described in the scenario is a compensating control. Compensating controls are put in place when an organization is unable to implement the ideal segregation of duties due to limited resources or staffing constraints. In this case, the small business does not have enough staff in the accounting department to segregate duties properly, which means that the comptroller, who writes the checks, also reconciles them against the ledger. To compensate for the lack of segregation of duties, the business conducts quarterly reviews where a different officer in the organization compares all the cleared checks against the ledger. This review helps to detect any potential fraud or errors and acts as a compensating control to mitigate the risks associated with the lack of segregation of duties.

upvoted 2 times

🗳️ 👤 **heinzlumpel** 1 year, 11 months ago

Selected Answer: C

It must be C only because on measurement to implement security is not taken. They are compensating is with a different security operation.

upvoted 2 times

🗳️ 👤 **SimonR2** 1 year, 11 months ago

Changing my answer to D, they are Detecting fraud by checking cleared cheques. I believe that is the more correct answer.

upvoted 1 times

🗳️ 👤 **SimonR2** 1 year, 11 months ago

They can't implement separation of duties so instead are carrying out these additional checks. The answer is compensating controls.

upvoted 2 times

🗳️ 👤 **kyky** 2 years ago

Selected Answer: D

Detective controls are implemented to identify and detect errors, fraud, or other irregularities that have already occurred. In this scenario, the quarterly review conducted by a different officer in the business compares all the cleared checks against the ledger. This process is designed to detect any discrepancies or fraudulent activities that may have taken place.

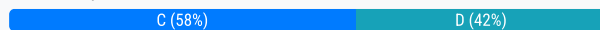
upvoted 3 times

A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network. Customers are not authorized to alter the configuration. The company deployed a software process to manage unauthorized changes to the appliance, log them, and forward them to a central repository for evaluation. Which of the following processes is the company using to ensure the appliance is not altered from its original configured state?

- A. CI/CD
- B. Software assurance
- C. Anti-tamper
- D. Change management

Suggested Answer: D

Community vote distribution



thenewpcgamer Highly Voted 2 years, 2 months ago

Selected Answer: C

Definition: Anti-Tamper is the systems engineering activities intended to deter and/or delay exploitation of critical technologies in a system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

Guys change management is a process to get changes approved by management before implementing changes. It is not a software that is deployed on a system to detect unauthorized changes.

This is also referring to a 3rd party company which likely wouldn't be involved in the company's change management process. It's a third party company that wants to know if someone is tampering/making changes to their device.

upvoted 9 times

PTcruiser Highly Voted 2 years, 8 months ago

Selected Answer: D

Key part "The company deployed a software process to manage unauthorized changes to the appliance, log them, and forward them to a central repository for evaluation"

change management - process through which changes to the configuration of information systems are monitored and controlled. Each individual component should have a separate document or database record that describes its initial state and subsequent changes

Anti-Tamper

- o Methods that make it difficult for an attacker to alter the authorized execution of software

- o Anti-tamper mechanisms include a field programmable gate array (FPGA) and a physically unclonable function (PUF)

upvoted 5 times

thenewpcgamer 2 years, 2 months ago

Change Management itself is not a software process. A software could be used to assist with change management documentation.

upvoted 2 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: C

C. Anti-tamper

upvoted 1 times

kmordalv 1 year, 7 months ago

Selected Answer: C

CompTIA is known for mixing issues to create confusion. Change management does not prevent disruption, therefore, the response sought is anti-tamper.

upvoted 1 times

🗨️ 👤 **Bayoneh** 1 year, 7 months ago

The process described aligns with the principles of change management, and it is a measure to ensure that unauthorized changes to the hardware security appliance are detected and addressed. Therefore, the most appropriate answer is:

D. Change management

In this context, the company is managing changes to the appliance's configuration by deploying a software process to detect and log unauthorized changes, forwarding them to a central repository for evaluation. This process is in line with change management practices, which involve controlling and monitoring changes to maintain the integrity and security of a system.

While "anti-tamper" (Option C) could also be a valid term, in the context of IT and security, processes that prevent or detect unauthorized changes are often considered part of change management practices.

- GPT

upvoted 1 times

🗨️ 👤 **Pavel019846457** 1 year, 7 months ago

Selected Answer: C

Anti-tamper measures are designed to detect and prevent unauthorized changes or tampering with a system or device.

upvoted 1 times

🗨️ 👤 **uday1985** 1 year, 9 months ago

How Anti-tampering will limit internal unauthorized changes.? change management ensure its authorized before its processed.

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: C

The company has implemented a software process to manage unauthorized changes to the appliance, log them, and forward them to a central repository for evaluation. This process is designed to detect and prevent any tampering or unauthorized modifications to the appliance's configuration. Anti-tamper measures are commonly employed to protect the integrity and security of hardware devices, ensuring that they remain in their intended state

upvoted 3 times

🗨️ 👤 **heinzelrumpel** 1 year, 11 months ago

Sorry, you are completely wrong. The procedure clearly describes Change Management. The device can be tampered with easily according to the description in the text. Change Management will detect it and is able to reverse.

upvoted 1 times

🗨️ 👤 **boletri** 2 years, 3 months ago

Selected Answer: D

Key here is "for evaluation".

upvoted 2 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Agree. I mulled this one over in Jason Dions course, and D seems to be the best answer here. "Process" and "Evaluation"

upvoted 1 times

🗨️ 👤 **prntscrn23** 2 years, 7 months ago

Selected Answer: D

It is asking for the process not the actual fix of the issue.

upvoted 2 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: C

Anti-tamper protection comes in many varieties from mechanical means like anti-tamper screws and holographic stickers to electronic detection methods. Tamper-proofing microprocessors often takes the form of encasing electronics or otherwise securing them, while attackers use techniques like physically probing or modifying them, freezing devices, and applying out-of-spec power or signals.

upvoted 2 times

🗨️ 👤 **Adrian831** 2 years, 8 months ago

anti-tamper it's more like a method/mechanism, not a process. The question ask for a process.

upvoted 3 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Great point. I am changing my answer to D

upvoted 4 times

🗨️ 👤 **skibby16** 1 year, 9 months ago

Wrong Anti Tamper is the correct answer

upvoted 1 times

🗨️ 👤 **Treymb6** 2 years, 9 months ago

Selected Answer: D

I originally wanted to pick anti-tamper but it specifically asked for a "process". I'm going with D.

upvoted 3 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: D

its change management - D

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Change management is the only one where you have to request approval / validation of changes before they go through like the question asks.

Anti tamper is incorrect.

Answer is D - Change management.

upvoted 2 times

🗨️ 👤 **bigerblue2002** 2 years, 9 months ago

I get anti tamper, but would that not stop the tampering. This is software that is recording unauthorized alterations, thus the changes are being made. This really looks like D to me. If you are going to use anti-tamper then why let the tampering occur and simply record it?

From a .gov site, Anti-tamper is defined as, Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

I still don't see that as what is happening here. Going D I guess.

upvoted 1 times

🗨️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: C

Anti tamper. Google it, same as question

upvoted 1 times

🗨️ 👤 **adamhoms** 2 years, 9 months ago

The change request management process in systems engineering is the process of requesting, determining attainability, planning, implementing, and evaluating of changes to a system. Its main goals are to support the processing and traceability of changes to an interconnected set of factors.

upvoted 1 times

🗨️ 👤 **cyberseckid** 2 years, 9 months ago

going with D only because it says process , and I think anti tamper is not a process

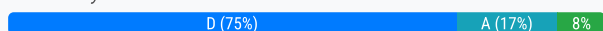
upvoted 2 times

During an incident, it is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which of the following should the security analyst do NEXT?

- A. Consult with the legal department for regulatory impact.
- B. Encrypt the database with available tools.
- C. Email the customers to inform them of the breach.
- D. Follow the incident communications process.

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Pavel019846457** 1 year, 7 months ago

Selected Answer: D

Incident communication process should include legal department as well.

upvoted 1 times

🗳️ 👤 **cyberrae** 2 years, 2 months ago

Selected Answer: A

Now I understand the answering being A - the question is saying this incident is occurring so the security should consult with legal next. If the incident just occurred or been discovered, then the next steps should be to follow the incident communications plan

upvoted 2 times

🗳️ 👤 **gwanedm** 2 years, 6 months ago

Selected Answer: B

I see this as B. remember the incident response procedures. They've determined an incident has taken place (Detection and Analysis). The next phase is containment which is limit the scope and magnitude of the incident

upvoted 1 times

🗳️ 👤 **jchutch2** 2 years, 8 months ago

Selected Answer: D

D positively

Per CompTIA's study guide, including legal representatives should be part of the communications plan.

upvoted 4 times

🗳️ 👤 **2Fish** 2 years, 3 months ago

Agree. Communications process should include legal.

upvoted 1 times

🗳️ 👤 **Adrian831** 2 years, 9 months ago

Selected Answer: D

Definitely D

upvoted 1 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: D

I think D is the best choice, wouldn't the incident communications process include contacting the legal department?

upvoted 2 times

🗳️ 👤 **Treymb6** 2 years, 9 months ago

I feel like the legal department is the safest bet. It is going to be a little different for each state. Consulting legal department is all around safest option.

upvoted 1 times

🗳️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: D

D. Communication with law enforcement and then affected customers

upvoted 1 times

  **adamhoms** 2 years, 9 months ago

lawyers should be consulted if an incident involves sensitive data (personally identifiable information, protected health information, payment card data, etc.) or could otherwise subject the company to liability. Accordingly, an effective incident response plan addresses the nuts and bolts of handling ordinary incidents, but also has well-defined triggers of when Legal should be called and how the legal team will interact with the rest of the response unit. That way, it is much less likely that someone says, "hey, maybe we should call Legal" too late in the process.

upvoted 2 times

As part of the senior leadership team's ongoing risk management activities, the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones. The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data. Which of the following would be appropriate for the security analyst to coordinate?

- A. A black-box penetration testing engagement
- B. A tabletop exercise
- C. Threat modeling
- D. A business impact analysis

Suggested Answer: B

Community vote distribution



amateurguy Highly Voted 2 years, 9 months ago

Selected Answer: D

Go with D.

upvoted 8 times

Dany_Suarez Highly Voted 2 years, 4 months ago

Selected Answer: B

Comptia guide says:

Training and Exercises-Part of the risk management framework is ongoing monitoring to detect new sources of risk or changed risk probabilities or impacts. Security controls will, of course, be tested by actual events, but it is best to be proactive and initiate training and exercises that test system security.

Tabletop Exercises - A tabletop exercise is a facilitator-led training event where staff practice responses to a particular risk scenario.

A BIA is carried out within the activities of a Business Continuity Management System (BCMS).

upvoted 6 times

RobV Most Recent 1 year, 6 months ago

Selected Answer: B

B. A tabletop exercise

Tabletop exercises are designed to simulate and evaluate an organization's response to a specific scenario, such as a security incident or a significant change in business processes. In this case, conducting a tabletop exercise would allow the senior leadership team and relevant personnel to discuss and test the response procedures, identify potential gaps in training or processes, and ensure that the team is adequately prepared to handle security challenges associated with the new business initiative.

While threat modeling (Option C) is valuable for identifying potential threats and vulnerabilities, it may not directly address the training and testing aspects emphasized in the question. Tabletop exercises, on the other hand, specifically involve personnel in a simulated scenario, helping to assess their readiness and the effectiveness of existing procedures.

upvoted 1 times

Gwatto 1 year, 7 months ago

"respond to new business initiative or significant changes to existing ones." This is a tabletop exercise

upvoted 1 times

EIDirec 1 year, 7 months ago

Selected Answer: C

Remember this task was given to a security analyst, so he's most likely going to respond with a security analyst task, he's not a business analyst, so threat modeling, but they are close

upvoted 1 times

mdmdmd 1 year, 7 months ago

Why Threat modeling, I thought it is a process to identify and enumerate threats so that effective mitigations can be prioritized ,developed ,and implemented. Option D seems reasonable
upvoted 2 times

🗨️ 👤 **Chilaqui1es** 1 year, 8 months ago

"Training and testing" I originally thought it was D but the more I think about it I am leaning towards B.
upvoted 1 times

🗨️ 👤 **skibby16** 1 year, 8 months ago

Selected Answer: C

Threat modeling is a process that helps identify and analyze the potential threats and vulnerabilities of a system or process. It can help evaluate the security risks and mitigation strategies of a new business process that would use existing infrastructure to process and store sensitive data. A black-box penetration testing engagement, a tabletop exercise, or a business impact analysis are other methods that can be used to assess the security or resilience of a system or process, but they are not as appropriate as threat modeling for coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones. Reference: https://owasp.org/www-community/Application_Threat_Modeling
upvoted 1 times

🗨️ 👤 **kumax** 1 year, 8 months ago

Selected Answer: D

ChatGPT:

To respond to new business initiatives or significant changes to existing ones, particularly when dealing with sensitive data and infrastructure, the security analyst should coordinate a Security Impact Assessment (SIA) or a Security Assessment that includes the following components.
upvoted 1 times

🗨️ 👤 **ElDirec** 1 year, 7 months ago

ChatGPT says Threat modeling now
upvoted 2 times

🗨️ 👤 **grelaman** 1 year, 9 months ago

Selected Answer: C

Threat modeling evaluates threats and risks to information systems, identifies the likelihood that each threat will succeed and assesses the organization's ability to respond to each identified threat. In this case, when considering a new business process involving sensitive data and existing infrastructure, threat modeling can help identify and address potential security threats and vulnerabilities before they become actual problems.
upvoted 2 times

🗨️ 👤 **grelaman** 1 year, 9 months ago

Don't forget that the CISO is involved in an ongoing risk management activities. Business impact analysis are related to the ability of the company to respond to disruptions (RTO/RPO/WRT/MTD)
upvoted 1 times

🗨️ 👤 **POWNED** 1 year, 11 months ago

Selected Answer: B

"Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones." Key word here is training. Threat modeling has nothing to do with training. Your best answer here is B.
upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: C

C. Threat modeling

Threat modeling is a methodology used to identify and assess potential threats and vulnerabilities in a system or process. It helps in understanding the security risks associated with new business initiatives or significant changes to existing ones. By conducting threat modeling, the security analyst can evaluate the potential impact of processing and storing sensitive data using the existing infrastructure
upvoted 2 times

🗨️ 👤 **karpal** 2 years ago

Selected Answer: B

key word is : "training and testing methodology" . I chose B
upvoted 2 times

🗨️ 👤 **khrid4** 2 years, 3 months ago

Selected Answer: C

I'm changing my answer to C. Threat modeling, after seeing another question within this dump. Keyword is "new business initiatives/process".

"Coordinating the right training and testing methodology" does not mean to act on testing and validation but more on "coordinating/planning" as I comprehend it.

upvoted 2 times

  **JoshuaXIV** 2 years, 2 months ago

Threat modeling is a useful process in identifying potential threats.

upvoted 1 times

  **AI75diablo** 2 years, 3 months ago

I am a MBCI and Disaster Recovery Specialist and the question is asking



"tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones."

When conducting a BIA you look to identify system criticality, MTPD/RTO, Impact of loss, workarounds and dependencies. After the fact it identifies best possible strategies to implement as a Business Continuity Plan ----- in this process there is no testing and training

Table top exercise are done to walk through and new implementations or significant changes to the originations to identify if the controls put in place meet business objectives and are fit for purpose



So answer should actually be B

upvoted 2 times

  **khrid4** 2 years, 3 months ago

I agree with this, After thinking thoroughly, B suits the "testing methodology" than D.

upvoted 1 times

  **R00ted** 2 years, 8 months ago

Selected Answer: D

The business impact analysis (BIA) is a formalized approach to risk prioritization that allows organizations to conduct their reviews in a structured manner. BIAs follow two different analysis methodologies:

upvoted 4 times

  **2Fish** 2 years, 3 months ago

Agree.

upvoted 1 times

  **Cizzla7049** 2 years, 9 months ago

Selected Answer: D

D is the answer

upvoted 4 times

  **Adrian831** 2 years, 9 months ago

Selected Answer: D

For me it's D, table top exercise has other meaning.

upvoted 3 times

Which of the following BEST describes how logging and monitoring work when entering into a public cloud relationship with a service provider?



- A. Logging and monitoring are not needed in a public cloud environment.
- B. Logging and monitoring are done by the data owners.
- C. Logging and monitoring duties are specified in the SLA and contract.
- D. Logging and monitoring are done by the service provider.

Suggested Answer: C

Community vote distribution

C (69%)

D (31%)

  **wico1337** Highly Voted 2 years, 8 months ago

Selected Answer: C

Honestly, seeing so many people say D, that I trusted, make me regret trusting their decisions for earlier answers. This is so blatantly C that I am shocked someone made it to this test without knowing it.



D is stating "as a matter of fact". When in reality, you can easily have cloud platforms in which you are in charge of logging/monitoring. Paas for example. Everything in the end will be defined in the contract or SLA.

upvoted 7 times

  **wico1337** 2 years, 8 months ago

Or even think about Iaas lol

upvoted 2 times

  **2Fish** 2 years, 3 months ago

Agree.. the verbiage can throw us off sometimes. In AWS, you subscribe to CloudTrail, CloudWatch, and GuardDuty. Now, while AWS actually logs the data, the company will monitor the alerts.

upvoted 1 times

  **chaddman** Most Recent 1 year, 8 months ago

Selected Answer: C

When entering into a public cloud relationship with a service provider, the responsibilities surrounding logging and monitoring are typically specified in the Service Level Agreement (SLA) and contract. These documents delineate the roles and responsibilities of both the cloud service provider and the customer regarding various aspects of the service, including security monitoring and logging. It's crucial to have these duties clearly outlined to ensure proper security measures are followed, and both parties are aware of their respective responsibilities. Therefore, the answer is:

C. Logging and monitoring duties are specified in the SLA and contract.

upvoted 1 times

  **grelaman** 1 year, 9 months ago

Selected Answer: D



While customers may have the option to configure and customize logging and monitoring settings to meet their specific needs, the service provider is responsible for the underlying infrastructure and the default monitoring and logging mechanisms.

upvoted 1 times

  **grelaman** 1 year, 9 months ago

The SLA and contract will typically define the specific metrics that will be logged and monitored, as well as the frequency and method with which the data will be collected and reported. The SLA may also specify the service provider's response time to any logging or monitoring alerts. In my opinion, SLA is not the best way to describe how logging and monitoring work in a cloud environment or when we are subscribing services to a Cloud provider.

upvoted 1 times

  **POWNED** 1 year, 11 months ago

Selected Answer: C

Its scary to see people voting on here that have no idea what they are talking about. When it comes to the cloud there is no 1 right answer here. What if the customer has a Iaas, PaaS, SaaS? The only and obvious answer here is C.

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: D

D. Logging and monitoring are done by the service provider.

When using a public cloud service, the responsibility for logging and monitoring typically lies with the service provider. Public cloud service providers have robust logging and monitoring systems in place to ensure the security, performance, and availability of their services.

upvoted 1 times

🗨️ 👤 **ksr933** 2 years, 2 months ago

Comptia material says SLA

Logging and Monitoring

Again, as part of standard secure software development practices, the API should provide sufficient logging and monitoring. Monitoring should provide alerts when an API is being bombarded with requests in a potential DoS attack, or being subject to multiple authentication or other errors, indicating a potential brute force or fuzzing attack.

Another potential issue is if the cloud provider does not supply access to log files or monitoring tools. This is most likely to be the case with a software as a service model. Requirements for logging and monitoring should be identified at the start of a contract and set out in an SLA with the provider.

upvoted 1 times

🗨️ 👤 **Dany_Suarez** 2 years, 4 months ago

Selected Answer: C

Comptia guide says:

Logging and Monitoring

Another potential issue is if the cloud provider does not supply access to log files or monitoring tools. This is most likely to be the case with a software as a service model.

Requirements for logging and monitoring should be identified at the start of a contract and set out in an SLA with the provider.

upvoted 2 times

🗨️ 👤 **gwanedm** 2 years, 6 months ago

Selected Answer: C

I will go with C

upvoted 2 times

🗨️ 👤 **Abyad** 2 years, 7 months ago

Selected Answer: C

6 Cloud Monitoring Best Practices

1. Use the Built-in Activity Monitoring

All leading cloud providers can be set to monitor every cloud activity – human, script or API-based – basically at no cost other than the storage used. These cloud activity logs can be sizable and verbose, so most enterprises keep them in the cloud to reduce bandwidth costs, allowing for larger datasets and longer retention.

2. Activate Logging on Everything You can and Retain it For at Least a Year

In addition to activity logs, the leading cloud providers offer detailed logging for every IaaS/PaaS capability offered – networking, containers, serverless and other services. The best practice is to log everything possible, including network flow logs. This pervasive visibility can be baselined and analyzed for patterns, providing the foundation for behavioral analytics-based threat detection

upvoted 2 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

Selected Answer: C

when entering public cloud relationship, before beginning to use public cloud service, there is a SLA/contract which mentions how the logging and monitoring service works while using the service. You can choose D, but it depends what kinds of cloud service you are getting from public cloud. If you are getting IaaS or PaaS, maybe you are responsible for logging and monitoring, so it mentions on the SLA/contract. On SaaS service provide provides logging and monitoring, but "AGAIN" it mentions on the SLA/contract. So the answer is not D, but C

upvoted 1 times

🗨️ 👤 **SolventCourseisSCAM** 2 years, 7 months ago

I am changing my answer to D

upvoted 1 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

I couldn't find any information in my research to support this but I thought it was odd how in the question the word public was specified for the type of cloud provider. Makes me wonder if companies are allowed to have monitoring privileges in a public environment

upvoted 1 times

🗨️ 👤 **forklord72** 2 years, 8 months ago

Going with C if I get this question, I never learned anywhere about there being a definitive answer on who is responsible in any cloud environment.

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: D

I agree with D

upvoted 1 times

🗨️ 👤 **SAAVYTECH** 2 years, 9 months ago

Selected Answer: D

When transitioning over to a cloud solution, an organization may lose visibility of certain points on the technology stack, particularly if it's subscribing to PaaS or SaaS solutions. Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse.

Chapman, Brent; Maymi, Fernando. CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158). McGraw Hill LLC. Kindle Edition.

upvoted 3 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

I actually don't have a 100% sure answer for this, I would think that the SLA would decide who does the logging and monitoring, could it be that sometimes the organization itself does the logging and monitoring and it doesn't always have to be done by the service provider? The other thing is they are saying that they are about to "go into a relationship", i think that doesn't necessarily mean that the cloud service provider is a cloud SECURITY service provider, they could be providing another cloud service.

If I had to go with an answer it would be C, Im going with SLA and contract.

upvoted 2 times

🗨️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: D

D is the answer

upvoted 2 times

During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity. The analyst also notes there is no other alert in place for this traffic. After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

- A. Share details of the security incident with the organization's human resources management team.
- B. Note the security incident so other analysts are aware the traffic is malicious.
- C. Communicate the security incident to the threat team for further review and analysis.
- D. Report the security incident to a manager for inclusion in the daily report.

Suggested Answer: C

Community vote distribution

C (61%)

B (39%)

  **Tag**  2 years, 8 months ago

Selected Answer: B

B is most in line of sight to what the question is asking.
best chance of detecting this activity

in the first line it says "the team has seen this same traffic"
prior to that it says "an analyst realizes"

this indicates to me that only 1 person on the team has become aware of it and the next thing he should do is make it known to the rest of the team.

it was already deduced that the traffic was related to malicious activity so i dont think the threat team needs to analyze it more plus that still wont allow them to actually detect it faster and more often
upvoted 11 times

  **forklord72** 2 years, 8 months ago

my thought process exactly, not sure how C would spread awareness of the traffic
upvoted 1 times

  **Comptia_Secret_Service** 2 years, 6 months ago

Humans are most often more susceptible to mistakes than systems, the line "The analyst also notes there is no other alert in place for this traffic" suggests that there is currently no detection or alerts in place to trigger and support analysts. Further review of the incident could help create rules and alerts that automatically trigger if the same incident happens again, analyst don't often monitor raw logs and events as there could be tens of millions of logs generated every minute. I am a security analyst myself, this is what we do in SOC. Answer is C.
upvoted 5 times

  **d8viev**  1 year, 7 months ago



Seems like if an analyst has seen this 3 times in a week and it resulted in confirmed malware activity, then it should be actively communicated to the threat team so they take some proactive actions for it (like create an alert???). Noting the incident seems like a passive response to a known threat for this repetitive issue. Especially since there have been 3 other incidents...apparently no one is reading the incident reports...

I also understand these test questions sometimes don't quite line up with reality. So I see how it could also be B.
upvoted 1 times

  **HereToStudy** 2 years, 2 months ago

Selected Answer: C

Duplicate question but answer B is different which is what I was leaning towards. So i guess it's C
#333
upvoted 1 times

  **Alizade** 2 years, 2 months ago

Selected Answer: C

C. Communicate the security incident to the threat team for further review and analysis.

By communicating the security incident to the threat team, the analyst ensures that the traffic patterns and indicators of compromise are properly analyzed and documented. The threat team can then work on developing and implementing appropriate detection and alerting mechanisms to identify similar traffic in the future, thus increasing the chance of detecting such incidents. This approach helps to improve the overall security posture of the organization.

upvoted 2 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

Selected Answer: C

C seems the most textbook way of responding to the incident rather than "taking note"

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

Agree, Threat team would be able to make adjustments to help "detect" this in the future.

upvoted 1 times

🗨️ 👤 **White_T_10** 2 years, 7 months ago

C. Incident has been resolved.

upvoted 1 times

🗨️ 👤 **mrodmv** 2 years, 7 months ago

Selected Answer: C

C, because the incident has been resolved already therefore it has been communicated to the team which means a post mortem (b) has been done already.

upvoted 3 times

🗨️ 👤 **Cizzla7049** 2 years, 7 months ago

Selected Answer: C

And what will seal the deal for C is there is no other alert for this . Threat team can create that rule/alert for the SIEM and have the engineers implement it. The rule alerts everyone automatically. Definitely C if you read the question very well.

upvoted 2 times

🗨️ 👤 **Cizzla7049** 2 years, 7 months ago

Selected Answer: C

C. Threat team can review it and give every other IOC related to it and they can be blocked either by automation or by spreading the word to other analysts. I know telling other analysts is how it works in real life but you can never tell with comptia. The most simple answer is never always right lol

upvoted 3 times

🗨️ 👤 **DaroKa** 2 years, 7 months ago

Selected Answer: B

"increase the chance of detecting this traffic in the future"

upvoted 1 times

🗨️ 👤 **anap2022** 2 years, 7 months ago

Selected Answer: B

I believe it would be B. The quickest way is to notify other analyst of the traffic so they can watch for it. Usually analyst notes are made and shared.

upvoted 1 times

🗨️ 👤 **TheStudiosPeepz** 2 years, 8 months ago

Selected Answer: C

B doesn't help.

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: C

I am voting for C.

upvoted 1 times

🗨️ 👤 **Abyad** 2 years, 7 months ago

C says for further review and analysis and the question says after resolving so we don't need further analysis!!!!

upvoted 1 times

🗨️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: C

C is the smartest choice.

upvoted 4 times

An organization's internal department frequently uses a cloud provider to store large amounts of sensitive data. A threat actor has deployed a virtual machine to attack another virtual machine to gain access to the data. Through the use of the cloud host's hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability the attacker has used to exploit the system?

- A. Sandbox the virtual machine.
- B. Implement an MFA solution.
- C. Update to the secure hypervisor version.
- D. Implement dedicated hardware for each customer.

Suggested Answer: B

Community vote distribution

C (61%)

B (24%)

Other

🗳️ 👤 **novolyus** 1 year, 7 months ago

Selected Answer: C

Cloud provider providing storage (IaaS). You cannot update the hypervisor but can configure MFA to access your infrastructure.
upvoted 2 times

🗳️ 👤 **Gwatto** 1 year, 7 months ago

I'm confused at why so many people are choosing C, no where in the question stated the hyperV was outdated .
upvoted 1 times

🗳️ 👤 **Pavel019846457** 1 year, 7 months ago

Selected Answer: C

Hypervisor is vulnerable if "A threat actor has deployed a virtual machine to attack another virtual machine". VM escape.
upvoted 2 times

🗳️ 👤 **heinzrumpel** 1 year, 11 months ago

Selected Answer: C

C because it is asking to remediate the ongoing situation, not future plans to do it better or to lower the risk from the beginning. Whoever is suggesting for MFA please reconsider your profession ;-)
upvoted 2 times

🗳️ 👤 **novolyus** 1 year, 7 months ago

Reconsider taking an English course so you could understand the question.
upvoted 1 times

🗳️ 👤 **uday1985** 1 year, 9 months ago

And what do you do for living? hard-core Security Analyst? how new vulnerabilities can be addressed? isn't MFA used to authorize access to these servers? and connection won't be allowed until it's authenticated. I will re-consider my career since the majority that start studying CS! have no background and knowledge to justify their answers!
upvoted 4 times

🗳️ 👤 **POWNED** 1 year, 11 months ago

Selected Answer: C

Thank god one person mentioned VM escape. The only way you are going to be able to hack into additional VM's is through VM escape which involves manipulating the hypervisor. The answer is C
upvoted 4 times

🗳️ 👤 **sus1801** 2 years, 2 months ago

The question says "A threat actor has deployed a virtual machine to attack another virtual machine to gain access to the data"
So option A and C is out of the way, as the vulnerability is in the cloud provider not the hypervisor, Option D could be a choice but that seems like a costly option, that leaves only option B to be correct
upvoted 1 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

The threat actor has exploited a vulnerability in the hypervisor to escalate access rights. To remediate this vulnerability, the organization should update to a secure version of the hypervisor. By doing so, the organization can ensure that the hypervisor is not vulnerable to known attacks and that access rights cannot be escalated in the same way as before. Sandboxing the virtual machine, implementing an MFA solution, or implementing dedicated hardware for each customer are not effective solutions to this particular vulnerability.

upvoted 4 times

🗨️ 👤 **Henry88** 2 years, 3 months ago

Selected Answer: B

Are we all reading the same question? There was absolutely nothing in this question that said anything about an outdated hypervisor version so how would anyone know that we need to update the hypervisor version? MFA is the best option.

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

This is a difficult question as we are not sure if this was an insider attack, or is the attacker using an escape attack etc. Does the attacker have priv esc to the actual hypervisor and or the running VM's on that hypervisor. If this was an escape attack then the mitigations are:

Mitigation:

- * Proper guest OS isolation from Host OS
- * Updated patching for Hypervisor
- * Regular software patching of virtual machine operating system
- * Running bare minimum resource-sharing features
- * Installing minimum software application, as they also could have vulnerabilities

upvoted 2 times

🗨️ 👤 **Eric1234** 2 years, 4 months ago

Selected Answer: B

Implement a MFA solution, answer is B. Only Cloud Provider has access to the host hypervisor. That is why the Adversary deployed a new VM to attack the existing VM. MFA would prevent anyone from compromising their Cloud Admin Account

upvoted 2 times

🗨️ 👤 **NickDrops** 2 years, 4 months ago

Selected Answer: B

I say the answer is B. The treat actor had to access the Cloud SP in the 1st place. Good luck getting around MFA when logging into the hypervisor.

upvoted 1 times

🗨️ 👤 **catastrophie** 2 years, 4 months ago

Selected Answer: B

B would most likely be the best answer for remediation in this scenario. Since nothing was specifically called out for an older software version on the hypervisor, I'll assume that it's up to date. The steps for remediation should be isolation, patches for the software version if any are available, after this you would do whatever remediation steps you could such as configuration changes, stricter access controls like MFA, then continue to monitor the system. So given the fact we don't know an accurate status of the current software version, MFA implementation would be the only guaranteed mitigation step to remediate a hypervisor vulnerability. Sandboxing VMs and dedicated hardware does not protect the system when the attacker has the capability to perform host escapes.

upvoted 2 times

🗨️ 👤 **TKW36** 2 years, 5 months ago

Selected Answer: C

C. Question specifically asks "Which of the following actions would be BEST to remediate the vulnerability the attacker has used to exploit the system?" which means remediate the hypervisor vulnerability. Sandboxing a virtual machine would mean isolating it from the other systems to prevent malicious code from spreading, but it won't address the vulnerability in the hypervisor. Implementing an MFA solution would provide an additional layer of security, but it wouldn't remediate the vulnerability. Dedicated hardware for each customer would isolate customers' data, but it wouldn't address the hypervisor vulnerabilities. Also it would be the cloud provider who updates the hypervisor, not the client, so this question is being asked by the perspective of the cloud provider.

upvoted 3 times

🗨️ 👤 **2Fish** 2 years, 3 months ago

I was not sure about this one, but agree with you and most everyone else on C. This is the Best answer from the ones. given.

upvoted 1 times

🗨️ 👤 **iking** 2 years, 6 months ago

Selected Answer: D

Those who answer C, i would say don't have any experience in the cloud at all. We are talking about cloud infrastructure where even using IAAS will not even allow touching the hypervisor, only the cloud provider can do the firmware update for you, and you cant even request it because different

companies are sharing the same host with your server, assuming this is a public cloud.

upvoted 2 times

🗨️ 👤 **iking** 2 years, 6 months ago

I would go for B but that doesn't help at all in the current scenario ("Through the use of the cloud host's hypervisor") where the actor has already infiltrated the hypervisor in the cloud, so he has the access to all VM in that specific host and can manipulate all VMs even in the other company who are sharing with that host (in that public cloud host, I will assume).

upvoted 1 times

🗨️ 👤 **iking** 2 years, 6 months ago

The best way to remediate this is to use a private cloud or dedicated server where you are the only company using that server and not shared with any other companies. This is costly for sure, but the most secure way of deploying servers in the cloud and will definitely remediate the problem. A lot of companies are using this, especially big companies, and has regulated and strict policies, just to be at peace about their data in the cloud.

D is the best answer to this question.

upvoted 2 times

🗨️ 👤 **catastrophie** 2 years, 4 months ago

No, not even remotely....

upvoted 1 times

🗨️ 👤 **DavidC5** 2 years, 8 months ago

Selected Answer: B

I feel like this question is highlighting horizontal privilege escalation so going with B.

upvoted 2 times

🗨️ 👤 **Tag** 2 years, 8 months ago

Selected Answer: C

MFA would be incorrect in this case

Yes MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability.

the vulnerability in this case would be the ability to escalate rights.

thus to remediate this, its safe to say that the application needs to be patched somehow

so C would be correct

upvoted 1 times

🗨️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: A

Where did it say the hypervisor version wasn't secure or that it is outdated?

upvoted 2 times

🗨️ 👤 **Adrian831** 2 years, 8 months ago

Well, first of all how hypervisor could be compromised if it doesn't have any vulnerability?

and second the question itself said "BEST to remediate the VULNERABILITY the attacker has used to exploit the system?"

So, I guess C makes a lot of sense here.

upvoted 2 times

🗨️ 👤 **AaronS1990** 2 years, 4 months ago

I'm thinking that the vulnerability could be the fact they aren't using MFA...

upvoted 1 times

🗨️ 👤 **sh4dali** 2 years, 9 months ago

Selected Answer: C

C is correct.

Virtual machine (VM) escape attacks target vulnerabilities in the hypervisor supporting a virtualized environment. The strongest control to protect hypervisors against these attacks is to keep them patched.

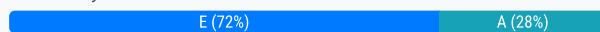
upvoted 3 times

At which of the following phases of the SDLC should security FIRST be involved?

- A. Design
- B. Maintenance
- C. Implementation
- D. Analysis
- E. Planning
- F. Testing

Suggested Answer: A

Community vote distribution



☐ **d8viev** 1 year, 7 months ago

Selected Answer: E

Shift-left

upvoted 1 times

☐ **catastrophie** 2 years, 4 months ago

E is always the answer when these types of questions are asked. If you see "At which phase of the *insert type of development or life cycle* should security included, first started, defined, implemented, etc?" The answer is always in the planning and requirements phase. You'll see lots of this within project management questions.

upvoted 4 times

☐ **2Fish** 2 years, 3 months ago

Agree 100%. Security should be discussed from the beginning. It is everyones responsibility.

upvoted 2 times

☐ **jleonard_ddc** 2 years, 5 months ago

Selected Answer: E

Obviously security should ideally be involved at all stages. The SDLC is as follows:

Planning

Requirements

Design

Implementation

Testing

Deployment

Maintenance

upvoted 2 times

☐ **chiquito** 2 years, 6 months ago

Selected Answer: D

Analysis may be the right answer as per CompTIA Cybersecurity Analyst (CySA+) Study Guide: Exam CS0-002, Second Edition

Requirement. Once an effort has been deemed feasible, it will typically go through an analysis and requirements definition phase. In this phase customer input is sought to determine what the desired functionality is, what the current system or application currently does and doesn't do, and what improvements are desired. Requirements may be ranked to determine which are most critical to the success of the project.

Tip

Security requirements definition is an important part of the analysis and requirements definition phase. It ensures that the application is designed to be secure and that secure coding practices are used.

upvoted 1 times

☐ **albano23412415** 2 years, 6 months ago

Selected Answer: A

ng, a secure SDLC involves integrating security testing and other activities into an existing development process. Examples include writing security requirements alongside functional requirements and performing an architecture risk analysis during the design phase of the SDLC.

upvoted 1 times

🗳️ 👤 **MrRobotJ** 2 years, 7 months ago

Selected Answer: E

Which phase of SDLC security is first?

Requirement Planning

First, you need to plan. While planning may be the most contentious phase of the secure software development life cycle, it's also often the most important. During this phase, you'll determine what your project's security requirements are.

upvoted 2 times

🗳️ 👤 **R00ted** 2 years, 8 months ago

Selected Answer: E

Security requirements definition is an important part of the analysis and requirements definition phase. It ensures that the application is designed to be secure and that secure coding practices are used.

upvoted 2 times

🗳️ 👤 **choboanon** 2 years, 8 months ago

Selected Answer: E

Planning is the first phase and security should be involved from the start.

upvoted 1 times

🗳️ 👤 **Whoah** 2 years, 7 months ago

Planning is the second phase behind design, according to my reading

upvoted 1 times

🗳️ 👤 **RoVasq3** 2 years, 8 months ago

Selected Answer: E

Embedding Security into All Phases of the SDLC

Ideally, you should secure each phase of the SDLC in the most appropriate manner for stakeholders present at that stage, while also ensuring that each security measure facilitates security practices across the whole project. Link <https://www.aquasec.com/cloud-native-academy/supply-chain-security/secure-software-development-lifecycle-ssdlc/>

upvoted 1 times

🗳️ 👤 **[Removed]** 2 years, 8 months ago

Selected Answer: E

I'm going with Planning on this one.

Security should be incorporated at every stage. The planning and requirements phase will be where the security requirements are planned out before being incorporated into the design.

upvoted 4 times

🗳️ 👤 **amateurguy** 2 years, 9 months ago

Selected Answer: A

Look at the phases:

Phase 1: Requirements.

Phase 2: Design. ...

Phase 3: Development. ...

Phase 4: Verification. ...

Phase 5: Maintenance and Evolution.

I believe the security person should be involved throughout the whole cycle and since phase 1 (requirements) is not a listed option, we have to with the next option which is Design.

So the answer i believe is A. Design.

Let me know.

upvoted 3 times

🗳️ 👤 **Tag** 2 years, 8 months ago

requirement and planning is synonymous in this case

E is the answer, you had the right thought lol

upvoted 2 times

🗳️ 👤 **marc4354345** 2 years, 9 months ago

security must be addressed already at analysis stage.

upvoted 1 times

  **marc4354345** 2 years, 6 months ago

E makes most sense. Planning.

upvoted 2 times

  **Adrian831** 2 years, 9 months ago

Selected Answer: A


A sounds good.

upvoted 1 times

  **Adrian831** 2 years, 8 months ago

Changing my answer to E. Planning

upvoted 1 times

  **adamhoms** 2 years, 9 months ago

Generally speaking, a secure SDLC involves integrating security testing and other activities into an existing development process. Examples include writing security requirements alongside functional requirements and performing an architecture risk analysis during the design phase of the SDLC.

upvoted 2 times

During routine monitoring, a security analyst identified the following enterprise network traffic:

Packet capture output:

No.	Source	Destination	Protocol	Info
105	66.187.224.210	192.168.12.21	DNS	Standard query response A 209.132.177.50
106	192.168.12.21	209.132.177.50	TCP	48890 > http [SYN] Seq=0 len=0 MSS=1460 TSV=1535
107	209.132.177.50	192.168.12.21	TCP	http > 48890 [SYN, ACK] Seq=0 Ack=1 Win=5792 len=0
108	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=1 Ack=1 len=0
109	192.168.12.21	209.132.177.50	HTTP	GET / HTTP/1.1

Which of the following BEST describes what the security analyst observed?

- A. 66.187.224.210 set up a DNS hijack with 192.168.12.21.
- B. 192.168.12.21 made a TCP connection to 66.187.224.210.
- C. 192.168.12.21 made a TCP connection to 209.132.177.50.
- D. 209.132.177.50 set up a TCP reset attack to 192.168.12.21.

Suggested Answer: C

Community vote distribution

C (100%)

☐ **CatoFong** 2 years, 4 months ago

Selected Answer: C

syn - syn/ack - ack

upvoted 4 times

☐ **2Fish** 2 years, 3 months ago

Agree.. finally another question with out all the crappy verbiage.

upvoted 4 times

☐ **NickDrops** 2 years, 4 months ago

Selected Answer: C

The 192 address asked the 66 address for DNS info, which it then used to connect to the 209 address and open a website/http.

upvoted 2 times

☐ **TheStudiosPeepz** 2 years, 8 months ago

Selected Answer: C

SYN means connection was made. Thus it's C

upvoted 1 times

☐ **NerdAlert** 2 years, 2 months ago

nah, SYN just means a connection was requested. Like dialing a phone number, but that doesn't mean anyone answers or that the number even rings/works

upvoted 1 times

☐ **AkhilAthkuri** 2 years, 8 months ago

3 way Handshake happened

upvoted 3 times

☐ **Adrian831** 2 years, 9 months ago

Selected Answer: C

Agree with C

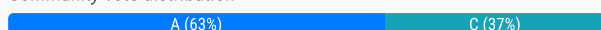
upvoted 1 times

Due to a rise in cyber attackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally. Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

- A. Implement privileged access management.
- B. Implement a risk management process.
- C. Implement multifactor authentication.
- D. Add more security resources to the environment.

Suggested Answer: A

Community vote distribution



jeonard_ddc Highly Voted 2 years, 3 months ago

Selected Answer: A

The company wants to protect data inside and out (literally). The best way to do that is to limit who has privileges to which sets of data. (ie, least privilege – that customers only have access to their own data, etc.)

WRONG ANSWERS

- B – Risk management is done to evaluate vulnerabilities and prioritize their handling to reduce impact. We're more concerned about sensitive data here than vulnerabilities.
- C – MFA can help ensure the right people are accessing data but doesn't guarantee users won't leak data accidentally or that a solution will limit their access accordingly.
- D – Similar to MFA, adding more security resources could protect access to the data but doesn't ensure the data itself is safe. Besides, what exactly constitutes 'security resources'?

upvoted 7 times

2Fish 2 years, 3 months ago

Agree. This is the best Answer from the ones given.

upvoted 2 times

PTcruiser Highly Voted 2 years, 8 months ago

Selected Answer: C

A. Implement privileged access management - assumes the threat actor gains access to low privileged user in the org but what about the customer externally

B. Implement a risk management process

o Identifies, evaluates, and prioritizes threats and vulnerabilities to reduce their negative impact

C. Implement multifactor authentication - is a solution that can work internally in the org and externally for the customers

D. Add more security resources to the environment - doesnt ensure data protection

going with C but this is a dumb question

upvoted 5 times

d8viev Most Recent 1 year, 7 months ago

Selected Answer: C

The answer is not A because privileged users are not the only users that have access to sensitive data. So that implementation only affects a small subset of users. Deploying internal and external MFA, on the otherhand, would be a great enterprise-wide countermeasure for all users.

upvoted 1 times

kumax 1 year, 8 months ago

Selected Answer: A

ChatGPT:

1. Data Encryption
2. Access Controls
3. Multi-Factor Authentication (MFA)

- 4. Data Loss Prevention (DLP) Solutions
 - 5. Endpoint Security
 - 6. Network Security
 - 7. Security Awareness Training
 - 8. Incident Response Plan
 - 9. Vendor Risk Management
 - 10. Regulatory Compliance,
- etc.

upvoted 1 times

🗨️ 👤 **kyky** 2 years ago

Selected Answer: C

Given the scenario described, the countermeasure that would BEST prevent the loss of customers' sensitive data is option C: Implement multifactor authentication.

Multifactor authentication (MFA) adds an extra layer of security by requiring users to provide multiple forms of identification before accessing sensitive data. This typically involves combining something the user knows (such as a password or PIN) with something the user has (such as a physical token or a mobile device) or something the user is (such as biometric data like a fingerprint or facial recognition). By implementing MFA, even if an attacker manages to obtain a user's password or credentials, they would still need access to the additional factor to successfully authenticate and access the data.

upvoted 1 times

🗨️ 👤 **Simpbizkit** 2 years, 2 months ago

Selected Answer: A

I agree that A would protect user's data internally and externally because PAM would manage what privileged users can do with data

upvoted 1 times

🗨️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: C

In this case, implementing MFA for accessing sensitive data can help prevent unauthorized access even if the attacker manages to bypass other security measures. Privileged access management (A) and risk management process (B) are important security measures, but they do not directly prevent data loss.

upvoted 1 times

🗨️ 👤 **Stiobhan** 2 years, 4 months ago

Selected Answer: A

Sometimes referred to as privileged identity management (PIM) or privileged access security (PAS), PAM is grounded in the principle of least privilege, wherein users only receive the minimum levels of access required to perform their job functions. The principle of least privilege is widely considered to be a cybersecurity best practice and is a fundamental step in protecting privileged access to high-value data and assets. By enforcing the principle of least privilege, organizations can reduce the attack surface and mitigate the risk from malicious insiders or external cyber attacks that can lead to costly data breaches. In summary, the less folk that have access to the PHI the less likely it is to be breached/abused etc....

<https://www.cyberark.com/what-is/privileged-access-management/>

upvoted 2 times

🗨️ 👤 **Eric1234** 2 years, 4 months ago

Selected Answer: A

Going with A

upvoted 1 times

🗨️ 👤 **absabs** 2 years, 4 months ago

focus on "protected by the organization internally and externally", so privileged access management

upvoted 1 times

🗨️ 👤 **CatoFong** 2 years, 4 months ago

Selected Answer: A

Agree with Nick. 1. PAM is correct

upvoted 1 times

🗨️ 👤 **NickDrops** 2 years, 4 months ago

Selected Answer: A



I think that it's A for 2 reasons.

1. I've never heard of MFA being used to turn on.

2. If it was an internal actor, MFA wouldn't stop anything because it would be an actual employee.

proper access management would hopefully prevent external threat actors and definitely prevent internal ones.

upvoted 4 times

  **Tag** 2 years, 8 months ago

Selected Answer: C

after careful review of the question

ive decided that C is the most appropriate

upvoted 1 times

  **Adrian831** 2 years, 9 months ago

Selected Answer: C

Thinking more about C

upvoted 1 times

A cybersecurity analyst needs to harden a server that is currently being used as a web server. The server needs to be accessible when entering `www.company.com` into the browser. Additionally, web pages require frequent updates, which are performed by a remote contractor. Given the following output:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
```

Not shown: 995 closed ports

PORT	STATE	SERVICE
22/tcp	open	ssh
23/tcp	open	telnet
53/tcp	open	domain
80/tcp	open	http
443/tcp	open	https

Which of the following should the cybersecurity analyst recommend to harden the server? (Choose two.)

- A. Uninstall the DNS service
- B. Perform a vulnerability scan.
- C. Change the server's IP to a private IP address.
- D. Disable the Telnet service.
- E. Block port 80 with the host-based firewall.
- F. Change the SSH port to a non-standard port.

Suggested Answer: DF

Community vote distribution



alohaBandit Highly Voted 2 years, 8 months ago

Selected Answer: AD

DNS i out & telnet is out!

upvoted 12 times

2Fish 2 years, 3 months ago

Agree. Telnet and DNS is not needed on a Web server.

upvoted 1 times

Simpbizkit 2 years, 2 months ago

Why would DNS not be needed on a web server?

upvoted 2 times

kiduuu 2 years, 2 months ago

<https://docs.cpanel.net/knowledge-base/general-systems-administration/how-to-configure-your-firewall-for-cpanel-services/>

upvoted 2 times

d8viev Most Recent 1 year, 7 months ago

Selected Answer: AD

D. is obvious.

A. DNS service needs to be enabled if the machine is performing the DNS role. The DNS server should be separate from the web server. If the machine needs to resolve DNS it can reach out to the other machine that performs that role.

Moving SSH to a non-standard port is "security by obscurity" which is not security. It will still show up on port scans, and they will find it.

A web server must have 80 and 443 open.

upvoted 1 times

SecurityGuyPP 1 year, 8 months ago

Selected Answer: AD

I will go with AD because:

-DNS server and a web server can run on the same machine, but it is recommended to separate them for security, performance, and scalability reasons.

-Removing telnet is a given.

upvoted 1 times

🗳️ 👤 **sudoptgoaway** 1 year, 9 months ago

DNS (Domain Name System) information is not typically stored on a web server. DNS is a distributed system that translates human-readable domain names (like `www.example.com`) into IP addresses (like `192.168.1.1`) that computers use to identify each other on the internet.

upvoted 1 times

🗳️ 👤 **Rori791** 1 year, 11 months ago

Selected Answer: DF

The best answer is: D & F

Option D is a good choice because it will help prevent unauthorized access to the server by disabling an unencrypted protocol.

Option F is also a good choice because changing the default port for SSH from 22 to a non-standard port will make it harder for attackers to identify and target the SSH service. This will add an extra layer of security to the server.

Option A is wrong since DNS is required for the server to be accessible via a domain name "server needs to be accessible when entering `www.company.com` into the browser".

Option B is not relevant.

Option C is also wrong because changing the server's IP to a private IP address will make it inaccessible via a public domain name.

Option E is not the best option since it will make the web server inaccessible via HTTP, which is required for the server to function as a web server (also option F is better)

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

But with an nmap scan, you can find that port too :D. A&D is the best answer in this case.

upvoted 1 times

🗳️ 👤 **JoInn** 2 years, 1 month ago

Selected Answer: DF

Disabling the Telnet service would harden the server by removing an insecure protocol that transmits data in cleartext and could allow unauthorized access to the server. Changing the SSH port to a non-standard port would harden the server by reducing the exposure to brute-force attacks or port scans that target the default SSH port (22). Uninstalling the DNS service, performing a vulnerability scan, changing the server's IP to a private IP address, or blocking port 80 with the host-based firewall would not harden the server or could affect its functionality as a web server. Reference: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

upvoted 4 times

🗳️ 👤 **MrNYC** 2 years, 1 month ago

The line "The server needs to be accessible when entering `www.company.com` into the browser" means You do need DNS(Port) 53 open. So I am leaning towards Telnet (Port 23) is out and HTTP is out (Port 80).

upvoted 1 times

🗳️ 👤 **Simpbizkit** 2 years, 2 months ago

Selected Answer: DE

I agree that you do not need telnet for a web server. However the question says that you need to be able to type in "`www.company.com`" to gain access. I'm pretty sure uninstalling the DNS service would make that impossible. Changing SSH's port is good but I think getting rid of HTTP would be better since it's the unsecure version of HTTPS and you already have that so it seems redundant.

upvoted 4 times

🗳️ 👤 **kiduuu** 2 years, 2 months ago

Selected Answer: DF

I really can't understand what is in the minds of some... It is a web server!!! If you closed port 53 on a webhost, it could potentially cause issues with the webhost's DNS resolution. Port 53 is used for DNS queries and responses, which are necessary for a web server to resolve domain names into IP addresses. If the webhost cannot resolve domain names, it may not be able to properly serve web pages or applications.

upvoted 3 times

🗳️ 👤 **Eric1234** 2 years, 4 months ago

Selected Answer: AD

Web Server does not need the DNS role installed and with SSH already installed why would you keep Telnet. AD

upvoted 3 times

🗄️ 👤 **absabs** 2 years, 4 months ago

Selected Answer: BD

My view is; he/she must research DNS service, HTTP port and SSH version. Why dont select B? Please discuss me. I going with B D
upvoted 1 times

🗄️ 👤 **NickDrops** 2 years, 4 months ago

Selected Answer: AD

It's A and D. You don't need DNS running on a web server. Other servers will provide the entries for that server to be found.
upvoted 4 times

🗄️ 👤 **MrRobotJ** 2 years, 7 months ago

Selected Answer: AD

Should be A & D
upvoted 1 times

🗄️ 👤 **MrRobotJ** 2 years, 7 months ago

<https://www.quora.com/Does-a-web-server-require-DNS>
upvoted 1 times

🗄️ 👤 **Whoah** 2 years, 7 months ago

Selected Answer: AD

DNS has no place on a web server, it is not inherently secure. Removing telnet is a given.
Port 80 is not unsecure unless you leave it so
upvoted 2 times

🗄️ 👤 **KingDeeko** 2 years, 8 months ago

Selected Answer: DF

Its definitely DF yall are doing it wrong lmao.. do your research.. there's nothing wrong with having port 80 open if its configured properly with security... port 22 should be changed because it is a common practice. it protects again attacks such as brute force and also it will cause a threat to do some digging if they were to try to find it which would through some flags..
upvoted 2 times

🗄️ 👤 **jleonard_ddc** 2 years, 3 months ago

SSH won't be vulnerable if it isn't open to the public. Just because the service is running doesn't mean it can't have access controls in place or firewall protections.
upvoted 1 times

🗄️ 👤 **PTcruiser** 2 years, 8 months ago

Selected Answer: DE

A host based firewall would allow you to block http since you have https which is more secure. I think Blocking DNS wouldn't allow someone to type www.company.com, they would have to type the IP address of the web server. And making the web server private IP would only make it accessible in the internal network
upvoted 3 times

🗄️ 👤 **Cizzla7049** 2 years, 9 months ago

Selected Answer: DE

DE
disable port 23 telnet. Disable port80, it's a finance server so it has to be secure https
upvoted 3 times

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct business overseas must have their mobile devices checked for malicious software or evidence of tampering upon their return. The information security department oversees this process, and no executive has had a device compromised. The Chief Information Security Officer wants to implement an additional safeguard to protect the organization's data.

Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

- A. Implement a mobile device wiping solution for use once the device returns home.
- B. Install a DLP solution to track data flow.
- C. Install an encryption solution on all mobile devices.
- D. Train employees to report a lost or stolen laptop to the security department immediately.

Suggested Answer: C

Community vote distribution

C (100%)

  **ryanzou** Highly Voted 2 years, 8 months ago

Selected Answer: C


C, same as #35

upvoted 6 times

  **2Fish** 2 years, 3 months ago

Agree. Encryption is the best solution to protect data if stolen.

upvoted 1 times



  **Bubu3k** 1 year, 11 months ago

that one has option A as in

"A. Implement a mobile device wiping solution for use if a device is lost or stolen."

which might actually make that answer better, but it's not the case here

upvoted 3 times

  **Mack_F** 1 year, 9 months ago

In question 35, mobile device wiping is the better option. If you look at choice A in this question and #35 they are different. 35 is A and this one is C

upvoted 1 times

  **R00ted** Most Recent 2 years, 8 months ago

Selected Answer: C

This is the best answer.

upvoted 2 times

  **Adrian831** 2 years, 8 months ago

Agree with C

upvoted 1 times

The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?


- A. A Linux-based system and mandatory training on Linux for all BYOD users
- B. A firewalled environment for client devices and a secure VDI for BYOD users
- C. A standardized anti-malware platform and a unified operating system vendor
- D. 802.1X to enforce company policy on BYOD user hardware

Suggested Answer: B

Community vote distribution

D (56%)

B (44%)

 **IanRogerStewart** Highly Voted 2 years, 4 months ago

Selected Answer: D

VDI from the BYOD device onto the company hardware isn't going to help the performance problems. NAC (802.1X) will allow the company to ensure only compliant equipment connects although in the real world it would just be simpler to buy new workstations!!!

upvoted 11 times

 **2Fish** 2 years, 3 months ago

Agree. If the device is non-compliant, it may be denied access to the network or placed in a quarantined or restricted network segment where it can be remediated before being granted full access to the network. This can help to ensure that devices connecting to the network meet the organization's security requirements.

upvoted 1 times

 **novolyus** 1 year, 7 months ago

No, you cannot reach this with only 802.1X.

upvoted 1 times

 **uday1985** 1 year, 9 months ago

How its not going to help? where they using VDI earlier ? VDI confirm that the devices used by employee are up to standards and the traffic is monitored by using the firewall. How d oyou plan to achieve that using 802.1X

upvoted 1 times

 **heinzeltumpel** 1 year, 11 months ago

Don't agree. The company cannot control whats on the BYOD devices nor can the company force user to install a company software on personally owned devices. What if a device is not compliant due to policies? The employee gets to go home an chill?

upvoted 3 times

 **heinzeltumpel** 1 year, 11 months ago

NAC, as mentioned above, in this scenario is only 802.1x. Nothing more, just simple Authentication checking. It is not able to enforce any other policies which might be implied ont the BYOD

upvoted 6 times


 **Sepu** Highly Voted 2 years, 2 months ago

Selected Answer: D

What is the point of BYOD if you are going to use a VDI anyway?

The answer is D. NAC will do the job.

upvoted 5 times

 **kiduuu** 2 years, 2 months ago

That make sense !

upvoted 1 times

 **uday1985** 1 year, 9 months ago

Maybe use VDI to control and secure the work environment that the user access? did you hear about Amazon Workspace before?

upvoted 1 times

🗄️ 👤 **ChopSNap** Most Recent 7 months, 1 week ago

Selected Answer: B

802.1x is only for authentication, both users and devices. VDI will provide a controlled environment with dedicated hardware that meets performance benchmarks for the BYOD devices to connect to. Users could use the same form-factor workstations that are causing the performance issues to run VDI, and get improved performance - if the VDI is hosted on upscaled hardware.

upvoted 1 times

🗄️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

Option D, which mentions 802.1X to enforce company policy on BYOD user hardware, is a valid security measure, and it may be part of an overall security strategy. 802.1X is a network access control (NAC) standard that provides a mechanism for authenticating devices trying to connect to a network. However, it alone may not be sufficient to address all security concerns related to BYOD.

The reason Option B may be a stronger choice is that it incorporates both a firewalled environment for client devices and a secure Virtual Desktop Infrastructure (VDI) for BYOD users. This combination offers a more comprehensive approach to security. The firewalled environment adds a layer of protection for client devices, and VDI allows for centralized control and management of the virtual desktops, reducing the potential risks associated with diverse and potentially less-secure BYOD hardware.

upvoted 1 times

🗄️ 👤 **32d799a** 1 year, 7 months ago

Selected Answer: B

B. A firewalled environment for client devices and a secure VDI for BYOD users

This option suggests implementing a firewalled environment for client devices, which helps protect against unauthorized access and potential security threats. Additionally, using a secure Virtual Desktop Infrastructure (VDI) for BYOD users can provide a controlled and secure environment for accessing company resources, minimizing the risk of compromising sensitive data.

upvoted 1 times

🗄️ 👤 **novolyus** 1 year, 7 months ago

Selected Answer: B

VDI acts like a jump host where only applications and services required are enabled.

802.1X is nothing more than authentication. How do you control an endpoint with ransomware, worms, RATs, outdated software,... You cannot check if a device is compliant only with 802.1X

upvoted 1 times

🗄️ 👤 **d8viev** 1 year, 7 months ago

Selected Answer: B

Here's why this is the best option:

A VDI environment allows the company to control the operating system and applications that the employees use for their work, regardless of the employee's personal device. This setup keeps company data within the company's controlled environment and does not store sensitive data on the employee's personal device.

A firewalled environment helps to protect the network by managing traffic to and from the VDI and the client devices, thus reducing the risk of malware or data exfiltration.

802.1X provides network port-based access control which is useful for authenticating devices that connect to the network. However, it does not address the security of the data on the devices themselves and how the devices are used outside of the network's environment.

upvoted 1 times

🗄️ 👤 **skibby16** 1 year, 8 months ago

Selected Answer: B

A firewalled environment for client devices and a secure VDI (Virtual Desktop Infrastructure) for BYOD users would be the most likely recommendation for securing the proposed solution. A firewalled environment can help isolate and protect the client devices from unauthorized network access or attacks. A secure VDI can provide a virtualized desktop environment for BYOD users that can be centrally managed and controlled by the organization. A VDI can also prevent data leakage or malware infection from BYOD devices, as the data and applications are stored on the server side rather than on the device itself

upvoted 1 times

🗄️ 👤 **heinzelrumpel** 1 year, 11 months ago

Selected Answer: B