



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



CERTIFICATION TEST

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

Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?



- A. Hacktivist
- B. Whistleblower
- C. Organized crime
- D. Unskilled attacker

Correct Answer: C

Community vote distribution


C (69%)

A (31%)

  **lauren2wright** Highly Voted 1 year, 1 month ago
C. Organized crime



Organized crime groups often have the resources, expertise, and networks to carry out sophisticated cyber attacks on behalf of governments or other entities for financial gain or political motives.

upvoted 20 times

  **PatientZero** Highly Voted 5 months, 2 weeks ago
Selected Answer: A



this website has become incredibly overpriced. Was able to buy contributor's access before now it's not even worth it. 3 months for 150?

upvoted 13 times

  **HarshaVardhanK** Most Recent 1 week, 3 days ago
Selected Answer: C



C. Organized Crime

upvoted 1 times

  **JotaJoe** 2 weeks, 3 days ago
Selected Answer: C

The correct answer should be "nation-state actor", but the most accurate between the options is: C - Organized Crime



upvoted 1 times

  **lilyharper** 3 weeks, 3 days ago
Selected Answer: C

C. Organized Crime



Thanks to Certs4Future I successfully cleared my SY0-701 exam today.

upvoted 2 times

  **Smozz** 3 weeks, 5 days ago
Selected Answer: C

Organized crime

upvoted 1 times

  **sheitaNyahou** 3 weeks, 6 days ago
Selected Answer: C

Free Palestine from nazionism

upvoted 1 times

  **Heavensent** 1 month ago
Selected Answer: A

Hacktivist

upvoted 1 times

  **babayaga4311** 1 month, 2 weeks ago
Selected Answer: C

C. Organized Crime

Thanks to Exam4Lead I successfully cleared my SY0-701 exam today.

Organized crime consists of individuals who have gained experience and made careers out of organized crime. In this case, organizations who are recruiting hackers would feel more comfortable recruiting groups who are experienced in this area of technology.

upvoted 8 times

🗲️ 👤 **kedu** 1 month, 3 weeks ago

Selected Answer: C

Heavily Sophisticated

upvoted 1 times

🗲️ 👤 **Moreo** 2 months, 1 week ago

Selected Answer: C

Organized crime groups often have the resources, expertise, and networks to carry out sophisticated cyber attacks on behalf of governments or other entities for financial gain or political motives.

upvoted 1 times

🗲️ 👤 **Elyo** 2 months, 3 weeks ago

Selected Answer: C

Organized crime is a category of transnational, national, or local groups of centralized enterprises run to engage in illegal activity, most commonly for profit.

upvoted 1 times

🗲️ 👤 **Rashjr1** 3 months, 3 weeks ago

Selected Answer: C

because with an organised crime threat actor they are always there for monetary gain

upvoted 1 times

🗲️ 👤 **otose** 4 months ago

Selected Answer: C

organized crime because it purely organized high skilled persdnnel

upvoted 1 times

🗲️ 👤 **Cyberfox9001** 4 months, 2 weeks ago

Selected Answer: C

C. Organized Crime

Organized crime consists of individuals who have gained experience and made careers out of organized crime. In this case, organizations who are recruiting hackers would feel more comfortable recruiting groups who are experienced in this area of technology.

upvoted 1 times

🗲️ 👤 **Hasss** 4 months, 2 weeks ago

Selected Answer: C

Organized crimes usually have a sophisticated team capable enough to pull of threats like these.

upvoted 1 times

🗲️ 👤 **AryzBeats** 4 months, 3 weeks ago

Selected Answer: C

Organized crime are usually treat actors that have high skill, capable of carrying out long and technical attacks

upvoted 1 times

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?



- A. Key stretching
- B. Data masking
- C. Steganography
- D. Salting

Correct Answer: D

Community vote distribution

D (88%)

12%

  **lauren2wright** Highly Voted 1 year, 1 month ago
D. Salting

Salting involves adding random data to the input of a one-way hash function to ensure that the same input will produce different hash values, thus making it more difficult for attackers to use precomputed hash tables (rainbow tables) to reverse engineer the original input.

upvoted 18 times

  **MAKOhunter33333333** Highly Voted 1 year, 1 month ago

Selected Answer: D

Key stretching is used for weak keys, it will hash the pw, then hash that, then hash the hash of the hash and so forth. Makes the cracking process longer for the attacker

Salting is adding random or unique extra character to the password so when cracked it is not the actual PW the attacker thinks

upvoted 5 times

  **sheitaNyahou** Most Recent 3 weeks, 6 days ago

Selected Answer: D

Salting

upvoted 1 times

  **Heavensent** 1 month ago

Selected Answer: A

Key stretching


upvoted 1 times

  **JackExam2025** 4 months, 1 week ago

Selected Answer: D

Salting is primarily used to ensure that even if two users have the same password, their hashes will differ due to the unique random salt added to each password before hashing. This helps prevent attacks like rainbow table attacks, where precomputed hash values are used to reverse the hash back to the original password.

upvoted 3 times

  **23711ec** 4 months, 2 weeks ago

Selected Answer: D

correct answer



upvoted 1 times

  **Hasss** 4 months, 2 weeks ago

Selected Answer: C

The extra complexity added before a one-way data transformation algorithm is salting,

upvoted 1 times

  **AryzBeats** 4 months, 3 weeks ago

Selected Answer: D

Salting is used to add complexity to the input of a one-way hash

upvoted 1 times

🗄️ 👤 **Laraa** 5 months, 2 weeks ago

Selected Answer: D

Salting is a technique used to add extra complexity to data, such as passwords, before applying a one-way transformation algorithm like hashing. The salt is a random value that is combined with the input data (e.g., a password) to produce a unique output even if the input data is the same. This process prevents attacks such as rainbow table attacks and ensures that identical inputs do not result in identical hashes.

upvoted 2 times

🗄️ 👤 **SHAGZZ** 5 months, 2 weeks ago

Selected Answer: D

salting in simpler terms is adding a random character before performing the hash(one way function algorithm)

upvoted 1 times

🗄️ 👤 **way12** 6 months, 1 week ago

Selected Answer: C

salting is used to enhance further security. salt is added to the input data before hashing

upvoted 1 times

🗄️ 👤 **JRCHENRY** 6 months, 1 week ago

Selected Answer: D

Salting is used to add extra complexity before using a one-way data transformation algorithm.

upvoted 1 times

🗄️ 👤 **88d4601** 7 months ago

Selected Answer: C

Salting

upvoted 1 times

🗄️ 👤 **buzzor** 9 months ago

salting is adding of random data to an existing hash to in order to increase the integrity of the hash by then performing a hash function producing hash values. it is used to prevent rainbow table attack (using precomputed hash tables).

upvoted 1 times

🗄️ 👤 **ermahasra** 10 months, 4 weeks ago

Selected Answer: D

D. Salting

In the context of CompTIA Security+, salting is a technique used to enhance the security of stored passwords. It involves adding a random value, known as a "salt," to a password before hashing it. This process helps to prevent various types of attacks, such as rainbow table attacks and certain brute-force attacks.

upvoted 4 times

🗄️ 👤 **[Removed]** 11 months, 1 week ago

Selected Answer: D

D. Salting

Salting is used to add extra complexity before using a one-way data transformation algorithm, such as a hash function. Salting involves adding a unique, random value to the input data before it is processed by the hash function, making it more resistant to certain types of attacks like rainbow table attacks.

upvoted 2 times

🗄️ 👤 **Lanka22** 1 year, 1 month ago

Selected Answer: D

Salting

upvoted 1 times

An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a "page not found" error message. Which of the following types of social engineering attacks occurred?

- A. Brand impersonation
- B. Pretexting
- C. Typosquatting
- D. Phishing

Correct Answer: D

Community vote distribution

D (91%)

6%

🗳️ 👤 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: D

Phishing is the fraudulent practice of sending emails, or other messages to cause an individual to reveal personal information.

This question does not specify if this email was pretexting to butter up the employee, or make email more convincing (pretexting), nor does it specify this email being a trusted brand, or waiting on employee to type incorrectly to steal information.

upvoted 13 times

🗳️ 👤 **sheitaNyahou** Most Recent 3 weeks, 6 days ago

Selected Answer: D

Phising

upvoted 1 times

🗳️ 👤 **Heavensent** 1 month ago

Selected Answer: D

Phishing

upvoted 1 times

🗳️ 👤 **JackExam2025** 4 months, 1 week ago

Selected Answer: D

Phishing is a type of social engineering attack where attackers trick individuals into revealing sensitive information (such as login credentials) by pretending to be a legitimate entity.

upvoted 2 times

🗳️ 👤 **examtaker01** 4 months, 2 weeks ago

Selected Answer: D

The correct answer is:

✓ D. Phishing

Breakdown;

The scenario describes a classic phishing attack, where:

The employee receives an email claiming to be from a payment website.

The email contains a malicious link that leads to a fake login page.

The employee enters their credentials, but instead of proceeding, they get a "page not found" error (likely because the attacker has already captured the credentials).

Why A is not the answer;

A. Brand impersonation

Brand impersonation happens when an attacker pretends to be a legitimate company (e.g., fake social media pages or fake customer service numbers).

While phishing often involves brand impersonation, the key element here is credential theft, making phishing the better answer.

upvoted 4 times

🗳️ 👤 **Cyberfox9001** 4 months, 2 weeks ago

Selected Answer: D

Phishing consists of sending emails that contain fake information or to acquire information from the user who opens an email.

upvoted 2 times

🗳️ 👤 **Hasss** 4 months, 2 weeks ago

Selected Answer: D

They are basically fishing for information that they aren't allowed to be privy to.

upvoted 1 times

🗳️ 👤 **AryzBeats** 4 months, 3 weeks ago

Selected Answer: D

Phishing is a practice used for sending fraudulent emails in hopes of retrieving sensitive data

upvoted 1 times

🗳️ 👤 **deedee2025** 5 months ago

Selected Answer: D

if a Technique was asked then Brand impersonation would have been the best answer....the best answer is phishing because phishing is a type of attack that involves fraudulent practice of sending email

upvoted 1 times

🗳️ 👤 **HungryRightNow** 6 months ago

Selected Answer: A

This isn't what most people said, so tell me why this is wrong: Phishing isn't a wrong answer, but Brand Impersonation -- which can be a type of phishing -- is the BEST answer.

upvoted 1 times

🗳️ 👤 **way12** 6 months, 1 week ago

Selected Answer: D

phishing takes place when you receive email asking for personnel information.

upvoted 1 times

🗳️ 👤 **JRCHENRY** 6 months, 1 week ago

Selected Answer: D

Phishing is a social engineering attack to trick people into releasing their personal information

upvoted 1 times

🗳️ 👤 **88d4601** 7 months ago

Selected Answer: C

Phishing

upvoted 1 times

🗳️ 👤 **Juls74** 7 months, 1 week ago

Selected Answer: D

Phishing is a social engineering attack where attackers send fraudulent emails or messages that appear to come from reputable sources. These emails often contain links to fake websites that steal personal information, such as login credentials. In this case, the employee was tricked into entering their login information on a phony payment website, resulting in a "page not found" error message.

upvoted 1 times

🗳️ 👤 **Gominolo** 11 months, 1 week ago

Selected Answer: A

A. Brand impersonation.

"In the context of email security, brand impersonation is a form of phishing cyber-attack that aims to solicit sensitive information from victims by posing as a legitimate brand."

That reply is more accurate than just Phishing.

upvoted 1 times

🗳️ 👤 **[Removed]** 11 months, 1 week ago

Selected Answer: D

D. Phishing

Phishing involves tricking individuals into providing sensitive information, such as login credentials, by pretending to be a legitimate entity. In this case, the employee was deceived into entering their login information on a fake website that impersonated a payment website.

upvoted 1 times

🗳️ 👤 **Luchis_69** 1 year, 1 month ago

Selected Answer: D

This ACL configuration first permits outbound DNS traffic originating from the device with the IP address 10.50.10.25 and then denies all other outbound DNS traffic.

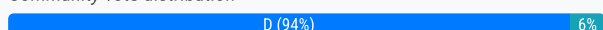
upvoted 2 times

An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

- A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53
- B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
- C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53
- D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Correct Answer: D

Community vote distribution



Baloyitum Highly Voted 1 year, 1 month ago

The correct ACL (Access Control List) to accomplish the goal of limiting outbound DNS traffic originating from the internal network to only one device with the IP address 10.50.10.25 would be option D:

Copy code

```
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
```

```
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
```

This configuration allows outbound DNS requests from the specific IP address 10.50.10.25 and denies outbound DNS requests from any other IP address.

upvoted 22 times

JotaJoe Most Recent 3 weeks, 2 days ago

Selected Answer: D

The correct ACL (Access Control List) to accomplish the goal of limiting outbound DNS traffic originating from the internal network to only one device with the IP address 10.50.10.25 would be option D:

Copy code

```
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
```

```
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
```

This configuration allows outbound DNS requests from the specific IP address 10.50.10.25 and denies outbound DNS requests from any other IP address.

upvoted 1 times

sheitaNyahou 3 weeks, 6 days ago

Selected Answer: D

```
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
```

```
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
```

upvoted 1 times

kedu 3 months, 3 weeks ago

Selected Answer: D

```
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
```

```
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53
```

upvoted 2 times

JackExam2025 4 months, 1 week ago

Selected Answer: D

Outbound DNS traffic needs to be allowed only from 10.50.10.25.

To achieve this, you first need to permit traffic from 10.50.10.25 to port 53 (DNS).

Then, you need to deny all other traffic to port 53.

upvoted 1 times

🗲️ 👤 **Hasss** 4 months, 2 weeks ago

Selected Answer: D

Beacuse its the only answer that has the same IP address on the outbound permit

upvoted 3 times

🗲️ 👤 **JRCHENRY** 6 months, 1 week ago

Selected Answer: D

Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

upvoted 1 times

🗲️ 👤 **MaxiPrince** 6 months, 2 weeks ago

Selected Answer: D

Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

upvoted 1 times

🗲️ 👤 **Rafili** 6 months, 3 weeks ago

Selected Answer: D

The line permit 10.50.10.25/32 0.0.0.0/0 port 53 allows DNS traffic only from the specified device (10.50.10.25) to any destination.

The line deny 0.0.0.0/0 0.0.0.0/0 port 53 blocks all other DNS traffic from any other device in the internal network.

So answer D for 100% sure!

upvoted 2 times

🗲️ 👤 **Juls74** 7 months, 1 week ago

Selected Answer: D

Permit 10.50.10.25/32 0.0.0.0/0 port 53: This rule allows outbound DNS requests from the device with the IP address 10.50.10.25.

Deny 0.0.0.0/0 0.0.0.0/0 port 53: This rule denies all other outbound DNS requests from any other devices on any IP address.

This combination ensures that only the specific device with IP address 10.50.10.25 can send outbound DNS requests, effectively limiting the outbound DNS traffic as desired.

upvoted 3 times

🗲️ 👤 **MZAINUL** 7 months, 1 week ago

Selected Answer: D

This configuration allows outbound DNS requests from the specific IP address 10.50.10.25 and denies outbound DNS requests from any other IP address.

upvoted 1 times

🗲️ 👤 **Luswepo** 9 months ago

Selected Answer: D

The correct firewall ACL configuration that will allow only the device with IP address 10.50.10.25 to send outbound DNS traffic while blocking all other devices is:

D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port**

Explanation:

- The first line allows outbound DNS requests (port 53) only from the device with IP address 10.50.10.25.
- The second line denies all other outbound DNS traffic from any other IP address.

This achieves the goal of limiting DNS traffic to a single device.

upvoted 2 times

🗲️ 👤 **d1f9467** 10 months, 2 weeks ago

Selected Answer: D

C: this option first allows all DNS traffic and then attempts to block traffic to 10.50.10.25, which is not the target.

upvoted 1 times

🗨️ 👤 **Grouthorax** 10 months, 4 weeks ago

Selected Answer: D

C is wrong. The statement would allow outbound DNS traffic from any IP and deny outbound traffic from IP 10.50.10.25 which is the opposite of what it asks for.

Correct answer is D

upvoted 2 times

🗨️ 👤 **tladytea** 11 months, 2 weeks ago

Selected Answer: D

D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Here's the reasoning:

- The first line Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 allows DNS traffic (port 53) from the specific IP address 10.50.10.25 to any destination.
- The second line Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53 denies DNS traffic (port 53) from any source to any destination, effectively blocking all other outbound DNS traffic.

upvoted 3 times

🗨️ 👤 **Olekjs** 11 months, 2 weeks ago

D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

because it only allow the device with the IP address 10.50.10.25 to send outbound DNS request on port 53, and denies all other devices from doing so

upvoted 1 times

🗨️ 👤 **oluabi.salami** 11 months, 3 weeks ago

D is the correct answer. Even co-pilot and chatGPT think so too. C is not correct.

Co-pilot:

Absolutely, setting up Access Control Lists (ACLs) on your firewall is a good way to manage outbound DNS traffic. Here's an example of how you might configure the ACLs to meet your requirements:

Allow DNS requests from 10.50.10.25

access-list 100 permit udp host 10.50.10.25 any eq 53

access-list 100 permit tcp host 10.50.10.25 any eq 53

Deny DNS requests from any other IP address

access-list 100 deny udp any any eq 53

access-list 100 deny tcp any any eq 53

upvoted 1 times

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

- A. SSO
- B. LEAP
- C. MFA
- D. PEAP

Correct Answer: A

Community vote distribution

A (100%)

  **lauren2wright**  1 year, 1 month ago

A. SSO (Single Sign-On)

Single Sign-On (SSO) enables users to authenticate once with their domain credentials and then access multiple applications without needing to re-enter their credentials each time. This aligns with the company's preference to use domain credentials and reduces the burden of managing multiple sets of credentials for different applications.



upvoted 18 times

  **sheitaNyahou**  3 weeks, 6 days ago

Selected Answer: A

SSo is the right answer

upvoted 2 times

  **JackExam2025** 4 months, 1 week ago

Selected Answer: A

SSO allows users to authenticate once with their domain credentials and then access multiple applications without needing to log in again for each one. This helps reduce the number of credentials employees need to manage



upvoted 2 times

  **Hasss** 4 months, 2 weeks ago

Selected Answer: A

sso- allows employees to only have to sign in once with out need to renter their passwords every time.

upvoted 1 times

  **AryzBeats** 4 months, 3 weeks ago

Selected Answer: A

Single sign on - sso



upvoted 1 times

  **JRCHENRY** 6 months, 1 week ago

Selected Answer: A

It's a technology that allows users to access multiple applications and websites with a single set of login credentials.

upvoted 2 times

  **88d4601** 7 months ago

Selected Answer: A

SSO is the right answer

upvoted 1 times

  **FrozenCarrot** 10 months, 1 week ago

Selected Answer: A

Single Sign-On

upvoted 1 times

  **dbrowndiver** 11 months ago

SSO (Single Sign-On) is the method that allows users to access multiple applications with a single set of credentials, typically the same credentials they use to access their domain or network. This is the best choice for reducing the number of credentials employees need to maintain while still providing access to new SaaS applications using their existing domain credentials.

What is SSO?

SSO (Single Sign-On) is an authentication process that allows users to log in once with a single set of credentials to access multiple applications or systems. Once authenticated, users can navigate between various services without needing to log in again, as long as the applications support SSO.

Why it fits the scenario:

By implementing SSO, employees can use their domain credentials to access the SaaS application, eliminating the need for separate credentials for each application. This simplifies the user experience and reduces the administrative burden of managing multiple passwords, which aligns with the company's preference for using domain credentials.

upvoted 3 times

  **CJMax01** 1 year ago

A. SSO (Single Sign-On)

upvoted 1 times

  **Etc_Shadow28000** 1 year ago

Selected Answer: A

SSO is the only option allowing for less login occurrences. The other options reflect security protocols

upvoted 1 times

  **vdrnz** 1 year ago

Selected Answer: A

A. SSO

upvoted 1 times

  **Lance711** 1 year, 1 month ago

Is SSO not more insecure than something like MFA? The more credentials needed, the more secure no?


upvoted 1 times

  **e56400d** 1 year ago

It's not asking which is more secure. It is asking which one will reduce the amount of credentials. SSO will reduce it because its only a single login.

MFA would not reduce credentials because it require multiple login factors.

upvoted 5 times

  **f26ddcd** 1 year, 1 month ago

Selected Answer: A

A. SSO

upvoted 1 times

  **shady23** 1 year, 1 month ago

Selected Answer: A

A. SSO

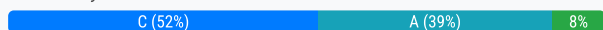
upvoted 1 times

Which of the following scenarios describes a possible business email compromise attack?

- A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
- B. Employees who open an email attachment receive messages demanding payment in order to access files.
- C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
- D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Correct Answer: C

Community vote distribution



lauren2wright Highly Voted 1 year, 1 month ago

C. In a BEC attack, the attacker typically impersonates a high-ranking executive or authority figure within the organization and requests sensitive information or actions from employees. In this case, the HR director is requesting log-in credentials for a cloud administrator account, which is a classic example of BEC where the attacker seeks to gain access to privileged accounts through deception.

upvoted 28 times

TheMichael 11 months, 2 weeks ago

Answer: A.

It could be C if there wasn't a better option, but a BEC is about impersonating, and in the answer choice C it doesn't specify that someone is acting as hr, whereas A is a better choice because they are clear that someone is being impersonated. Your boss requests documents all the time, they don't need to demand it. The choice is clearly A.

upvoted 13 times

Snoozzey 10 months, 3 weeks ago

The best answer is C. The HR Director is not your boss, but someone high in your organization. They are asking for cloud administrator credentials, which has nothing to do with HR, so there is a chance that the directors email account has been compromised and the hacker is now hoping that you will just give in to their request because of the higher rank. In this situation you would follow up with the HR Director in person to determine if they actually made the request and if they really need the credentials for a legitimate reason.

upvoted 6 times

a4e15bd 10 months, 2 weeks ago

The fact that the email has the executive's name in the display field strongly suggest impersonation which is a hallmark of BEC. Both A and C involve impersonation which is central to BEC with scenario A being a classic BEC because it is specifically leveraging the executives identity to request gift card which is a common BEC tactic.

upvoted 2 times

Aces155 6 months, 1 week ago

But the exec's name being in a field doesn't indicate there's a compromise. Receiving a direct email from the HR director indicates that the HR director's email has been compromised.

upvoted 10 times

1chung Most Recent 5 days, 4 hours ago

Selected Answer: C

I go with C

upvoted 1 times

319b362 1 week, 3 days ago

Selected Answer: A

Why A is the correct answer:

This is a classic and well-documented BEC scenario.

The attacker spoofs or impersonates an executive, often using display name tricks.

They send a socially engineered request, like asking for gift cards or wire transfers.

No links or attachments — just urgent, manipulative language.

This matches the FBI's official definition of BEC:

"A scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. It is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques."

upvoted 1 times

  **Burkltlon** 1 week, 4 days ago

Selected Answer: A

A is a classic BEC attack where the attacker impersonates an executive for financial gain (gift cards).

C is spear-phishing that also fits within BEC, focusing on credential theft by impersonating an HR director.

upvoted 2 times

  **analog4ever** 1 week, 4 days ago

Selected Answer: C

C is the best answer here. BEC is all about the attacker using a compromised account to conduct financial fraud or other type of scam. A is only indicating the email has the executive name in the display field and not necessarily from a compromised account.

upvoted 1 times

  **Jforged** 2 weeks, 2 days ago

Selected Answer: A

The best answer is A.

This scenario describes a classic Business Email Compromise (BEC) attack known as CEO fraud. In these attacks, a cybercriminal impersonates a high-ranking executive—often using a spoofed email address or just the display name—to trick an employee into taking urgent action, like buying gift cards or wiring money.

Let's quickly break down the others:

- B is more indicative of a ransomware attack, where files are encrypted and payment is demanded.
- C could be a phishing or credential harvesting attempt, but unless the HR director's identity is spoofed or compromised, it doesn't fully align with BEC.
- D is a phishing attack using a fake login page, which is common but not specific to BEC.

upvoted 1 times

  **JotaJoe** 2 weeks, 3 days ago

Selected Answer: C

A or C coincide with BEC definition (Impersonation of High Officers or HR); A is a typical BEC, C is a sophisticated BEC.

upvoted 1 times

  **nnameo2** 2 weeks, 4 days ago

Selected Answer: A

it is the only answer that has an attacker impersonating a high executiveso A is the answer

upvoted 1 times

  **Sparky80** 1 month, 1 week ago

Selected Answer: C

A BEC involves a fraudulent email that appears to come from a trusted executive or employee and is used to trick someone into transferring money, sensitive data, or credentials.

upvoted 1 times

  **fisher004** 1 month, 2 weeks ago

Selected Answer: C

The correct answer is C.

Business email compromise (BEC) is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential company info. The culprit poses as a trusted figure, then asks for a fake bill to be paid or for sensitive data they can use in another scam. It is a type of phishing attack that targets organizations with a view to steal money or sensitive information.

Only option where a trusted entity is impersonated and a request for sensitive information is made is C.

upvoted 1 times

  **Jon_Million** 1 month, 3 weeks ago

Selected Answer: A

This scenario describes a Business Email Compromise (BEC) attack:

BEC attacks typically involve impersonating a trusted figure in the organization (like a CEO or executive).

The attacker spoofs the display name to make the email look legitimate.

These emails often ask for urgent actions such as wiring money, sending sensitive data, or purchasing gift cards.

They usually don't involve attachments or obvious malware – just social engineering.

upvoted 1 times

  **Ekim149** 1 month, 4 weeks ago

Selected Answer: A

A Business Email Compromise (BEC) is a targeted social engineering attack where the attacker impersonates a company executive or high-level employee (like a CEO or CFO) to trick an employee—often in finance or HR—into:

-Sending money (e.g., wiring funds or buying gift cards)

-Disclosing sensitive information



-Changing payment account details

✓ Why A is correct:

The attacker spoofs the executive's name in the "From" field, attempting to trick the employee into acting quickly without verifying the request.

Gift card scams are a common variant of BEC, especially those pretending to be from executives asking assistants or finance staff to urgently buy cards.

upvoted 1 times

  **8f23125** 2 months, 1 week ago

Selected Answer: A

Option | Scenario | Type of Attack

A | Impersonates an executive asking for gift cards | ✓ BEC attack (common tactic)

B | Ransom message after opening an attachment | ✗ Ransomware, not BEC

C | Credential theft request from HR director | ✗ Phishing or Social Engineering, but not necessarily BEC

D | Link to a fake email login portal | ✗ Phishing, not BEC

upvoted 3 times

  **eroc1990** 2 months, 1 week ago

Selected Answer: C

For those answering A, this attack doesn't necessarily need to come from an internal address. Although it can in some cases, in quite a few cases the attack originates from a freemail user that changed their display name to match the display name of a C level or other executive. Option C is the only one (as of April 18, 2025) that could originate from inside the organization that fits the bill.

upvoted 1 times

  **ZhugeLiang** 3 months, 1 week ago

Selected Answer: A

Email account compromise (EAC) vs BEC

In many cases the objective of a BEC attacker and EAC attacker are the same: They want to steal money, data or other sensitive information.

However, the key difference is that in a BEC attack, the hacker is merely posing as a trusted figure, such as a business executive, lawyer, or important vendor, usually via a spoofed email account. That person then attempts to direct an employee or other person to take a given action, such as wiring funds to the attacker's account.

In EAC attacks, however, the attacker breaches a legitimate email account and acts as the owner of that account. With access to real credentials, the actor is able to conduct fraudulent activity and bypass multi-factor authentication tools.

upvoted 2 times

  **IT_dude_in_training** 3 months, 1 week ago

Selected Answer: C

Business Email Compromise (BEC) typically involves attackers impersonating a trusted authority—like an executive, HR director, or other high-level personnel—to deceive employees into taking actions that compromise security or financial assets. In Option C, the email appears to be from someone in a position of trust (the HR director) making a request that seems unusual (asking for login credentials), which fits the classic BEC pattern.

upvoted 1 times

  **Brian_Douglas** 3 months, 3 weeks ago

Selected Answer: A

I believe it is A, as they muddled the question to state "display field" and not simply From:

It best meets a BEC attach when you change the question to read from the CEO.

upvoted 1 times

A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?

- A. Jump server
- B. RADIUS
- C. HSM
- D. Load balancer

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **MahiMahiMahi** Highly Voted 1 year ago

Selected Answer: A

Maybe it's my ADHD but that is worded in a way that is very difficult to understand,
upvoted 23 times

🗳️ 👤 **Freshly** 8 months, 2 weeks ago

I'm still reading this. 🙄
upvoted 2 times

🗳️ 👤 **d4a5620** 10 months, 3 weeks ago

yeah i had to read this like 4x before answering
upvoted 4 times

🗳️ 👤 **rjbb** Highly Voted 1 year, 1 month ago

Selected Answer: A

It would be a jump server.

A jump server is a secure node that sits between the untrusted network and the secure zone (where the Database servers are).
upvoted 17 times

🗳️ 👤 **Kekeee** Most Recent 3 weeks, 5 days ago

Selected Answer: A

Think of a Jump Server like a mantrap.
upvoted 1 times

🗳️ 👤 **kedu** 1 month, 3 weeks ago

Selected Answer: A

Jump server: Acts as an intermediary, controlling access to a network's internal resources.
upvoted 1 times

🗳️ 👤 **JackExam2025** 4 months, 1 week ago

Selected Answer: A

Jump server is the right choice because it's designed to allow access to otherwise restricted networks or systems, offering an additional layer of security by acting as a controlled entry point.
upvoted 1 times

🗳️ 👤 **Hasss** 4 months, 2 weeks ago

Selected Answer: A

jump server
upvoted 1 times

🗳️ 👤 **JRCHENRY** 6 months, 1 week ago

Selected Answer: A

A jump server is a secure computer system that acts as an intermediary between a less trusted network (like the internet) and a more secure, internal network. It's essentially a "gateway" that allows authorized users to access and manage devices within the secure network.
upvoted 1 times

🗨️ 👤 **Rafili** 6 months, 3 weeks ago

Selected Answer: A

A jump server (or jump box) is a secure computer that acts as a bridge or intermediary between a less secure network (the administrators' workstations) and a more secure network (the database servers). Database administrators can connect to the jump server and then access the database servers, providing an additional layer of security by controlling access and monitoring their actions.

upvoted 1 times

🗨️ 👤 **ProudFather** 6 months, 4 weeks ago

Selected Answer: A

Jump Server: A jump server is a dedicated server that acts as an intermediary between the database administrator's workstation and the database servers. The database administrator can log into the jump server and then use it to access the database servers using secure protocols like SSH.

upvoted 1 times

🗨️ 👤 **dbrowndiver** 11 months ago

Selected Answer: A

A jump server, also known as a jump host or bastion host, is a secure system used to bridge the gap between a secure network segment and a less secure one. It acts as a gateway, allowing authorized users to connect to servers in a restricted network segment securely.

upvoted 4 times

🗨️ 👤 **dbrowndiver** 11 months ago

Jump servers are commonly used in environments where direct access to sensitive network segments is restricted to minimize the attack surface and enhance security.

upvoted 3 times

🗨️ 👤 **Lanka22** 1 year, 1 month ago

Selected Answer: A

It would be a jump server

upvoted 1 times

🗨️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: A

A. Jump server

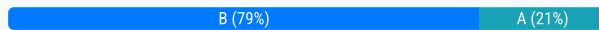
upvoted 2 times

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

- A. NGFW
- B. WAF
- C. TLS
- D. SD-WAN

Correct Answer: B

Community vote distribution



CookieChip Highly Voted 1 year, 1 month ago

B is the correct one

B. WAF (Web Application Firewall)

- A. NGFW (Next-Generation Firewall)
- C. TLS (Transport Layer Security)
- D. SD-WAN (Software-Defined Wide Area Network)

upvoted 20 times

AaronR2000 4 months, 3 weeks ago

A lot of the questions test your knowledge of the acronyms. Spelling it out like this helps!

upvoted 6 times

Mehsotopes Highly Voted 1 year, 1 month ago

Selected Answer: B

A Web Application Firewall (WAF) is for ensuring the security of an HTTP application like WordPress, or Magento against threats like SQL injection, or XSS.

upvoted 18 times

JackExam2025 Most Recent 4 months, 1 week ago

Selected Answer: B

WAF is the best solution for preventing application-specific attacks like buffer overflows

upvoted 3 times

Hasss 4 months, 2 weeks ago

Selected Answer: B

web APP fireeall

upvoted 2 times

AlternateEgo 5 months, 3 weeks ago

Selected Answer: B

I can see why the "correct" answer is WAF, but the question is silly. Why use your WAF to try to block buffer overflow attacks? Why not have the application developers add or fix input validation on the web forms, which is what's really needed. How would you know what bit-length to restrict inputs to for your WAF rule without consulting the developers? And if you are consulting the developers about this, just have them fix it at the source. I'm all for defense in depth, but it doesn't seem realistic to try to block this at the WAF or NGFW.

upvoted 3 times

Fatneck 7 months ago

Selected Answer: B

The answer is B and not A because it says "internet-facing website was compromised." That is specifically what WAF's are designed for. Next-Gen's operate at Layer 7 and provide application-level inspection but are designed for network level protection across services.

upvoted 5 times

viktorrdlyi 7 months ago

Selected Answer: A

NGFW is much more effective than WAF.

upvoted 1 times

  **braveheart22** 8 months, 1 week ago

Selected Answer: A



NGFW is the correct answer.

When it comes to defending against buffer overflow attacks, a Next-Generation Firewall (NGFW) is generally more effective than a Web Application Firewall (WAF). Here's why:

NGFW Capabilities: NGFWs provide deep packet inspection, advanced threat detection, and the ability to identify and block malicious traffic based on patterns and behaviors. They can also enforce security policies at the network level, which helps prevent exploitation attempts before they reach the application.

WAF Limitations: While WAFs are designed to protect web applications by filtering and monitoring HTTP traffic, they primarily focus on application-layer attacks like SQL injection and cross-site scripting (XSS). Buffer overflow attacks, which often target vulnerabilities in software rather than web applications, may not be as effectively mitigated by a WAF.



upvoted 4 times

  **JoeShmo** 8 months, 2 weeks ago

Selected Answer: A

A NGFW would better protect against buffer overflow attacks thanks to deep packet inspection and IDS/IPS. A WAF would protect better against SQL injections and XSS.


upvoted 2 times

  **Markeze** 9 months, 2 weeks ago

Selected Answer: A

cuz its a web application fire, and it's main purpose is to protect web applications from external threats

upvoted 1 times

  **Markeze** 9 months, 2 weeks ago

sorry, was meant to select option b

upvoted 2 times

  **dbrowndiver** 11 months ago

Selected Answer: B

A WAF inspects incoming and outgoing web traffic to detect and block malicious payloads that may exploit application vulnerabilities, such as buffer overflows.

upvoted 4 times

  **shady23** 1 year, 1 month ago

Selected Answer: B

b.WAF Web Application Firewall

upvoted 1 times

An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

- A. Multifactor authentication
- B. Permissions assignment
- C. Access management
- D. Password complexity

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **oluabi.salami** Highly Voted 🍎 1 year, 1 month ago

A. Multifactor; there's a need to add "something you have", apart from "something you (they) know".
upvoted 10 times

🗳️ 👤 **Sh_ade** Most Recent 🕒 2 months, 3 weeks ago

Selected Answer: A

Multifactor Authentication
upvoted 1 times

🗳️ 👤 **Piyabhola** 3 months ago

Selected Answer: A

Doesnt the question ask which of the following which implies more than one?
upvoted 2 times

🗳️ 👤 **IT_dude_in_training** 3 months, 1 week ago

Selected Answer: A

ultifactor Authentication (MFA) adds an extra layer of security beyond just a password. Even if an attacker manages to obtain a user's password, they would still be unable to log in without providing additional verification (such as a code from a mobile device, a biometric factor, or a hardware token). This additional layer makes unauthorized access significantly more difficult to achieve, thus preventing attacks like the one described.
upvoted 2 times

🗳️ 👤 **JackExam2025** 4 months, 1 week ago

Selected Answer: A

MFA is the best way to prevent unauthorized access, even if attackers have compromised passwords. It provides an additional layer of defense against this type of attack.
upvoted 2 times

🗳️ 👤 **Hasss** 4 months, 2 weeks ago

Selected Answer: A

MFA should be required
upvoted 1 times

🗳️ 👤 **Etc_Shadow28000** 9 months ago

Selected Answer: A

To prevent unauthorized logins from suspicious IP addresses and enhance the security of user accounts, the administrator should implement:

A. Multifactor authentication

Multifactor authentication (MFA) requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN. This security measure significantly reduces the likelihood of unauthorized access because even if an attacker has the password, they would still need the additional verification factor(s), such as a code from a mobile device, a fingerprint, or a hardware token.
upvoted 4 times

🗳️ 👤 **dbrowndiver** 9 months ago

Selected Answer: A

In this scenario, the administrator has identified that users' accounts are being accessed from suspicious IP addresses, suggesting that unauthorized parties have obtained the users' passwords. Simply resetting passwords does not address the root of the problem, as attackers could potentially gain access again if they acquire the new passwords.

Blocking Unauthorized Login Attempts: The attacker would be unable to complete the login process from a suspicious IP address without the second authentication factor, preventing the compromise from succeeding.



Also, Immediate User Awareness: Users will become immediately aware of unauthorized attempts on their accounts if they receive unexpected MFA prompts, allowing them to report suspicious activity to administrators quickly.

upvoted 2 times

  **emputu22** 1 year, 1 month ago

A. implement Multi-Factor Authentication (MFA) serves as an additional security measure.

upvoted 3 times

  **Yoez** 1 year, 1 month ago

For me : A

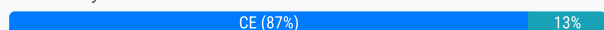
upvoted 2 times

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

- A. Typosquatting
- B. Phishing
- C. Impersonation
- D. Vishing
- E. Smishing
- F. Misinformation

Correct Answer: CE

Community vote distribution



Etc_Shadow28000 Highly Voted 9 months ago

Selected Answer: CE

In this scenario, where an employee receives a text message appearing to be from the payroll department asking for credential verification, the following social engineering techniques are being attempted:

C. Impersonation

- The attacker is pretending to be a trusted entity (the payroll department) to gain the employee's trust and obtain their credentials.

E. Smishing

- Smishing (SMS phishing) involves sending fraudulent text messages to trick individuals into revealing personal information, such as credentials, by clicking on a link or responding to the message.

upvoted 16 times

FennecLola Highly Voted 7 months ago

Selected Answer: CE

Vishing = voice

Phishing = email

Smishing = text

upvoted 10 times

IT_dude_in_training Most Recent 3 months, 1 week ago

Selected Answer: BE

Although impersonation is indeed a tactic used in the attack (the attacker is impersonating the payroll department), the key focus of the attack is the method used (a fraudulent text message aimed at credential theft) rather than simply the act of pretending to be someone else. That is why the answers phishing (B) and smishing (E) are more precise for this scenario.

upvoted 2 times

JackExam2025 4 months, 1 week ago

Selected Answer: CE

Given that the employee only receives a text message (not a phone call), the correct answers would be:

E. Smishing

C. Impersonation

upvoted 2 times

oldbutgold 4 months, 2 weeks ago

Selected Answer: BE

CompTIA's official guide states:

"Smishing: A phishing attack that uses SMS text communications as the vector."

and

"Phishing: "Persuades or tricks the target into interacting with a malicious resource disguised as a trusted one, traditionally using email as the

vector."

It is not impersonation because the Comptia Official guide specifically associates impersonation with direct engagement and persuasion techniques rather than mass communication tactics like smishing or phishing

upvoted 4 times

🗨️ 👤 **Elyo** 2 months, 3 weeks ago

I agree 100%

upvoted 1 times

🗨️ 👤 **Hasss** 4 months, 2 weeks ago

Selected Answer: CE

impersonation and smishing

upvoted 1 times

🗨️ 👤 **Cyborg1407** 8 months, 3 weeks ago

Selected Answer: CE

Impersonation is a technique

Smishing is a technique while Phishing which is also close is a Form. Impersonation and Smishing are under the category of Phishing

upvoted 1 times

🗨️ 👤 **dbrowndiver** 9 months ago

Selected Answer: CE

Answer C: Pretending to Be Payroll: The text message claims to be from the payroll department, a trusted entity within the company. This impersonation aims to create a sense of urgency and legitimacy, convincing the employee to comply with the request for credential verification.

The attacker is leveraging the employee's trust in the payroll department to obtain sensitive information, which is a classic example of impersonation in social engineering.

Answer E: The attack occurs through a text message, making it a clear case of smishing. The attacker uses SMS to deliver the deceptive message, which asks for credential verification under the guise of being from a legitimate source.

Why it is important, since the message is delivered via text and is attempting to harvest credentials, it aligns perfectly with the definition of smishing.

upvoted 1 times

🗨️ 👤 **pedrwc7** 9 months, 1 week ago

Selected Answer: CE

A. Typosquatting (Impersonation of legitimate URL)

B. Phishing (Emails)

C. Impersonation (Acting as someone)

D. Vishing (Voice Phishing)

E. Smishing (Message Phishing or Text Phishing)

F. Misinformation (Providing wrong information or fake information or news)

upvoted 6 times

🗨️ 👤 **Markeze** 9 months, 2 weeks ago

Selected Answer: CE

The attacker is likely using a combination of C. Impersonation and E. Smishing to trick the employee into revealing their credentials.

upvoted 2 times

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

Selected Answer: CE

C.Impersonation and E.Smishing

upvoted 1 times

🗨️ 👤 **emputu22** 1 year ago

the answer is C.Impersonation and E.Smishing

upvoted 1 times

🗨️ 👤 **c80f5c5** 1 year ago

phishing by classic definition is over email. Its a similar idea but going strictly by textbook definition it doesn't apply

upvoted 2 times

🗨️ 👤 **f26ddcd** 1 year, 1 month ago

Selected Answer: CE

Smishing & Impersonate

upvoted 1 times

🗨️ 👤 **The_Body** 1 year, 1 month ago

Phishing = email

Vishing = voice / phone call

Smishing = SMS / Tex messages

upvoted 3 times

🗨️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: BE

B. PhishingE. Smishing

upvoted 3 times

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

Selected Answer: CE

This one is tricky, because Smishing is a part of Phishing. Its one of those annoying questions that Vendors like to throw at exam takers. Smishing is the most specific and direct answer to this question. Answer is CE.

upvoted 3 times

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated: "I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).


- A. Cancel current employee recognition gift cards.
- B. Add a smishing exercise to the annual company training.
- C. Issue a general email warning to the company.
- D. Have the CEO change phone numbers.
- E. Conduct a forensic investigation on the CEO's phone.
- F. Implement mobile device management.

Correct Answer: BC

Community vote distribution

BC (92%)

8%

 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: BC

It is already known that the message is not being sent from the CEO, & awareness of this attack should be known among the company by using the proper training to identify when an attacker is smishing using employee likeness.

It is not known if devices are compromised, but if employees are aware of the situation, then that can be figured out as well.

upvoted 12 times

 **AbdullahMohammad251** Highly Voted 9 months ago

Selected Answer: BC

A fraudulent message was sent without spoofing the sender's number, indicating the message did not come from a legitimate source and the phone wasn't stolen. Therefore, we don't need to change numbers or conduct a forensic investigation on the CEO's phone. We will first inform the employees about the current smishing attack. Then, adjust the annual Company training to include awareness of and protection against similar smishing attacks.

upvoted 6 times

 **IT_dude_in_training** Most Recent 3 months, 1 week ago

Selected Answer: BC

B. Add a smishing exercise to the annual company training Smishing is a type of phishing attack via text messages. Incorporating it into annual company training will help employees recognize such fraudulent attempts and improve overall security awareness.

C. Issue a general email warning to the company This will quickly alert all employees about the specific phishing attempt and provide guidance on how to handle such situations, reducing the risk of future incidents.

upvoted 2 times

 **JackExam2025** 4 months, 1 week ago

Selected Answer: BC

The best responses are to train employees through a smishing exercise and alert the entire company through an email warning to prevent further attacks.

upvoted 1 times

 **habbeysax** 5 months, 3 weeks ago

Selected Answer: BC

A fraudulent message was sent without the sender's number being spoofed, confirming it did not originate from a legitimate source and that the phone has not been stolen. Consequently, there is no need to change numbers or conduct a forensic investigation on the CEO's phone. Our immediate action will be to inform employees about the ongoing smishing attack. Additionally, we will update the annual company training to include awareness and prevention of similar smishing attacks.

upvoted 1 times

 **JRCHENRY** 6 months, 1 week ago

Selected Answer: BC

Proper training to identify smishing and Employee awareness.

upvoted 1 times

🗳️ 👤 **ProudFather** 6 months, 4 weeks ago

Selected Answer: BC

BC seems to be the most reasonable options. As the company with need to be trained and made aware of such attacks so they do not fall victim to this in the future.

upvoted 1 times

🗳️ 👤 **famuza77** 8 months, 2 weeks ago

Selected Answer: BF

How not implementing Mobile Device Management is gonna help on the situation? Technical measures are more importante than annual trainings? stop asking GTP for responses and think

upvoted 3 times

🗳️ 👤 **shootweb** 3 months, 1 week ago

MDM is helpful in many cases, but this is a social engineering scenario where MDM falls short, whereas an email alert does not.

When the specifics are unknown, we must opt for a broad and immediate countermeasure that mitigates risk almost instantly (C) rather than a specific technical control that takes time to implement and does not address the issue—social engineering (F). Thus, the answer is BC.

upvoted 1 times

🗳️ 👤 **TheeLotus** 4 months, 1 week ago

This is correct in my opinion. You should have an immediate response to secure what has been breached. I feel like creating a training takes weeks to create and doesnt address the problem immediately

upvoted 1 times

🗳️ 👤 **dbrowndiver** 9 months ago

Selected Answer: BC

In this scenario, employees have received a fraudulent text message impersonating the CEO, aiming to trick them into purchasing and sending gift cards. The attack is a classic example of smishing, a type of phishing conducted through SMS

Add a smishing exercise to the annual company training-Training employees through realistic exercises will prepare them for recognizing smishing attempts in the future. They will learn how to spot red flags in messages that seem urgent and authoritative but are suspicious in nature.

Issue a general email warning to the company-o Alerting the organization helps contain the threat and reduces the chance of employees inadvertently engaging with the scam. It is an immediate response that mitigates risk by stopping the scam in its tracks.

upvoted 3 times

🗳️ 👤 **Segunmx** 9 months ago

Selected Answer: BC

These are the correct answers. General email warnings to the employees and there's a need for more trainings.

upvoted 1 times

🗳️ 👤 **AbdullahMohammad251** 1 year ago

Selected Answer: BC

A fraudulent message was used, and the sender's number was not spoofed, meaning the message didn't come from a legitimate source. The question didn't mention the phone was stolen either. Therefore, we don't need to change numbers or conduct a forensic investigation on the CEO's phone. First, we will inform the employees about the current smishing attack. Then, we will adjust our annual company training to include protection against smishing attacks.

upvoted 2 times

🗳️ 👤 **hasquaati** 1 year, 1 month ago

Selected Answer: BC

BC, I eliminated the incorrect questions to this one.

upvoted 2 times

🗳️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: BC

B. Add a smishing exercise to the annual company training.

C. Issue a general email warning to the company.

upvoted 2 times

🗳️ 👤 **Yoez** 1 year, 1 month ago

Correct Answer: BC

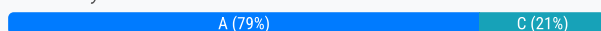
upvoted 2 times

A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

- A. A thorough analysis of the supply chain
- B. A legally enforceable corporate acquisition policy
- C. A right to audit clause in vendor contracts and SOWs
- D. An in-depth penetration test of all suppliers and vendors

Correct Answer: A

Community vote distribution



🗳️ 👤 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: A

An analysis would safely address if there was a lack of reliability, or authenticity when procuring hardware from a supplier to protect the company.
upvoted 13 times

🗳️ 👤 **a4e15bd** 10 months, 2 weeks ago

The correct answer is C:

While understanding the supply chain is important, it doesn't directly address the ability to enforce compliance or verify the authenticity of the hardware being procured.

A right to audit clause in vendor contracts and SOWs is a direct control measure that allows the company to verify that vendors are supplying genuine hardware and by having that right the company can inspect and verify the hardware's authenticity.

upvoted 9 times

🗳️ 👤 **3dk1** 8 months, 2 weeks ago

I agree, I thought it was C at first as well.

C. A right to audit clause in vendor contracts and SOWs

Including a "right to audit" clause in contracts and statements of work (SOWs) allows the company to verify the authenticity of the hardware and ensure that suppliers and vendors are providing certified, legitimate equipment. This directly addresses the risk of procuring counterfeit hardware by enabling periodic checks and accountability for the suppliers.

A thorough analysis of the supply chain (A) is also useful, but the "right to audit" clause provides more actionable oversight and enforcement regarding vendor practices.

upvoted 1 times

🗳️ 👤 **JackExam2025** 4 months, 1 week ago

Typically, audits happen after procurement, whereas supply chain analysis helps prevent counterfeit hardware from being acquired in the first place.

upvoted 8 times

🗳️ 👤 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: A

A penetration test would be checking the security practices of your supply chain to ensure they are not easily tampered with, but does not address the lack of reliability, & authenticity that would protect a company from the possible procurement of faulty supplies/hardware like an analysis would.

An enforced acquisition policy would be a bad practice especially if the parts were faulty.

A right to audit clause, & Statement of Work (SOW) is the first step to allowing an analysis, or penetration test of vendor services, & goods.

upvoted 8 times

🗳️ 👤 **35b2595** Most Recent 2 months, 1 week ago

Selected Answer: A

Audit after the fact

upvoted 1 times

🗳️ 👤 **IT_dude_in_training** 3 months, 1 week ago

Selected Answer: A

A. A thorough analysis of the supply chain. When a company is required to use certified hardware, the integrity of the supply chain is critical. Conducting a thorough analysis of the supply chain ensures that hardware is sourced from trusted and verified suppliers. Why not B. A legally enforceable corporate acquisition policy: While this policy can set expectations, it doesn't actively verify the legitimacy of the hardware before purchase.?

upvoted 2 times

🗳️ 👤 **Samuel07** 3 months, 3 weeks ago

Selected Answer: C

A right to audit clause, ensure that you have control over what is being supplied and not just rely on supplier previous record.

upvoted 2 times

🗳️ 👤 **JackExam2025** 4 months, 1 week ago

Thorough analysis of the supply chain is the best approach to mitigate the risks associated with procuring counterfeit hardware. It focuses on ensuring that hardware is sourced from legitimate, certified vendors and suppliers.

upvoted 1 times

🗳️ 👤 **Leek23** 4 months, 3 weeks ago

Selected Answer: A

A. A thorough analysis of the supply chain

A thorough analysis of the supply chain helps identify and mitigate risks related to counterfeit hardware. By assessing the origin and authenticity of hardware components, verifying suppliers, and ensuring compliance with standards, the company can reduce the chances of receiving counterfeit or substandard hardware.

While the other options might be useful in different contexts, supply chain analysis specifically addresses the issue of procuring counterfeit hardware.

upvoted 1 times

🗳️ 👤 **Midos** 4 months, 3 weeks ago

Selected Answer: C

The best answer to the question is C: A right to audit clause in vendor contracts and SOWs.

Here's why:

Option C: This option ensures that the company has the legal right to inspect the hardware and its supply chain, which can help mitigate the risks associated with procuring counterfeit hardware. It provides a contractual obligation for the vendor to allow audits, ensuring that the company can verify the authenticity of the hardware before deployment.

While options A and B are also valid practices for managing supply chain risks, they do not directly address the specific risk of procuring counterfeit hardware. Option D is an excellent practice for identifying vulnerabilities in a network, but it does not specifically address the issue of counterfeit hardware.

In summary, having the legal right to audit vendors and their supply chains is the most direct and effective way to address the risks associated with procuring counterfeit hardware.

upvoted 1 times

🗳️ 👤 **babujiu** 5 months, 2 weeks ago

Selected Answer: A

The company should implement a supply chain risk management (SCRM) program.

upvoted 1 times

🗳️ 👤 **atta_papa23** 5 months, 3 weeks ago

Selected Answer: A

In the process of conducting due diligence, companies can request for (external) audits which will fall under the right to audit clause. Right to audit clause is not only after the fact

upvoted 1 times

🗳️ 👤 **41c27e6** 6 months ago

Selected Answer: A

I was about to say C, although correct answer is A - bcoz audit is AFTER the transaction. We want to investigate first, before buying anything from the supplier.

upvoted 2 times

🗨️ 👤 **Bito808** 8 months, 1 week ago

I think the key word is "procuring". This involves getting quotes from vendors. Some requirements may only allow components and manufacturing from US based vendors. That's where you need to be mindful of the supply chain. Case example - some brands were found to be beaoning information to foreign countries.

upvoted 1 times

🗨️ 👤 **User92** 9 months ago

Selected Answer: A

While "C" is a valuable measure, it primarily ensures compliance and accountability after the fact. It allows for the detection of issues during audits but doesn't proactively prevent counterfeit hardware from entering the supply chain. "A" is a more proactive approach. It involves evaluating and monitoring the entire supply chain to identify and mitigate risks before counterfeit hardware can be procured. So, it should be "A" - correct answer.

upvoted 3 times

🗨️ 👤 **3330278_111** 10 months, 1 week ago

Selected Answer: C

I did a lot of back and forth with ChatGPT regarding this topic, and even brought up some of the points people were making here. The first response it got was also A. But after discussing what both options (A & C) can offer as a solution to this problem, it eventually changed it's mind to C. To me C makes most sense as it provides an actionable solution that provides direct control

upvoted 3 times

🗨️ 👤 **nap61** 10 months, 1 week ago

Selected Answer: C

You cannot do a thorough analysis of the supply chain without a right to audit. ;-)

Also, a right to audit will be fundamental to separate the supplier that allow (and become a supplier) from those one that would not allow auditing (and not become a supplier).

upvoted 1 times

🗨️ 👤 **tamdod** 10 months, 2 weeks ago

Trick question? Is Assessment the same as analysis as far as Comptia is concerned? Vendor assessment is a thorough background check for potential suppliers that allows an organization to gauge their due diligence, competence, and dependability for the safeguarding of business interests and stringent quality control.

upvoted 2 times

🗨️ 👤 **dbrowndiver** 11 months ago

Selected Answer: C

Vendor Accountability: By including a right to audit clause, the company ensures vendors are accountable for providing certified hardware. This clause can serve as a deterrent against the supply of counterfeit products, as vendors know their processes and products can be reviewed at any time.

Verification of Authenticity: Audits can include checks on the supply chain processes, manufacturing practices, and documentation related to the origin and certification of hardware. This ensures that only legitimate products are used in network construction.

Just saying...

upvoted 3 times

Which of the following provides the details about the terms of a test with a third-party penetration tester?

- A. Rules of engagement
- B. Supply chain analysis
- C. Right to audit clause
- D. Due diligence

Correct Answer: A

Community vote distribution

A (96%)

4%

 **Etc_Shadow28000** Highly Voted 9 months ago

Selected Answer: A

The correct option that provides details about the terms of a test with a third-party penetration tester is:

A. Rules of engagement

Rules of engagement (RoE) outline the scope, objectives, limitations, and boundaries of the penetration test. This document ensures both parties understand what is allowed and expected during the testing process, including which systems can be tested, the methods to be used, the timing of the tests, and how the results will be reported and handled.

- B: This involves assessing the risks associated with the supply chain and third-party vendors, not specifically the terms of a penetration test.

- C: This clause in a contract allows one party to audit the other, typically related to compliance and security practices, but does not detail the terms of a penetration test.

- D: This is the process of investigating and evaluating a business or person before signing a contract, but it doesn't provide the specific terms of a penetration test.
upvoted 18 times

 **JackExam2025** Most Recent 4 months ago

Selected Answer: A

Rules of engagement are the key document that specifies the terms and conditions for a penetration test with a third-party tester
upvoted 1 times

 **shady23** 9 months ago

Selected Answer: A

A. Rules of engagement

Rules of engagement (ROE) outline the terms, conditions, and constraints of a penetration testing engagement between an organization and a third-party penetration tester. They specify what actions the tester is authorized to take, the scope of the testing, the systems and networks that can be assessed, the timing of the testing, and any legal or compliance considerations.
upvoted 4 times

 **dbrowndiver** 9 months ago

Selected Answer: A

In the context of a penetration test with a third-party tester, the Rules of Engagement (RoE) document is crucial. This document outlines the specific terms and conditions under which the penetration test will be conducted, ensuring clarity and mutual understanding between the organization and the tester. The Rules of Engagement is essential for setting clear expectations and boundaries, ensuring that both parties are aligned on the test's objectives and constraints, and protecting the organization's assets and operations during the test.
upvoted 1 times

 **PAWarriors** 10 months, 2 weeks ago

Correct answer is C. Rules of engagement and clear methodology are established beforehand when performing a Penetration test.
upvoted 1 times

🗨️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

Selected Answer: A

"Details about the terms of a test with a third-party penetration tester?"

Need to know DETAILS of what is allowed during a pentest, before ENGAGING
upvoted 2 times

🗨️ 👤 **Abcd123321** 1 year, 1 month ago

Selected Answer: A

Definitions: Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions.

upvoted 3 times

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

Selected Answer: C

Right to audit clause allows you to audit vendors compliance

upvoted 1 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

I think the Correct Answer is A but im not sure100 percent.

upvoted 1 times


A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

- A. Active
- B. Passive
- C. Defensive
- D. Offensive

Correct Answer: A

Community vote distribution

A (100%)

 **shady23** Highly Voted 1 year, 1 month ago

Selected Answer: A

A. Active

Active reconnaissance involves actively probing and scanning the target environment to gather information. This typically includes activities such as port and service scans, vulnerability scans, and other direct interactions with the target systems to identify potential weaknesses or entry points.

Passive reconnaissance, on the other hand, involves gathering information without directly interacting with the target systems, such as monitoring network traffic or analyzing publicly available information.

Options C and D, defensive and offensive reconnaissance, respectively, are not standard reconnaissance types typically used in the context of penetration testing.

upvoted 23 times

 **JackExam2025** Most Recent 4 months ago

Selected Answer: A

Interacting with the target systems, the reconnaissance type is active

upvoted 1 times

 **EngAbood** 6 months ago

Selected Answer: A

Active for sure :)

upvoted 1 times

 **dbrowndiver** 9 months ago

Selected Answer: A

Active reconnaissance involves directly interacting with the target systems to gather information. This type of reconnaissance is often more intrusive because it sends packets or requests to the target to elicit responses, allowing the tester to gather detailed information about the target's configuration and potential weaknesses.

In this Scenario Application:

Direct Interaction: By performing port and service scans, the tester is "actively" sending packets to the target systems to determine which ports are open and what services are running. This direct interaction is characteristic of active reconnaissance.

Used for Detailed Information Gathering: Active reconnaissance allows the Pen tester to gather precise details about the target's network, such as identifying specific services, versions, and potential entry points for further testing.

This is why it pertains and fits:

The nature of port and service scanning, which involves direct communication with the target systems, is aligned with the concept of active reconnaissance. It aims to provide a clear understanding of the target's network infrastructure and potential vulnerabilities.

upvoted 2 times

 **PAWarriors** 10 months, 2 weeks ago

Selected Answer: A

Correct answer is A.

Active Reconnaissance: Engaging with the target system directly, such as scanning for open ports using tools like Nmap.

Passive Reconnaissance: Gathering information without direct engagement, like using open-source intelligence or WHOIS to collect data

upvoted 1 times

🗨️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

Selected Answer: A

NMAP is an active scan.

upvoted 3 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

Correct Answer: A

upvoted 3 times

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

- A. IRP
- B. DRP
- C. RPO
- D. SDLC

Correct Answer: B

Community vote distribution

B (96%)

4%

🗳️ 👤 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: B

RPO would cover amount of data that is expected to be recovered given a failure while DRP encompasses the whole recovery process necessary to restore the system.

upvoted 19 times

🗳️ 👤 **PukaSudu** Highly Voted 1 year, 1 month ago

Selected Answer: B

Disaster Recovery Plan

upvoted 12 times

🗳️ 👤 **Divine2021** Most Recent 1 month, 1 week ago

Selected Answer: B

Answer B

upvoted 1 times

🗳️ 👤 **kedu** 1 month, 3 weeks ago

Selected Answer: B

Disaster Recovery Plan (DRP): The DRP should cover communication procedures, recovery time objectives (RTO), and recovery point objectives (RPO).

upvoted 1 times

🗳️ 👤 **JackExam2025** 4 months ago

Selected Answer: B

Disaster Recovery Plan (DRP) is the required plan to properly manage the restore process in the event of system failure

upvoted 2 times

🗳️ 👤 **Bawaa** 5 months ago

Selected Answer: B

Disaster recovery plan

upvoted 1 times

🗳️ 👤 **_thelastturtle** 5 months, 1 week ago

Selected Answer: A

I thought IRP was a response plan but seems like it's a plan to proactivity prevent any incidents

upvoted 4 times

🗳️ 👤 **Segunmx** 9 months ago

The answer is B. Disaster Recovery Plan (DRP).

upvoted 2 times

🗳️ 👤 **dbrowndiver** 11 months ago

Selected Answer: B

The DRP provides detailed instructions on how to restore systems, applications, and data, enabling the organization to return to normal operations as quickly as possible after a failure.

upvoted 2 times

🗳️ 👤 **SHADTECH123** 1 year, 1 month ago

Selected Answer: B

B. DRP (Disaster Recovery Plan)

Explanation:

A Disaster Recovery Plan (DRP) is essential for managing the restore process in the event of system failure. It provides a detailed strategy for recovering data, systems, and applications, ensuring that business operations can resume as quickly as possible after a disaster. While an IRP handles immediate incident response, and RPO and SDLC are related to specific aspects of data recovery and system development, the DRP is specifically focused on comprehensive recovery and continuity planning.

upvoted 7 times

🗨️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

Selected Answer: B

Disaster RECOVERY Plan goes on how to restore business to be operational again

upvoted 2 times

🗨️ 👤 **f71cbb0** 1 year, 1 month ago

Selected Answer: B

An IRP defines how to detect, contain, analyze, and resolve security incidents, while a DRP outlines how to restore critical systems and data after a major disruption, such as system failure

upvoted 4 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

Correct Answer: B

upvoted 2 times

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A. Jailbreaking
- B. Memory injection
- C. Resource reuse
- D. Side loading

Correct Answer: D

Community vote distribution

D (100%)

🗲️ 👤 **MahiMahiMahi** Highly Voted 👍 1 year ago

Selected Answer: D

D. Side loading is the act of installing software outside of the manufacturers approved repository.
upvoted 14 times

🗲️ 👤 **Mehsotopes** Highly Voted 👍 1 year, 1 month ago

Selected Answer: D

Jailbreaking is privilege escalating a device, & memory injection is executing any form of code into the memory section of a computer typically with malicious intent.
upvoted 7 times

🗲️ 👤 **NXGENSYSSEN** 8 months, 3 weeks ago

Jailbreaking is about bypassing iOS restriction but does not allow you to install!! Think about you need to jailbreak the device, then you can do sideloading
upvoted 3 times

🗲️ 👤 **BevMe** Most Recent ⌚ 8 months, 1 week ago

Selected Answer: D

Sideload is a vulnerability applicable to mobile devices and entails installing apps from unofficial sources, bypassing the device's default appstore.
upvoted 1 times

🗲️ 👤 **dbrowndiver** 11 months ago

Selected Answer: D

o This vulnerability directly pertains to the installation of software from unapproved sources, making side loading a prime example of a security risk associated with bypassing official repositories.
upvoted 3 times

🗲️ 👤 **Alvesbtc** 11 months, 1 week ago

Selected Answer: D

Side loading is the process of installing applications or files onto a device, such as a smartphone, tablet, or computer, without using the device's official app store or authorized distribution channels. This method allows users to bypass the standard app store or marketplace and install software directly, often from an external source like a third-party website or local storage.
upvoted 3 times

A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```


Which of the following attacks is most likely occurring?

- A. Password spraying
- B. Account forgery
- C. Pass-the-hash
- D. Brute-force

Correct Answer: A

Community vote distribution

A (100%)

 **Luchis_69** Highly Voted 1 year, 1 month ago

Selected Answer: A

Password spraying is a type of brute-force attack used to gain unauthorized access to user accounts by systematically attempting a small number of commonly used passwords against many user accounts. Unlike traditional brute-force attacks, which attempt many different passwords against a single user account, password spraying involves trying a few commonly used passwords against a large number of accounts.

upvoted 16 times

 **Oluwatobi4880** Most Recent 4 months, 1 week ago

Selected Answer: A

Spring2023 was sprayed to different accounts

upvoted 1 times

 **habbeysax** 5 months, 3 weeks ago

Selected Answer: A

The repeated use of the password "Spring2023" across multiple accounts (administrator, jsmith, guest, cpolk, fmartin) strongly suggests a password spraying attack. This method involves attempting a single, commonly used or default password across various user accounts.

By distributing the attempts across multiple accounts instead of targeting just one, the attacker reduces the likelihood of triggering account lockouts. This approach allows them to avoid detection and bypass the alerts typically associated with brute-force attacks.

upvoted 2 times

 **[Removed]** 9 months, 3 weeks ago

Selected Answer: A

Agree with A

upvoted 2 times

 **PAWarriors** 10 months, 2 weeks ago

Selected Answer: A

Correct answer is A.

Password Spraying is a brute force attach that tries a few common passwords against many usernames or accounts. This is effective because it avoids account lockouts and targets weak passwords.

upvoted 2 times

 **dbrowndiver** 11 months ago

Selected Answer: A

The use of the same password, Spring2023, across various accounts (administrator, jsmith, guest, cpolk, fmartin) is a classic indication of password spraying. Attackers often use this technique with passwords they expect might be used by several users, particularly common or default passwords.

This Attack will avoid Account Lockouts, by trying the same password on multiple accounts rather than focusing on a single account, the attacker minimizes the risk of locking out any one user, which would alert the system to a brute-force attack.

upvoted 2 times

🗲️ 👤 **PukaSudu** 1 year, 1 month ago

Selected Answer: A

A. Password spraying

upvoted 2 times

🗲️ 👤 **PukaSudu** 1 year, 1 month ago

A. Password spraying

upvoted 1 times

🗲️ 👤 **f71cbb0** 1 year, 1 month ago

Selected Answer: A

Correct Answer: A

upvoted 1 times

🗲️ 👤 **Abcd123321** 1 year, 1 month ago

Selected Answer: A

Password spraying is a cyberattack tactic that involves a hacker using a single password to try and break into multiple target accounts.

upvoted 4 times

🗲️ 👤 **Yoez** 1 year, 1 month ago

Correct Answer: A

upvoted 1 times

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones
- B. Subject role
- C. Adaptive identity
- D. Threat scope reduction

Correct Answer: B

Community vote distribution



SHADTECH123 Highly Voted 1 year, 1 month ago

Selected Answer: A

A. Secured Zones

Explanation:

In the context of implementing Zero Trust principles within the data plane, secured zones are most relevant. Zero Trust principles emphasize the need to eliminate implicit trust and enforce strict access controls. By evaluating and implementing secured zones, an organization can ensure that data is compartmentalized and that access is tightly controlled, aligning with the core tenets of Zero Trust. This approach helps to contain threats and limit lateral movement within the network, providing a strong foundation for a Zero Trust architecture.

upvoted 32 times

maxxem45 1 year ago

According to the The Official CompTIA Security+ Study Guide (Exam SY0-701) 9th Edition, which is the latest edition, the Zero Trust Architecture is implemented in the CONTROL and DATA planes. The CONTROL plane has the Adaptive identity, Threat Scope Reduction, Policy-Driven Access Control and Policy Decision Point functions; while the DATA plane has the Subject, Policy Enforcement Point and Implicit Trusted Zones functions.

In the question, the key word is "...principles within the DATA PLANE,..." and only Answer B: Subject, is in the DATA within the DATA plane.

upvoted 48 times

Konversation 2 months, 3 weeks ago

Correct. Beside the Study Guide, also the NIST Special Publication 800-207 "Zero Trust Architecture" confirms it.

upvoted 3 times

Innana 5 months ago

Secured zones belong to the control plane. It is stated in CompTIA SY0701 exam objectives

upvoted 1 times

a4e15bd 11 months, 2 weeks ago

Threat Scope Reduction is also relevant as it focuses on minimizing the potential attack surface and limiting the impact of any security breach. However, Secured Zones directly implements the concept of segmentation and isolation which is a foundational element of Zero Trust architecture. So the most relevant choice is Secured Zones.

upvoted 2 times

SHADTECH123 1 year, 1 month ago

While Threat Scope Reduction (D) is important, it is a broader concept that includes multiple strategies, not specifically focused on the data plane. Secured Zones (A) directly address data plane segmentation, a key aspect of Zero Trust to prevent unauthorized lateral movement within the network.

upvoted 5 times

AutoroTink Highly Voted 1 year, 1 month ago

Selected Answer: B

From Dion Training:

Control Plane: Adaptive Identity, Threat Scope Reduction, Policy-Driven Access Control, and secured zones.

Data Plane: Subject/system, policy engine, policy administrator, and establishing policy enforcement points.

(I've also been trying to verify this from other locations...it's been a challenge!)

upvoted 24 times

  **TKone** 3 months, 1 week ago

You know how to help people understand things. Thank you very much!

upvoted 3 times

  **1chung** Most Recent 4 days, 23 hours ago

Selected Answer: A

I go with A

upvoted 1 times

  **319b362** 1 week, 3 days ago

Selected Answer: B

In a Zero Trust architecture, the data plane is where actual access to resources happens – such as file reads, API calls, database queries, or any operation involving protected data.

upvoted 1 times

  **Cybermatthew** 1 week, 3 days ago

Selected Answer: A

Security zones are extremely relevant in implementing Zero trust principles.

upvoted 1 times

  **Deuces** 1 week, 5 days ago

Selected Answer: A

It's Secured Zones

upvoted 1 times

  **Jforged** 2 weeks, 2 days ago

Selected Answer: A

A. Secured Zones

In the context of the data plane, which is responsible for the movement of data, secured zones refer to the segmentation and isolation of data resources to enforce detailed access controls. This approach aligns directly with Zero Trust principles, which emphasize least privilege access, microsegmentation, and continuous verification of access requests.


upvoted 1 times

  **oreinn** 2 weeks, 3 days ago

Selected Answer: D

Zero Trust principles focus on minimizing the attack surface and reducing the potential impact of a breach by assuming no inherent trust, even within the network. In the context of the data plane, which handles the actual transmission and processing of data, threat scope reduction is critical. This involves measures like micro-segmentation, least privilege access, and encrypting data in transit to limit the potential damage from unauthorized access or lateral movement within the network.

upvoted 1 times

  **Ekim149** 1 month, 4 weeks ago

Selected Answer: B

The keyword in this question is "evaluating" the implementation of Zero Trust principles within the "Data plne". So the answer is B (Subject role) which is the only element in Data plane.

upvoted 1 times

  **monstamash** 2 months ago



Selected Answer: B

In Zero Trust, everything must be verified – not just the network location but who the user or system (the "subject") is, and what role they have.

When evaluating the data plane (where actual access to resources like data or applications happens), evaluating the subject's role ensures only authorized roles can access specific data or services.

This matches the principle of least privilege, a core part of Z

upvoted 1 times

  **8f23125** 2 months, 1 week ago

Selected Answer: B

Defines what access a user or service (subject) has to data based on their role.

Highly relevant—Zero Trust enforces least-privilege access based on role, identity, and context.

upvoted 1 times

🗳️ 👤 **158e3e5** 2 months, 2 weeks ago

Selected Answer: B

B. Subject Role

upvoted 1 times

🗳️ 👤 **ItAd** 3 months, 1 week ago

Selected Answer: B

Zero Trust principles within the data plane focus on enforcing strict access controls to ensure that only authorized entities (subjects) can access specific data resources. Evaluating subject roles aligns with Zero Trust because:

Least Privilege Access: Zero Trust enforces the principle of least privilege, meaning that access to data is granted based on predefined roles and responsibilities.

Role-Based Access Control (RBAC): Subject roles define what actions a user, service, or device can perform on data within the data plane.

Continuous Verification: Access is granted dynamically based on role, identity, and other contextual factors (e.g., device security posture or network conditions).

upvoted 1 times

🗳️ 👤 **gcracker618** 3 months, 1 week ago

Selected Answer: B

This question stinks. At first I would have answered "A" as Implicit trust zones are part of the Data Plane and it was listed first. HOWEVER, the BEST answer is likely Subject role. Subject role is listed as part of data plane in much more plain, simple terms.

upvoted 1 times

🗳️ 👤 **Ejigi** 4 months ago

Selected Answer: C

The decision to trust is based upon adaptive identity authentication (get certified, get ahead)

upvoted 1 times

🗳️ 👤 **Oluwatobi4880** 4 months, 1 week ago

Selected Answer: B

When evaluating the implementation of Zero Trust principles within the data plane, the most relevant factor for an analyst to evaluate would be:

B. Subject role

It is crucial to assess how roles and identities are managed and enforced to ensure secure access and control within the Zero Trust framework. By focusing on subject roles, the analyst can determine how access controls and permissions are applied to users, ensuring that only the right individuals have access to the necessary data, consistent with the principles of Zero Trust.

upvoted 1 times

🗳️ 👤 **KSoLL** 4 months, 1 week ago

Selected Answer: B

B. Subject role

Keywords in this question is [Data plane] & [Zero Trust]

The control plane layout the policies and procedures

Control plane typically encompasses several key elements:

1. Adaptive identity
2. Threat Scope Reduction
3. Policy-Driven Access Control
4. Secured Zones

The data plane is going to ensure that the policies properly executed

Data planes consists of:

1. Subject/System
2. Policy Enforcement Point

I got this information from Jason Dion videos [Section 2: Fundamentals of Security - 15. Zero Trust (OBJ 1.2)]

upvoted 1 times

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

- A. RDP server
- B. Jump server
- C. Proxy server
- D. Hypervisor

Correct Answer: B

Community vote distribution



🗳️ 👤 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: B

A Proxy Server is used to fetch Internet content requested for access by internal users, & can also be configured to cache content for a specified amount of time so that subsequent requests for content are satisfied locally instead of from the Internet.

A Jump Server protects internal company resources that would have no reason to be accessed by the outside.

upvoted 14 times

🗳️ 👤 **Etc_Shadow28000** Highly Voted 1 year ago

Selected Answer: B

To create an added layer of security by preventing unauthorized access to internal company resources, the best solution would be:

B. Jump server

A jump server (or jump box) acts as a controlled access point that administrators must go through to access internal resources. It creates an additional layer of security by acting as a secure intermediary, allowing only authorized users to access internal servers and systems. This reduces the attack surface by limiting direct access to sensitive resources and can be closely monitored and secured.

upvoted 10 times

🗳️ 👤 **Markie100** Most Recent 4 months, 3 weeks ago

Selected Answer: B

A jump server is the best solution for creating an added layer of security by preventing unauthorized access to internal company resources, as it provides controlled access, isolation, and monitoring capabilities.

upvoted 1 times

🗳️ 👤 **braveheart22** 7 months, 3 weeks ago

Selected Answer: B

The correct answer is B.

Jump Server: Secure access point for administrators to connect to internal systems, used to enforce strong access controls for remote management.

Proxy Server: on the other hand is an Intermediary for controlling traffic, used for web filtering, caching, and traffic anonymization.

upvoted 1 times

🗳️ 👤 **Donny_575** 8 months, 1 week ago

Selected Answer: C

Proxy servers can be either forward or reverse. A reverse proxy server would create an added layer of security by preventing unauthorized access to internal company resources by filtering unapproved IPs. A jump server provides admins with a secure, direct route into internal networks. It does not add an additional layer of security to the internal network

upvoted 1 times

🗳️ 👤 **Syl0** 9 months, 3 weeks ago

RDP - Remote Desktop Protocol Server

Jump server - Creates a barrier between network

Proxy Server - Grant access to Internet

Hypervisor - hosts several VMs at one time

upvoted 6 times

🗨️ 👤 **dbrowndiver** 11 months ago

Selected Answer: B

Isolation and Monitoring: Jump servers provide isolation between different network segments, allowing for detailed monitoring and logging of access attempts. This helps in detecting and responding to unauthorized access attempts swiftly.

Reduced Attack Surface: By limiting the entry points to critical systems, a jump server reduces the attack surface, making it harder for attackers to find vulnerabilities in the system.

upvoted 3 times

🗨️ 👤 **SHADTECH123** 1 year, 1 month ago

Selected Answer: B

ump Server is designed to provide an additional layer of security by acting as a secure intermediary between the user's workstation and internal company resources. It ensures that all access to sensitive internal resources goes through a controlled and monitored access point, enhancing security by preventing unauthorized direct access.

upvoted 1 times

🗨️ 👤 **SHADTECH123** 1 year, 1 month ago

Selected Answer: B

Jump Server is specifically designed to add an extra layer of security by serving as a controlled access point. It ensures that all access to internal resources must pass through this secure intermediary, allowing for enhanced monitoring, logging, and restriction of unauthorized access.

upvoted 1 times

🗨️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: B

B. Jump server

upvoted 1 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

Correct Answer: B

upvoted 1 times

🗨️ 👤 **e5c1bb5** 1 year, 1 month ago

Selected Answer: B

jump servers are specifically hardened and act as a chokepoint and access point to internal resources. The idea being its the only way in and its damn hard to compromise it. correct me if you have other ideas. thank you

upvoted 4 times

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. encryption=off
- B. http://
- C. www.*.com
- D. :443

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **SHADTECH123** Highly Voted 1 year, 1 month ago

Selected Answer: B

Blocking the string "http://" is the best way to prohibit access to non-encrypted websites. Non-encrypted websites use HTTP, while encrypted websites use HTTPS. This ensures only non-encrypted traffic is blocked without affecting encrypted websites.

- A. encryption=off: Not a consistent identifier for non-encrypted websites.
 - C. www.*.com: Too broad, blocks both encrypted and non-encrypted websites.
 - D. :443: Indicates HTTPS traffic, blocking it would deny access to encrypted websites.
- upvoted 10 times

🗳️ 👤 **dbrowndiver** Most Recent 9 months ago

Selected Answer: B

The http:// string in a URL indicates that the website is using the Hypertext Transfer Protocol (HTTP) without encryption. HTTP does not provide encryption, meaning data transmitted between the user and the website can be intercepted and read by third parties.

Scenario Application: Identifying Non-Encrypted Sites: By scanning for the http:// string, the web filter can identify URLs that begin with this protocol, which signifies a lack of encryption. Blocking these URLs effectively prevents users from accessing non-encrypted websites.

Security Enhancement: Prohibiting access to http:// ensures that users are only visiting websites that use HTTPS (https://), which encrypts data and provides a secure communication channel.

Scanning for http:// directly targets non-encrypted web traffic, making it the most appropriate choice for denying access to such sites. This ensures that only encrypted websites, which protect data privacy and integrity, are accessible.

upvoted 3 times

🗳️ 👤 **PAWarriors** 10 months, 2 weeks ago

Selected Answer: B

http:// --> Non encrypted websites.

https:// --> Encrypted websites

> Correct answer is B.

upvoted 2 times

🗳️ 👤 **sahir47** 11 months, 4 weeks ago

as it searches for a string match in a URL so the answer would be B as when the http:// is typed in the url a match will be found and the access would be blocked

upvoted 1 times

🗳️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

Selected Answer: B

A: idk, never seen this in a URL

B: Specific to unsecured websites

C: This can resolve to literally any site HTTP or HTTPS, too vague

D: port 443 is https/secure

upvoted 2 times

  **Jimmy1017** 1 year, 1 month ago

Selected Answer: B

Http is not secure but https is.

upvoted 1 times

  **shady23** 1 year, 1 month ago

Selected Answer: B

http://

upvoted 1 times

  **Mehsotopes** 1 year, 1 month ago

Selected Answer: B

http:// is an insecure protocol running on port 80 that uses unencrypted traceable data for communication on uncertified, & unprotected websites. It is indicated that you are on one of these insecure websites by a warning, or lack of padlock in your web search URL.

upvoted 2 times

During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

- A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
- B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0
- C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0
- D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Correct Answer: B

Community vote distribution

B (100%)

dbrowndiver Highly Voted 11 months ago

Selected Answer: B

Source: 10.1.4.9/32 specifies the exact malicious IP address to block.

Destination: 0.0.0.0/0 indicates all possible destinations within the network.

Action: deny specifies that traffic from this source IP should be blocked.

• Scenario Application:

Blocking Malicious IP: This rule effectively blocks any incoming traffic from the IP address 10.1.4.9 from accessing any part of the network.

Inbound Rule: As an inbound rule, it prevents traffic from the specified IP from entering the network, which aligns with the requirement to block the malicious IP. This rule directly addresses the need to block the specified IP address, fulfilling the requirement by denying access to all destinations, effectively preventing any communication from the malicious IP.

upvoted 5 times

4e3bda6 Most Recent 3 weeks, 3 days ago

Selected Answer: B

B. access-list inbound deny ip source 10.1.4.9/32

upvoted 1 times

PukaSudu 1 year, 1 month ago

Selected Answer: B

B. access-list inbound deny ip source 10.1.4.9/32

upvoted 1 times

SHADTECH123 1 year, 1 month ago

Selected Answer: B

B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0

Explanation:

This rule specifically denies all inbound traffic from the malicious IP address 10.1.4.9 to any destination within the network. This is the correct way to block the malicious IP address.

upvoted 3 times

shady23 1 year, 1 month ago

Selected Answer: B

B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0

upvoted 1 times

Mehsotopes 1 year, 1 month ago

Selected Answer: B

/32 would cover all possible subnets, & their communicating devices within the IP range, & destination 0.0.0.0/0 would cover the gateway surface of your network.

upvoted 2 times

rjbb 1 year, 1 month ago

A correction to this, /32 would block only this IP address.

but B is still the correct answer.

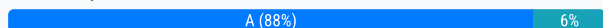
upvoted 3 times

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

- A. Implementing a bastion host
- B. Deploying a perimeter network
- C. Installing a WAF
- D. Utilizing single sign-on

Correct Answer: A

Community vote distribution



metzen227 Highly Voted 1 year, 1 month ago

Implementing a bastion host: A bastion host is a highly secured server located on a perimeter network (also known as a DMZ) that is designed to withstand attacks. It acts as a gateway between internal and external networks, allowing access only to specific services and applications. Users must authenticate themselves to the bastion host before accessing internal resources. This option provides a controlled entry point into the internal network, reducing the attack surface.

upvoted 26 times

e5c1bb5 Highly Voted 1 year, 1 month ago

Selected Answer: A

so from my understanding the bastion host and jump server are similar if not the name. the bastion host is not on the exam objectives. i think ill still go with A because it is the most secure. maybe its a no credit question?

upvoted 5 times

Markie100 Most Recent 4 months, 3 weeks ago

Selected Answer: A

Implementing a bastion host is the most secure method for providing administrative access to internal resources while minimizing traffic through the security boundary. It ensures controlled, monitored, and hardened access, aligning with best practices for securing administrative workflows.

upvoted 1 times

_thelastturtle 5 months, 1 week ago

Selected Answer: B

I thought a bastion would be for external users.

upvoted 2 times

kai001 9 months, 3 weeks ago

Selected Answer: A

A bastion host is a highly secured server designed to be the single point of entry for administrative access to internal resources. It acts as a gateway, allowing administrators to connect securely to internal systems without directly exposing those systems to the outside world. Only specific, authorized traffic (e.g., SSH or RDP) is allowed, and the bastion host is heavily monitored and hardened against attacks, thus minimizing the traffic allowed through the security boundary.

upvoted 4 times

c469c8e 10 months, 1 week ago

Selected Answer: C

A bastion host is only to provide access from public to private network. Question is to provide administrative access to internal resources. This excludes bastion host. Only response is WAF

upvoted 2 times

3dk1 7 months, 3 weeks ago

A WAF (Web application firewall) is for managing security on web applications.

upvoted 2 times

dbrowndiver 11 months ago

Selected Answer: A

The bastion host serves as a hardened gateway, where all administrative access to the internal network is funneled. This limits the exposure of the internal network to only a single, secure entry point.

Security Features: Bastion hosts are typically configured with strong security measures, such as multi-factor authentication, logging, and monitoring, to ensure that only authorized users can access internal resources.

upvoted 1 times

  **SHADTECH123** 1 year, 1 month ago

Selected Answer: A

Implementing a bastion host provides a highly secure method for administrative access to internal resources while minimizing traffic through the security boundary. It serves as a single entry point for remote administrative access, enforcing strong authentication and access controls before allowing access to internal systems.

upvoted 1 times

  **shady23** 1 year, 1 month ago

Selected Answer: A

A. Implementing a bastion host

The keyword in the question that makes option A correct is "minimizing the traffic allowed through the security boundary."

Implementing a bastion host allows for strict control over inbound traffic from external networks by acting as a single point of entry. Users connect to the bastion host, and from there, access to internal resources is provided. This setup minimizes the direct traffic flow to internal resources, as all external access is channeled through the bastion host, which can enforce security measures such as authentication, authorization, and logging. This effectively reduces the amount of traffic allowed through the security boundary while still providing access to internal resources for administrative purposes.

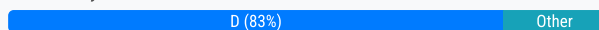
upvoted 3 times

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

- A. Application
- B. IPS/IDS
- C. Network
- D. Endpoint

Correct Answer: D

Community vote distribution



metzen227 **Highly Voted** 1 year, 1 month ago

Endpoint logs: Endpoint logs, also known as host logs, record events and activities that occur on individual endpoints (such as laptops, desktops, or servers). These logs can include information about processes, applications, system events, user logins, file accesses, and more. Endpoint logs are a valuable source of data for investigating security incidents on specific devices, including information about the executables running on the machine.

For the investigation described in the scenario, the most appropriate data source for obtaining additional information about the executable running on the employee's corporate laptop is Endpoint logs. Endpoint logs can provide detailed insights into the processes and executables running on the machine, helping the security analyst to further analyze and respond to the potential security threat.

upvoted 19 times

e5c1bb5 **Highly Voted** 1 year, 1 month ago

Selected Answer: D

employees laptop=endpoint

upvoted 12 times

leonbre **Most Recent** 4 weeks ago

Selected Answer: D

Endpoint logs provide detailed information about processes and executables running on a device, including file paths, hashes, and execution timestamps.

upvoted 2 times

slackbot 3 months, 1 week ago

Selected Answer: A

why not application logs? these will reveal what the application actually does? unless this is something explicitly mentioned by ComTIA that it must be the system logs, i would pick the app logs

upvoted 2 times

justin_es6 10 months, 1 week ago

Selected Answer: C

we see network we wrong

upvoted 1 times

dbrowndiver 11 months ago

Selected Answer: D

Endpoint logs can provide information about the executable in question, including its name, path, hash values, execution history, and associated processes. This data is crucial for identifying potentially malicious executables and understanding their behavior on the system.

upvoted 3 times

SHADTECH123 1 year, 1 month ago

Selected Answer: D

Endpoint logs are the most suitable data source for gathering additional information about the executable running on the employee's corporate laptop. These logs contain detailed information about processes, executables, and activities occurring on the endpoint, enabling the security analyst to understand the behavior of the executable and its potential impact on the system and network.

upvoted 3 times

  **shady23** 1 year, 1 month ago

Selected Answer: D

D. Endpoint

upvoted 1 times

  **e5c1bb5** 1 year, 1 month ago

to further clarify, endpoint logs are stored on the actual device so the data their looking for should be in endpoint logs.

upvoted 5 times

A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks. SIEM alerts have not yet been configured. Which of the following best describes what the security analyst should do to identify this behavior?

- A. Digital forensics
- B. E-discovery
- C. Incident response
- D. Threat hunting

Correct Answer: D

Community vote distribution

D (100%)

metzen227 Highly Voted 1 year, 1 month ago

Threat hunting: Threat hunting involves proactively searching for and identifying potential security threats or indicators of compromise (IOCs) within an organization's network environment. It typically involves the use of advanced analytics, threat intelligence, and specialized tools to detect suspicious behavior or anomalies that may indicate the presence of a threat actor.

In the scenario described, where SIEM alerts have not yet been configured to detect the new tactic malicious actors are using, the most appropriate action for the security analyst is Threat hunting. By engaging in threat hunting activities, the security analyst can proactively search for signs of the new tactic within the network environment, helping to identify and mitigate potential security risks before they escalate into full-blown incidents.

upvoted 18 times

SHADTECH123 Highly Voted 9 months ago

Selected Answer: D

Threat hunting involves proactive searching for signs of compromise or suspicious activities within the network. Since SIEM alerts have not been configured to detect the new tactic, engaging in threat hunting allows the security analyst to actively search for indicators of compromise and emerging threats before they escalate into security incidents.

upvoted 7 times

itone333 Most Recent 4 months ago

Selected Answer: D

If the SIEM ain't been configured, then you gotta go look for the threat..

upvoted 3 times

kai001 9 months ago

Selected Answer: D

Threat hunting is a proactive approach used by security analysts to search for signs of malicious activity that might have bypassed existing security measures, such as SIEM alerts. Since the SIEM has not been configured for this new tactic, threat hunting allows the analyst to manually investigate network traffic, logs, endpoints, and other data sources to identify suspicious behavior based on the new information provided by the cyber operations team.

upvoted 1 times

dbrowndiver 9 months ago

Selected Answer: D

In this scenario, the security analyst needs to proactively search for signs of the new malicious tactic being used in the network, especially since SIEM alerts are not yet configured to detect this behavior.


• Scenario Application:

Proactive Investigation: With the lack of SIEM alerts, threat hunting allows the analyst to manually search for indicators of the new tactic within network logs, endpoint data, and other security information sources.

Adaptability: Threat hunters adapt their techniques based on new intelligence, such as the information provided by the cyber operations team, to identify potential threats that automated systems might miss.

Threat hunting is particularly useful when dealing with new or unknown attack tactics that have not yet been incorporated into automated detection systems. By manually analyzing the environment, analysts can identify and understand the behavior of threats, leading to better future alert configurations.

upvoted 2 times

  **hasquaati** 1 year, 1 month ago

Selected Answer: D

Good answer

upvoted 1 times

A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

- A. Accept
- B. Transfer
- C. Mitigate
- D. Avoid

Correct Answer: B

Community vote distribution

B (89%)

11%

  **metzen227**  1 year, 1 month ago

Transfer: Transferring a risk involves shifting some or all of the risk to another party, such as an insurance provider, through contractual agreements or financial arrangements. If the company purchases cyber insurance to address items listed on the risk register, it represents a risk transfer strategy. The company is transferring the financial burden of potential cyber incidents to the insurance provider, who will compensate the company for covered losses.

Given the scenario described, the strategy represented by the company's purchase of cyber insurance to address items listed on the risk register is Transfer. The company is transferring some of the financial consequences of potential cyber incidents to the insurance provider through the purchase of insurance coverage.

upvoted 23 times

  **itone333**  4 months ago

Selected Answer: B

Transferring the risk to the insurance company(3rd party).

upvoted 1 times

  **Markie100** 4 months, 3 weeks ago

Selected Answer: B

By purchasing cyber insurance, the company is not eliminating or reducing the risk but is instead ensuring that the financial burden of a potential cyber incident is covered by the insurer.



upvoted 2 times

  **_thelastturtle** 5 months, 1 week ago

Selected Answer: C

I thought the RR would be used to make informed decisions, mitigating any risks

upvoted 1 times

  **Oca8ee9** 6 months, 3 weeks ago

Selected Answer: B

Insurance transfers risks to the insurance provider

upvoted 1 times

  **PAWarriors** 10 months, 2 weeks ago

Selected Answer: B

Correct answer is B (Transfer).

> The company purchased cyber insurance in order to transfer the risk to another party, in this case, the insurance company.

upvoted 4 times

A security administrator would like to protect data on employees' laptops. Which of the following encryption techniques should the security administrator use?

- A. Partition
- B. Asymmetric
- C. Full disk
- D. Database

Correct Answer: C

Community vote distribution

C (100%)

  **rjbb** Highly Voted 1 year, 1 month ago

Selected Answer: C

The answer is C - Full disk encryption, this encrypts the whole storage drive of the device, including OS, files, app data, etc.

the reason its not the other options

partition encryption - only encrypts the partition, meaning if there are multiple partitions then some of them could be left unencrypted and a threat actor could steal data in them.

Asymmetric encryption - is an encryption technique using Public Key, private key methodology.

Database encryption - is used to encrypt databases (schema) or data within the databases.

upvoted 11 times

  **PAWarriors** Most Recent 10 months, 2 weeks ago

Selected Answer: C

Answer is C --> Full disk encryption encrypts the entire hard drive to protect all of the data being stored on it, hence protecting the user's laptop

upvoted 2 times

  **Th3irdEye** 1 year, 1 month ago

Selected Answer: C

I think it's C

upvoted 2 times

  **Abcd123321** 1 year, 1 month ago

Selected Answer: C

Full Disk Encryption (FDE)

○ Encrypts the entire hard drive

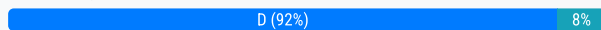
upvoted 4 times

Which of the following security control types does an acceptable use policy best represent?

- A. Detective
- B. Compensating
- C. Corrective
- D. Preventive

Correct Answer: D

Community vote distribution



TheMichael Highly Voted 1 year ago

Selected Answer: D

D. Preventive

AUP is pretty obviously trying to prevent things from happening.

It's not A. Detective because it doesn't detect anything. It's a policy.

It's not B. Compensating because it isn't making up for any other policy included in the question.

It's not C. Corrective because it doesn't correct anything on its own, it's simply a policy that is to be followed.

So it could only be D. Preventive, as it prevents people from doing things that might compromise the network.

upvoted 16 times

uday1985 10 months, 2 weeks ago

How a standard policy without enforced controls can prevent someone from clicking a link or visiting malicious sites? it doesn't prevent! but would deter them! pretty much like Security Camera! it won't stop anyone from stealing! it will just deter them

upvoted 3 times

noragami Highly Voted 9 months ago

Selected Answer: D

An acceptable use policy best represents:

D. Preventive

An acceptable use policy is designed to prevent security incidents by defining the acceptable and unacceptable behaviors and actions for users within an organization. By setting clear guidelines and expectations, it aims to prevent misuse and ensure that users adhere to security protocols, thereby reducing the risk of security breaches.

upvoted 8 times

braveheart22 Most Recent 7 months, 3 weeks ago

Selected Answer: D

An Acceptable Use Policy sets guidelines and rules for how users should behave when using an organization's network, devices, and other resources. It is preventive in nature because it aims to prevent improper behavior and reduce the likelihood of security incidents before they occur by clearly defining acceptable and unacceptable actions.

Preventive controls aim to deter security violations or unwanted behaviors from happening in the first place. AUPs prevent misuse of resources by setting clear boundaries on what is and isn't allowed, such as restrictions on accessing certain websites or using unauthorized software.

upvoted 1 times

Exemplary 8 months, 3 weeks ago

I find myself wondering if the actual exam uses "Directive" as A instead of Detective. Jason Dion's course actually used AUP as its example of a Directive Control:

Directive Controls - Often rooted in policy or documentation and set the standards for behavior within an org. Ex. Acceptable Use Policies (AUPs).

Guides the entire process.

upvoted 2 times

dbrowndiver 9 months ago

Selected Answer: D

An acceptable use policy serves as a preventive measure by clearly outlining what constitutes acceptable and unacceptable behavior. This deters employees from engaging in activities that could lead to security breaches or misuse of resources.

Education: By educating users about proper usage and potential consequences of violations, the policy reduces the likelihood of accidental or intentional security incidents.

Legal and Compliance: AUPs also help establish a legal framework for acceptable use, which can prevent legal liabilities and ensure compliance with regulatory requirements.

Why it is the best choice:

The primary goal of an AUP is to prevent misuse of IT resources by setting clear expectations and guidelines. By defining what is acceptable, the policy acts as a preventive control, helping to mitigate risks before they materialize.

upvoted 1 times

  **PAWarriors** 9 months ago

Selected Answer: D

Acceptable Use Policy (AUP) is a preventive security control type. AUP is a document that outlines the do's and don'ts for users when interacting with an organization's IT systems and resources and defines appropriate and prohibited use of IT systems/resources as a preventive security control.

upvoted 1 times

  **dbrowndiver** 11 months ago

Selected Answer: D

By restricting access to the administrator console to just the IT manager and the help desk lead, the IT manager is implementing least privilege. This ensures that only those who need elevated access for their roles can use administrative functions, reducing the risk of unauthorized changes or misuse.

upvoted 1 times

  **ebomuchekingsley** 11 months, 2 weeks ago

Policies are usually a type of preventive admin control.

upvoted 4 times

  **elbarozz** 1 year ago

Selected Answer: D

its clearly D

upvoted 3 times

  **Gadoof** 1 year ago

Selected Answer: B

It's impossible for a policy to be a detective, corrective, or preventative control as a policy CANNOT stop/prevent, or detect any attack in any way. It has to be B

upvoted 3 times

  **kinny4000** 1 year ago

Due to the consequences a user will face if they breach the AUP, it acts as a deterrent. It does actually prevent a lot.

upvoted 5 times

  **MAKOhunter33333333** 1 year, 1 month ago

Selected Answer: D

AUP = lets user know what is acceptable and allowed to prevent them from performing certain activity

upvoted 4 times

  **rjbb** 1 year, 1 month ago

Selected Answer: D

preventive - an acceptable use policy enforces rules to users to use company resources.

example - company A states that in order to access files in the company server you must connect to your company VPN when working from home.

This prevents you from connecting from an insecure network.

upvoted 2 times

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

- A. Hardening
- B. Employee monitoring
- C. Configuration enforcement
- D. Least privilege

Correct Answer: D

Community vote distribution

D (100%)

metzen227 Highly Voted 1 year, 1 month ago

Least privilege: Least privilege is a security principle that states that users should only be granted the minimum level of access or permissions necessary to perform their job functions. By restricting access to the administrator console of the help desk software to only the IT manager and the help desk lead, the IT manager is adhering to the principle of least privilege, ensuring that only those individuals who require administrative access have it, thereby reducing the risk of unauthorized access and potential misuse.

Given the scenario described, the security technique that the IT manager is setting up by restricting access to the administrator console of the help desk software is Least privilege. This approach aligns with the principle of least privilege by granting administrative access only to individuals who need it to perform their job responsibilities.

upvoted 14 times

1LL337 Highly Voted 11 months ago

Selected Answer: D

Eliminating unnecessary access = Least Privilege

upvoted 6 times

gollum9 Most Recent 6 months, 3 weeks ago

Selected Answer: D

D. Least privilege

upvoted 1 times

Limah 11 months ago

Access is the key word here

upvoted 3 times

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

- A. Risk tolerance
- B. Risk transfer
- C. Risk register
- D. Risk analysis

Correct Answer: C

Community vote distribution

C (100%)

MAKOhunter33333333 Highly Voted 1 year, 1 month ago

Selected Answer: C

Think of register as registry, all the details of stuff
upvoted 10 times

Etc_Shadow28000 Highly Voted 1 year ago

Selected Answer: C

C. Risk register

A risk register is a tool commonly used in risk management that records details of all identified risks, including descriptions, responsible parties, risk categories, likelihood and impact, mitigation measures, and thresholds for action. It serves as a central repository for all information about risks, making it easier to manage and track them.

upvoted 9 times

gollum9 Most Recent 6 months, 3 weeks ago

Selected Answer: C

C. Risk register
upvoted 1 times

dbrowndiver 11 months ago

Selected Answer: C

A risk register is a comprehensive document that captures all identified risks within an organization. It includes detailed information about each risk, including descriptions, responsible parties, mitigation strategies, impact assessments, and thresholds for acceptable risk levels.
upvoted 2 times

PukaSudu 1 year, 1 month ago

Selected Answer: C

register
upvoted 1 times

metzen227 1 year, 1 month ago

Risk register: A risk register is a document or database used to record information about identified risks, including their likelihood, potential impact, responsible parties, mitigation strategies, and thresholds for triggering response actions. It serves as a central repository for managing and tracking risks throughout their lifecycle. The risk register is the most likely option among the choices provided to be used to document risks, responsible parties, and thresholds.

Given the options provided, the most likely choice to be used to document risks, responsible parties, and thresholds is Risk register. The risk register serves as a comprehensive tool for documenting and managing risks, including key information such as responsible parties and thresholds for triggering response actions.

upvoted 5 times

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Disaster recovery plan
- B. Incident response procedure
- C. Business continuity plan
- D. Change management procedure

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **CyberPark17** Highly Voted 👍 1 year, 1 month ago

Selected Answer: D

The keyword is "new" firewall rules. Any change must be adhered to change management procedures.

upvoted 22 times

🗳️ 👤 **MAKOhunter33333333** Highly Voted 👍 1 year, 1 month ago

Selected Answer: D

Want to make sure the new WF rules do not interfere or cause disruption in service and network, submit a change management request or else you be in big doo doo

upvoted 12 times

🗳️ 👤 **9149f41** Most Recent 🕒 4 months, 3 weeks ago

Selected Answer: D

Disaster recovery, incident response, and business continuity plans are relevant to an incident or disaster, but in the question, there is no such incident or disaster mentioned. A change in the system could be done for many reasons, like updating, adding, or deleting any rule.

upvoted 1 times

🗳️ 👤 **gollum9** 6 months, 3 weeks ago

Selected Answer: D

D. Change management procedure

upvoted 1 times

🗳️ 👤 **dbrowndiver** 11 months ago

Selected Answer: D

Implementing new firewall rules is a significant change to the network security infrastructure. Adhering to change management procedures ensures these changes are made systematically, reducing the risk of errors and enhancing the security posture.

upvoted 6 times

🗳️ 👤 **An381038** 1 year, 1 month ago

Selected Answer: D

D. Change management procedure

upvoted 6 times

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

- A. Open-source intelligence
- B. Bug bounty
- C. Red team
- D. Penetration testing

Correct Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **gollum9** 6 months, 3 weeks ago

Selected Answer: B

B. Bug bounty
upvoted 1 times

🗳️ 👤 **dbrowndiver** 11 months ago

Selected Answer: B

The scenario describes a program where the company invites external individuals, often called ethical hackers or researchers, to find vulnerabilities in its application and offers compensation based on the discoveries. Bug bounty programs are initiatives where organizations invite external researchers to test their software or systems for vulnerabilities. Researchers are rewarded with financial compensation, recognition, or both, based on the severity and impact of the vulnerabilities they find.

upvoted 1 times

🗳️ 👤 **Etc_Shadow28000** 1 year ago

Selected Answer: B

B. Bug bounty

A bug bounty program incentivizes external security researchers to find and report vulnerabilities in a company's applications or systems. Researchers are compensated based on the severity and impact of the vulnerabilities they uncover, helping the company to improve its security posture by leveraging a wide range of expertise.

upvoted 4 times

🗳️ 👤 **Jimmy1017** 1 year, 1 month ago

Selected Answer: B

B bug bounty because they're paying non employees to find vulnerabilities.
upvoted 4 times

🗳️ 👤 **Abcd123321** 1 year, 1 month ago

Selected Answer: B

Bug bounty hunters can earn money by discovering zero-day vulnerabilities
upvoted 3 times

Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

- A. Insider
- B. Unskilled attacker
- C. Nation-state
- D. Hacktivist

Correct Answer: C

Community vote distribution

C (100%)

MAK0hunter33333333 Highly Voted 1 year, 1 month ago

Selected Answer: C

Think of China right now, they hacking into CIKR and are heavily funded. NATION STATE.

upvoted 9 times

Abcd123321 Highly Voted 1 year, 1 month ago

Selected Answer: C

Nation-state Actor

■ Groups or individuals that are sponsored by a government to conduct cyber operations against other nations, organizations, or individuals

upvoted 7 times

ProudFather Most Recent 6 months, 4 weeks ago

Selected Answer: C

Nation-state

Nation-state actors often have significant financial resources, advanced technical capabilities, and the backing of a government. This enables them to launch sophisticated and well-resourced attacks against critical infrastructure and systems in other countries.

upvoted 2 times

dbrowndiver 11 months ago

Selected Answer: C

o Nation-state actors are government-backed groups or organizations that engage in cyber activities as part of national interests. They have significant financial and technical resources and often target critical infrastructure, defense systems, and other high-value targets in foreign countries. The nation-state is the most likely threat actor to use vast financial resources for international cyber attacks, aligning with the scenario's description of attacking critical systems across borders.

upvoted 5 times

Which of the following enables the use of an input field to run commands that can view or manipulate data?

- A. Cross-site scripting
- B. Side loading
- C. Buffer overflow
- D. SQL injection

Correct Answer: D

Community vote distribution

D (100%)

  **Etc_Shadow28000** Highly Voted 9 months ago

Selected Answer: D

The correct answer is:

D. SQL injection

SQL injection is a type of attack that involves inserting malicious SQL statements into an input field. These statements can then be executed by the database, allowing the attacker to view or manipulate the data. This can lead to unauthorized access to the database, data leakage, or even the modification and deletion of data.

Here's why the other options are not correct in this context:

- A.

This involves injecting malicious scripts into webpages viewed by other users, but it does not specifically involve running commands that directly view or manipulate data in a database.

- B

This typically refers to installing applications from unofficial sources, not related to input fields and running commands.

-C.

This involves exploiting a program by writing more data to a buffer than it can hold, potentially allowing the execution of arbitrary code, but it does not specifically use input fields to run commands on data.

upvoted 29 times

  **aws_guru1** 9 months, 1 week ago

Thanks for the detailed analysis!

upvoted 5 times

  **metzen227** Highly Voted 1 year, 1 month ago

SQL injection: SQL injection involves inserting malicious SQL queries into input fields or other user-controllable data sources to manipulate the database backend. By exploiting SQL injection vulnerabilities, attackers can execute arbitrary SQL commands that can view, modify, or delete data stored in the database. This technique directly enables the use of an input field to run commands that manipulate data.

Therefore, the correct answer is SQL injection. It allows attackers to execute commands through input fields to manipulate data within a database.

upvoted 14 times

  **shootweb** Most Recent 3 months, 1 week ago

Selected Answer: D

Even though I believe the answer is D (SQLi) I still think A (XSS) is a valid answer. The question does not specify whether "data" refers specifically to application data or database data. If the question explicitly mentioned "database data," then SQL Injection (D) would be 100% correct.

Why can it be A then? When an XSS script runs, it can view, modify, or exfiltrate data. A simple example would be grabbing and replacing cookies, which requires the ability to view and manipulate data. XSS can also exhibit CSRF-like behavior, as it can steal a session and use it to interact with APIs as if it were the victim, which also requires viewing and manipulating data.

upvoted 2 times

  **PAWarriors** 10 months, 2 weeks ago

Selected Answer: D

Correct answer is D (SQL injection).

> SQL injection Involves inserting malicious SQL code into input fields.

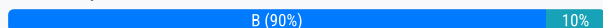
upvoted 2 times

Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data. Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

- A. Encrypted
- B. Intellectual property
- C. Critical
- D. Data in transit

Correct Answer: B

Community vote distribution



matmarcm Highly Voted 1 year, 1 month ago

B. Intellectual property

Employees in R&D are typically involved in creating, developing, and improving products, technologies, or processes. The data they handle often includes sensitive and proprietary information
upvoted 15 times

Etc_Shadow28000 Highly Voted 9 months ago

Selected Answer: B

B. Intellectual property

Research and development teams typically handle sensitive information related to new inventions, designs, processes, and technologies. This type of data is considered intellectual property (IP) and is crucial for maintaining a competitive edge in the market. Protecting this data from unauthorized access, theft, or misuse is a primary concern, hence the extensive training provided to these employees.
upvoted 10 times

sentinell Most Recent 3 weeks, 1 day ago

Selected Answer: B

Employees in research and development (R&D) typically work on new products, technologies, designs, or innovations. The type of data they handle most often includes:

Trade secrets

Product prototypes

Design plans

Source code

Technical research

All of these fall under the category of intellectual property (IP) – which needs strong protection to prevent theft, loss, or industrial espionage.

! Why not the other options?

A. Encrypted – Encryption is a method of protecting data, not a type of data.

C. Critical – While R&D data can be critical, this is a broader term that could apply to many departments.

D. Data in transit – This refers to data being transmitted over a network. Again, it's a data state, not a type.
upvoted 1 times



monstamash 2 months ago

Selected Answer: B

Employees in Research and Development (R&D) work with innovative ideas, designs, patents, product formulas, prototypes, and trade secrets — all of which are considered intellectual property (IP).

Protecting IP is critical to a company's competitive advantage, and that's why R&D teams receive extensive security training.

upvoted 1 times

  **sherkhan82** 3 months, 2 weeks ago

Selected Answer: C

It is not Intellectual Property because that is publicly available information and is usually copyrighted/trademarked so it doesn't need to be protected.

The answer is Critical data because this is highly sensitive data, if exposed could cause harm to the business.

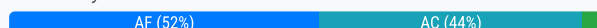
upvoted 1 times

A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs. Which of the following security benefits do these actions provide? (Choose two.)

- A. If a security incident occurs on the device, the correct employee can be notified.
- B. The security team will be able to send user awareness training to the appropriate device.
- C. Users can be mapped to their devices when configuring software MFA tokens.
- D. User-based firewall policies can be correctly targeted to the appropriate laptops.
- E. When conducting penetration testing, the security team will be able to target the desired laptops.
- F. Company data can be accounted for when the employee leaves the organization.

Correct Answer: AF

Community vote distribution



SHADTECH123 Highly Voted 1 year, 1 month ago

AC

A. If a security incident occurs on the device, the correct employee can be notified.

By associating devices with specific employees, the security team can quickly identify and notify the responsible employee in the event of a security incident. This helps in timely incident response and remediation.

C. Users can be mapped to their devices when configuring software MFA tokens.

Associating devices with employee IDs allows for accurate mapping of users to their devices. This is particularly important when setting up and managing multi-factor authentication (MFA) tokens, ensuring they are configured for the correct devices and users.

upvoted 11 times

shootweb 3 months, 1 week ago

AF.

Asset tags help identify ownership, not authentication credentials. MFA is tied to user identity (employee ID) rather than a specific device. A user can log in from multiple devices, and MFA will still work because it verifies the user's credentials, not the physical device. You said it best:

"Associating devices with employee IDs allows for accurate mapping of users to their devices." From this, we can see that MFA plays no role in identifying a device.

F directly aligns with the primary priority of cybersecurity professionals: protecting company data.

upvoted 4 times

1chung Most Recent 4 days, 10 hours ago

Selected Answer: AF

I go with AF

upvoted 1 times

0e6bd20 1 week, 1 day ago

Selected Answer: AF

I asked the AI god after it said A and F, and this is the response I got (ChatGPT o3 advanced reasoning model):

Is C plausible?

Not really.

Software-based MFA tokens (TOTP apps, push agents, etc.) are almost always tied to the user account, not to a specific workstation. Whether or not a laptop carries an inventory sticker has no bearing on enrolling or mapping that token—the enrolment happens in the identity platform and follows the user wherever they log in. Asset tagging is great for ownership, incident response, and off-boarding (A, F), but it doesn't materially simplify MFA token provisioning, so C isn't considered a core security benefit here.

upvoted 1 times

🗨️ 👤 **1chung** 1 month, 2 weeks ago

Selected Answer: AB

I go with AB

upvoted 1 times

🗨️ 👤 **Konversation** 3 months ago

Selected Answer: AF

AF

There are no doubts about A.

C or F is the question. While both are reasonable, there is no reference to MFA in the CompTIA Student Guide nor their WBT related to Asset Management.

The strongest reference is "Assigning asset ownership involves designating specific individuals or teams within the organization as responsible for particular assets to establish a clear chain of accountability for asset security, maintenance, and ongoing management". This means, F is more likely excepted in the exam, in my opinion.

upvoted 4 times

🗨️ 👤 **kamax5400** 3 months, 3 weeks ago

Selected Answer: AF

A & F is the answer

upvoted 1 times

🗨️ 👤 **prabh1251** 3 months, 3 weeks ago

Selected Answer: AF

a & f is correct

upvoted 1 times

🗨️ 👤 **Oluwatobi4880** 4 months, 1 week ago

Selected Answer: AC

The answer is not A and F because of the specific nature of the security benefits related to inventory stickers and employee IDs. Let's break down why:

A. If a security incident occurs on the device, the correct employee can be notified.

This option makes sense as a benefit because labeling and associating devices with employee IDs allow for the effective tracking and notification of the relevant employee in case of a security incident on their device.

F. Company data can be accounted for when the employee leaves the organization.

While this seems relevant, the actual process of accounting for company data when an employee leaves is broader and involves policy and process beyond simply labeling a device. Although asset tracking helps with inventory management, the label itself doesn't directly manage or account for the data on the device when an employee departs.

Instead, the more direct security benefits from labeling devices would be:

C. Users can be mapped to their devices when configuring software MFA tokens.

upvoted 2 times

🗨️ 👤 **Russell15** 4 months, 2 weeks ago

Selected Answer: AF

Every one agrees A:

I say F because when employees leave the company, their assigned device can be tracked, retrieved, and properly wiped to ensure company data is not lost or leaked.

Most MFAs are configured per user not per device.

upvoted 3 times

🗨️ 👤 **gavin1776** 4 months, 3 weeks ago

Selected Answer: AC

I don't see the answer being F. It would help account for company property, but how would asset tags help account for data?

upvoted 1 times

🗨️ 👤 **Innana** 5 months ago

Selected Answer: AF

We had that question in the course and A and F were correct answers

upvoted 4 times

🗨️ 👤 **agp2684** 5 months, 1 week ago

Selected Answer: AF

It should be A and F, although option A isn't 100% realistic. Why? The question mentioned only that they are adding asset stickers, but simply having a sticker doesn't mean that the asset ID matches with the computer name

upvoted 2 times

🗨️ 👤 **ITExperts** 5 months, 1 week ago

Selected Answer: AF

has to be A and F

upvoted 3 times

🗨️ 👤 **BFG_Nick** 5 months, 2 weeks ago

Selected Answer: AC

AC because that's what we use at my company

upvoted 3 times

🗨️ 👤 **babujju** 5 months, 2 weeks ago

Selected Answer: AC

A. If a security incident occurs on the device, the correct employee can be notified.

Asset inventory stickers and association with employee IDs help identify the user responsible for a device, making it possible to notify them if a security incident occurs.

C. Users can be mapped to their devices when configuring software MFA tokens.

Associating devices with employee IDs ensures that software Multi-Factor Authentication (MFA) tokens can be correctly configured for the right user on the right device.

upvoted 3 times

🗨️ 👤 **Aces155** 5 months, 3 weeks ago

Selected Answer: AC

AC, I think everyone can agree with A. I'm choosing C over F because when they had us set up MFA pins at work they said it was more secure than passwords because it validated our device to our identity and the pin would only work on our specific laptops

upvoted 2 times

🗨️ 👤 **TmNvrWts** 6 months, 2 weeks ago

Selected Answer: AC

F. Company data can be accounted for when the employee leaves the organization.: While asset tracking helps manage hardware, accounting for data is a broader process involving data access and permissions, not just inventory stickers.

upvoted 3 times

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring training.
- D. Implement a phishing campaign.

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **e5c1bb5** Highly Voted 1 year, 1 month ago

Selected Answer: C

C. its the only thing that actually changes.
working remote you'd still be able to receive phishing training.
upvoted 13 times

🗳️ 👤 **Etc_Shadow28000** Highly Voted 1 year ago

Selected Answer: C

To improve the situational and environmental awareness of existing users as they transition from remote to in-office work, the best option is:

C. Modify the content of recurring training.

Modifying the content of recurring training to include specific topics relevant to the transition from remote to in-office work will ensure that users are aware of the new security protocols and potential threats they might face in the office environment. This approach provides a structured and comprehensive way to address the unique aspects of both environments and helps reinforce best practices.

upvoted 6 times

🗳️ 👤 **Chidazz** Most Recent 5 months ago

Selected Answer: C

Modify the content of recurring training.
upvoted 1 times

🗳️ 👤 **MaxiPrince** 6 months, 2 weeks ago

Selected Answer: C

Modify the content of recurring training.
upvoted 2 times

🗳️ 👤 **dbrowndiver** 11 months ago

Selected Answer: C

By updating the content of recurring training, the organization can focus specifically on the differences between remote and in-office security environments. This includes new physical security measures, data protection protocols, and situational awareness needed within the office space.
upvoted 1 times

🗳️ 👤 **Dlove** 11 months, 2 weeks ago

Selected Answer: C

C. Modify the content of recurring training

This answer choice is the only one that makes sense. Process of elimination guys.
upvoted 1 times

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

- A. Packet captures
- B. Vulnerability scans
- C. Metadata
- D. Dashboard

Correct Answer: D

Community vote distribution

D (100%)

metzen227 Highly Voted 1 year, 1 month ago

Dashboard: A dashboard is a graphical user interface that provides at-a-glance views of key performance indicators (KPIs) and other important metrics. In the context of cybersecurity, a dashboard can be used to present summarized information about security incidents, including the number of incidents, their severity, affected systems, and trends over time. Dashboards can provide a visually appealing and easy-to-understand way to present quarterly incident reports to the board of directors, making them the most suitable option among the choices provided.

Therefore, the systems administrator should use Dashboard to present the quarterly incident reports to the board of directors. A dashboard can effectively summarize incident data and provide a visually appealing presentation format for the board's review.

upvoted 9 times

MAK0hunter3333333 Highly Voted 1 year, 1 month ago

Selected Answer: D

Board of directors wants something easy to look at since they likely have little knowledge.

upvoted 5 times

slackbot Most Recent 3 months ago

Selected Answer: D

say Director presentation and you should think of 2 things:

- powerpoint
- excel

upvoted 1 times

dbrowndiver 9 months ago

Selected Answer: D

Dashboards offer a clear and intuitive way to present complex data, making it easier for board members to grasp the overall security posture and trends over time.

Customizable Information: The dashboard can be tailored to highlight specific metrics relevant to the board, such as the number of incidents, types of threats, and trends in security incidents, providing actionable insights.

Dashboards can present both real-time data and historical trends, allowing the board to see how the organization is performing over the quarter.

upvoted 4 times

shady23 1 year, 1 month ago

Selected Answer: D

D. Dashboard

upvoted 2 times

Mehsotopes 1 year, 1 month ago

Selected Answer: D

A dashboard allows for a full display of information in an easily readable form for network operators to make decisions off of.

upvoted 2 times

A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

- A. The end user changed the file permissions.
- B. A cryptographic collision was detected.
- C. A snapshot of the file system was taken.
- D. A rootkit was deployed.

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Penguin1730** Highly Voted 1 year, 1 month ago

D. A rootkit was deployed.

A change in the hash of a critical system file like cmd.exe, without any corresponding patches or updates being applied, is a strong indicator of potential malicious activity. A rootkit is a type of malware that can modify system files and hide its presence to maintain persistent and privileged access to a system. If a rootkit has altered cmd.exe, it could be an attempt to replace the legitimate command prompt with a malicious version, or to modify its behavior for nefarious purposes. This is a serious security concern and should be investigated immediately.

upvoted 21 times

🗳️ 👤 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: D

A rootkit can be snuck into a system, & provide functions for an attacker to tamper with system configuration settings without the knowledge of owners, or system administrators.

upvoted 6 times

🗳️ 👤 **dbrowndiver** Most Recent 11 months ago

Selected Answer: D

o The hash change of a critical system file like cmd.exe without authorized patches indicates potential malware activity, with rootkits being a prime suspect due to their method of operation.

upvoted 3 times

🗳️ 👤 **SHADTECH123** 1 year, 1 month ago

Selected Answer: D

Changes to the hash of system files, such as cmd.exe, without corresponding patching activity, are often indicative of unauthorized modifications, such as those caused by malware or rootkits.

Rootkits are malicious software designed to conceal their presence or the presence of other malware on a system. They often modify system files like cmd.exe to maintain persistence and evade detection.

upvoted 3 times

Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?

- A. Client
- B. Third-party vendor
- C. Cloud provider
- D. DBA

Correct Answer: A

Community vote distribution

A (90%)

10%

metzen227 Highly Voted 1 year, 1 month ago

Client: In the shared responsibility model, the client, or cloud customer, is responsible for securing their data and applications running on the cloud infrastructure. This includes configuring security settings, implementing access controls, and managing user permissions for their resources. However, the specific responsibility for securing the company's database in an Infrastructure as a Service (IaaS) model depends on the division of responsibilities outlined in the model.

Given the options provided and the context of the shared responsibility model for a cloud environment, the most appropriate role responsible for securing the company's database in an IaaS model would be Client. The client is typically responsible for securing their data and applications, including databases, within the cloud infrastructure. However, the DBA would also play a significant role in implementing database security measures within the IaaS environment, working in collaboration with the client's security team.

upvoted 14 times

dbrowndiver Highly Voted 11 months ago

Selected Answer: A

In the IaaS model, the client is responsible for securing everything above the infrastructure layer provided by the cloud provider. This includes the operating system, applications, and data, which encompasses the security of databases.

upvoted 10 times

sentinell Most Recent 3 weeks, 1 day ago

Selected Answer: A

Client is the right answer

upvoted 1 times

Dimpo_Oz 7 months ago

Selected Answer: A

Whilst D the Database admin would seem to be the obvious choice the question asks secure not administer, getting the DBA alone to secure is inadequate, you will also need others to completely secure meaning the best answer is A client

upvoted 1 times

spencer0328 11 months, 4 weeks ago

Selected Answer: D

Exactly D. DBA ,which means Database administrator.

upvoted 2 times

agp2684 5 months, 1 week ago

You are mistaken. In the cloud shared responsibility model, the DBA is not mentioned; it just refers to the client

upvoted 2 times

shady23 1 year, 1 month ago

Selected Answer: A

A. Client

upvoted 5 times

Mehsotopes 1 year, 1 month ago

Selected Answer: A

The client is the one who is utilizing the data, & would be responsible in the handling, & security of database within the infrastructure provided by the Cloud Provider, or Third-Party Vendor.

upvoted 8 times

  **e5c1bb5** 1 year, 1 month ago

while a database sounds like a physical piece of equipment, it typically is not. Therefore in the IAAS model configuring the security of the database should be settings, firewall, and othertechnologies that cloud providers typically wont mess with.

upvoted 2 times

A client asked a security company to provide a document outlining the project, the cost, and the completion time frame. Which of the following documents should the company provide to the client?

- A. MSA
- B. SLA
- C. BPA
- D. SOW

Correct Answer: D

Community vote distribution

D (97%)

🗳️ **Etc_Shadow28000** Highly Voted 1 year ago

Selected Answer: D

The company should provide the client with a Statement of Work (SOW).

A Statement of Work is a document that outlines the details of a project, including the scope, deliverables, timeline, and cost. It is used to ensure that both the client and the service provider have a clear understanding of the project's requirements and expectations.

- MSA (Master Service Agreement) An overarching contract that defines the terms and conditions under which services will be provided.
- SLA (Service Level Agreement) A contract that defines the level of service expected from the service provider.
- BPA (Business Partnership Agreement) An agreement that defines the relationship and responsibilities between business partners.

Therefore, the correct answer is:

D. SOW

upvoted 27 times

🗳️ **metzen227** Highly Voted 1 year, 1 month ago

SOW (Statement of Work): A Statement of Work is a document that outlines the specific details of a project, including the project scope, objectives, deliverables, milestones, resources, timelines, and costs. It provides a detailed description of the work to be performed and the expectations of both the client and the service provider. A SOW is commonly used in project-based engagements to ensure clarity and alignment between the parties involved.

upvoted 9 times

🗳️ **9149f41** Most Recent 4 months, 3 weeks ago

Selected Answer: D

An SLA is a preliminary contract that includes details like the MSP team's (provider's) response times, uptime guarantees, or performance metrics.

A SOW, on the other hand, focuses on the actual work or tasks of the project, such as deliverables, scope, and timelines. The question specifically asks for details about the project itself, like cost and time, which are covered in the SOW.

upvoted 1 times

🗳️ **[Removed]** 9 months, 3 weeks ago

Selected Answer: D

Agree with D

upvoted 2 times

🗳️ **qacollin** 11 months ago

This seems to be a new term. It's not on the 601

upvoted 1 times

🗳️ **PukaSudu** 1 year, 1 month ago

Selected Answer: B

The Work Order (WO) or Statement of Work (SOW) is a document that provides detailed instructions and requirements for a specific task within a project to be carried out by the vendor. It may include information on deliverables, timelines, and costs.

upvoted 1 times

  **e5c1bb5** 1 year, 1 month ago

Selected Answer: D

SOW=statement of work

upvoted 6 times

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

- A. Secure cookies
- B. Version control
- C. Input validation
- D. Code signing

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **hasquaati** Highly Voted 👍 1 year, 1 month ago

Selected Answer: C

Answer is C. Its important to make sure that javascript code can not be inputted and executed into Form fields.
upvoted 10 times

🗳️ 👤 **PAWarriors** Highly Voted 👍 10 months, 1 week ago

Selected Answer: C

Correct answer is C.

Cross-Site Scripting (XSS) can be mitigated with proper input validation.
upvoted 7 times

🗳️ 👤 **SHADTECH123** Most Recent 🕒 9 months ago

Selected Answer: C

A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

- A. Secure cookies
- B. Version control
- C. Input validation
- D. Code signing

upvoted 4 times

🗳️ 👤 **kinny4000** 1 year ago

Thanks bro

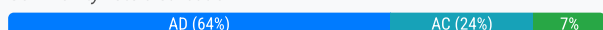
upvoted 17 times

Which of the following must be considered when designing a high-availability network? (Choose two).

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

Correct Answer: AD

Community vote distribution



Etc_Shadow28000 Highly Voted 1 year ago

Selected Answer: AD

When designing a high-availability network, two key considerations are:

- A. Ease of recovery
- D. Responsiveness

- Ease of recovery. This is essential for high availability because the network must be able to recover quickly from failures to minimize downtime.
 - Responsiveness. Ensuring that the network can handle high traffic loads and respond quickly to user requests is crucial for maintaining high availability.

Other factors like physical isolation, ability to patch, attack surface, and extensible authentication are important for security and maintenance but are not primary considerations for high availability.

Therefore, the correct answers are:

- A. Ease of recovery
 - D. Responsiveness
- upvoted 25 times

MarDog Highly Voted 10 months, 2 weeks ago

- A. Ease of Recovery and C. Physical Isolation
- upvoted 7 times

slackbot Most Recent 3 months ago

Selected Answer: AC

bad wording again. is this about high availability/resiliency or redundancy?

A suggests redundancy

C suggests redundancy

D suggests resilience

Question is asking about resiliency

so, it looks like the only reasonable answer is D. Both A and C should not be correct.

so, it would seem they are asking about redundancy, not resiliency in which case we get A and C

good job again compTIA

upvoted 2 times

jaylom 3 months, 1 week ago

Selected Answer: AC

The Answer should be A: Ease of recovery and C: Physical isolation.

-I know that the answer says A and D, but think about it, responsiveness is built upon a working system, and If a single point of failure occurs, then responsiveness will mean nothing.

The question asks what "must" be considered for availability, so A: Ease of recovery minimizes downtime and increases availability, and C: Physical isolation eliminates a single point of failure and provides availability.

-Even though responsiveness is also important, it is still built upon a working system, and if a single point of failure occurs, then responsiveness will not matter.

upvoted 3 times

🗳️ 👤 **tsummey** 4 months, 1 week ago

Selected Answer: AC

High availability focuses on redundancy, fault tolerance, and recovery mechanisms rather than just speed. The more correct answers remain Ease of recovery and Physical isolation, as they directly impact the ability of a network to remain operational despite failures.

upvoted 2 times

🗳️ 👤 **CZAR88** 5 months, 2 weeks ago

Selected Answer: AE

ttack surface

- How many ways into your home?
 - Doors, windows, basements
- Everything can be a vulnerability
 - Application code
 - Open ports
- Authentication process
 - Human error
- Minimize the surface
 - Audit the code
 - Block ports on the firewall
 - Monitor network traffic in real-time

upvoted 2 times

🗳️ 👤 **KSoLL** 4 months, 1 week ago

This Question is talking about the CIA Triad. Since its talking about About "(A)Availability" - The answer is A&D. Attack Surface is more in the (I)Integrity since you talk about open ports, Application code, Block ports on firewalls, etc.., Those are all related to making sure the integrity of our data is safe to transfer. Availability ensures that information and resources are accessible and functional when needed by authorized users. Just remember the 5 nine rules (99.999%) Systems will always have downtime and companies would like to have less down time as less as possible. Ease of recovery and the Responsiveness will help ensure this.

upvoted 3 times

🗳️ 👤 **MaxiPrince** 6 months, 2 weeks ago

Selected Answer: AD

A & D Ease of recovery/Responsiveness

upvoted 1 times

🗳️ 👤 **3dk1** 7 months, 3 weeks ago

Selected Answer: AD

Prof Messer's video explains it well.

upvoted 1 times

🗳️ 👤 **Bito808** 8 months, 1 week ago

Think of doing an online purchase. Which would minimally affect your transaction? Which shortens system downtime?

upvoted 1 times

🗳️ 👤 **3330278_111** 9 months ago

Selected Answer: AC

I was pretty confident about AD at first.

However, availability focuses on minimizing downtime and ensuring continuous operation. Physical Isolation provides redundancy and protection against failures, which is a fundamental aspect of high availability, ensuring that issues in one part of the network do not impact the overall availability of services. Physical isolation helps prevent a single point of failure from affecting the entire network.

While responsiveness is important for performance, it is not specifically a high-availability consideration. High availability focuses on ensuring that systems remain operational and recover quickly from failures, rather than optimizing performance.

upvoted 2 times

🗨️ 👤 **NONS3c** 9 months ago

Selected Answer: AD

A. Ease of recovery

High availability requires systems to recover quickly and easily in case of failure. This ensures minimal downtime and fast restoration of services.

D. Responsiveness

A high-availability network must respond quickly to changes or failures to maintain uptime. This includes quick failover mechanisms and the ability to rapidly address network issues.

upvoted 3 times

🗨️ 👤 **cri88** 10 months, 1 week ago

Selected Answer: AC

When designing a high-availability network, two key considerations are:

Ease of recovery: This refers to the network's ability to quickly and efficiently recover from failures or disruptions. Having redundant components, failover mechanisms, and well-defined recovery procedures in place is crucial.

Physical isolation: Ensuring that critical components are physically separated helps prevent single points of failure and enhances network resilience.

upvoted 2 times

🗨️ 👤 **a4e15bd** 10 months, 2 weeks ago

A & D

A. Ease of Recovery, ensure quick restoration after a failure.

D. Responsiveness, ensures the network can handle the load and maintain availability

upvoted 1 times

🗨️ 👤 **dbrowndiver** 11 months ago

Selected Answer: AD

High-availability networks require robust recovery processes to ensure that services can be restored rapidly after any failure, minimizing the impact on users and maintaining service continuity.

Responsiveness is crucial for a high-availability network, as it ensures that the network can handle unexpected changes and continue delivering services efficiently, even under stress or during failures.

upvoted 1 times

🗨️ 👤 **ILOVECOMPTIA** 11 months, 1 week ago

Ease of recovery = HA

Ability to patch = security

Physical isolation = HA (because nobody can touch it)

Responsiveness = Performance

Attack surface = Security

Extensible authentication = Security

upvoted 4 times

🗨️ 👤 **uday1985** 10 months, 1 week ago

Physical isolation doesn't guarantee availability, it restricts access.

upvoted 2 times

🗨️ 👤 **cdsu** 1 year ago

Why not A and E?

It's a tough question.

upvoted 2 times

🗨️ 👤 **f26ddcd** 1 year ago

Selected Answer: AD

A. Ease of recovery

D. Responsiveness

upvoted 1 times

A technician needs to apply a high-priority patch to a production system. Which of the following steps should be taken first?

- A. Air gap the system.
- B. Move the system to a different network segment.
- C. Create a change control request.
- D. Apply the patch to the system.

Correct Answer: C

Community vote distribution

C (100%)

Abcd123321 Highly Voted 1 year, 1 month ago

Selected Answer: C

Change Control is the process that management uses to identify, document and authorize changes to an IT environment. It minimizes the likelihood of disruptions, unauthorized alterations and errors. The change control procedures should be designed with the size and complexity of the environment in mind.

upvoted 13 times

3037402 Most Recent 4 months, 3 weeks ago

Selected Answer: C

create a change control request

upvoted 1 times

9149f41 4 months, 3 weeks ago

Selected Answer: C

B, moving the system to a different network segment is ideal for the minimal disruption in the production. To do that, you need a Change Control Request first, as it is usually mandatory for most of the company, and it may have involve health, finance, skill work force, etc

upvoted 1 times

MaxiPrince 6 months, 2 weeks ago

Selected Answer: C

Create a change control request.

upvoted 1 times

ProudFather 6 months, 4 weeks ago

Selected Answer: C

C. Create a change control request.

Before applying any changes to a production system, especially a high-priority patch, it's crucial to follow established change management procedures. This involves creating a change control request that outlines the proposed change, its impact, and the necessary steps to implement it. This step helps ensure that the change is properly authorized, documented, and coordinated with other teams.

Once the change control request is approved, the technician can proceed with the other steps, such as testing the patch in a controlled environment and then deploying it to the production system.

upvoted 3 times

dbrowndiver 11 months ago

Selected Answer: C

o Creating a change control request is a standard best practice for managing changes in a production environment. It ensures that the patch is applied systematically and with the necessary oversight, reducing the chance of errors or unforeseen issues.

upvoted 3 times

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

- A. To gather IoCs for the investigation
- B. To discover which systems have been affected
- C. To eradicate any trace of malware on the network
- D. To prevent future incidents of the same nature

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **MaxiPrince** 6 months, 2 weeks ago

Selected Answer: D

To prevent future incidents of the same nature
upvoted 1 times

🗳️ 👤 **Oca8ee9** 6 months, 3 weeks ago

Selected Answer: D

Without RCA, we can't prevent repeats.
upvoted 1 times

🗳️ 👤 **braveheart22** 7 months, 3 weeks ago

Selected Answer: D

Root cause analysis (RCA) is an important part of incident response because its primary goal is to identify the underlying cause of an incident so that measures can be taken to prevent similar incidents from occurring in the future.
upvoted 2 times

🗳️ 👤 **dbrowndiver** 11 months ago

Selected Answer: D

Root cause analysis is fundamental to preventing future incidents by addressing the underlying issues rather than merely treating the symptoms. This approach helps build a more resilient security infrastructure. Also, Conducting RCA contributes to continuous improvement in security practices, policies, and technologies, enhancing the organization's overall security posture.
upvoted 3 times

🗳️ 👤 **f71cbb0** 1 year, 1 month ago

Selected Answer: D

that's the purpose of root cause
upvoted 1 times

🗳️ 👤 **Abcd123321** 1 year, 1 month ago

Selected Answer: D

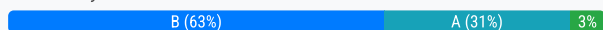
Root cause analysis
■ Identifies the incident's source and how to prevent it in the future
upvoted 4 times

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

- A. Fines
- B. Audit findings
- C. Sanctions
- D. Reputation damage

Correct Answer: B

Community vote distribution



Etc_Shadow28000 Highly Voted 9 months ago

Selected Answer: B

B. Audit findings

While fines, sanctions, and reputation damage can be potential consequences of failing to meet PCI DSS compliance, the most immediate and likely outcome of failing an internal PCI DSS compliance assessment is the generation of audit findings. These findings will detail the areas of non-compliance and typically result in the organization needing to take corrective actions to address the identified issues. If the findings are not addressed, this could lead to further consequences such as fines, sanctions, or reputation damage.

Therefore, the correct answer is:

B. Audit findings
upvoted 18 times

Zoots_1 7 months, 3 weeks ago

B. Audit findings

would be correct if this was done externally by a third party, however internal audits produce findings right away, meaning that the organization has immediate access to these results. For that reason, audit findings can indeed seem less impactful than fines if we're focusing on the actual consequences of failing to meet PCI DSS requirements.

Correct answer is A. Fines
upvoted 4 times

kambam 6 months, 3 weeks ago

Internal is keyword here. You are not going to report yourself and cause yourself to be fined. External audit would have to report and therefore fines would be more applicable. Audit findings is correct.
upvoted 9 times

319b362 Most Recent 1 week, 4 days ago

Selected Answer: A

Audit Findings vs. Fines

Audit findings are more commonly the output of a QSA-led audit, not necessarily the primary consequence of failing an internal self-assessment.

Fines, on the other hand, can be imposed even without a breach, just for non-compliance, especially for Level 1 merchants or service providers (which large banks are).
upvoted 1 times

Valen2259 2 months ago

Selected Answer: B

B. Audit findings (though a really bad question/answer in reality)

Internal PCI DSS assessments are typically conducted to identify gaps before an official external audit or regulator review. Failing an internal assessment would primarily result in audit findings — documented issues that need to be addressed before the next official evaluation.

However, in reality if the report is leaked which inevitably occurs (and the worry impact of the board) would be D. Reputation damage as this would lose the public trust and impact key stakeholders.

upvoted 1 times

🗳️ 👤 **tsummey** 4 months, 1 week ago

Selected Answer: B

The answer is audit findings. The question references an "internal" compliance assessment. An internal compliance assessment is a tool used to identify and address any gaps that must be closed before the actual PCI assessment.

upvoted 1 times

🗳️ 👤 **475a567** 4 months, 1 week ago

Selected Answer: A

internal assessment, not external. can allow time to fix before a governmental audit

upvoted 2 times

🗳️ 👤 **Russell15** 4 months, 2 weeks ago

Selected Answer: B

I at first thought A: fines, as the assessment is an audit and the findings are what cause it to fail, but after you submit your configurations, UARs, etc. for the audit. If you fail they will tell you why you failed and what you need to fix it to be compliant. Failing multiple times or having a breach due to being non-compliant can result in the fines as they are not the first outcome of an audit.

upvoted 2 times

🗳️ 👤 **93bdd7c** 5 months ago

Selected Answer: A

If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. Audit findings, while important, are typically the result of an external assessment and not the direct consequence of an internal assessment. The bank must address these findings to avoid further penalties.

upvoted 3 times

🗳️ 👤 **YokuDoku** 5 months, 3 weeks ago

Selected Answer: A

Audit findings. Audit findings are the results of an external PCI DSS compliance assessment that is performed by a QSA or an approved scanning vendor (ASV). An external assessment is required for certain entities that handle a large volume of cardholder data or have a history of non-compliance. An external assessment may also be triggered by a security incident or a request from the payment card brands. Audit findings may reveal the gaps and weaknesses in the bank's security controls and recommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself.

References:

1. CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 388.
2. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: PCI DSS (5:12).
3. PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4.
4. PCI Security Standards Council, PCI DSS FAQs, questions 8-30

upvoted 3 times

🗳️ 👤 **YokuDoku** 5 months, 3 weeks ago

Selected Answer: A

If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. An internal PCI DSS compliance assessment is a self-assessment that the bank performs to evaluate its own compliance with the PCI DSS requirements. The bank must submit the results of the internal assessment to the payment card brands or their designated agents, such as acquirers or qualified security assessors (QSAs). If the internal assessment reveals that the bank is not compliant with the PCI DSS requirements, the payment card brands may impose fines on

the bank as a penalty for violating the PCI DSS contract. The amount and frequency of the fines may vary depending on the severity and duration of the non-compliance, the number and type of cardholder data compromised, and the level of cooperation and remediation from the bank. The fines can range from thousands to millions of dollars per month, and can increase over time if the non-compliance is not resolved.

upvoted 2 times

🗳️ 👤 **YokuDoku** 5 months, 3 weeks ago

Selected Answer: A

PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.

upvoted 2 times

🗳️ 👤 **EngAbood** 5 months, 4 weeks ago

Selected Answer: D

copilot said D ...:) i dont know look ok to me ..

upvoted 1 times

🗳️ 👤 **darpanne** 6 months, 2 weeks ago

Selected Answer: B

Audit findings indicate specific areas of non-compliance or gaps in security controls that need to be addressed to meet PCI DSS requirements other options are for external assessment

upvoted 1 times

🗳️ 👤 **Nuel247** 6 months, 4 weeks ago

Selected Answer: C

Sanction will

upvoted 1 times

🗳️ 👤 **1ohndc923** 7 months ago

Selected Answer: A

It's actually A (Fines) because the internal PCI DSS assessment results must be sent to the bank's payment card brands or their agents. The payment card brands will then issue a fine because again, even though it's an internal assessment, it must be submitted to the other party - hence resulting in being fined.

upvoted 3 times

🗳️ 👤 **Dimpo_Oz** 7 months ago

Selected Answer: B

The key word is internal ruling out every answer other than B

upvoted 2 times

🗳️ 👤 **Cloudboy** 7 months, 1 week ago

the answer is B audit finding, the question says "internal PCI DSS compliance assessment"

upvoted 2 times

🗳️ 👤 **Damique** 7 months, 1 week ago

Selected Answer: A

When a financial institution, such as a large bank, fails to meet PCI DSS requirements, the most immediate consequence is typically a fine.

upvoted 1 times

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

- A. Capacity planning
- B. Redundancy
- C. Geographic dispersion
- D. Tabletop exercise

Correct Answer: A

Community vote distribution

A (100%)

SHADTECH123 Highly Voted 1 year, 1 month ago

Selected Answer: A

A. Capacity planning

Explanation: Capacity planning involves determining the staffing levels needed to sustain business operations during a disruption. This ensures that the organization has sufficient human resources to maintain essential functions and minimize downtime.

upvoted 8 times

PAWarriors Most Recent 10 months, 1 week ago

Selected Answer: A

Correct answer is A.

Capacity Planning is used to ensure the right number of people with the right skills for strategic objectives.

upvoted 3 times

dbrowndiver 11 months ago

Selected Answer: A

Capacity planning is the correct answer because it involves determining the necessary staffing levels and other resources required to sustain business operations during a disruption. Capacity planning is a crucial step in ensuring that the business can continue functioning effectively even with reduced personnel or resources.

upvoted 2 times

Zach123654 11 months, 3 weeks ago

Selected Answer: A

GPT!!!

upvoted 1 times

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

- A. Data masking
- B. Encryption
- C. Geolocation policy
- D. Data sovereignty regulation

Correct Answer: C

Community vote distribution

C (100%)

Abcd123321 **Highly Voted** 1 year, 1 month ago

Selected Answer: C

What is Geolocation Protection?

Organizations may implement access control policies that restrict or allow access to certain resources based on the geographic location of users or devices. For example, they might limit access to sensitive systems only to users connecting from specific geographic regions or countries.

upvoted 8 times

HungryRightNow **Most Recent** 5 months, 4 weeks ago

Selected Answer: C

Ask Netflix how well a geolocation policy holds up to a VPN

upvoted 3 times

dbrowndiver 9 months ago

Selected Answer: C

Implementing a geolocation policy allows the company to configure the SaaS application to block access from IP addresses originating in high-risk countries. This is accomplished by using IP geolocation data to determine where a connection attempt is coming from.

Geolocation policies are effective for preventing unauthorized access based on geographic location, ensuring that sensitive documents remain secure from individuals in regions identified as high-risk.

Geolocation policies provide precise control over access based on the user's location, making them an ideal solution for preventing access from specific countries while maintaining access for authorized users in safe regions that is why it is best for this situation.

upvoted 4 times

PAWarriors 10 months, 1 week ago

Selected Answer: C

Correct answer is C.

"Documents cannot be accessed by individuals in high-risk COUNTRIES" --> Geolocation policy.

upvoted 1 times

Zach123654 11 months, 3 weeks ago

Selected Answer: C

GPT!!!!

upvoted 2 times

Which of the following is a hardware-specific vulnerability?

- A. Firmware version
- B. Buffer overflow
- C. SQL injection
- D. Cross-site scripting

Correct Answer: A

Community vote distribution

A (100%)

  **dbrowndiver** 11 months ago

Selected Answer: A

Vulnerabilities in firmware are specific to the hardware they control, as different hardware may have different firmware versions with unique vulnerabilities. For example, an outdated firmware version might have security flaws that can be exploited, affecting the hardware's security posture. Firmware vulnerabilities are intrinsically tied to the hardware on which they run, making them hardware-specific. An outdated or improperly secured firmware version can introduce vulnerabilities unique to that hardware platform.

upvoted 2 times

  **Zach123654** 11 months, 3 weeks ago

Selected Answer: A

GPT!!!

upvoted 2 times

  **SHADTECH123** 1 year, 1 month ago

Selected Answer: A

the firmware version (option A) is directly related to the hardware and represents a potential point of vulnerability that attackers could exploit. Firmware is the software that controls the basic functionality of hardware devices, and vulnerabilities in firmware can lead to security breaches. Options B, C, and D (buffer overflow, SQL injection, and cross-site scripting) are software vulnerabilities and are not inherently tied to hardware components.

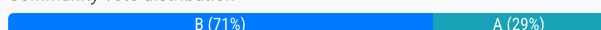
upvoted 4 times

While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

- A. Documenting the new policy in a change request and submitting the request to change management
- B. Testing the policy in a non-production environment before enabling the policy in the production network
- C. Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy
- D. Including an "allow any" policy above the "deny any" policy

Correct Answer: B

Community vote distribution



Exemplary Highly Voted 8 months, 3 weeks ago

Frankly it should be both A and B. Submitting it to change management does not prevent the issue if it isn't caught by change management, and testing it in non-prod would but also shouldn't be done without a request to change management.

It's a different question than the previous one regarding change management: Yes the technician SHOULD put in a change management request first, but that's not the question, the question is what would prevent it and the change management request does not prevent an issue, rather it lets everyone know what is happening and provides a backout plan if issues come up. That still does not PREVENT the issue though so /shrug
upvoted 18 times

SHADTECH123 Highly Voted 1 year, 1 month ago

Selected Answer: B

Testing the policy in a non-production environment allows for the identification and resolution of any unforeseen issues, such as servers becoming unreachable, before implementing the policy in the production network. This ensures that any potential impact on business operations is minimized.
upvoted 15 times

slackbot Most Recent 3 months ago

Selected Answer: A

you got this wrong. change management is not about documenting, it is about evaluating the request. if properly reviewed - it will not be allowed. and we are not talking about who does their work well and not - we cannot speculate if change management fails and this is approved. change management (A) should be correct
upvoted 1 times

MarysSon 3 months, 1 week ago

Selected Answer: B

B is the best answer. A change request can be submitted and approved, but problems will arise if the approved change is not applied correctly. Testing the change in a non-production environment will reveal errors before they can affect production.
upvoted 1 times

prabh1251 3 months, 1 week ago

Selected Answer: B

After successful testing and change approval, apply the policy in the production environment.
upvoted 1 times

Andyhung1303 4 months, 3 weeks ago

Selected Answer: A

Maybe i guess
upvoted 1 times

TECHBOSS 5 months, 2 weeks ago

Selected Answer: B

Answer: B
Procedurally "A" should and needs to occur first, However those 2 steps by themselves won't prevent this Even though those changes will still have to

be tested in a non-production environment. Even if the CAB approves the request, ONLY seeing it in action will let anyone know that it will interfere with servers. Testing is the ACTION that will prevent it.

upvoted 1 times

🗨️ 👤 **darpanne** 6 months, 2 weeks ago

Selected Answer: B

Testing the policy in a non-production environment allows the technician to identify and fix any unintended consequences before implementing the rule in the production network. This ensures the servers and critical services remain reachable while maintaining security.

upvoted 1 times

🗨️ 👤 **MaxiPrince** 6 months, 2 weeks ago

Selected Answer: B

. Testing the policy in a non-production environment before enabling the policy in the production network

upvoted 1 times

🗨️ 👤 **MaxiPrince** 6 months, 4 weeks ago

Selected Answer: B

Test policy in no prod environment

upvoted 1 times

🗨️ 👤 **43a41d4** 7 months ago

Selected Answer: B

Since the question mentions that the technician has already updates the policy, we can assume that he got approval first to implement the solution. But, for a good technician to perform well and avoid any issues, he should test the changes in a non-production environment. Both questions A and B are good answers, but B est is the best one in this case.

upvoted 1 times

🗨️ 👤 **3dk1** 7 months, 3 weeks ago

Selected Answer: A

B is something that should have been done. HOWEVER, if we documented the new change and submitted a change request this issue could have been prevented as well.

upvoted 1 times

🗨️ 👤 **Bito808** 8 months, 1 week ago

Selected Answer: A

The answer is "A"! You will get fired if you did not put in a change request before testing or implementing anything! It needs to be documented and approved FIRST! This will determine if you need equipment, resources, special access, or if there's even budget!

upvoted 2 times

🗨️ 👤 **Bito808** 8 months, 1 week ago

The answer is "A"! You will get fired if you did not put in a change request before testing or implementing anything! It needs to be documented and approved FIRST! This will determine if you need equipment, resources, special access, or if there's even budget!

upvoted 1 times

🗨️ 👤 **User92** 9 months ago

Selected Answer: A

Should be A, check Question #30

upvoted 1 times

🗨️ 👤 **User92** 9 months ago

Selected Answer: A

Change Management Processes: Schedule maintenance windows, Thorough backout plans, Consistent "testing" post-implementation

upvoted 2 times

🗨️ 👤 **Gigz_77** 9 months ago

Selected Answer: A

A. Documenting the new policy in a change request and submitting the request to change management

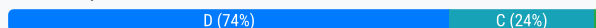
upvoted 1 times

An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?

- A. Real-time recovery
- B. Hot
- C. Cold
- D. Warm

Correct Answer: D

Community vote distribution



Abcd123321 Highly Voted 1 year, 1 month ago

Selected Answer: D

Warm Sites

- Not fully equipped, but fundamentals in place
- Can be up and running within a few days
- Cheaper than hot sites but with a slight delay

Cold Sites

- Fewer facilities than warm sites
- May be just an empty building, ready in 1-2 months
- Cost-effective but adds more recovery time

upvoted 23 times

SHADTECH123 Highly Voted 1 year, 1 month ago

Selected Answer: D

A warm site offers a balance between cost-effectiveness and recovery time objectives (RTO) and recovery point objectives (RPO). It typically has some pre-installed infrastructure and data backups but may require additional configuration and data restoration before becoming fully operational. Given the RTO and RPO values of around two days, a warm site provides a reasonable compromise between cost and recovery capability.

upvoted 10 times

319b362 Most Recent 1 week, 4 days ago

Selected Answer: C

Explanation:

A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster. Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 387

upvoted 1 times

Jforged 2 weeks, 1 day ago

Selected Answer: C

A cold site is the most cost-effective option because it provides the necessary infrastructure but lacks pre-configured hardware, software, or active data replication. Given the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of around two days, a cold site is suitable since it allows for recovery within that timeframe while keeping costs low.

upvoted 1 times

6d565fd 4 weeks, 1 day ago

Selected Answer: C

References: CompTIA Security+ SY0-701 Certification Study Guide, page 387; Backup Types -SY0-601

CompTIA Security+ : 2.5, video at 4:50

upvoted 1 times

🗨️ 👤 **Welderboy** 1 month, 2 weeks ago

Selected Answer: C

RTO and RPO values around two days are generally associated with a cold site. A cold site is a backup facility that typically has minimal or no hardware equipment installed, making it cost-effective but requiring time to set up after a disaster. In contrast, hot sites have fully configured hardware and software, enabling faster recovery with lower RTOs and RPOs. Warm sites offer a middle ground with some hardware and software pre-installed.

upvoted 1 times

🗨️ 👤 **Valen2259** 2 months ago

Selected Answer: D

D. Warm Site:

Again another ambiguous Q/A.. and could be cold site, though Cold sites have only basic infrastructure, space, power and cooling..you need servers/networking to restore to the RPO/RTO hence it has to WARM

Site Type Setup Readiness Data Freshness RTO Cost

Hot Site Fully operational Real-time / near-real-time Minutes to hours Very High

Warm Site Partial setup Hours to days old Hours to a day Moderate

Cold Site Bare minimum None (must be restored) Days to weeks

upvoted 1 times

🗨️ 👤 **8f23125** 2 months, 1 week ago

Selected Answer: C

With an RTO and RPO around 2 days, and cost-benefit as a priority, a cold site is the best fit.

upvoted 2 times

🗨️ 👤 **tsummey** 4 months, 1 week ago

Selected Answer: D

In my experience, a cold site will rarely, if ever, have a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) value of 2 days.

upvoted 2 times

🗨️ 👤 **Turtle** 4 months, 1 week ago

Selected Answer: C

If you need a balance between cost and recovery speed, a warm site is a good option. If cost is the main concern and downtime of a few days is acceptable, a cold site is better.

upvoted 1 times

🗨️ 👤 **pindinga1** 5 months, 2 weeks ago

Selected Answer: D

Cold Sites

- Fewer facilities than warm sites
- May be just an empty building, ready in 1-2 months
- Cost-effective but adds more recovery time

upvoted 2 times

🗨️ 👤 **ramzie** 5 months, 3 weeks ago

Selected Answer: D

warm site

upvoted 1 times

🗨️ 👤 **musaabokisec** 5 months, 4 weeks ago

Selected Answer: C

A cold site is the best option for the organization's requirements, balancing low cost with an acceptable two-day RTO and RPO, making it the most cost-effective solution.

upvoted 2 times

🗨️ 👤 **ProudFather** 6 months ago

Selected Answer: A

A cold site is the most cost-effective option for a backup data center because it is essentially an empty facility with basic utilities (e.g., power, cooling, and connectivity) but no active hardware or pre-installed systems. Since the organization has an RTO (Recovery Time Objective) and RPO

(Recovery Point Objective) of around two days, a cold site is suitable as it provides enough time to set up and restore operations while keeping costs low.

upvoted 1 times

🗨️ 👤 **Benny_On** 6 months, 3 weeks ago

Selected Answer: C

I think C is best answer. You can see line "cost-benefit as the PRIMARY requirement and RTO and RPO" on question.

upvoted 1 times

🗨️ 👤 **Damique** 7 months, 1 week ago

Selected Answer: C

A cold site is the most cost-effective option because it provides basic infrastructure, such as a physical space with power, cooling, and network connectivity, but it does not have active IT systems or pre-configured data.

upvoted 2 times

🗨️ 👤 **sireym1** 7 months, 1 week ago

Selected Answer: C

Cold sites typically require time to set up the necessary systems, which aligns with the two-day RTO/RPO requirements. They are less expensive compared to hot or warm sites because they do not have pre-installed equipment or active data replication.

A cold site provides the best balance between cost and the organization's relatively long RTO/RPO requirements (two days).

A warm site has some infrastructure pre-configured and can be brought online faster than a cold site, but it is more expensive. This would be suitable for a scenario where RTO and RPO are shorter than two days, but it's overkill for this case.

upvoted 2 times

A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following best describes this policy?

- A. Enumeration
- B. Sanitization
- C. Destruction
- D. Inventory

Correct Answer: B

Community vote distribution

B (100%)

  **barracouto** Highly Voted  11 months, 2 weeks ago

securely wiped ... clorox wipes.... clorox wipes clean and sanitize... B Sanitization
upvoted 21 times

  **SHADTECH123** Highly Voted  1 year, 1 month ago

Selected Answer: B

B. Sanitization

Explanation:


Sanitization involves securely erasing data from hard drives to ensure that it cannot be recovered or accessed by unauthorized individuals. This process is essential before decommissioned systems are sent to recycling to protect sensitive information. Enumeration, destruction, and inventory do not specifically refer to the secure erasure of data from hard drives.

upvoted 9 times

  **csecurity** Most Recent  1 month, 2 weeks ago

Selected Answer: B

Yes sanitization,
upvoted 1 times

  **MaxiPrince** 6 months, 4 weeks ago

Selected Answer: B

.Sanitation
upvoted 1 times


  **SHADTECH123** 1 year, 1 month ago

B. Sanitization

Explanation:

Sanitization involves securely erasing data from hard drives to ensure that it cannot be recovered or accessed by unauthorized individuals. This process is essential before decommissioned systems are sent to recycling to protect sensitive information. Enumeration, destruction, and inventory do not specifically refer to the secure erasure of data from hard drives.

upvoted 2 times

  **Jimmy1017** 1 year, 1 month ago

Selected Answer: B

Sanitation makes the most sense if sending it to a recycling company afterwards.
upvoted 2 times

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

- A. Private
- B. Critical
- C. Sensitive
- D. Public

Correct Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **Osechabelo** Highly Voted 1 year, 1 month ago

C. Sensitive

Sensitive - Intellectual property, PII, PHI

- Confidential - Very sensitive, must be approved to view
 - Public / Unclassified - No restrictions on viewing the data
 - Private / Classified / Restricted
 - Restricted access, may require an NDA
 - Critical - Data should always be available
- upvoted 24 times

🗳️ 👤 **HungryRightNow** Most Recent 5 months, 4 weeks ago

Selected Answer: C

Sensitive data = Individual's important information (PII)

Critical data = The company's important information (Trade secrets)

upvoted 4 times

🗳️ 👤 **jade290** 8 months, 3 weeks ago

Selected Answer: C

C is correct.

Sensitive

* Information that, if disclosed or compromised, could cause significant harm to individuals, organizations, or national security.

Examples:

- Personally identifiable information (PII) such as social security numbers, health records, financial information
- Trade secrets, intellectual property, government classified information

upvoted 1 times

🗳️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: C

C. Sensitive -phi

upvoted 2 times

🗳️ 👤 **e5c1bb5** 1 year, 1 month ago

Selected Answer: C

Sensitive - Intellectual property, PII, PHI

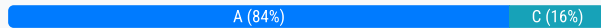
upvoted 2 times

A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

- A. Local data protection regulations
- B. Risks from hackers residing in other countries
- C. Impacts to existing contractual obligations
- D. Time zone differences in log correlation

Correct Answer: A

Community vote distribution



Osechabelo Highly Voted 1 year, 1 month ago

A. Local data protection regulations
Laws may prohibit where data is stored
– GDPR (General Data Protection Regulation)
– Data collected on EU citizens must be stored in the EU
upvoted 13 times

barracouto Highly Voted 11 months, 2 weeks ago

Selected Answer: A

When a U.S.-based cloud-hosting provider is considering expanding its data centers to new international locations, the first thing they should consider is local data protection regulations. These regulations govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries have different regulations, such as the GDPR in the EU or PIPEDA in Canada. Compliance with these regulations is crucial to avoid legal penalties, fines, or reputational damage
upvoted 12 times

Dimpo_Oz Most Recent 7 months ago

Selected Answer: A

Expanding not relocating so existing contracts are not affected
upvoted 4 times

Bito808 8 months, 1 week ago

From reading the discussion, I think in a hierarchy, the Local Data Protection Regulations would be on top. It would then determine how the contract is written to adhere to legal restrictions. That's my reasoning from working with legal departments.
upvoted 1 times

buffalobill 9 months, 2 weeks ago

Selected Answer: A

Existing contracts cannot be impacted by adding a new DC... customers dont have to use it
upvoted 1 times

Twphill 9 months, 3 weeks ago

Selected Answer: C

Your existing contractual obligations on how your client's data is stored should be considered first.
upvoted 1 times

ServerBrain 10 months ago

Selected Answer: A

Local data protection regulations in those locations that the provider wants to expand services to.
upvoted 2 times

tamdod 10 months, 2 weeks ago

What is GPT? -
upvoted 1 times

Dr_Network 11 months, 3 weeks ago

Selected Answer: C

C because its the existing Contract obligations that need to be reviewed to see if there is any agreement for data sovereignty you need to adhere too. Local Data Protection regulations are something to consider but are irrelevant if you don't have contract obligations to adhere to them (example you have contracts that mention storing HIPPA or financial data)

upvoted 3 times

  **Zach123654** 11 months, 3 weeks ago

Selected Answer: A

GPT!!!

upvoted 3 times

Which of the following would be the best way to block unknown programs from executing?

- A. Access control list
- B. Application allow list
- C. Host-based firewall
- D. DLP solution

Correct Answer: B

Community vote distribution

B (100%)

 **123456789User** Highly Voted 1 year ago

Selected Answer: B

Application allow list only allows trusted applications or files to run
upvoted 8 times

 **4320d25** Highly Voted 9 months ago

Selected Answer: B

An application allow list (also called whitelisting) restricts a system to only allow specific, pre-approved programs to run. Any program not on the allow list will be blocked from executing, making it highly effective at preventing unknown or unauthorized software from running on a system.
upvoted 6 times

 **Zach123654** Most Recent 11 months, 3 weeks ago

Selected Answer: B

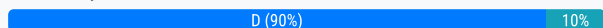
GPT!!!
upvoted 3 times

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering. Which of the following teams will conduct this assessment activity?

- A. White
- B. Purple
- C. Blue
- D. Red

Correct Answer: D

Community vote distribution



🗳️ 👤 **Jimmy1017** Highly Voted 1 year, 1 month ago

Selected Answer: D

D because red teams are offensive and blue teams are defensive
upvoted 11 times

🗳️ 👤 **Abcd123321** Highly Voted 1 year, 1 month ago

Selected Answer: D

Offensive Penetration Testing

- Known as "red teaming"
 - Actively seeks vulnerabilities and attempts to exploit them, like a real cyber attack
 - Helps uncover and report vulnerabilities to improve security
 - Can simulate real-world attacks and gain support for cybersecurity investments
- upvoted 9 times

🗳️ 👤 **vm_mscs** Most Recent 4 months, 4 weeks ago

Selected Answer: D

The company hired someone from outside. Pen testing is offensive, so red team.
upvoted 1 times

🗳️ 👤 **s1_move** 7 months, 2 weeks ago

Correct Answer: D. Red Team (Offensive - key word)

- A. White team ensures security testing is conducted within legal and ethical boundaries
 - B. Purple team combines aspects of red and blue teams
 - C. Blue team is defensive
- upvoted 4 times

🗳️ 👤 **PAWarriors** 10 months ago

Selected Answer: D

Correct answer is D.

Red team conducts offensive attacks, while the blue team detects and responds. Also, purple teaming combines elements of offensive and defensive testing.
upvoted 2 times

🗳️ 👤 **dbrowndiver** 11 months ago



Selected Answer: B

Authenticity Verification: Code signing assures users and developers that the code is genuine and originates from a legitimate source. If the code is altered, the digital signature becomes invalid, alerting users to potential tampering.
upvoted 4 times

🗳️ 👤 **barracouto** 11 months, 2 weeks ago

Selected Answer: D

offensive security... im offended.. im mad.. so mad my face is red... D. Red
upvoted 6 times

  **User1208** 10 months, 2 weeks ago

If you got really frustrated, you face gonna turn from red to purple...lol just kidding, also agree it should be D: Red
upvoted 3 times

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

- A. Testing input validation on the user input fields
- B. Performing code signing on company-developed software
- C. Performing static code analysis on the software
- D. Ensuring secure cookies are use

Correct Answer: B

Community vote distribution

B (100%)

SHADTECH123 Highly Voted 1 year, 1 month ago

Selected Answer: B

Code signing involves applying a digital signature to software, verifying the identity of the developer and ensuring that the code has not been altered or tampered with since it was signed. This process provides assurance of the authenticity and integrity of the software. Testing input validation, performing static code analysis, and ensuring secure cookies are important security practices but do not specifically address the need to verify the authenticity of the code.

upvoted 10 times

MaxiPrince Most Recent 6 months, 2 weeks ago

Selected Answer: B

Performing code signing on company-developed software

upvoted 1 times

PAWarriors 10 months ago

Selected Answer: B

B.

Code signing utilizes digital signatures to verify code authenticity and confirms the software author's identity and integrity

upvoted 1 times

dbrowndiver 11 months ago

Selected Answer: B

Authenticity Verification: Code signing assures users and developers that the code is genuine and originates from a legitimate source. If the code is altered, the digital signature becomes invalid, alerting users to potential tampering.

upvoted 1 times

Osechabelo 1 year, 1 month ago

B. Performing code signing on company-developed software

upvoted 1 times

Which of the following can be used to identify potential attacker activities without affecting production servers?

- A. Honeypot
- B. Video surveillance
- C. Zero Trust
- D. Geofencing

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **123456789User** Highly Voted 👍 1 year ago

Selected Answer: A

Honeypot - a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts on systems.
upvoted 11 times

🗳️ 👤 **Osechabelo** Highly Voted 👍 1 year, 1 month ago

A. Honeypot

• Attract the bad guys - And trap them there

upvoted 5 times

🗳️ 👤 **e43d250** Most Recent ⌚ 5 months, 2 weeks ago

Selected Answer: A

A. Honeypot

upvoted 1 times

🗳️ 👤 **Shadyshinies** 10 months, 2 weeks ago

Would that not require servers and resources to do a honeypot which then interrupts server production by extension. I feel like b would make sense since it wouldn't affect servers and can detect attackers. Idk though

upvoted 2 times

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?


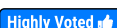
- A. Analysis
- B. Lessons learned
- C. Detection
- D. Containment

Correct Answer: A

Community vote distribution

A (82%)

B (18%)

  **hasquaati**  1 year, 1 month ago

Selected Answer: A

Answer is A because you need to conduct an analysis to find out what the source of the incident was.

upvoted 12 times

  **darpanne**  6 months, 2 weeks ago

Selected Answer: A

In the Analysis phase, the team examines logs, network traffic, artifacts, and other relevant data to determine:

The root cause of the incident

How the incident occurred

The systems and data affected

Indicators of Compromise (IOCs)

Possible paths for remediation and prevention

upvoted 6 times

  **89fdeb4**  6 months, 2 weeks ago

Selected Answer: A

It can't be "Lessons learned" because we're still investigating. "During an Investigation"



upvoted 6 times

  **racer99_** 7 months, 1 week ago

Selected Answer: B

This q tripped me up for a long time until i looked up the IRP stages. If you look it up you'll see that "Lessons learned" includes finding out what the source of the incident was. There is no such "analysis" stage in IRP. Correct answer here is B

upvoted 1 times

  **sireyml** 7 months, 1 week ago



Selected Answer: A

Emphasis on "During an investigation".

During an incident response, analysis refers to the process of investigating and understanding the source of the incident, including determining how the incident occurred, identifying the root cause, and gathering the necessary evidence to support further actions. This is a key part of incident response where the team works to fully comprehend the nature of the incident and its origins.

"Lessons learned" is an activity that takes place after the incident has been resolved.

upvoted 2 times

  **chalaka** 7 months, 3 weeks ago

Selected Answer: A

A. Analysis

In the incident response process, analysis involves examining evidence and data to determine the cause and source of an incident. This phase helps the incident response team understand how the incident occurred, who or what caused it, and the extent of its impact.


upvoted 1 times

  **3dk1** 8 months, 1 week ago

Going with A.

The problem with B is that it is post incident, this question is "During an investigation". I agree that you will investigate the root cause in the Lessons Learned portion as well, but this is at the END, not during.

upvoted 2 times

  **nyyankee718** 8 months, 1 week ago

It said "During an investigation" NOT during the incident so B

upvoted 1 times

  **c7b3ff0** 8 months, 2 weeks ago

Selected Answer: B

Lessons Learned - Review severe incidents to determine the root cause, whether they were avoidable, and how to avoid them in the future.

Analysis - determine if an incident has actually occurred and assign it a priority level.

upvoted 2 times

  **deejay2** 8 months, 2 weeks ago

I think lessons learned is the right answer. Lesson's learned deals with post recovery(not during the investigation) and meets with everyone that was affected by the incident to get feedback and learn ways to improve to prevent this from happening next time. Analysis deals with the incident while the incident is happening, not after.

upvoted 1 times

  **nap61** 8 months, 3 weeks ago

Selected Answer: B

From CompTIA Security Guide

Analysis - After the detection process reports one or more indicators, in the analysis process, the first responder investigates the data to determine whether a genuine incident has been identified and what level of priority it should be assigned. Conversely, the report might be categorized as a false positive and dismissed.

Lessons Learned - The lessons learned process reviews severe security incidents to determine their root cause, whether they were avoidable, and how to avoid them in the future. The lessons learned process should invoke root cause analysis or the effort to determine how the incident was able to occur. A lot of models have been developed to structure root cause analysis. One is the "Five Whys" model. This starts with a statement of the problem and then poses successive "Why" questions to drill down to root causes.

So, to understand the source of incident, or root cause, in in LESSONS LEARNED.

upvoted 4 times

  **cyoncon** 9 months ago

B, post incident

upvoted 1 times

  **Sol_tyty** 10 months, 2 weeks ago

Selected Answer: A

GPT!!!

upvoted 1 times

  **Etc_Shadow28000** 1 year ago

Selected Answer: A

A. Analysis

During an investigation, the incident response team engages in the process of understanding the source of an incident through analysis. This involves examining the data and evidence collected to determine how the incident occurred, its origin, and its impact.

Therefore, the correct answer is:

A. Analysis

upvoted 4 times

A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

- A. Conduct an audit.
- B. Initiate a penetration test.
- C. Rescan the network.
- D. Submit a report.

Correct Answer: C

Community vote distribution

C (100%)

SHADTECH123 Highly Voted 1 year, 1 month ago

Selected Answer: C

Rescanning the network is essential to verify that the previously identified vulnerabilities have been successfully remediated and to ensure that no new vulnerabilities have been introduced. This step confirms the effectiveness of the remediation efforts before moving on to further actions such as audits, penetration tests, or reporting.

upvoted 12 times

hasquaati Highly Voted 1 year, 1 month ago

Selected Answer: C

Answer is C. Rescan the network to find if the remediation is working and is not causing other vulnerabilities.

upvoted 6 times

8f23125 Most Recent 2 months, 1 week ago

Selected Answer: C

• C. Rescan the network. (To ensure no more vulnerabilities are left behind after remediation)

upvoted 1 times

3dk1 8 months, 1 week ago

C. Rescan the network

upvoted 1 times

KAljunn 9 months, 4 weeks ago

Selected Answer: C

The next step should be C. Rescan the network.

After vulnerabilities are remediated, a rescan is essential to verify that the identified vulnerabilities have been properly addressed and no new vulnerabilities have emerged as a result of the remediation efforts. This helps ensure the network is now secure and that the remediations were effective.

upvoted 1 times

Sol_tyty 10 months, 2 weeks ago

Selected Answer: C

GPT!!!

upvoted 1 times

CookieChip 1 year ago

Rescan the network, and once all is clear, that's the time you can Conduct an audit.

upvoted 2 times

Osechabelo 1 year, 1 month ago



A. Conduct an audit.

• Audit

– Check remediated systems to ensure the patch

was successfully deployed (professor-messer-sy0-701-comptia-security-plus-course-notes-v106)

upvoted 5 times

  **8f23125** 2 months, 1 week ago

Validation of remediation

- The vulnerability is now patched
 - Does the patch really stop the exploit?
 - Did you patch all vulnerable systems?
- Rescanning
 - Perform an extensive vulnerability scan

upvoted 1 times

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device. Which of the following best describes the user's activity?

- A. Penetration testing
- B. Phishing campaign
- C. External audit
- D. Insider threat

Correct Answer: D

Community vote distribution

D (100%)

 **Dlove** Highly Voted 11 months, 1 week ago

Selected Answer: D

D. Insider Threat

An insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.
upvoted 8 times

 **Sol_tyty** Most Recent 10 months, 2 weeks ago

Selected Answer: D

GPT!!!

upvoted 1 times

Which of the following allows for the attribution of messages to individuals?

- A. Adaptive identity
- B. Non-repudiation
- C. Authentication
- D. Access logs

Correct Answer: B

Community vote distribution

B (93%)

8%

 **Yoez** Highly Voted 1 year, 1 month ago

I can't understand the sentence. Bad question
upvoted 57 times


 **uday1985** 10 months, 2 weeks ago

Message attribute associated with a person!!!! its verifying that a specific individual sent the message! this is non-repudiation !! Ez lemon squeezy
upvoted 10 times

 **123456789User** Highly Voted 1 year ago

Selected Answer: B

Non-repudiation - provides proof of the origin. Prevents individuals from denying involvement in sending the message.
upvoted 14 times

 **_thelastturtle** Most Recent 4 months, 3 weeks ago


Selected Answer: D

Didnt understand the question
upvoted 3 times

 **braveheart22** 7 months, 3 weeks ago

Selected Answer: B

The correct answer is B. Non-repudiation.
Non-repudiation refers to the ability to ensure that a person or entity cannot deny having sent or received a message. It provides a way to attribute actions or messages to specific individuals, typically through mechanisms such as digital signatures or secure logging. This guarantees that the sender of the message cannot later claim they did not send it, offering legal and security assurances.
upvoted 4 times

 **KelvinYau** 7 months, 4 weeks ago

Selected Answer: B

i don't understand this question.
upvoted 2 times

 **deejay2** 8 months ago

Nevermind, attribution means acknowledgement. So, B is right.
upvoted 1 times

 **deejay2** 8 months, 2 weeks ago

If attribution means source, the answer is C.
upvoted 1 times

 **dbrowndiver** 9 months ago

Selected Answer: B

Attribution of Messages: By implementing non-repudiation, organizations can confirm the source of a message or transaction. This is essential for legal and security purposes, as it prevents individuals from denying their actions or communications.
Digital Signatures: Commonly used in emails and transactions, digital signatures are a key component of non-repudiation, as they uniquely identify the sender and confirm the message's origin.

Why it is the best choice is bc Non-repudiation directly addresses the need to attribute messages to individuals, ensuring accountability and trust in communications.

upvoted 4 times

🗨️ 👤 **d4a5620** 9 months, 4 weeks ago

Selected Answer: B

The wording on this question is absolutely horrendous but the answer is B

upvoted 8 times

🗨️ 👤 **Arshedconoco** 11 months, 1 week ago

So true that the wording of this question is very bad

upvoted 3 times

🗨️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: B

B. Non-repudiation

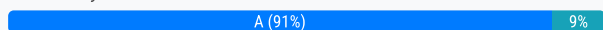
upvoted 8 times

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

- A. Automation
- B. Compliance checklist
- C. Attestation
- D. Manual audit

Correct Answer: A

Community vote distribution



SHADTECH123 Highly Voted 9 months ago

Selected Answer: A

Automation involves using tools and scripts to regularly check and report on the security settings of servers. This method ensures consistent, real-time monitoring and can quickly detect any unauthorized changes. It is more reliable and efficient compared to manual methods, compliance checklists, or periodic attestations, which may not capture changes as promptly or consistently.

upvoted 19 times

8f23125 Most Recent 2 months, 1 week ago

Selected Answer: A

Automation is the best way to consistently and reliably detect changes in security settings on servers daily (or even in real time).

Tools like configuration management systems (e.g., Ansible, Chef, Puppet), file integrity monitoring (e.g., Tripwire), or SIEM solutions can automatically check for and alert on unauthorized changes.

upvoted 1 times

Markie100 4 months, 3 weeks ago

Selected Answer: A

Automation ensures real-time monitoring, reduces human error, and provides scalability, making it the best choice for daily determination of security setting modifications.

upvoted 1 times

daulaexamen 5 months, 2 weeks ago

Selected Answer: C

You want the servers to be security attested - that they don't have vulns. I think the term is more specific than automation

upvoted 1 times

Bito808 8 months, 1 week ago

Selected Answer: C

Change management logs are often signed by administrators, to track changes that may have been done to servers. This is a form attestation.

upvoted 1 times

dbrowndiver 9 months ago

Selected Answer: A

Automation involves using tools and scripts to perform tasks automatically without manual intervention. In the context of security, automation can be used to regularly check server configurations, security settings, and detect unauthorized changes.

-Consistency: Automated tools can run checks daily without fail, ensuring that any modifications to security settings are promptly identified and reported.

-Efficiency: Automation reduces the need for manual labor, allowing IT teams to focus on other critical tasks while ensuring that security settings are continuously monitored.

-Real-Time Alerts: Automation tools can be configured to send alerts or notifications whenever a security setting is changed, enabling quick responses to potential security breaches.

upvoted 2 times

Osechabelo 1 year, 1 month ago

- Attestation

- Provides an opinion of truth or accuracy of a company's security positioning

upvoted 2 times

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

- A. SCAP
- B. NetFlow
- C. Antivirus
- D. DLP

Correct Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **123456789User** Highly Voted 👍 1 year ago

Selected Answer: D

Data Loss Prevention protects sensitive information from loss, corruption, misuse, or unauthorized access.

upvoted 12 times

🗳️ 👤 **MaxiPrince** Most Recent ⌚ 6 months, 4 weeks ago

Selected Answer: D

Data loss Protection

upvoted 2 times

🗳️ 👤 **3dk1** 8 months, 1 week ago

Definitely DLP. I learned about this in a Microsoft exam last year too.

upvoted 4 times

🗳️ 👤 **dbrowndiver** 9 months ago

Selected Answer: D

Data Loss Prevention (DLP) solutions monitor, detect, and block sensitive data from being sent outside an organization through email, file transfers, and other communication methods. DLP can be configured to detect specific data patterns, such as social security numbers, credit card information, or other forms of PII.

As it pertains to this Scenario Application:

-Accidental Data Leakage: If an employee accidentally emails a file containing PII, a DLP tool can automatically detect this based on pre-configured rules and patterns that identify sensitive data.

-Policy Enforcement: DLP can enforce security policies by alerting administrators or blocking the email from being sent if it contains PII, thereby preventing data breaches.

DLP tools are designed to handle situations like accidental data leakage, making them the most suitable choice for detecting and preventing unauthorized transmission of PII.

upvoted 4 times

An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as \$, |, :, &, ` , and ? from variables set by forms in a web application.

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- A. Identify embedded keys
- B. Code debugging
- C. Input validation
- D. Static code analysis

Correct Answer: C

Community vote distribution

C (100%)

 **123456789User** Highly Voted 1 year ago

Selected Answer: C

Input validation is the process of analyzing inputs and disallowing those which are considered unsuitable. I.e: Only allowing accepted inputs based on specific criteria

upvoted 17 times

 **dbrowndiver** Highly Voted 9 months ago

Selected Answer: C

As it pertains to this Scenario Application:

-Removing Special Characters: The use of regular expressions to strip special characters from form variables is a method of input validation. By removing potentially dangerous characters, the application minimizes the risk of executing unintended commands or code.

-Security Enhancement: Input validation helps ensure that only expected and safe input is processed, thereby protecting the application from malicious attacks that exploit unvalidated input.

The policy directly describes a practice used to validate and sanitize user input, which is the essence of input validation. This technique is crucial for maintaining the security of web applications by preventing injection-based attacks.

upvoted 5 times

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

- A. Place posters around the office to raise awareness of common phishing activities.
- B. Implement email security filters to prevent phishing emails from being delivered.
- C. Update the EDR policies to block automatic execution of downloaded programs.
- D. Create additional training for users to recognize the signs of phishing attempts.

Correct Answer: C

Community vote distribution

C (82%)

Other

🗳️ 👤 **SHADTECH123** Highly Voted 👍 9 months ago

Selected Answer: C

Updating the Endpoint Detection and Response (EDR) policies to block the automatic execution of downloaded programs helps to mitigate the risk by preventing malicious software from running even if a user clicks on a phishing link. This technical control directly addresses the potential consequences of a phishing attack by stopping harmful actions from taking place after the initial click, thus reducing the overall impact of the phishing campaign.

While raising awareness (option A), implementing email security filters (option B), and creating additional training (option D) are all valuable preventive measures, they do not directly reduce the impact after a phishing link is clicked.

upvoted 34 times

🗳️ 👤 **AliRi** 1 week, 6 days ago

key part is "impact when a user clicks on a link".

Well said.

upvoted 2 times

🗳️ 👤 **43a41d4** 7 months ago

You're explanation is clean. Thank you.

upvoted 1 times

🗳️ 👤 **KO_** 8 months, 3 weeks ago

Well explained

upvoted 2 times

🗳️ 👤 **barracouto** Highly Voted 👍 11 months, 2 weeks ago

C is the only one that that can actually be controlled by the analyst.. You can train as much as you want but that doesn't mean people listen...

Source: all of us here using an exam dump after watching Messers course :)

upvoted 13 times

🗳️ 👤 **uday1985** 10 months, 2 weeks ago

interesting! how can you block fileless code executions ? When the last time you have encountered an actual exe in a phishing campaign? how about obfuscated scripts? this won't even stop clicking on link to steal information!

upvoted 3 times

🗳️ 👤 **1chung** Most Recent 🕒 1 month, 1 week ago

Selected Answer: D

I go with D

upvoted 1 times

🗳️ 👤 **tsummey** 4 months, 1 week ago

Selected Answer: D

After reading the question a few times, I'm changing my answer to D. The first time around I didn't catch that a security analyst and management are assessing the organizational performance of a recent phishing campaign. This implies a phishing test. The best course of action based on too many

user click-throughs is education.

upvoted 1 times

🗳️ 👤 **tsummey** 4 months, 1 week ago

Selected Answer: B

The correct answer is B. EDR solutions like CrowdStrike do not provide direct link click-through protection. I'd like to better understand how modifying an EDR policy would prevent users from clicking on a phishing link without outright blocking all links they attempt to open.

A Secure Email Gateway (SEG) / Email Security Gateway (ESG) is responsible for filtering malicious emails containing phishing URLs or attachments. Click-through protection is a key feature of ESGs like Proofpoint, Microsoft Defender for Office 365, and Mimecast. Admins can adjust filtering aggressiveness, and in this case, it's likely that the current settings were too lenient, allowing phishing emails through.

The best course of action is to modify ESG security filters to prevent these emails from reaching users. Ideally, this would be complemented by reviewing and enhancing security awareness training to reinforce phishing detection skills.

upvoted 2 times

🗳️ 👤 **MarysSon** 2 months, 4 weeks ago

The question addresses what happens when a user DOES click on a phishing link. This is past the point of preventing the link from being clicked. EDR prevents the damage from taking effect. That's why C is the correct answer.

upvoted 1 times

🗳️ 👤 **darpanne** 6 months, 2 weeks ago

Selected Answer: C

C because Question is about when a user clicks on a link in a phishing message

upvoted 1 times

🗳️ 👤 **Spoude1001** 7 months ago

Selected Answer: B

By implementing advanced email security filters, the organization can significantly reduce the likelihood of phishing emails reaching employees in the first place.

upvoted 1 times

🗳️ 👤 **Bito808** 8 months, 1 week ago

Blocking automatic execution does not block all Phishing emails. Some Phishing emails try to redirect you or get you to contact a bad actor. This action is more focused on malware prevention, not necessarily Phishing attempts.

upvoted 1 times

🗳️ 👤 **Etc_Shadow28000** 9 months ago

Selected Answer: C

C. Update the EDR policies to block automatic execution of downloaded programs.

While raising awareness, implementing email filters, and providing additional training are important measures, updating Endpoint Detection and Response (EDR) policies to block the automatic execution of downloaded programs directly addresses the issue of reducing the impact when a user clicks on a phishing link. This approach helps prevent malicious software from being executed on the user's system, thus mitigating potential harm.

Therefore, the correct answer is:

C. Update the EDR policies to block automatic execution of downloaded programs.

upvoted 4 times

🗳️ 👤 **Gigz_77** 9 months ago

Selected Answer: B

I think the best option is B.

C. Phishing doesn't always come with executable files. It can redirect users to malicious pages which clones legitimate sites too when clicked on phishing links.

D. This is an option too. But no matter how many trainings the organizations give to employees, they still fall for phishing emails

upvoted 2 times

🗳️ 👤 **Yurp** 9 months, 2 weeks ago

Selected Answer: C

"reduce the impact when a user *clicks* on a link"

read carefully, C is the only one that makes sense for someone who has already clicked a link.

upvoted 3 times

🗳️ 👤 **cri88** 10 months ago

Selected Answer: B

We can rule out:

- C. Update the EDR policies to block automatic execution of downloaded programs.

Given that the phishing link could lead to a serverless execution, which doesn't rely on downloading and executing a program on the user's machine, this answer would not fully address the risk. Or what if the link is a scam? Login details are still entered, so the impact when a user clicks on a link in a phishing message is still there.

- A (Posters) and D (Training) focus on awareness and education, which are crucial for reducing click-through rates over time but do not directly prevent or mitigate the technical impact of a user clicking on a phishing link.

So B is in my opinion the best answer.

upvoted 2 times

🗳️ 👤 **nap61** 10 months, 2 weeks ago

Selected Answer: C

"...wants to reduce the impact when a user clicks on a link in a phishing message..."

upvoted 4 times

🗳️ 👤 **EfaChux** 11 months ago

Selected Answer: D

Phishing is more of social engineering attack and most times does not involve download or running of malicious applications on the user system. More awareness is what is required to secure users against this kind of attacks

upvoted 3 times

🗳️ 👤 **dbrowndiver** 11 months ago

Selected Answer: C

Implementing EDR policy updates directly addresses the risk posed by phishing attacks by stopping malicious code from executing, thereby reducing the potential impact of users clicking on phishing links.

upvoted 2 times

🗳️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

Selected Answer: C

Wants to reduce impact AFTER clicking the link. C is the only one that, B is preventive and happens before the user can even click the email

upvoted 3 times

🗳️ 👤 **AbdullahMohammad251** 1 year, 1 month ago

Selected Answer: C

Options A, B, and D represent proactive measures designed to mitigate the risk of exposure to phishing emails or clicking on their links. However, should a phishing email evade our security measures and be clicked by an employee, it becomes imperative to prevent any downloaded files from executing. Updating Endpoint Detection and Response (EDR) policies to block the automatic execution of downloaded programs would effectively thwart the attack.

upvoted 6 times

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?


- A. Compensating control
- B. Network segmentation
- C. Transfer of risk
- D. SNMP traps

Correct Answer: A

Community vote distribution

A (93%)

7%

 **shady23** Highly Voted 1 year, 1 month ago

Selected Answer: A

A. Compensating control


w, the keyword in the question is "legacy". Suppose that you have a legacy Linux server which is not compatible with those network-based firewalls, routers and multi-layer switches which is preventing you not just from building VLANs (Network Segmentation), but also from applying white-listing ACL technique against malicious IP addresses. So, what you're going to do is you are going to use host-based firewalls as a compensation for network appliances to be able to accomplish the similar end-result

upvoted 32 times

 **Grouthorax** 10 months, 1 week ago

Appreciate your explanation

upvoted 5 times

 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: A

It is not mentioned that internal IP addresses have been separated from other network IP addresses, but that the host-based firewall is only allowed to communicate with, & protect specific internal IP addresses, this would compensate for threats by mitigating possible attack surfaces that those internal addresses might be vulnerable to from OUTSIDE the network.

upvoted 13 times

 **Yoez** 1 year, 1 month ago

I agree with you

upvoted 1 times

 **Chidazz** Most Recent 5 months ago

Selected Answer: A

The correct answer is:

A. Compensating control

Explanation:

A compensating control is a security measure implemented to meet security requirements when the primary control is not feasible due to technical or business constraints. In this case, since the system is a legacy Linux system, it might not support modern security features like centralized firewall management. Instead, a host-based firewall is used to restrict access to specific internal IP addresses, serving as an alternative security control.

B. Network segmentation refers to dividing a network into separate segments to enhance security and performance, but it is not directly related to a host-based firewall rule.

C. Transfer of risk involves shifting risk to another entity, such as purchasing cybersecurity insurance, which is not relevant here.

D. SNMP traps are notifications sent from network devices for monitoring and alerting, which also do not apply in this context.

upvoted 1 times

 **Etc_Shadow28000** 9 months ago

Selected Answer: A

A. Compensating control

A compensating control is a security measure that is put in place to satisfy the requirements of a security policy or standard when the primary control cannot be implemented. In this case, the host-based firewall on a legacy Linux system allowing connections from only specific internal IP addresses serves as a compensating control to protect the system by limiting access to trusted sources.

Therefore, the correct answer is:

A. Compensating control

upvoted 4 times

🗲️ 👤 **dbrowndiver** 11 months ago

Selected Answer: A

The implementation of a host-based firewall to restrict access is a compensating control because it mitigates the risks associated with potential vulnerabilities in a legacy system by providing an additional layer of protection.

upvoted 2 times

🗲️ 👤 **f26ddcd** 1 year, 1 month ago

Selected Answer: A

Compensating control

upvoted 1 times

🗲️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

Selected Answer: A

Whenever there is legacy mentioned it is 99% always going to be compensating controls or compensation.

upvoted 3 times

🗲️ 👤 **AutoroTink** 1 year, 1 month ago

Selected Answer: B

In the context of the question, which involves a host-based firewall on a legacy Linux system allowing connections from only specific internal IP addresses, the primary goal is to enhance security by limiting access. This is a direct control measure rather than a compensating one. The firewall is not compensating for the inability to implement another control; it is the control itself, enforcing access restrictions based on IP addresses. Configuring the firewall to only allow connections to specific IP addresses, it is segmenting its network.

upvoted 3 times

🗲️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: A

A. Compensating control

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Answer B.

upvoted 2 times

🗲️ 👤 **e5c1bb5** 1 year, 1 month ago

Selected Answer: B

logical network segmentation includes ACL implementation to allow or dissallow specific IP addresses to communicate with a particular device.

upvoted 1 times

🗲️ 👤 **Punjistetics** 1 year, 1 month ago

B. Network segmentation.

Network segmentation involves dividing a computer network into smaller, isolated networks to improve security and reduce the impact of potential security breaches. By configuring the host-based firewall to allow connections only from specific internal IP addresses, the system is effectively segmenting the network to limit communication to authorized entities, thus enhancing security.

Options such as compensating control (A), transfer of risk (C), and SNMP traps (D) do not accurately describe the scenario of restricting connections to specific internal IP addresses through a host-based firewall

upvoted 6 times

The management team notices that new accounts that are set up manually do not always have correct access or permissions. Which of the following automation techniques should a systems administrator use to streamline account creation?

- A. Guard rail script
- B. Ticketing workflow
- C. Escalation script
- D. User provisioning script

Correct Answer: D

Community vote distribution

D (100%)

 **Etc_Shadow28000** Highly Voted 1 year ago

Selected Answer: D

D. User provisioning script

A user provisioning script automates the process of creating user accounts, ensuring that each new account is set up with the correct access and permissions consistently. This helps prevent errors that can occur with manual account creation.

Therefore, the correct answer is:

D. User provisioning script

upvoted 12 times

 **dbrowndiver** Highly Voted 11 months ago

Selected Answer: D

A user provisioning script is the most effective automation technique for ensuring that new accounts are created consistently with the correct access and permissions. Provisioning

User scripts automate the process of creating, managing, and maintaining user accounts and permissions. These scripts ensure that accounts are set up according to predefined policies and role-based access controls, minimizing errors and inconsistencies. This solution addresses the problem directly by automating and standardizing the account creation process, ensuring that new accounts are consistently provisioned with the correct settings.

upvoted 7 times

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

- A. Corrective
- B. Preventive
- C. Detective
- D. Deterrent

Correct Answer: C

Community vote distribution

C (100%)

 **Etc_Shadow28000** Highly Voted 1 year ago

Selected Answer: C

C. Detective

By setting up a Security Information and Event Management (SIEM) system and assigning an analyst to review the logs on a weekly basis, the company is implementing a detective control. Detective controls are designed to identify and alert on potential security incidents, allowing the organization to take appropriate action after an event has occurred.

Therefore, the correct answer is:

C. Detective

upvoted 11 times

 **dbrowndiver** Most Recent 11 months ago

Selected Answer: C

A Security Information and Event Management (SIEM) system is primarily used to detect security incidents by collecting and analyzing logs from various sources. The setup of a SIEM system and regular log reviews is focused on identifying incidents, making it a classic example of a detective control, which is intended to uncover issues rather than prevent them.

upvoted 4 times

 **Hayder81** 1 year ago

C. Detective

upvoted 4 times

A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

- A. Serverless framework
- B. Type 1 hypervisor
- C. SD-WAN
- D. SDN

Correct Answer: A

Community vote distribution

A (100%)

 **Etc_Shadow28000** Highly Voted 1 year ago

Selected Answer: A

A. Serverless framework

A serverless framework is a cloud-based application-hosting solution that allows developers to build and run applications without managing the underlying infrastructure. It is typically a low-cost option because it charges based on the actual usage of the resources rather than requiring the provisioning of dedicated servers.

Therefore, the correct answer is:

A. Serverless framework
upvoted 16 times

 **dbrowndiver** Most Recent 11 months ago

Selected Answer: A

Serverless computing is ideal for applications with variable workloads and those that require scalable solutions without the overhead of managing infrastructure, making it a low-cost and efficient option for application hosting in the cloud.

upvoted 3 times

 **SHADTECH123** 1 year, 1 month ago

Selected Answer: A

A serverless framework allows developers to build and run applications without managing the underlying infrastructure.

upvoted 3 times

A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

- A. Tuning
- B. Aggregating
- C. Quarantining
- D. Archiving

Correct Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **jovines** Highly Voted 1 year, 1 month ago

The act of ignoring detected activity in the future is described as A. Tuning.

Tuning refers to the process of adjusting the configuration of a system, in this case, the security operations center's detection systems, to reduce or eliminate the number of false positives. In this context, if the so-called "malicious activity" is determined to be normal and is expected to recur, the system can be tuned to ignore this activity in the future, preventing unnecessary alerts.

Please note that while the other options (B. Aggregating, C. Quarantining, D. Archiving) are activities related to managing and responding to security events, they do not specifically apply to the scenario of ignoring detected activity in the future.

upvoted 23 times

🗳️ 👤 **Mehsotopes** Highly Voted 1 year, 1 month ago

Selected Answer: A

Tuning is setting a monitoring system to have higher, or lower threat detection standards.

upvoted 10 times

🗳️ 👤 **MarysSon** Most Recent 3 months, 1 week ago

Selected Answer: A

But the real answer is E - None of the above. Tuning is an act of adjusting and optimizing a set of configurations to reduce risk, improve security, and improve performance. That is hardly ignoring. A system might ignore a symptom. but the security administrator does not. This question should be rephrased.

upvoted 1 times

🗳️ 👤 **NONS3c** 9 months, 4 weeks ago

Selected Answer: A

"malicious activity detected on a server is normal" this is a key word it mean that we have fail positive so tuning working on fixing and improve performance or efficiency.

upvoted 3 times

🗳️ 👤 **dbrowndiver** 11 months ago

Selected Answer: A

Tuning is the process of configuring security tools and systems to reduce false positives and ensure that alerts are meaningful. It involves adjusting the parameters and rules of the detection systems to ignore certain activities that have been determined to be normal or non-threatening. Tuning is also the appropriate action to take when a particular activity has been analyzed and deemed safe, allowing the security system to ignore similar future alerts and reducing unnecessary alert fatigue.

upvoted 3 times

A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

- A. The user jsmith's account has been locked out.
- B. A keylogger is installed on jsmith's workstation.
- C. An attacker is attempting to brute force jsmith's account.
- D. Ransomware has been deployed in the domain.

Correct Answer: C

Community vote distribution

C (60%)


B (40%)

 **dbrowndiver** Highly Voted 11 months ago

Selected Answer: C

The scenario perfectly matches a common security issue where attackers gain partial access through stolen credentials but are thwarted by MFA, which they try to bypass unsuccessfully. The repeated success in password authentication suggests that the attacker has access to jsmith's password, but the failure of MFA points to an attempt to guess or brute-force the MFA code.

upvoted 11 times

 **nyyankee718** Highly Voted 11 months, 3 weeks ago

Selected Answer: B

Can be B or C, but leaning B

Since they already have the password, its not a brute force attack

upvoted 7 times

 **a4e15bd** 11 months, 1 week ago

I thought the same, but trying multiple MFA codes is also considered brute force.

upvoted 19 times

 **KSoLL** 4 months, 1 week ago

Well the best issue would be quarantined the keylogger still. If you only deal with the brute force problem. The issue will still be there since the key logger is still on the device. You can fix the issue with brute force all you want but if I will still know your password every time you log in.


upvoted 1 times

 **KSoLL** 4 months, 1 week ago

"You can fix the issue with brute force all you want but the keylogger issue will still record the users input, every time the user logs in"

Sorry fixing my grammar

upvoted 1 times

 **Tiagonbt** Most Recent 2 weeks, 3 days ago

Selected Answer: C

Even if the keystrokes were captured using a keylogger and the attacker has the password, the act of using them repeatedly is indicative of brute force.

upvoted 1 times

 **shootweb** 3 months, 1 week ago

Selected Answer: C

C.

It's not B because you can brute-force anything. A brute-force attack relies on trial and error and isn't limited to passwords—you can brute-force usernames, URLs, directories, parameters, MFA, etc.

This could very well be a case of someone whose credentials (username and password) were leaked on the dark web, which also rules out B. The attacker knows the username and password but doesn't have access to the MFA, so they are brute-forcing it.

upvoted 2 times

🗲️ 👤 **KSoLL** 4 months, 1 week ago

Selected Answer: B

The answer is B.

Why is it B? because If it was brute force the Password authentication would have failed and not successful. When brute force occurs, it means that the attacker is running a script to input different kind of password until it hit the right one. In this case the attacker knew the password since the password authentication successful for all four logins. And someone that say MFA failed is a brute force. yes that can be true but the right answer would be still B since the keylogger was the main issue. If MFA wasn't in place the hacker would have access to the account.

upvoted 1 times

🗲️ 👤 **justin1995** 4 months, 2 weeks ago

Selected Answer: B

there should be invalid passwords if brute force

upvoted 1 times

🗲️ 👤 **Ashtom** 4 months, 3 weeks ago

Selected Answer: B

in class we learned the best solution against keyloggers is MFA

upvoted 1 times

🗲️ 👤 **vm_mscs** 4 months, 4 weeks ago

Selected Answer: B

Someone without access to MFA successfully enters password. Password is known, how? I choose B.

upvoted 1 times

🗲️ 👤 **fufuuu** 5 months, 2 weeks ago

Selected Answer: B

B. A keylogger is installed on jsmith's workstation.

upvoted 1 times

🗲️ 👤 **Aces155** 5 months, 3 weeks ago

Selected Answer: C

I think this is a poorly written question.

A. If the user entered their MFA token incorrectly a bunch of times it possible that the system locked them out so it's not working.

B. This could be how the threat actor obtained the user's password

C. While foolish and a waste of time, attempting to guess the MFA code is essentially the same trying to guess the user's password, thus making it a brute force attack.

Given the limited information we have I'm going with C

upvoted 1 times

🗲️ 👤 **Aces155** 5 months, 2 weeks ago

Actually, now that I've thought about it some more, given how unlikely and foolish it would be to try to brute force an MFA token, I think it's more likely jsmith has a keylogger installed on his device, so B.

upvoted 1 times

🗲️ 👤 **Coznet** 5 months, 3 weeks ago

Selected Answer: B

B: Keylogger got the PW and is stuck on MFA.

C is incorrect as MFA code changes every time so you cant brute force it. It would be possible to try the SAME code every time until you got lucky or got locked out but that aint BF.

upvoted 2 times

🗲️ 👤 **MaxiPrince** 6 months, 2 weeks ago

Selected Answer: C

An attacker is attempting to brute force jsmith's account

upvoted 1 times

🗲️ 👤 **Damique** 7 months ago

Selected Answer: B

It is not a brute force attack since the hacker already has the password because of the keylogger

upvoted 2 times

  **Greyhat** 7 months, 1 week ago

The correct answer is A. The user jsmith's account has been locked out. This is because the log shows multiple failed attempts with an "invalid code" error, which is typically a result of too many incorrect password attempts. This would trigger an account lockout policy to prevent brute-force attacks.

Option B. There is no indication of a keylogger in the log. Keyloggers typically don't trigger account lockouts.

Option C. While this might be a possible scenario, the log doesn't explicitly show a brute-force attack. The "invalid code" error suggests a lockout due to incorrect password attempts, not a brute force attack.

Option D. There is no indication of ransomware in the log. Ransomware typically doesn't trigger account lockouts.

upvoted 1 times

  **barracouto** 9 months ago

Selected Answer: C

The log entries show multiple successful password authentications followed by multiple failed MFA (Multi-Factor Authentication) attempts due to invalid codes. This pattern suggests that the user's password has been correctly entered multiple times, but the MFA codes are consistently failing.

The best explanation for what the security analyst has discovered is:

C. An attacker is attempting to brute force jsmith's account.

The repeated successful password authentications followed by failed MFA attempts indicate that an attacker may have obtained the user's password and is now trying to bypass the second layer of security, the MFA, by attempting multiple invalid codes.

upvoted 4 times

  **Etc_Shadow28000** 1 year ago

Selected Answer: C

The log entries indicate that the user "jsmith" has successfully authenticated with a password but has repeatedly failed the Multi-Factor Authentication (MFA) step due to an invalid code. This pattern suggests that the correct password is known or has been compromised, but the attacker is unable to provide the correct MFA code.

Given this information, the most likely explanation is:

C. An attacker is attempting to brute force jsmith's account.

The repeated MFA failures suggest that someone other than the legitimate user is trying to gain access, potentially indicating a brute force attempt or another form of unauthorized access where the password is known, but the second factor of authentication is not.

upvoted 3 times

  **leedsbarber** 1 year ago

Selected Answer: C

Brute force involves trying different combinations of passwords/other credentials. This attacker knows the username and password and is clearly not guessing. A keylogger would know the username and password, but not have access to the MFA.

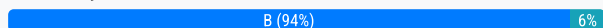
upvoted 4 times

A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

- A. Clustering servers
- B. Geographic dispersion
- C. Load balancers
- D. Off-site backups

Correct Answer: B

Community vote distribution



barracouto Highly Voted 9 months ago

Selected Answer: B

Given the concern about weather events causing damage to the server room and resulting downtime, the company should consider measures that protect against physical damage and ensure business continuity. The most relevant option for this scenario is:

B. Geographic dispersion

Geographic dispersion involves placing critical infrastructure in multiple, geographically distant locations. This strategy ensures that even if one site is affected by a weather event, operations can continue at another site, minimizing downtime and maintaining availability.

upvoted 10 times

Alexikaun Most Recent 5 months, 2 weeks ago

Selected Answer: B

Geographic dispersion ensures that servers are located in different physical locations, reducing the risk of all servers being affected by a single weather event.

upvoted 3 times

Gadoof 6 months, 1 week ago

Selected Answer: B

I think a geographic dispersion would essentially be a CDN or Content Delivery Network, though this could cover a variety of technologies that provide redundancy across geographic locations.

upvoted 1 times

c2b4969 6 months, 1 week ago

Selected Answer: D

I think this can be B or D. I chose D because if you have back ups, then data can be restored in the event of a disaster

upvoted 1 times

RIDA_007 9 months, 1 week ago

Correct it's B.

geographical dispersal refers to placing physical distances between duplicate systems so the organization can avoid damages to both the primary and alternate resources from the same disaster.

upvoted 4 times

dbrowndiver 11 months ago

Selected Answer: B

In this scenario, option B. Geographic dispersion is the correct answer because it provides a comprehensive solution to the risk of weather-related damage to the server room. By spreading resources across multiple locations, the company can maintain service continuity and minimize downtime, even when one location is affected by severe weather conditions.

upvoted 2 times

123456789User 1 year ago

Selected Answer: B

distributing your infrastructure across multiple physical locations makes it so if you lose one site to weather or a disaster of sorts, you can continue operating via another location

upvoted 3 times

Which of the following is a primary security concern for a company setting up a BYOD program?

- A. End of life
- B. Buffer overflow
- C. VM escape
- D. Jailbreaking

Correct Answer: D

Community vote distribution

D (100%)

 **barracouto** Highly Voted 12 months ago

Selected Answer: D

When setting up a Bring Your Own Device (BYOD) program, the primary security concern is ensuring that personal devices, which may not be under the company's direct control, do not introduce security risks into the organization. Among the options provided, the most relevant concern is:

D. Jailbreaking

Jailbreaking refers to removing the manufacturer's restrictions on a device, which can compromise the security of the device. This makes it more susceptible to malware and unauthorized access, posing a significant risk to the company's network and data when such a device is connected.
upvoted 10 times

 **Alexikaun** Most Recent 5 months, 2 weeks ago

Selected Answer: D

Jailbreaking (or rooting) a device removes the manufacturer's restrictions, potentially exposing the device to security vulnerabilities and malicious software. This can compromise the security of the company's network and data.
upvoted 2 times

 **dbrowndiver** 11 months ago

Selected Answer: D

In this scenario, D. Jailbreaking is the correct answer because it directly affects the security of personal devices used in a BYOD program. Jailbreaking removes built-in security controls, making devices vulnerable to various threats, and is a primary concern for companies allowing personal devices to access corporate networks and data.
upvoted 2 times

 **jennyka76** 1 year ago

D

Jailbreaking is the process of removing software restrictions that a device manufacturer has intentionally put in place. This allows users to gain more control over their device, such as:

- Installing custom firmware
- Installing third-party applications
- Choosing their operating system
- Getting apps from unofficial stores
- Turning their phone into a hotspot
- Changing the look and operation of their phone
- Changing phone settings at the administrator level

upvoted 3 times



A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks. Which of the following analysis elements did the company most likely use in making this decision?

- A. MTTR
- B. RTO
- C. ARO
- D. MTBF

Correct Answer: C

Community vote distribution

C (100%)

  **e5c1bb5** Highly Voted 1 year, 1 month ago

Selected Answer: C

MTTR= mean time to repair
RTO=recovery time objective
ARO= annualized rate of occurrence
MTBF= mean time between failures.

ARO is it
upvoted 29 times

  **barracouto** Highly Voted 9 months ago

Selected Answer: C

MTTR (Mean Time to Repair): This measures the average time it takes to repair a system or component after a failure. It is used to assess how quickly an organization can respond to and fix issues.

RTO (Recovery Time Objective): This is the maximum acceptable amount of time that a system or application can be down after a failure or disaster. It defines the target time for recovery.

ARO (Annualized Rate of Occurrence): This estimates the frequency with which a specific risk or event is expected to occur in a year. It helps in assessing the likelihood of risks.

MTBF (Mean Time Between Failures): This measures the average time between failures of a system or component. It is used to predict the reliability and performance of systems over time.

In the context of the company deciding to remove ransomware coverage to reduce costs, they likely assessed the ARO (Annualized Rate of Occurrence) to determine how often ransomware attacks are expected to occur and decided the risk was low enough to justify the cost savings.
upvoted 16 times

  **itone333** Most Recent 3 months, 4 weeks ago

Selected Answer: C

Soon as I saw the word 'annual', I already knew what time it was.
upvoted 1 times

  **MaxiPrince** 6 months, 2 weeks ago

Selected Answer: C

annualized rate of occurrence
upvoted 1 times

  **dbrowndiver** 11 months ago

Selected Answer: C

In this scenario, option C. ARO (Annualized Rate of Occurrence) is the correct answer because it assesses the frequency of ransomware attacks. The company likely used ARO to evaluate the likelihood of such incidents occurring and decided that the probability did not justify the cost of insurance coverage for ransomware, leading to the decision to reduce the policy cost.

upvoted 1 times

Which of the following is the most likely to be included as an element of communication in a security awareness program?

- A. Reporting phishing attempts or other suspicious activities
- B. Detecting insider threats using anomalous behavior recognition
- C. Verifying information when modifying wire transfer data
- D. Performing social engineering as part of third-party penetration testing

Correct Answer: A

Community vote distribution

A (100%)

  **c80f5c5** Highly Voted 1 year ago

Selected Answer: A

Easiest way to think of this question is this security awareness program is likely to be made company wide for the avg employee with no computer skills. B C D are all for the cybersecurity team specifically
upvoted 14 times

  **d4a5620** Highly Voted 9 months, 4 weeks ago

Selected Answer: A

The keyword here is "communication" and reporting is the only answer option given that effectively communicates phishing attempts
upvoted 7 times

  **MaxiPrince** Most Recent 6 months, 2 weeks ago

Selected Answer: A

Reporting phishing attempts or other suspicious activities
upvoted 1 times

  **chasingsummer** 10 months, 2 weeks ago

Selected Answer: A

The most likely answer is A.
upvoted 1 times

HOTSPOT -

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS -

Not all attacks and remediation actions will be used.

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

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	<div> <div></div> <div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div> </div>	<div> <div></div> <div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div> </div>
The attack establishes a connection, which allows remote commands to be executed.	User	<div> <div></div> <div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div> </div>	<div> <div></div> <div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div> </div>
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	<div> <div></div> <div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div> </div>	<div> <div></div> <div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div> </div>
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	<div> <div></div> <div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div> </div>	<div> <div></div> <div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div> </div>
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	<div> <div></div> <div>Botnet</div> <div>RAT</div> <div>Logic Bomb</div> <div>Backdoor</div> <div>Virus</div> <div>Spyware</div> <div>Worm</div> <div>Adware</div> <div>Ransomware</div> <div>Keylogger</div> <div>Phishing</div> </div>	<div> <div></div> <div>Enable DDoS protection</div> <div>Patch vulnerable systems</div> <div>Disable vulnerable services</div> <div>Change the default system password</div> <div>Update the cryptographic algorithms</div> <div>Change the default application password</div> <div>Implement 2FA using push notification</div> <div>Conduct a code review</div> <div>Implement application fuzzing</div> <div>Implement a host-based IPS</div> <div>Disable remote access services</div> </div>

Correct Answer:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Virus	Patch vulnerable systems
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Implement 2FA using push notification
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

🗨️ 👤 **Th3irdEye** Highly Voted 1 year, 1 month ago

I think the 3rd line is wrong.

It should be:

Database server / Worm / Change the default application password

The prompt talks about compromising an SQL database with well known credentials. So you need to change the app default password to fix this. It also talks about the attack being self propagating which would make it a worm.

I believe the rest of the answers are correct.

upvoted 64 times

🗨️ 👤 **c80f5c5** Highly Voted 1 year ago

These are the answers I got when I took a Sec+ bootcamp for work, they went over this lab during the course.

1. Botnet - Enable DDos
2. RAT - Implement Host based IPS
3. Worm - Change default application password
4. Keylogger - Disable remote access services
5. Backdoor - Conduct code review

I've seen various answers around the web. I'm going with these.

upvoted 37 times

🗨️ 👤 **GnawingCow** 6 months, 1 week ago

How would keylogger equate to disabling remote access services? Keyloggers do not rely on remote access services (like RDP, VNC, etc.) to operate. Instead, they typically record keystrokes locally and then send the collected data over the network to a remote attacker, either via an internet connection, email, or other methods. 2FA, on the other hand, if implemented correctly would render a keylogger useless

upvoted 7 times

🗨️ 👤 **KSoLL** 4 months, 1 week ago

MFA prevents keylogging.

MFA consist of the "5 Something" -something you are, something you know, something you have, etc...

Since Keylogger attacks the "something you know", which are the users credentials. They still have to attack other vectors. like "Something you have" - like a one-time code.

Key logging only happens per device, Very rare for you to have a multiple devices compromised with key logging because the user would have to installed the malicious malware on to that device also. Hope that helps

upvoted 2 times

🗨️ 👤 **GnawingCow** 6 months, 1 week ago

Furthermore, RAT = Remote Access Trojan. I believe disabling remote access services makes more sense for this option

upvoted 5 times

🗄️ 👤 **splus** Most Recent 1 month ago

This is the answer:

- 1 Botnet - Enable DDoS protection
- 2 RAT - Implement 2FA plus push notification
- 3 Worm - Implement a host-based IPS
- 4 Keylogger - Patch vulnerable systems
- 5 Backdoor - Conduct a code review

upvoted 1 times

🗄️ 👤 **Arh2** 1 month ago

The answer is virus and not worm because it is not replicating and they already know the know passwords. It would be a virus because it is self propagating which means to spread and not replicate

upvoted 1 times

🗄️ 👤 **Stunomatic** 4 months ago

1. Botnet - Enable DDos
2. RAT - Implement Host based IPS
3. Worm - Change default application password
4. Keylogger - Implement 2FA - (disabling is not a remediate action.)
5. Backdoor - Conduct code review

upvoted 3 times

🗄️ 👤 **ramzie** 5 months, 1 week ago

correct answer 1. Botnet – Enable DDos protection

2. RAT – Disable Remote access services
3. Worm – patch the vulnerable system
4. Keylogger – implement 2fa using push notifications
5. Backdoor – conduct a code review

upvoted 6 times

🗄️ 👤 **darpanne** 6 months, 2 weeks ago

- A. Botnet - Enable DDos
- B. RAT - Implement Host based IPS
- C. Worm - Change default application password
- D. Keylogger - Disable remote access services
- E. Backdoor - Conduct code review

upvoted 2 times

🗄️ 👤 **PAWarriors** 10 months ago

Correct order:

- A. Botnet - Enable DDos
- B. RAT - Implement Host based IPS
- C. Worm - Change default application password
- D. Keylogger - Disable remote access services
- E. Backdoor - Conduct code review

upvoted 2 times

🗄️ 👤 **a4e15bd** 10 months, 2 weeks ago

- 1- Botnet - Enable DDos
2. RAT - Disable remote services
3. Worm - Change default application password
4. Keylogger - Enable MFA
5. Backdoor - Conduct a code review.

upvoted 8 times

🗄️ 👤 **chasingsummer** 10 months, 2 weeks ago

These make sense to me:

1. Botnet > Enable DDos protection
2. RAT > Implement a host-based IPS

3. Worm > Change the default application password
4. Keylogger > Implement 2FA using push notification
5. Backdoor > Conduct a code review

upvoted 5 times

🗨️ 👤 **Zaydis** 11 months, 2 weeks ago

Upon vast research these make the best sense.

1. Botnet - Enable DDos
2. RAT - Disable remote access services
3. Worm - Change default application password
4. Keylogger - Implement a host-based IPS
5. Backdoor - Conduct code review

upvoted 13 times

🗨️ 👤 **Etc_Shadow28000** 1 year ago

1 An attacker sends multiple SYN packets from multiple sources.

- Botnet
- Enable DDoS protection

2 The attack establishes a connection, which allows remote commands to be executed.

- Attack Identified. RAT Remote Access Trojan
- BEST Preventive or Remediation Action. Disable remote access services

3 The attack is self-propagating and compromises a SQL database using well-known credentials as it moves through the network.

- Attack Identified. Worm
- BEST Preventive or Remediation Action. Patch vulnerable systems

4 The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.

- Attack Identified. Keylogger
- BEST Preventive or Remediation Action. Conduct a code review

5 The attacker embeds hidden access in an internally developed application that bypasses account login.

- Attack Identified. Backdoor
- BEST Preventive or Remediation Action. Implement a host-based IPS

upvoted 8 times

HOTSPOT -

You are a security administrator investigating a potential infection on a network.

INSTRUCTIONS -

Click on each host and firewall. Review all logs to determine which host originated the infection and then identify if each remaining host is clean or infected.

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

192.168.10.22

```

4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31 Warn Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32 Warn Scheduled update disabled by process scvh0st.exe

```

192.168.10.37

```

4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

```

192.168.10.41



```

4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

```

Firewall



Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

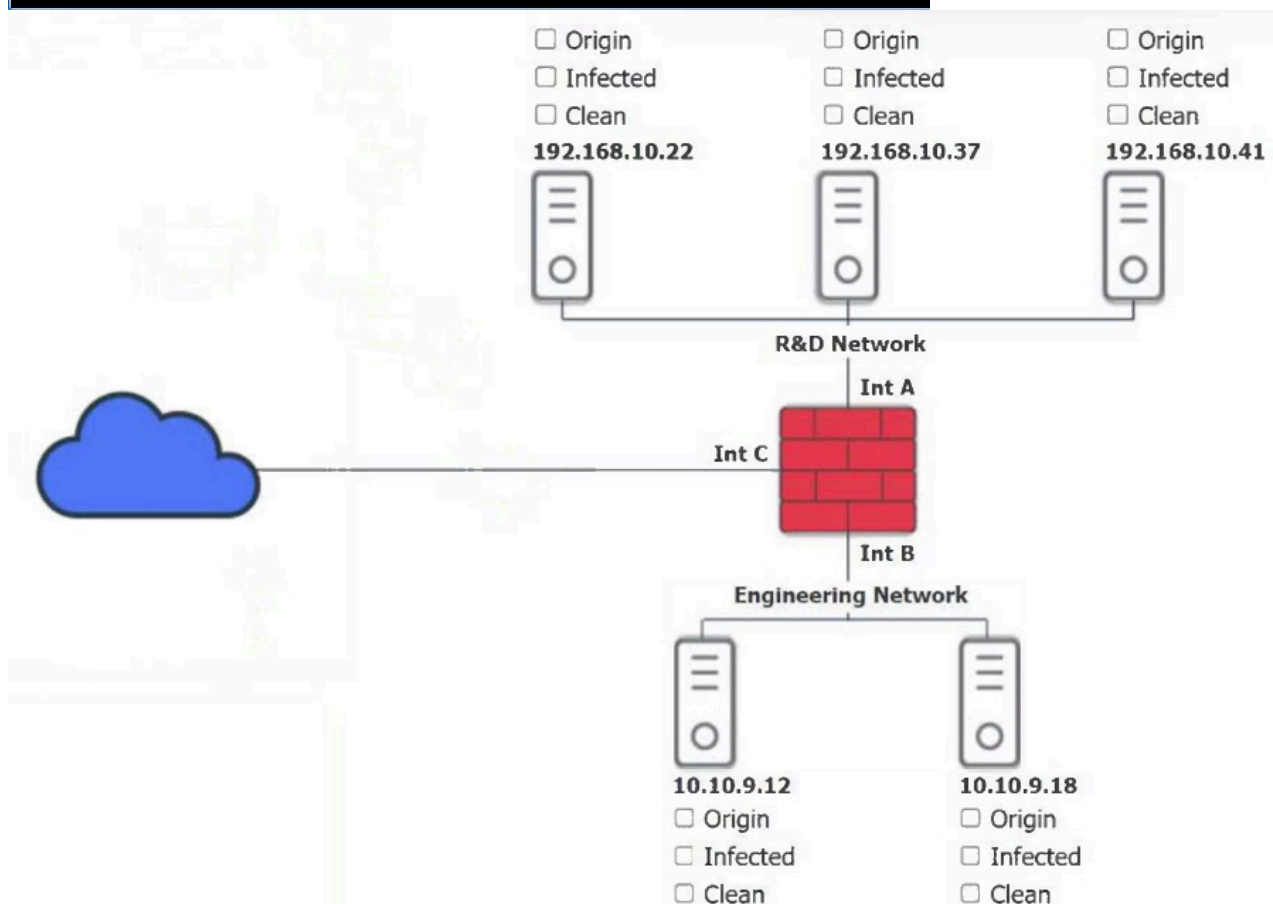
```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 1
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```



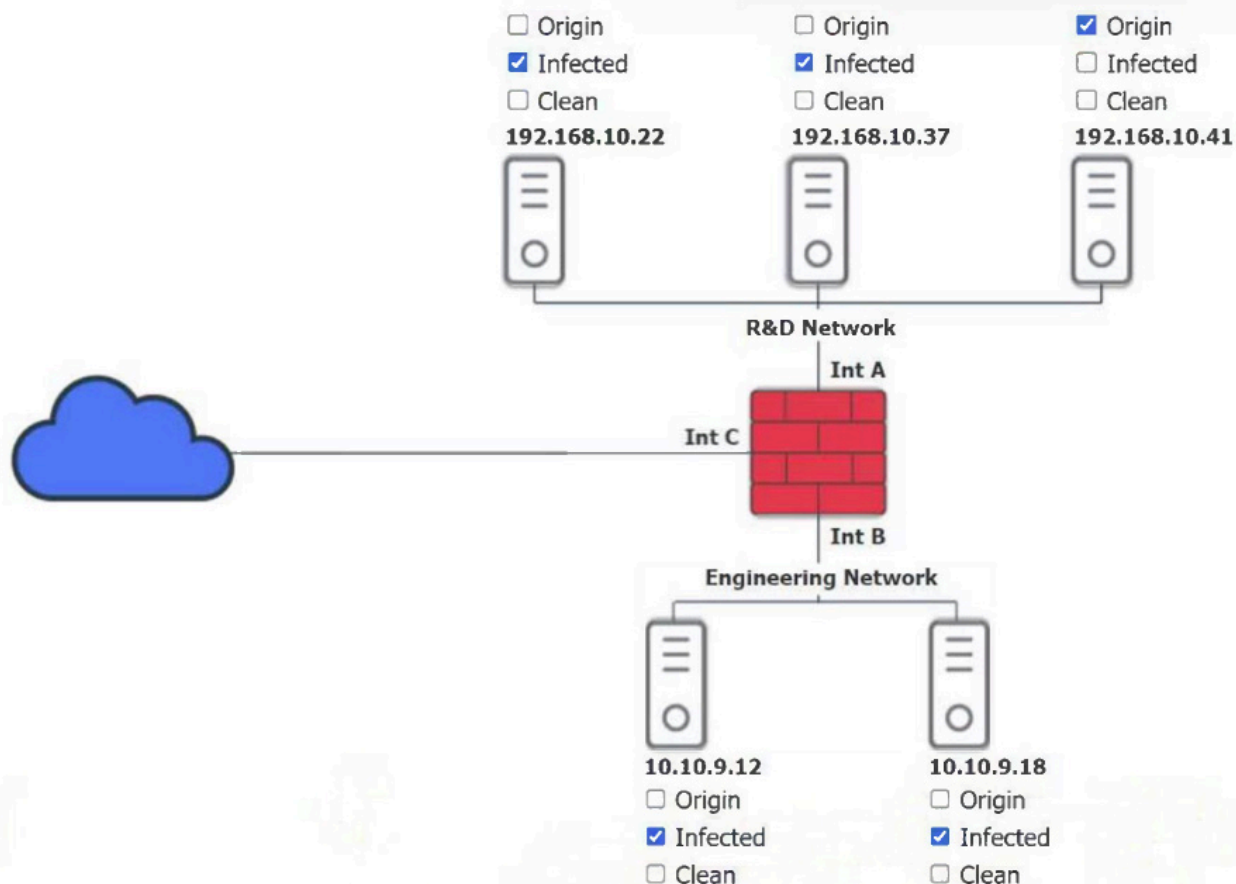
```

4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30

```



Correct Answer:



Fazliddin4515 Highly Voted 1 year, 1 month ago

Why Are you choosing random answers.

Here is real answers => {

22 is Origin. It has started infection first.

37 is Clean, because it is able to get new updates and quarantine malicious file.

41 is Infected, because it was not able to quarantine infected file.

12 is Clean, because it is able to get new updates and quarantine malicious file.

18 is Infected, because it was not able get new update and quarantine file.

These are real answers.

upvoted 136 times

baguttebandit 1 month, 3 weeks ago

these are correct

upvoted 1 times

MLKTKN 4 months, 3 weeks ago

Quarantine doesn't mean it hasn't infected. 37 and 12 still suspicious we don't. Know yet if it is clean or infected, I say all are infected and 22 is the origin

upvoted 1 times

MLKTKN 4 months, 3 weeks ago

could you please someone tell me whether the reveal solutions are correct or not because it says 41 is origin and remain is infected

upvoted 2 times

trustedtester2 5 months ago

This is the right answer, ignore all the rest of people saying another things

upvoted 2 times

c80f5c5 Highly Voted 1 year ago

Commenting to reiterate Fazliddin's comment:

.22 infected at 2:31AM, it was infected 12 hrs before all other IPs

.37 clean, quarantined at 2:43PM

.41 infected at 2:43PM
.12 clean, quarantined at 2:43PM
.18 infected at 2:43PM

I took a Sec+ Bootcamp and they went over this lab, these are the answers they gave us.

upvoted 37 times

  **Arh2** Most Recent 1 month ago

41 origin since it enabled smbv1

Everything else in infected because even if quarantined it is still not cleaned because a device is not considered cleaned until removed completely

upvoted 1 times

  **Arh2** 1 month ago

Wouldnt .41 be the Origin since it enable smbv1 on the 17th which is a legacy protocol vulnerable to a ton of things

upvoted 1 times

  **kamax5400** 4 months ago

Here are the solutions:



41 origin

37 infected

18 Infected

12 infected

upvoted 1 times

  **Russell15** 3 months, 4 weeks ago

No.

.22 is the origin since at 2:31AM, it was infected 12 hrs before all other IPs

.37 clean, quarantined at 2:43PM

.41 infected at 2:43PM

.12 clean, quarantined at 2:43PM



.18 infected at 2:43PM

upvoted 1 times

  **Arh2** 1 month ago

41 initially enabled the ports to allow 22 to infect and spread. 41 is origin look at the firewall for smbv1

upvoted 1 times

  **MLKTKN** 4 months, 4 weeks ago

REVEAL SOLUTION says so the REVEAL SOLUTIONS are not correct? 22 Infected

37 infected

41 origin

12 infected

18 Infected

upvoted 2 times

  **AKA1987** 5 months ago

192.168.10.22 ✓ Clean

192.168.10.37 ☐ Infected

192.168.10.41 ☐ Infected

10.10.9.12 ☐ Infected

10.10.9.18 ☐ Infected (Origin) - The firewall logs indicate that 10.10.9.18 was the first to establish outbound communication (16:01:44) to an external IP (57.203.54.183) over SSL (port 443). This is an early indicator that 10.10.9.18 may be the true origin of the infection.

upvoted 4 times

  **AKA1987** 5 months ago

DeepSeek says:

Host Status

192.168.10.22 ✓ Clean

192.168.10.37 ☐ Infected (Origin)

192.168.10.41 ☐ Infected

10.10.9.12 ☐ Infected

10.10.9.18 ☐ Infected

upvoted 1 times

🗨️ 👤 **MLKTKN** 4 months, 3 weeks ago

no deepseek says 22 is origin

upvoted 2 times

🗨️ 👤 **1798e2e** 8 months, 1 week ago

smbv1 looks to be the obvious port of issue, however there's a bigger giveaway above it that has an rpc call happening from .22. Blaster worm is malware that uses RPC to infect and transfer. The difference between gpt and reality can be staggering sometimes. Fazliddin has this right. a pc that has quarantined something is not considered infected as it's now sitting in a secure system preventing any further transfer/ malicious activity.

upvoted 2 times

🗨️ 👤 **01a4c2e** 8 months, 1 week ago

10.22

~~~~~

scvh0st.exe disabled schedule scan and update on 4/18 @ 2:31-32

(Infected/Origin)

FW >>> 4/18 @ 2:31 57.203.55.29:8080 http

10.37

~~~~~

scvh0st.exe found and quarantined on 4/18 @ 14:37

(Clean)

10.41

~~~~~

scvh0st.exe matched heuristic pattern but unable to quarantine file

on 4/18 @ 14:37

and then after another scan was not listed a quarantined.

(Infected)

9.12

~~~~~

scvh0st.exe found and quarantined on 4/18 @ 14:37

(Clean)

9.18

~~~~~

scvh0st.exe matched heuristic pattern but unable to quarantine file

on 4/18 @ 14:37

and then after another scan was not listed a quarantined.

(Infected)

upvoted 5 times

🗨️ 👤 **Monopeeya** 8 months, 4 weeks ago

.37 reached out over the internet after the initial virus scan on the 17th, which we know can detect the virus regardless of infected status. It was on 443 (secure port) but was using SSL (outdated insecure) instead of TLS. This was their "gotcha".

Viruses do not come out of nowhere. It had to be one of the two that reached out to the internet after the first scan. You would not see the lateral communication of IPs on either side of the firewall because they are not talking across it. The 192 side of the firewall were the only ones to start trying to make connections to check software version of the 10 side of the firewall.

.22 - smbv1 - least secure. Had AV scan completely disabled.

.41 .18 - smbv2 - little more secure. Was able to prevent definition updates. Preventing QT.

.12 .37 - smbv3 - secure. Was not able to modify AV scan. Definitions updated. Malware QT.

upvoted 2 times

🗨️ 👤 **Monopeeya** 8 months, 4 weeks ago



TLDR THE ORIGIN IS NOT .22

.37 Origin (QT'd)

.22 (Still Infected)



.41 (Still Infected)

.12 (QT'd)

.18 (Still Infected)

I do not know if Comptia considers a host with quarantined malware as infected, but all PCs had the malware. Here is the break down if you are interested..

upvoted 1 times

  **jsmthy** 9 months, 1 week ago

22 Infected

37 Origin

41 Infected

12 Clean

18 Infected

192.168.10.37 is the origin point because it is 1 of 2 IP addresses that accessed the public internet prior to 02:30, has a visible file transfer chain, and is tied to active reconnaissance activity. Furthermore, we must note the firewall's location means only cross firewall access is recorded to the log. Lateral movement is not recorded.

Let's get rid of the incumbent answer: 22 can't be the origin because we must take the host log on the 17th as fact that 22 was clean at that time, otherwise the scan should have triggered the heuristic match on the 17th. It would not have started its own infection when it was perfectly fine and there is no proof of other file transfers other than the firewall itself.

No, I believe 22 was selected as a host with persistence and the process looks like this:

37 is infected at 16:01 via a malicious file.

12 is infected at 16:35 via SMBv2.

12 sends out a ping sweep at 23:58, identifying active machines on the network.

22 executes post-exploit payload at 02:30.

18 performs what looks like exfiltration (9GB) at 02:39.

This is the limit of what I see with these logs. Maybe I'm overthinking it since it is this a Comptia exam.

upvoted 1 times

  **FrozenCarrot** 9 months, 3 weeks ago

10.22 Origin

10.37 Clean

10.41 Infected

9.12 Clean

9.18 Infected

upvoted 2 times

  **PAWarriors** 10 months ago

Correct answers:

10.22 --> started the infection and scvh0st.exe disabled scheduled scan and update. (Origin)

10.37 --> the malicious file was in quarantine and it got a new update. (Clean)

10.41 --> No update unable to quarantine file. (Infected)

9.12 --> the malicious file was in quarantine and it got a new update. (Clean)

9.18 --> No update and unable to quarantine. (Infected)

upvoted 2 times

  **3330278\_111** 10 months, 1 week ago

If .22 is the Origin, then it's also infected, right? The scan got disabled right away, and it continued spreading to the other computers afterwards. So I'm checking both Origin and Infected for .22 if they allow me to

upvoted 2 times

  **barracouto** 11 months, 2 weeks ago

If I get this question i'm going to think "OH boy do I miss cici's pizza"

22- Origin - OH

CICI



37 - Clean

41 - Infected

12 - Clean

18 - Infected

upvoted 12 times

  **Viknikpik** 4 months, 2 weeks ago

Did you get this question, were any of the question on there.

upvoted 1 times

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

- A. Preparation
- B. Recovery
- C. Lessons learned
- D. Analysis

**Correct Answer: A**

*Community vote distribution*

A (75%)

C (25%)

 **Etc\_Shadow28000** Highly Voted 1 year ago


**Selected Answer: A**

A. Preparation

The preparation phase in the incident response process is when a security analyst reviews roles and responsibilities. This phase involves planning and setting up the necessary tools, processes, and team structures to effectively respond to potential security incidents.


Therefore, the correct answer is:

A. Preparation  
upvoted 16 times

 **RTUL45** Most Recent 1 week, 6 days ago

**Selected Answer: C**

Preparation is proactive (assign roles)  
Lessons Learned is reflective (review roles)  
upvoted 1 times

 **jennyka76** 6 months, 1 week ago

**Selected Answer: A**

In the incident response process, a security analyst reviews roles and responsibilities during the "Preparation" phase; this is where the incident response plan is established, outlining who is responsible for what tasks during a security incident, ensuring everyone understands their role and how to respond effectively.  
upvoted 1 times

 **nap61** 8 months, 3 weeks ago

**Selected Answer: C**

From CompTIA guide  
Preparation—makes the system resilient to attack in the first place. This includes hardening systems, writing policies and procedures, and setting up confidential lines of communication. It also implies creating incident response resources and procedures  
Lessons learned—analyzes the incident and responses to identify whether procedures or systems could be improved. It is imperative to document the incident. Outputs from this phase feed back into a new preparation phase in the cycle  
Also...  
The lessons learned process reviews severe security incidents to determine their root cause, whether they were avoidable, and how to avoid them in the future.  
So, the world REVIEW is in the LESSON LEARN.  
upvoted 2 times

 **Cee007** 9 months, 4 weeks ago

**Selected Answer: A**

A. Preparation

upvoted 1 times

  **dbrowndiver** 11 months ago

**Selected Answer: A**

The Preparation phase is the initial step in the incident response process where an organization establishes the foundation for handling potential incidents. It involves planning, setting up necessary tools, and defining roles and responsibilities.

upvoted 2 times

  **a4e15bd** 11 months, 1 week ago

The correct phase for reviewing and defining roles and responsibilities in the incident response process is the preparation phase. Lessons Learned is more about reviewing the entire incident after it has been resolved, identifying what went well and what didn't and making improvements for future responses.

upvoted 1 times

  **AutoroTink** 1 year ago

**Selected Answer: A**

This is a tough one! "The Preparation phase includes not only the initial establishment of roles and responsibilities but also their ongoing review and maintenance". I feel like these two steps kind of can blend into each other...review/lessons learned of one incident, can be preparation for the next incident.

upvoted 3 times

  **leedsbarber** 1 year ago

**Selected Answer: A**

Roles and responsibilities should be regularly reviewed, not just after an event. This enables good preparation.

Events are reviewed retrospectively, that's when lessons are learned.

upvoted 3 times

  **MahiMahiMahi** 1 year ago

**Selected Answer: C**

C. Review seems to be the key word here.

upvoted 3 times

  **mr\_reyes** 1 year, 1 month ago

**Selected Answer: C**

Given the options, the phase in the incident response process when a security analyst reviews roles and responsibilities is the Lessons learned phase. During this phase, the team reflects on their performance, identifies gaps, and ensures that roles and responsibilities are well-defined and understood for future incidents. The keyword in this question is "reviews". In the Lessons Learned step we review the roles to see if anything needs to be changed, in the preparation step we are just creating the roles, nothing to review yet.

upvoted 3 times

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

- A. Console access
- B. Routing protocols
- C. VLANs
- D. Web-based administration

**Correct Answer:** D

Community vote distribution

D (100%)

 **499c5c4** Highly Voted 1 year ago

The most appropriate option to disable to harden the routers would be:

D. Web-based administration

Web-based administration, also known as remote management or HTTP/HTTPS access, is a common feature in routers that allows administrators to manage the device remotely using a web browser. However, this feature also introduces a potential vulnerability, as it opens up the router to potential web-based attacks.

Disabling web-based administration would reduce the attack surface and prevent potential exploits, making the router more secure.

Console access (A) is necessary for local management, routing protocols (B) are essential for network operation, and VLANs (C) are used for network segmentation and security. Disabling web-based administration (D) is the most appropriate option to harden the router.

upvoted 25 times

 **chasingsummer** Most Recent 10 months, 2 weeks ago

**Selected Answer: D**

D. Web-based administration

upvoted 1 times

A security administrator needs a method to secure data in an environment that includes some form of checks so track any changes. Which of the following should the administrator set up to achieve this goal?

- A. SPF
- B. GPO
- C. NAC
- D. FIM

**Correct Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **Etc\_Shadow28000** Highly Voted 👍 1 year ago

**Selected Answer: D**

D. FIM (File Integrity Monitoring)

File Integrity Monitoring (FIM) is a security technology that monitors and detects changes in files. FIM solutions can track modifications, access, or deletions of files and notify administrators of any changes, thus ensuring data integrity and security.

Therefore, the correct answer is:

D. FIM

upvoted 12 times

🗳️ 👤 **Exemplary** Highly Voted 👍 8 months, 3 weeks ago

Note to the admins: There is a typo in this one.

"checks SO track any changes" should be

"checks TO track any changes"

upvoted 11 times

🗳️ 👤 **Russell15** 3 months, 4 weeks ago

They probably do this on purpose for copywrite purposes, also the reason they get some answers wrong.

upvoted 1 times

🗳️ 👤 **Syl0** Most Recent 🕒 9 months, 4 weeks ago

SPF - Sender policy framework - identify mail servers that are allowed to send emails to domain

GPO - Group Policy Object - let admin control and implement a group of settings

NAC - Network Access Control - Restricts unauthorised users and devices from gaining access to the network

FIM - File Integrity Monitoring - security process that monitors and analyses integrity of asset

upvoted 8 times

🗳️ 👤 **whatsupdeepak** 1 year, 1 month ago

FIM - stands for File Integrity Monitoring, which is a method to secure data by detecting any changes

upvoted 4 times

🗳️ 👤 **Abcd123321** 1 year, 1 month ago

**Selected Answer: D**

File Integrity Monitoring (FIM)

■ Validates the integrity of operating system and application software files by comparing their current state with a known, good baseline

■ Identifies changes to

- Binary files
- System and Application Files
- Configuration and Parameter Files

■ Monitors critical system files for changes using agents and hash digests, triggering alerts when unauthorized changes occur  
upvoted 2 times

An administrator is reviewing a single server's security logs and discovers the following:

| Keywords      | Date and Time          | Source                     | Event ID | Task Category |
|---------------|------------------------|----------------------------|----------|---------------|
| Audit Failure | 09/16/2022 11:13:05 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:07 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:09 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:11 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:13 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:15 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:17 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:19 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:21 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:23 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:25 AM | Microsoft Windows security | 4625     | Logon         |
| Audit Failure | 09/16/2022 11:13:27 AM | Microsoft Windows security | 4625     | Logon         |

Which of the following best describes the action captured in this log file?

- A. Brute-force attack
- B. Privilege escalation
- C. Failed password audit
- D. Forgotten password by the user

**Correct Answer: A**

Community vote distribution

A (100%)

 **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer: A**

A. Brute-force attack

The log shows multiple failed login attempts within a very short time frame, which is characteristic of a brute-force attack. In a brute-force attack, an attacker attempts many different passwords or passphrases with the hope of eventually guessing correctly. The pattern of frequent and continuous login failures seen in the log entries aligns with this type of attack.

Therefore, the correct answer is:

A. Brute-force attack  
upvoted 10 times

 **PAWarriors** Most Recent 10 months ago

**Selected Answer: A**

A. Brute-force attack



--> Event ID 4625 is logged for any logon failure. It generates on the computer where logon attempt was made.

--> In this scenario we can see multiple login attempts every few seconds indicating that this is a potential brute-force attack.

upvoted 2 times

A security engineer is implementing FDE for all laptops in an organization. Which of the following are the most important for the engineer to consider as part of the planning process? (Choose two.)

- A. Key escrow
- B. TPM presence
- C. Digital signatures
- D. Data tokenization
- E. Public key management
- F. Certificate authority linking

**Correct Answer:** AB

Community vote distribution

AB (100%)

 **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer:** AB

- A. Key escrow
- B. TPM presence

- **Key escrow:** This is important to ensure that encryption keys can be recovered in case they are lost or forgotten. It is a crucial consideration for Full Disk Encryption (FDE) to maintain access to data even if issues arise with the primary encryption keys.

- **TPM presence:** Trusted Platform Module (TPM) is a hardware-based security feature that can store encryption keys securely. Ensuring the presence of TPM on laptops enhances the security of FDE by protecting the encryption keys from being accessed or tampered with.

Therefore, the most important considerations for the security engineer are:

- A. Key escrow
  - B. TPM presence
- upvoted 13 times

 **9149f41** Most Recent 4 months, 3 weeks ago

**Selected Answer:** AB

In the planning process, finding a safe place for the encryption key is the most important.

Key escrow is a software-based, and TPM is a hardware-based system where we can keep the encryption key for future decryptions.

Other options are not relevant in the planning process of FDE.

upvoted 4 times

 **3dk1** 8 months, 1 week ago

AB for sure.

Here is why E is not one of them (ai generated, but I agree with the answer)

Public key management is essential in many cryptographic processes, but it's not as directly relevant to Full Disk Encryption (FDE) for the following reasons:

FDE primarily uses symmetric encryption: Most FDE solutions rely on symmetric encryption, where the same key is used to both encrypt and decrypt the data. This differs from public key infrastructure (PKI), which involves asymmetric encryption, where a public key encrypts and a private key decrypts. While PKI is critical in other areas (like securing communications, emails, or verifying identities), it's not central to how FDE typically functions.

Public key management is more relevant for data in transit: PKI and public key management are often used for securing data in transit (e.g., SSL/TLS

for web traffic) or ensuring non-repudiation (via digital signatures). FDE is focused on securing data at rest, where symmetric keys (often stored in TPM) are used for encryption, not public/private key pairs.

upvoted 2 times

🗨️ 👤 **dbrowndiver** 11 months ago

Selected Answer: AB

In this scenario, A. Key escrow and B. TPM presence are the most important considerations for implementing Full Disk Encryption (FDE) on laptops. These elements ensure that encryption keys are securely managed and stored, providing both data security and recoverability in case of lost keys, and that hardware-based security is used to protect against unauthorized access.

upvoted 1 times

🗨️ 👤 **Shaman73** 1 year ago

Selected Answer: AB

A. Key escrow

B. TPM presence

upvoted 1 times

🗨️ 👤 **shady23** 1 year, 1 month ago

Selected Answer: AB

A. Key escrow

B. TPM presence

upvoted 1 times

🗨️ 👤 **shady23** 1 year, 1 month ago

Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.

TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and

upvoted 1 times

🗨️ 👤 **Fazliddin4515** 1 year, 1 month ago

I think E is also correct one

upvoted 1 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

I don't think so that are the correct answers.

upvoted 1 times

🗨️ 👤 **e5c1bb5** 1 year, 1 month ago

Selected Answer: AB

this one is tough because public key management is fundamental to full disc encryption. that being said, key escrow is arguably more important for the following reasons.

public key's are used to encrypt the data and the PRIVATE key is used to decrypt the data.

once the data is encrypted, i would argue who holds the keys (another department or another 3rd party) is more important than establishing the encryption (because thats kind of the easy part). TPM presence is even more fundamental to FDE than the public key is because without it, you cant even consider FDE. those are my thoughts going with AB for now. please share your thoughts. if i didnt pick AB i'd go BE

upvoted 2 times

A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

- A. Changing the remote desktop port to a non-standard number
- B. Setting up a VPN and placing the jump server inside the firewall
- C. Using a proxy for web connections from the remote desktop server
- D. Connecting the remote server to the domain and increasing the password length

**Correct Answer:** B

Community vote distribution

B (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: B**

Setting up a VPN and placing the jump server inside the firewall is the most secure approach because it reduces the attack surface and ensures that only authorized users can access the remote desktop service. This solution addresses the primary security concern of protecting sensitive production systems by ensuring that only verified users can gain access, thus minimizing the attack surface and potential vulnerabilities.

upvoted 10 times

  **9149f41** Most Recent 4 months, 3 weeks ago



**Selected Answer: B**

Why C is correct:

The issue is relevant with a remote server, not a web application. A proxy for web connections would only secure web traffic, not the remote desktop protocol (RDP) traffic.



RD, as well as any server or computer connection, are designed as a VPN, not a proxy.

upvoted 2 times

  **9149f41** 4 months, 3 weeks ago

apology, the title would be: WHY C IS NOT CORRECT.

upvoted 2 times

  **MaxiPrince** 6 months, 2 weeks ago

**Selected Answer: B**

Setting up a VPN and placing the jump server inside the firewall

upvoted 1 times

  **Shaman73** 1 year ago

**Selected Answer: B**

B. Setting up a VPN and placing the jump server inside the firewall

upvoted 2 times

  **MahiMahiMahi** 1 year ago

**Selected Answer: B**

B. Setting up a VPN and placing the jump server inside the firewall

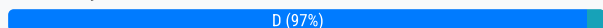
upvoted 2 times

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

- A. ACL
- B. DLP
- C. IDS
- D. IPS

**Correct Answer: D**

Community vote distribution



**AutoroTink** Highly Voted 1 year, 1 month ago

**Selected Answer: D**

An IPS is designed to continuously monitor network traffic and take immediate action to block potential threats based on known signatures. It's an active security measure that not only detects but also prevents the exploitation of known vulnerabilities.

- A. ACL (Access Control List): ACLs are used to control the flow of traffic based on rules, but they are not dynamic enough to monitor or block signature-based attacks effectively.
- B. DLP (Data Loss Prevention): DLP systems are focused on preventing data breaches by detecting and blocking potential data leaks/exfiltration, not on monitoring or blocking attacks per se.
- C. IDS (Intrusion Detection System): While an IDS can detect known signature-based attacks, it does not block them; it only alerts the system administrators of the potential threat.
- D. IPS (Intrusion Prevention System): As mentioned, an IPS actively monitors and blocks attacks, making it the most suitable option for the scenario described.

upvoted 19 times

**barracouto** Highly Voted 9 months ago

**Selected Answer: D**

ACL (Access Control List): Used to control network traffic and define which users or system processes have permissions to access resources or perform operations on a network.

DLP (Data Loss Prevention): Designed to prevent sensitive data from being lost, misused, or accessed by unauthorized users, and to monitor data transfers to ensure compliance with data protection policies.

IDS (Intrusion Detection System): Monitors network or system activities for malicious activities or policy violations. An IDS alerts administrators of potential threats but does not take action to block them.

IPS (Intrusion Prevention System): Monitors and controls network and system activities to protect against malicious activities by detecting and preventing attacks in real-time. An IPS can block traffic that matches known attack signatures.

Correct Answer: D. IPS

The IPS is the appropriate solution as it can monitor and block known signature-based attacks.

upvoted 5 times

**Collapsar** Most Recent 9 months ago

**Selected Answer: D**

An IPS is designed to continuously monitor network traffic and take immediate action to block potential threats based on known signatures. It's an active security measure that not only detects but also prevents the exploitation of known vulnerabilities.

- A. ACL (Access Control List): ACLs are used to control the flow of traffic based on rules, but they are not dynamic enough to monitor or block signature-based attacks effectively.
- B. DLP (Data Loss Prevention): DLP systems are focused on preventing data breaches by detecting and blocking potential data leaks/exfiltration, not

on monitoring or blocking attacks per se.

C. IDS (Intrusion Detection System): While an IDS can detect known signature-based attacks, it does not block them; it only alerts the system administrators of the potential threat.

D. IPS (Intrusion Prevention System): As mentioned, an IPS actively monitors and blocks attacks, making it the most suitable option for the scenario described.

upvoted 1 times

🗳️ 👤 **bufffalobilli** 9 months, 2 weeks ago

**Selected Answer: D**

And block

upvoted 1 times

🗳️ 👤 **a0bfa81** 9 months, 2 weeks ago

**Selected Answer: D**

D. IPS - Intrusion Prevention System  
is the correct answer

upvoted 1 times

🗳️ 👤 **93a09c9** 10 months, 4 weeks ago

D is the correct answer here. The answer is most definitely not C.

upvoted 1 times

🗳️ 👤 **Etc\_Shadow28000** 1 year ago

**Selected Answer: D**

D. IPS (Intrusion Prevention System)

An Intrusion Prevention System (IPS) is designed to monitor network and/or system activities for malicious activities or policy violations and can take actions to block or prevent those activities. Since the enterprise is dealing with known signature-based attacks, an IPS is the best solution because it can actively block these attacks by using signatures to identify and mitigate them in real-time.

Therefore, the correct answer is:

D. IPS

upvoted 1 times

🗳️ 👤 **Shaman73** 1 year ago

**Selected Answer: D**

D:

IPS

upvoted 1 times

🗳️ 👤 **SHADTECH123** 1 year, 1 month ago

**Selected Answer: D**

An Intrusion Prevention System (IPS) is designed to monitor network traffic for suspicious activity, and it can take proactive steps to block or prevent those activities in real-time. IPS uses signature-based detection to identify known vulnerabilities and exploits, making it particularly effective against attacks that exploit well-documented and widely known browser vulnerabilities.

upvoted 3 times

🗳️ 👤 **shady23** 1 year, 1 month ago

**Selected Answer: D**

D. IPS

upvoted 1 times

🗳️ 👤 **Mehsotopes** 1 year, 1 month ago

**Selected Answer: C**

An IPS system being configured can have a chance of blocking code that certain systems with newer web browsers may need, or not be vulnerable to at all. An IDS would allow you to be notified of these recognized signatures, & determine if it's appropriate to allow, or not.

Another safe option would be to know what systems are using older browser versions, & update them, if not, then segment them specifically, & use an IPS appliance if anti-virus automation is what is necessary.

upvoted 1 times

🗳️ 👤 **e5c1bb5** 1 year, 1 month ago

**Selected Answer: D**

was confused by "correct answer" IPS for sure

upvoted 1 times

  **Kevans242** 1 year, 1 month ago

**Selected Answer: D**

Definitely D

upvoted 1 times

  **e56400d** 1 year, 1 month ago

Can someone explain to me why the answer is IDS?

IDS only alerts, it does not block anything. IPS alerts and blocks suspicious activity. Therefore, the answer should be IPS.

upvoted 2 times

Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included. Which of the following best describes how the controls should be set up?

- A. Remote access points should fail closed.
- B. Logging controls should fail open.
- C. Safety controls should fail open.
- D. Logical security controls should fail closed.

**Correct Answer:** C

Community vote distribution

C (89%)

11%

 **dbrowndiver**  11 months ago

**Selected Answer: C**

Safety controls failing open is a critical design principle that ensures human life is prioritized in the event of a failure. This principle applies to situations where failing open provides an immediate safety benefit, such as allowing exit doors to unlock automatically during a fire.

upvoted 7 times

 **Cristian\_Ykz** 6 months, 2 weeks ago

This is generally not a good idea, as it could lead to unsafe conditions. For example, a fire alarm system that fails open might not alert people to a real fire.

upvoted 1 times

 **shootweb** 3 months, 1 week ago

I think you are confusing "false positive" with "fail open".

A fire alarm system that fails open means it will trigger the alarm in the event of a system failure. This ensures that occupants can evacuate safely, even if there's no actual fire.

upvoted 4 times

 **MarysSon**  3 months, 1 week ago

**Selected Answer: C**

The question says human life considerations are included. Human life is the main concern. C is the only answer that adequately addresses the safety of the workforce.


upvoted 2 times

 **41c27e6** 6 months ago

**Selected Answer: D**

Logical security controls. If there is a failure in the security system (such as a logical security control), the system should default to a more secure state, blocking any unauthorized access

upvoted 1 times

 **Cristian\_Ykz** 6 months, 2 weeks ago

**Selected Answer: D**

I think the key to the answer lies in "Logical Security Controls"

Logical security controls (such as firewalls, ACLs, authentication, etc.) must fail-safe (close) upon failure to ensure that the system remains secure and unauthorized access is blocked. This helps proactively protect critical data and resources, reducing exposure to risk.

If there were no specification of the control applied, this would not be a good option.


upvoted 1 times

 **Shaman73** 1 year ago

**Selected Answer: C**

C. Safety controls should fail open.

upvoted 1 times

 **Yoez** 1 year, 1 month ago



**Selected Answer: C**

C. Safety controls should fail open: Safety controls, such as fire suppression systems or emergency exits, should indeed fail open. This means that in the event of a failure or malfunction, they should default to a state that ensures safety, such as allowing people to exit a building or mitigating hazards.

upvoted 4 times

  **Mehsotopes** 1 year, 1 month ago

**Selected Answer: C**

Fail Open:

\* Activates specified controls; in this case, safety measures such as sprinklers, or alarm systems to ensure the safety of staff members, & system devices.

Fail Close:

\* Locks controls such as access to the perimeter, & devices to protect from exfiltration.

upvoted 3 times

Which of the following would be best suited for constantly changing environments?

- A. RTOS
- B. Containers
- C. Embedded systems
- D. SCADA

**Correct Answer:** B

Community vote distribution

B (100%)

  **c469c8e** Highly Voted 10 months, 1 week ago

lacking context  
upvoted 9 times

  **dbrowndiver** Highly Voted 9 months ago

**Selected Answer: B**

In this scenario, Choice B is the correct answer. Containers is the correct answer because they are specifically designed to provide flexibility and scalability in constantly changing environments. Containers allow for rapid deployment and scaling, making them ideal for dynamic applications that need to adapt to frequent changes and updates. Furthermore containers are particularly well-suited for microservices architectures, continuous integration/continuous deployment (CI/CD) pipelines, and environments that need to rapidly adapt to change. Technologies like Docker and Kubernetes have made containers popular for modern application deployment.

upvoted 8 times

  **Syl0** Most Recent 9 months, 3 weeks ago

RTOS - real time OS  
SCADA - supervisory control and data acquisition  
upvoted 4 times

  **Shaman73** 1 year ago

**Selected Answer: B**

B containers  
upvoted 1 times

  **c18525f** 1 year ago

B containers  
upvoted 1 times

  **CyberPark17** 1 year, 1 month ago

answer is D, Containers, they provide a consistent and isolated environment for applications to run, regardless of the underlying infrastructure. They are highly portable and can be quickly deployed, making them a flexible solution for dynamic environments where applications need to be scaled, updated, or moved frequently. Real-time operating systems (RTOS) are designed for predictable and deterministic tasks, while embedded systems and SCADA are more specialized and may not be as adaptable to rapidly changing conditions.

upvoted 5 times

Which of the following incident response activities ensures evidence is properly handled?

- A. E-discovery
- B. Chain of custody
- C. Legal hold
- D. Preservation

**Correct Answer: B**

Community vote distribution

B (96%) 4%

 **dbrowndiver** Highly Voted 11 months ago

In this scenario, choice B is correct . Chain of custody is the correct answer because it is specifically designed to ensure that evidence is properly handled, tracked, and documented throughout the incident response process. This approach ensures the integrity and admissibility of evidence in legal settings by maintaining a clear and reliable record of its handling.

upvoted 7 times

 **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer: B**


B. Chain of custody

Chain of custody is the process that ensures evidence is properly handled and documented throughout its lifecycle. It tracks the evidence from the time it is collected, through its transportation, storage, and presentation in court, ensuring that it has not been altered or tampered with. Maintaining a proper chain of custody is critical for ensuring the integrity and admissibility of the evidence in legal proceedings.

Therefore, the correct answer is:

B. Chain of custody

upvoted 5 times

 **9149f41** Most Recent 4 months, 3 weeks ago


**Selected Answer: C**

Why C and D are not correct here:

Evidence of the properly handled is a broader term that including the whole court order.

Chain of custody is a broader concept that can include legal hold and preservation as part of its overall process.

upvoted 1 times

 **986d14e** 10 months, 1 week ago

**Selected Answer: B**

The answer is B. E-discovery has nothing to do with this.

upvoted 3 times

 **93a09c9** 10 months, 4 weeks ago

**Selected Answer: B**

The answer is B. E-discovery has nothing to do with this.

upvoted 3 times

 **Shaman73** 1 year ago

**Selected Answer: B**

B. Chain of custody

upvoted 1 times

 **SHADTECH123** 1 year, 1 month ago

**Selected Answer: B**

Chain of custody refers to the process of documenting the handling of evidence from the time it is collected until it is presented in court. This documentation includes details on who collected the evidence, how it was collected, transported, stored, and any transfers of possession

upvoted 3 times

🗨️ 👤 **Abcd123321** 1 year, 1 month ago

**Selected Answer: B**

Chain of Custody

- Documented and verifiable record that tracks the handling, transfer, and preservation of digital evidence from the moment it is collected until it is presented in a court of law

upvoted 1 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

**Selected Answer: B**

for me is B

upvoted 3 times

🗨️ 👤 **shady23** 1 year, 1 month ago

**Selected Answer: B**

B. Chain of custody

upvoted 2 times

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

**Selected Answer: B**

The correct answer is B. Chain of custody.

Chain of custody refers to the documentation and processes used to maintain control and accountability of evidence during an investigation. It ensures that evidence is properly handled, preserved, and protected from tampering, alteration, or loss.

upvoted 2 times

An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account. Which of the following would most likely prevent this activity in the future?

- A. Standardizing security incident reporting
- B. Executing regular phishing campaigns
- C. Implementing insider threat detection measures
- D. Updating processes for sending wire transfers

**Correct Answer:** D

Community vote distribution

D (83%)

B (17%)

  **Etc\_Shadow28000** Highly Voted 9 months ago

**Selected Answer: D**

D. Updating processes for sending wire transfers

Updating the processes for sending wire transfers would most likely prevent this type of activity in the future. This could include implementing additional verification steps, such as requiring multiple levels of approval, verifying new payment instructions through a separate communication channel, or implementing a callback procedure to confirm the authenticity of the instructions.



Therefore, the correct answer is:

D. Updating processes for sending wire transfers  
upvoted 11 times

  **danielbadasu** 2 weeks, 3 days ago

Well said

upvoted 1 times

  **braveheart22** Most Recent 7 months, 3 weeks ago

**Selected Answer: D**

The Answer: D. Updating processes for sending wire transfers

This approach directly addresses the root cause of the fraudulent transaction – the lack of a secure, verified process for handling wire transfers – and would help prevent similar incidents from occurring in the future.

upvoted 2 times

  **dbrowndiver** 9 months ago

**Selected Answer: D**

In this scenario, the option should be D because updating processes for sending wire transfers is the best choice, it directly tackles the procedural weakness that allowed the fraudulent transaction to occur. Implementing verification and approval procedures can prevent similar incidents by ensuring that all payment instructions are authenticated and verified before any money is transferred, thereby reducing the risk of fraud.

upvoted 3 times

  **EfaChux** 10 months, 2 weeks ago

**Selected Answer: B**

The accounting clerk acted in ignorance. more phishing campaigns would have prevented the transfer

upvoted 3 times

  **3330278\_111** 10 months, 1 week ago

It doesn't really prevent it the same way that updating a process for sending a wire transfer would. What phishing campaigns do is reduce the likelihood of it happening again, which isn't what the question is asking for

upvoted 3 times

  **mshaheerm** 6 months, 1 week ago

The question is asking exactly this: "Which of the following would most likely prevent this activity in the future?" I think the answer is B

upvoted 1 times

🗨️ 👤 **3396ee7** 1 year ago

A is the correct answer

upvoted 2 times

🗨️ 👤 **8f23125** 2 months, 1 week ago

A. Standardizing security incident reporting: Helps after an incident occurs but doesn't prevent it.

upvoted 1 times

🗨️ 👤 **Shaman73** 1 year ago

**Selected Answer: D**

D. Updating processes for sending wire transfers

upvoted 1 times



A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

- A. Off-the-shelf software
- B. Orchestration
- C. Baseline
- D. Policy enforcement

**Correct Answer:** B

Community vote distribution

B (100%)

  **e5c1bb5** Highly Voted 1 year, 1 month ago

**Selected Answer: B**

A makes no sense

B orchestration and automation are treated as the same in the exam objectives so not sure on this one

C establishing a baseline (confused on this one) a baseline for what? if it means a baseline for account creation then yes, if it means a baseline like a policy then no..

D policy enforcement.. idk if you'd need to write a script for that as much as you'd rely on software..

going with B since the first part of the question doesnt mention automation/orchestration even though the question is very poorly worded.

upvoted 11 times

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: B**

Orchestration provides a comprehensive approach to automating complex workflows, making it an excellent choice for efficiently managing account creation processes in large-scale environments.Orchestration is ideal for automating the creation of user accounts, as it can handle the sequence of tasks required to set up accounts, such as creating usernames, assigning permissions, configuring email, and setting up directory services.

upvoted 6 times

  **Shaman73** Most Recent 1 year ago

**Selected Answer: B**

B. Orchestration

upvoted 1 times

  **c80f5c5** 1 year ago

Orchestration refers to the automated configuration, management, and coordination of complex computer systems, applications, and services. In the context of creating a script for account creation, orchestration is a good use case because it allows the systems administrator to automate the entire process of creating user accounts efficiently and accurately, thereby saving time and reducing human error.

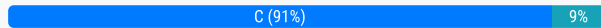
upvoted 4 times

A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

- A. Processor
- B. Custodian
- C. Subject
- D. Owner

**Correct Answer:** C

Community vote distribution



**E0tero** Highly Voted 1 year, 1 month ago

From Professor Messer study notes:

Data subject

- Any information relating to an identified or identifiable natural person
  - An individual with personal data
- This includes everyone
  - Name, ID number, address information, genetic makeup, physical characteristics, location data, etc.
  - You are the data subject
- Laws and regulations
  - Privacy is ideally defined from the perspective of the data subject

Data owner

- Accountable for specific data, often a senior officer
- VP of Sales owns the customer relationship data
- Treasurer owns the financial information

I'm also going with C.

upvoted 17 times

**Etc\_Shadow28000** Highly Voted 9 months ago

Selected Answer: C

C. Subject

In the context of data roles, the customer whose sensitive data is being collected, modified, and stored is referred to as the "Subject." The data subject is the individual to whom the data pertains.

Therefore, the correct answer is:

C. Subject

upvoted 8 times

**9149f41** Most Recent 4 months, 3 weeks ago

Selected Answer: C

Easy to remember the role:

- Owner (D): The hospital (owns and controls the data).
- Processor (A): The cloud service provider (processes the data on behalf of the hospital).
- Custodian (B): The IT team (manages the technical aspects of the data).
- Subject (C): The patient (the individual whose data is being collected).



The question says: Which of the following data roles describes the customer? So, the customer is always a SUBJECT.

upvoted 7 times

🗨️ 👤 **Dimpo\_Oz** 7 months ago

**Selected Answer: C**

Data is object

person interacting with object is subject

upvoted 1 times

🗨️ 👤 **AutoroTink** 9 months ago

**Selected Answer: C**

The Marketing Department Head or other senior-level manager is likely something like the Data Protection Officer or Owner, responsible for the data. The Infrastructure Team are likely the Custodians.

The data is likely being collected and processed by lower-level employees and/or automated processes. These would be the Data Processors.

That leaves the customer whose data is being collected. They aren't the owners of their own data (like others have stated), but they are the data subject. So C is the most accurate answer.

upvoted 3 times

🗨️ 👤 **Fhaddad81** 9 months, 4 weeks ago

D is the correct Answer as Data subject is who own the data while Owner is the customer that data subject given their data. Data subject is not mentioned on Udemy course !!

upvoted 1 times

🗨️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: C**

chat gpt

upvoted 1 times

🗨️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: C**

In this scenario, the customers are the data subjects because the sensitive information collected, modified, and stored by the marketing department pertains to them. The customers are the individuals whose data is being processed.

upvoted 3 times

🗨️ 👤 **Shaman73** 1 year ago

**Selected Answer: C**

C. Subject

upvoted 1 times

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

**Selected Answer: C**

Answer is c. Technically the customer does own their own data, however in the Cybersecurity context the Owner is someone within the organization. According to ISO/IEC 27001, the data owner is responsible for ensuring the confidentiality, integrity, and availability of information assets.

upvoted 2 times

🗨️ 👤 **Xavierallen9711** 1 year, 1 month ago

**Selected Answer: D**

Owner is the right answer

upvoted 1 times

🗨️ 👤 **fd4ea1a** 7 months, 1 week ago

Owner is the person collecting the data. Subject is who the data belongs to or who actually provided it.

A subject will always be the customer.

upvoted 1 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

**Selected Answer: C**

C. Subject

In this scenario, the customer is the subject of the sensitive data being collected, modified, and stored by the marketing department. The customer's data is being processed and managed by the marketing department, but the customer themselves is the subject of that data. They are the individuals to whom the data pertains.

upvoted 4 times

🗨️ 👤 **e5c1bb5** 1 year, 1 month ago

**Selected Answer: C**

although not covered in study material ive looked at, the customer is definately not the processor or the controller. owners are usually senior management so thats out. going with subject.

upvoted 2 times

🗨️ 👤 **E0tero** 1 year, 1 month ago

It is for Professor Messer's SY0-701 notes.

upvoted 1 times

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

**Selected Answer: D**

Why wouldn't the customer be the data owner? I don't remember Data Subject being apart of the 701 Course

upvoted 2 times

🗨️ 👤 **E0tero** 1 year, 1 month ago

5.4 Summarize elements of effective security compliance.

upvoted 1 times

Which of the following describes the maximum allowance of accepted risk?

- A. Risk indicator
- B. Risk level
- C. Risk score
- D. Risk threshold

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: D**

This refers to the point or level of risk that an organization is willing to tolerate. Beyond this threshold, actions must be taken to mitigate or reduce the risk to an acceptable level. It defines the boundary between acceptable and unacceptable risk.

-The risk threshold is essentially the upper limit of risk that is deemed acceptable by an organization. It serves as a guideline for decision-making regarding risk management and response strategies.

-Organizations set risk thresholds based on their risk appetite and tolerance, helping them determine when to take action and allocate resources for risk mitigation.

upvoted 9 times

 **Robuste7** Most Recent 5 months, 1 week ago

**Selected Answer: D**

A risk threshold is the maximum level of risk an individual or organization is willing to accept before taking action to reduce or mitigate it.

In simple terms, it's the line you won't cross when it comes to taking risks. Anything above this level requires intervention to manage or reduce the risk.

upvoted 1 times

 **Shaman73** 1 year ago

**Selected Answer: D**

D. Risk threshold

upvoted 1 times

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

- A. A worm is propagating across the network.
- B. Data is being exfiltrated.
- C. A logic bomb is deleting data.
- D. Ransomware is encrypting files.

**Correct Answer:** B

Community vote distribution

B (100%)

dbrowndiver Highly Voted 11 months ago

Selected Answer: B

The scenario describes an internal system sending unusual and large amounts of DNS queries to external systems, especially during non-business hours. This behavior is indicative of data exfiltration, where an attacker tries to move data out of the network covertly.

upvoted 6 times

baronvon Highly Voted 10 months, 3 weeks ago

Selected Answer: B

B. Data is being exfiltrated.

A large volume of DNS queries to external systems during non-business hours can indicate that data is being exfiltrated. Attackers often use DNS queries to covertly extract data from compromised systems, as DNS traffic is less likely to be scrutinized compared to other types of network traffic.

upvoted 5 times

MaxiPrince Most Recent 6 months, 2 weeks ago

Selected Answer: B

Data is being exfiltrated.

upvoted 1 times

Shaman73 1 year ago

Selected Answer: B

B. Data is being exfiltrated.

upvoted 2 times

MahiMahiMahi 1 year ago

Selected Answer: B

B. Data is being exfiltrated.

upvoted 2 times

A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

- A. Default credentials
- B. Non-segmented network
- C. Supply chain vendor
- D. Vulnerable software

**Correct Answer:** C

Community vote distribution



**Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer: B**

B. Non-segmented network

Opening ports on a firewall for a new system introduces the risk that the new system might be deployed on a non-segmented network. This means that the new system and its traffic could potentially be exposed to other parts of the network, increasing the risk of lateral movement by an attacker if the system is compromised. Network segmentation helps in containing potential breaches and limiting access to sensitive areas of the network.

Therefore, the correct answer is:

B. Non-segmented network  
upvoted 22 times

**Eracle** 5 months, 3 weeks ago

The question is "risk IN THE new system" not for the existing system  
upvoted 5 times

**hasquaati** Highly Voted 1 year, 1 month ago

**Selected Answer: C**

I am thinking that opening firewall ports is a Layer 3 and Layer 4 issue and not a Layer 7 vulnerability, which is where the Vulnerable software would fit in. I would be more concerned about the Cloud provider which is why I am choosing C: Supply Chain Vendor.  
upvoted 14 times

**1chung** Most Recent 1 month ago

**Selected Answer: D**

I go with D  
upvoted 1 times

**n3412** 2 months, 1 week ago

**Selected Answer: C**

In this scenario, the technician is opening firewall ports to support a SaaS (Software as a Service) provider, which means that part of the system relies on external services managed by a third party. This introduces a supply chain risk because the organization now depends on the security posture and integrity of the SaaS provider.  
upvoted 3 times

**JoeRealCool** 2 months, 3 weeks ago

**Selected Answer: C**

C and D are both correct, but C is more correct simply because it mentions the SaaS. SaaS is, in it's own way, part of the supply chain.  
upvoted 1 times

**squishy\_fishy** 3 months, 4 weeks ago

**Selected Answer: C**

Since the new system is provided and supported by a SaaS (Software-as-a-Service) provider, the primary risk is third-party security vulnerabilities associated with the supply chain vendor.

Why is this a risk?

The SaaS provider could have weak security controls, leading to data breaches or unauthorized access.

If the SaaS provider is compromised, attackers could use their access to infiltrate your organization's systems.

Opening firewall ports increases exposure to potential supply chain attacks, especially if the SaaS vendor has vulnerabilities in their infrastructure.

upvoted 2 times

🗳️ 👤 **Strissel** 4 months ago

**Selected Answer: C**

Straight from the CompTIA study guide the answer is supply chain vendor. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices.

upvoted 1 times

🗳️ 👤 **Oluwatobi4880** 4 months, 1 week ago

**Selected Answer: D**

The correct answer is D. Vulnerable software.

Opening ports on a firewall can expose the system to potential vulnerabilities in the software being used, which may be exploited by attackers if the software is not kept updated or if it contains inherent security weaknesses.

upvoted 2 times

🗳️ 👤 **Markie100** 4 months, 3 weeks ago

**Selected Answer: C**

The risk in the new system being deployed and supported by a SaaS (Software as a Service) provider is C. Supply chain vendor.

Supply chain vendor (C): When relying on a SaaS provider, the security of the system is partially dependent on the vendor's practices. If the vendor has weak security controls, it could introduce risks such as data breaches, vulnerabilities, or compliance issues. This is a significant concern because the organization has limited control over the vendor's security measures.

(A): While default credentials are a risk, they are typically associated with initial setup and configuration, not directly related to the SaaS provider or firewall port configuration.

(B): Network segmentation is important for security, but it is not directly tied to the SaaS provider or the act of opening firewall ports.

(D): Vulnerable software is a risk, but it is more relevant to the software running on the system rather than the SaaS provider or firewall configuration.

upvoted 1 times

🗳️ 👤 **ITExperts** 5 months, 1 week ago

**Selected Answer: B**

B is the answer

upvoted 1 times

🗳️ 👤 **beebax** 5 months, 1 week ago

**Selected Answer: D**

This directly points to flaws within the software itself, making it a specific and critical risk in the new system.

upvoted 1 times

🗳️ 👤 **760b372** 5 months, 2 weeks ago

**Selected Answer: D**

Opening ports creates potential entry points into the system. If the system or software being deployed has vulnerabilities, attackers can exploit the open ports to compromise the system.

upvoted 1 times

🗳️ 👤 **41c27e6** 6 months ago

**Selected Answer: C**

C: Supply Chain Vendor.

upvoted 2 times

🗳️ 👤 **Benny\_On** 6 months, 3 weeks ago

**Selected Answer: D**

I think zero-day vulnerability on new system can be out-of-hands Cloud Provider, so i think D will be fit answer

upvoted 1 times

🗳️ 👤 **Benny\_On** 6 months, 3 weeks ago

Additional, be attention to key word of the question "Risk on new system"

upvoted 1 times

🗨️ 👤 **ProudFather** 6 months, 4 weeks ago

**Selected Answer: C**

C. Supply chain vendor

The primary risk in this scenario is the supply chain vendor. Since the system is a SaaS offering, the security of the underlying infrastructure and applications relies heavily on the vendor's security practices.

Here's a breakdown of why the other options aren't as relevant: the most significant risk in this scenario is the potential for vulnerabilities or security breaches within the SaaS provider's infrastructure or applications.

upvoted 2 times

🗨️ 👤 **Fourgehan** 7 months ago

**Selected Answer: C**

When deploying and supporting a system provided by a SaaS (Software as a Service) vendor, the supply chain vendor risk becomes a primary concern. The organization is relying on the SaaS provider for security, availability, and compliance. Risks include:

The SaaS provider's systems being compromised.

Lack of transparency in the vendor's security measures.

Potential vulnerabilities in the SaaS platform affecting the organization.

These risks emphasize the importance of vendor assessments, contractual security requirements, and regular audits

upvoted 1 times

🗨️ 👤 **Dimpo\_Oz** 7 months ago

**Selected Answer: C**

you are opening firewall for a third party, ie allowing a third party into your network bringing all their vulnerabilities along for the ride. Supply chain vendor by definition

upvoted 1 times

A systems administrator is working on a solution with the following requirements:

- Provide a secure zone.
- Enforce a company-wide access control policy.
- Reduce the scope of threats.

Which of the following is the systems administrator setting up?

- A. Zero Trust
- B. AAA
- C. Non-repudiation
- D. CIA

**Correct Answer:** A

Community vote distribution



A (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer:** A

Zero Trust is a security framework that aligns perfectly with the given requirements. It emphasizes strict access control, minimizing trust, and ensuring that all access requests are verified, making it an ideal choice for creating a secure environment.

upvoted 11 times

  **squishy\_fishy** Most Recent 3 months, 4 weeks ago

**Selected Answer:** A

The Zero Trust security model is based on the principle of “never trust, always verify.” It aligns with the given requirements:

Provide a secure zone – Zero Trust micro-segmentation ensures that only authorized users and devices can access specific network areas.

Enforce a company-wide access control policy – Zero Trust implements strict access controls using authentication and least privilege principles.

Reduce the scope of threats – By assuming that threats exist inside and outside the network, Zero Trust reduces attack surfaces and prevents lateral movement by attackers.

Zero Trust requires continuous authentication and authorization, using technologies such as multi-factor authentication (MFA), identity-based access controls, and network segmentation.

upvoted 1 times

  **9149f41** 4 months, 3 weeks ago

**Selected Answer:** A

Why D. CIA is not correct:

CIA (Confidentiality, Integrity, Availability):

CIA is a security model that focuses on protecting data, but it is not a framework or architecture like Zero Trust. It does not directly address the requirements listed.

upvoted 2 times

  **squishy\_fishy** 3 months, 4 weeks ago

CIA is a foundational security principle, not a specific security framework like Zero Trust.

CIA ensures data protection, but it does not specifically address access control enforcement and segmentation.

upvoted 1 times

  **Shaman73** 1 year ago

**Selected Answer:** A

A. Zero Trust

upvoted 1 times



Which of the following involves an attempt to take advantage of database misconfigurations?


- A. Buffer overflow
- B. SQL injection
- C. VM escape
- D. Memory injection

**Correct Answer:** B

Community vote distribution

B (92%)

8%

  **internslayer** Highly Voted 10 months, 2 weeks ago

My problem with this question is that it's not a misconfigured database that allows SQL injection, it's improperly sanitized user input fields in applications/web pages.

upvoted 11 times

  **MAKOhunter33333333** Highly Voted 1 year, 1 month ago

**Selected Answer:** B

SQL Injection takes advantage of the misconfiguration of SQL databases and that do not validate input

upvoted 6 times

  **Linas312** Most Recent 2 months, 1 week ago

**Selected Answer:** A

There is literally no correct answer, I'm even more mad to see the answer "SQL injection", SQLi happens because a service/application that interacts with the DB is not coded "Safely" or doesn't handle user input correctly, SQLi never happens because the DB itself is misconfigured

upvoted 1 times

  **dbrowndiver** 11 months ago

**Selected Answer:** B

SQL injection is an attack that targets vulnerabilities in a database by injecting malicious SQL code into input fields. It takes advantage of misconfigured or improperly secured databases that do not validate or sanitize user input.

upvoted 5 times

  **Shaman73** 1 year ago

**Selected Answer:** B

B. SQL injection

upvoted 1 times

Which of the following is used to validate a certificate when it is presented to a user?

- A. OCSP
- B. CSR
- C. CA
- D. CRC

**Correct Answer: A**

Community vote distribution

A (68%)

C (32%)

  **c80f5c5** Highly Voted 1 year ago

CA issues and manages certificates.

OSCP - Online Certificate Status Protocol, a protocol that checks a certificate for validity and if its been revoked (by the CA).



The answer is OSCP. CA is like Congress, OSCP is like police. Congress records laws and writes them but don't actually enforce anything. Police enforce them

upvoted 48 times

  **danielbadasu** 2 weeks, 3 days ago

Well explained

upvoted 1 times

  **braveheart22** Most Recent 7 months, 3 weeks ago

**Selected Answer: A**

A is the right answer from my point of view.

OCSP (Online Certificate Status Protocol):

OCSP is used to validate the revocation status of a digital certificate. When a certificate is presented to a user, OCSP allows the recipient to query the Certificate Authority (CA) in real time to check if the certificate has been revoked before its expiration date. This is especially useful for determining whether a certificate is still valid or if it has been revoked due to compromise or other reasons.

Relevant to the question: OCSP helps in validating the revocation status of a certificate when it is presented.

upvoted 4 times

  **2fd1029** 9 months, 2 weeks ago

**Selected Answer: A**

Gotta be A. Can't be the CA because the CA issues the certs but isn't referred to for validating them, that's the CRL or OCSP.

upvoted 1 times

  **Cee007** 9 months, 4 weeks ago

**Selected Answer: A**

A OCSP

upvoted 1 times

  **a4e15bd** 10 months, 2 weeks ago

It is A OCSP

This is a mechanism used to check the validity of a certificate in real time. When a certificate is presented, the user's system queries the OCSP responder to verify that the certificate is still valid and has not be revoked by CA.

The CA is responsible for issuing, revoking and managing digital certificates, but it does not perform the real time validation of the certificates.

upvoted 2 times

  **chasingsummer** 10 months, 2 weeks ago

**Selected Answer: A**

I don't think they are trying to trick us. I pick the simple answer.

upvoted 1 times

  **Crucible\_Bro** 10 months, 3 weeks ago

Selected Answer: A

A. Online Certificate Status Protocol is the actual protocol that is validating the request.

A CA simply manages those validations.

upvoted 1 times

dbrowndiver 11 months ago

Selected Answer: A

When a certificate is presented to a user as written in the scenario(e.g., when visiting a secure website), the system can use OCSP to query the CA's OCSP responder. This helps determine whether the certificate is still valid or has been revoked.

-Real-Time Validation: Unlike Certificate Revocation Lists (CRLs), which are static lists of revoked certificates, OCSP provides dynamic, up-to-date information about the certificate's status, allowing for timely detection of compromised or invalid certificates.

Why this is the best fit: Security Assurance: By using OCSP, systems can ensure that a presented certificate is not only genuine but also has not been revoked due to compromise or other reasons. This real-time validation is critical for maintaining secure communications.

upvoted 2 times

WOW\_ThatsCrazy 12 months ago

Selected Answer: A

OCSP is used to validate the status of a digital certificate in real-time. When a certificate is presented to a user, the OCSP responder can be queried to check if the certificate is still valid or if it has been revoked. This provides a more efficient and timely method of certificate validation compared to traditional CRL (Certificate Revocation List) checks.

upvoted 2 times

Etc\_Shadow28000 1 year ago

Selected Answer: A

A. OCSP (Online Certificate Status Protocol)

OCSP is used to validate a certificate when it is presented to a user by checking the certificate's revocation status. It provides real-time status information about the validity of a certificate, ensuring that it has not been revoked.

Therefore, the correct answer is:

A. OCSP

upvoted 2 times

drosas84 1 year ago

Selected Answer: C

the question is tricky. It is basically asking what is "used" to validate a certificate when it is presented to a user. Meaning, what do you use to validate a certificate when giving it to a user to use? a CA.

An OCSP checks whether a certificate is valid or revoked, it doesn't validate a certificate.

This is how I read the question.

upvoted 4 times

a4e15bd 11 months, 1 week ago

I think you are just contradicting yourself in the last part. If OCSP checks whether a certificate is valid or not, that is validating the certificate.

upvoted 1 times

edmondme 1 year ago

Selected Answer: A

They are looking for the protocol OCSP

upvoted 1 times

Shaman73 1 year ago

Selected Answer: A

A. OCSP

upvoted 1 times

123456789User 1 year ago

Selected Answer: C

Certificate Authority

upvoted 3 times

One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

- A. Virtualization
- B. Firmware
- C. Application
- D. Operating system

**Correct Answer:** B

Community vote distribution

B (100%)

dbrowndiver Highly Voted 11 months ago

Selected Answer: B

Firmware is the correct answer because a BIOS update addresses vulnerabilities at the firmware level. The BIOS is an essential component of the system's firmware, and updates to it are intended to fix security vulnerabilities, improve compatibility, and enhance overall system stability.

upvoted 8 times

SHAGZZ Most Recent 5 months ago

Selected Answer: B

BIOS is simply "Basic Input/Output System"

upvoted 1 times

Shaman73 1 year ago

Selected Answer: B

B. Firmware

upvoted 1 times

Which of the following is used to quantitatively measure the criticality of a vulnerability?

- A. CVE
- B. CVSS
- C. CIA
- D. CERT

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **leedsbarber** Highly Voted 1 year, 1 month ago  
Answer is B

A - Common Vulnerabilities & Exposures is a dictionary of known threats.  
B - Common Vulnerability Scoring System quantifies how critical a vulnerability is.  
C - Confidentiality, Integrity & Availability is a security concept.  
D - Computer Emergency Response Team - the title speaks for itself!  
upvoted 15 times

🗳️ 👤 **Abcd123321** Highly Voted 1 year, 1 month ago  
Selected Answer: B  
Common Vulnerability Scoring System (CVSS)

- Used to provide a numerical score reflecting the severity of a vulnerability (0 to 10)
- Scores are used to categorize vulnerabilities as none, low, medium, high, or critical
- Scores assist in prioritizing remediation efforts but do not account for existing mitigations

upvoted 6 times

🗳️ 👤 **Chickenbuttbrown** Most Recent 6 months, 1 week ago  
Selected Answer: B  
i cant even say this question  
upvoted 2 times

🗳️ 👤 **MaxiPrince** 6 months, 2 weeks ago  
Selected Answer: B  
Common Vulnerability Scoring System  
upvoted 1 times

🗳️ 👤 **braveheart22** 7 months, 3 weeks ago  
Selected Answer: B  
B is the way to go.

CVSS (Common Vulnerability Scoring System) is the system specifically designed to quantitatively measure the criticality or severity of a vulnerability based on factors such as exploitability and potential impact. It provides a numerical score that helps organizations prioritize vulnerability management efforts.  
upvoted 1 times

🗳️ 👤 **dbrowndiver** 11 months ago  
Selected Answer: B  
CVSS (Common Vulnerability Scoring System) is the correct answer because it is specifically designed to quantitatively measure the criticality of a vulnerability. CVSS provides a standardized scoring mechanism that helps organizations assess the severity and impact of vulnerabilities, allowing for effective prioritization and remediation efforts.  
upvoted 4 times

 **Shaman73** 1 year ago

**Selected Answer: B**

B. CVSS

upvoted 2 times

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

- A. Configure all systems to log scheduled tasks.
- B. Collect and monitor all traffic exiting the network.
- C. Block traffic based on known malicious signatures.
- D. Install endpoint management software on all systems

**Correct Answer:** D

Community vote distribution

D (100%)

dbrowndiver Highly Voted 11 months ago

Selected Answer: D

Install endpoint management software on all systems is the correct answer because it offers a comprehensive solution for monitoring and managing workstations and servers. Endpoint management software provides visibility into unauthorized changes, detects unapproved software installations, and enforces security policies, making it the most effective choice for ensuring system integrity and compliance.

upvoted 7 times

9149f41 Most Recent 4 months, 3 weeks ago

Selected Answer: D

Why B is not correct: Collect and monitor all traffic exiting the network.

The questions are all about hardware, not network. But the B is relevant with network traffic.

upvoted 1 times

MaxiPrince 6 months, 2 weeks ago

Selected Answer: D

Install endpoint management software on all systems

upvoted 1 times

famuza77 8 months, 2 weeks ago

I thought Endpoints managment were only for workstations and no servers.

upvoted 1 times

Shaman73 1 year ago

Selected Answer: D

D. Install endpoint management software on all systems

upvoted 4 times

An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

- A. Data in use
- B. Data in transit
- C. Geographic restrictions
- D. Data sovereignty

**Correct Answer:** B

*Community vote distribution*

B (100%)

dbrowndiver **Highly Voted** 11 months ago

**Selected Answer: B**

Data in transit is the correct answer because a VPN is specifically designed to protect data as it moves between two locations. By encrypting the data and securing the communication path, the VPN ensures that information remains confidential and secure during transmission, making it the most relevant choice for this scenario.

upvoted 9 times

MaxiPrince **Most Recent** 6 months, 2 weeks ago

**Selected Answer: B**

Data in transit

upvoted 1 times

Zach123654 11 months, 2 weeks ago

**Selected Answer: B**

GPT!!!

upvoted 1 times

Shaman73 1 year ago

**Selected Answer: B**

B. Data in transit

upvoted 1 times



After reviewing the following vulnerability scanning report:

```
Server:192.168.14.6
Service: Telnet
Port: 23 Protocol: TCP
Status: Open Severity: High
Vulnerability: Use of an insecure network protocol
```

A security analyst performs the following test:

```
nmap -p 23 192.168.14.6 --script telnet-encryption
```

```
PORT      STATE SERVICE REASON
23/tcp    open  telnet  syn-ack
| telnet encryption:
|_ Telnet server supports encryption
```

Which of the following would the security analyst conclude for this reported vulnerability?

- A. It is a false positive.
- B. A rescan is required.
- C. It is considered noise.
- D. Compensating controls exist.

**Correct Answer: A**

Community vote distribution

A (57%)

D (42%)

 **mr\_reyes** Highly Voted 1 year, 1 month ago

**Selected Answer: A**

False Positive:

A false positive occurs when a vulnerability scanner incorrectly identifies a vulnerability that doesn't actually exist. In this case, the initial vulnerability report flagged the use of an insecure network protocol (Telnet) on the server at 192.168.14.6.

However, the follow-up test using Nmap with the telnet-encryption script revealed that the Telnet server supports encryption. Since encryption enhances security, the initial report was incorrect.

Therefore, the conclusion is that the initial report was a false positive.

upvoted 19 times

 **a4e15bd** 11 months ago

Telnet itself is inherently insecure and it transmits data including passwords in plaintext making it vulnerable to interception and eavesdropping.

While using encryption with telnet is not typical but it is possible, however there are other secure alternatives out there like SSH. So while it is true that Telnet is an insecure protocol, having encryption is just a compensating control here. So the answer is D.

upvoted 21 times

 **420JhonnySins69** 9 months, 3 weeks ago

Option D is the more reasonable.

Compensating controls. is a secondary/supporting security control that prevents the vulnerability from being exploited.  
(encryption in this case)

False Positive: believes that there's a vulnerability but when physically checked is not there.  
(Telnet is being used, the vulnerability of plain text is there.)

False positive

[https://youtu.be/EJL0h4u871w?list=PL7XJSuT7Dq\\_UDJgYoQGIW9viwM5hc4C7n&t=6652](https://youtu.be/EJL0h4u871w?list=PL7XJSuT7Dq_UDJgYoQGIW9viwM5hc4C7n&t=6652)

Objective (4.3 Explain various activities associated with vulnerability management)

[https://youtu.be/EJL0h4u871w?list=PL7XJSuT7Dq\\_UDJgYoQGIW9viwM5hc4C7n&t=7199](https://youtu.be/EJL0h4u871w?list=PL7XJSuT7Dq_UDJgYoQGIW9viwM5hc4C7n&t=7199)

upvoted 12 times

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: A**

Why This Is a False Positive:

1. Understanding Telnet:

General Security Issues: Telnet typically transmits data in plaintext, making it susceptible to eavesdropping and other security vulnerabilities. This is why it is often flagged in security scans.

2. Encryption Support:

Security Enhancement: The presence of encryption changes the security profile of Telnet. If encryption is supported and properly implemented, the transmission of data is secure, counteracting the usual vulnerabilities associated with Telnet.

3. Initial Assessment:

Misinterpretation: The initial report indicated a vulnerability due to a general assumption that Telnet is insecure, without verifying the specific configuration that includes encryption.

4. Conclusion:

False Positive: Since the Telnet server supports encryption, the assumption of insecurity was incorrect. The vulnerability scanner flagged an issue based on typical characteristics rather than the actual configuration of this specific Telnet implementation.



upvoted 9 times

  **1chung** Most Recent 3 days, 3 hours ago

**Selected Answer: D**

I go with D

upvoted 1 times



  **Linus312** 2 months, 3 weeks ago

**Selected Answer: A**

Horrible question, Telnet is an insecure protocol by design, encryption or no encryption.. period

Nmap scan only confirms that it supports encryption, means nothing really, should look to implement something more secure like SSH or jumpbox.. if that's what is meant by D. that would be the answer however the "Theory question" answer here is probably A.

upvoted 1 times

  **Commando9800** 3 months, 2 weeks ago

**Selected Answer: D**

D. Compensating controls exist.

My explaining:

Vulnerability detected is : Use of an insecure network protocol

Having an encryption doesn't change the fact that Telnet is an insecure protocol

The answer would be False Positive if the vulnerability detected was lack of encryption

In the end Compia decide the ultimate truth in this exam so



upvoted 1 times

  **testpan** 3 months, 2 weeks ago

**Selected Answer: A**

According to ChatGPT , it says origin report is "Use of an insecure network protocol", but when using nmap to test , it discover "Telnet server supports encryption" , so it means this is contradict to the origin report, so this is False Positive

upvoted 1 times

  **Russell15** 3 months, 3 weeks ago

**Selected Answer: D**

False positive (A) would mean Telnet was incorrectly flagged as insecure—but Telnet is still a risk by default.

Compensating controls (D) is correct because encryption helps mitigate the risk, but the risk still exists.

upvoted 4 times

  **Catalyst33** 4 months, 3 weeks ago

**Selected Answer: D**

Adding encryption to telnet does not make it as secure as SSH which the scanner would not pick up as a vulnerability. Sure you have encryption, but what about authentication?

upvoted 2 times

  **Rackup** 5 months ago

**Selected Answer: A**

The vulnerability scanner flagged the use of Telnet as an insecure network protocol, which is typically true because Telnet is unencrypted. However, the security analyst ran a test using Nmap and found that the Telnet server supports encryption. This suggests that the reported vulnerability was a false positive. Since the server supports encryption, the actual risk is mitigated, and the vulnerability scanning report is inaccurate in this context.

upvoted 1 times

🗄️ 👤 **WTD34** 5 months, 1 week ago

**Selected Answer: D**

The question is asking "what can be concluded". We know that telnet is unsafe by default. We also know that there is an option for encryption as said by the last line "telnet server supports encryption". Thus the answer must be that we can conclude Compensating Controls Exist. answer is D

upvoted 2 times

🗄️ 👤 **limatsao** 5 months, 1 week ago

**Selected Answer: A**

The correct answer is:

A. It is a false positive.

Explanation:

The vulnerability scan initially flagged the use of Telnet as insecure because Telnet traditionally sends data, including credentials, in plaintext. However, the nmap test with the --script telnet-encryption option shows that the Telnet server supports encryption, which mitigates the reported risk.

This means the vulnerability scanner flagged the issue without accounting for the encryption capability, leading to a false positive.

Why the other options are incorrect:

B. A rescan is required: The manual test using nmap already confirmed that encryption is supported, so a rescan is unnecessary.

C. It is considered noise: Noise refers to irrelevant or unimportant alerts. This finding was important to verify but is ultimately a false positive, not noise.

D. Compensating controls exist: The encryption supported by the Telnet server is not a compensating control but a direct mitigation of the issue.

upvoted 1 times

🗄️ 👤 **Storcaks** 5 months, 1 week ago

**Selected Answer: D**

The scan only reports that the telnet server SUPPORTS encryption, but there's no information that state that it is required to use encryption by a client. A client that doesn't know the server supports encryption will most likely use default settings without it. Unlike SSH which is always encrypted by default. Telnet itself is inherently insecure just like FTP is. With this in mind the only choice that makes sense is D.

upvoted 2 times

🗄️ 👤 **Anyio** 5 months, 1 week ago

**Selected Answer: A**

By the way, this is a better use case of compensating controls: An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system.

upvoted 1 times

🗄️ 👤 **Anyio** 5 months, 1 week ago

**Selected Answer: A**

The Answer is A: If the only issue that makes Telnet unsafe is because Telnet traditionally uses unencrypted communication, because it now clearly shows that it has been taken care of.

The Answer is D: If there are other reasons not to use telnet besides it being unencrypted. If you can mention any other reasons or vulnerabilities then D will be the answer as encrypting it will just be a compensating solution.

upvoted 1 times

🗄️ 👤 **1022572** 5 months, 3 weeks ago

**Selected Answer: D**

The security scan shows telnet port as open and so did the NMAP scan.

It is not a false positive

A rescan is not required

It is not noise

D. Compensating Controls is the only correct answer.

upvoted 3 times

🗄️ 👤 **41c27e6** 6 months ago



Selected Answer: D

Impossible to be A, here is why:

Telnet itself is ALWAYS unencrypted. So, the vulnerability identified is TRUE.

However, there are techniques to support Telnet security and data encryption (like VPN).

upvoted 2 times

  **darpanne** 6 months, 2 weeks ago

Selected Answer: D

Most vulnerability scanners (e.g., Nessus, Qualys, OpenVAS) flag Telnet as a vulnerability by default because it is inherently insecure, transmitting data in plaintext. Even with encryption enabled, Telnet remains risky compared to alternatives like SSH due to:

Lack of MFA and Kerberos support,

No data integrity checks,

Susceptibility to brute-force attacks,

Absence of session protection.

If encryption exists:

Modern scanners may detect it and lower the severity but will still warn about Telnet use since the protocol itself is outdated and insecure.

Conclusion: Security professionals consider Telnet deprecated and risky, regardless of encryption. Thus, it is not a false positive, and D (compensating controls exist) is correct here.

upvoted 2 times

An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system. Which of the following best describes the actions taken by the organization?

- A. Exception
- B. Segmentation
- C. Risk transfer
- D. Compensating controls

**Correct Answer: D**

Community vote distribution

D (96%)

4%

🗳️ 👤 **Th3irdEye** Highly Voted 1 year, 1 month ago

**Selected Answer: D**

The word "legacy" should inform that this action is compensating.

upvoted 11 times

🗳️ 👤 **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer: D**

D. Compensating controls

The actions taken by the organization—disabling unneeded services and placing a firewall in front of a business-critical legacy system—are examples of compensating controls. Compensating controls are security measures that are implemented to mitigate risk when the primary controls are not feasible or sufficient. In this case, since the legacy system might have inherent vulnerabilities that cannot be fully addressed, the organization has implemented additional controls to reduce the risk.

Therefore, the correct answer is:

D. Compensating controls

upvoted 9 times

🗳️ 👤 **EngAbood** Most Recent 5 months ago

**Selected Answer: D**

Legacy = Compensating

upvoted 2 times

🗳️ 👤 **G30** 6 months ago

**Selected Answer: D**

By implementing compensating controls (disabling unneeded services and using a firewall), the organization is mitigating the risks associated with the legacy system in the absence of being able to fully secure it through traditional means.

upvoted 1 times

🗳️ 👤 **deejay2** 8 months, 1 week ago

Segmentation means separate, you're not separating anything. You're disabling one thing and inputting something else to implement additional security. D is correct.

upvoted 1 times

🗳️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: D**

Compensating controls is the best choice because the actions taken by the organization are intended to mitigate the risks associated with a legacy system when more standard security measures cannot be applied. By implementing these alternative controls, the organization effectively enhances the security of the legacy system without requiring direct updates or changes to its structure.

upvoted 2 times

🗳️ 👤 **CyberPark17** 1 year, 1 month ago

**Selected Answer: B**

best describes the "actions taken"??

Segmentation is the action taken by the organisation to have Compensating controls. B is the correct answer. Hope that helps.

upvoted 1 times

  **networkmen** 1 year, 1 month ago

**Selected Answer: D**

It is a business critical legacy system - i would go with D Compensating controls

upvoted 1 times

  **johnsongr8** 1 year, 1 month ago

The actions taken by the organization best describe

D. Compensating controls.

These measures are implemented to mitigate potential risks associated with the legacy system, ensuring its security despite inherent vulnerabilities.

upvoted 2 times

  **SHADTECH123** 1 year, 1 month ago

**Selected Answer: D**

Compensating controls are alternative measures implemented to mitigate the risk of a vulnerability when the primary controls cannot be applied. In this scenario, the organization has:

Disabled unneeded services: This reduces the attack surface of the legacy system, limiting potential vulnerabilities.

Placed a firewall in front of the system: This provides an additional layer of security, controlling and monitoring the traffic to and from the legacy system.

upvoted 1 times

  **whatsupdeepak** 1 year, 1 month ago

D - Compensating controls

upvoted 1 times

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

- A. EAP
- B. DHCP
- C. IPSec
- D. NAT

**Correct Answer:** C

Community vote distribution

C (100%)

 **dbrowndiver**  11 months ago

**Selected Answer: C**

IPSec is ideal for establishing a secure connection between a security consultant's device and a client's network, ensuring confidentiality, integrity, and authenticity of data transmitted over the connection.

upvoted 8 times

 **Nilab**  8 months, 1 week ago

**Selected Answer: C**

Easiest - IPSEC

upvoted 1 times

 **Syl0** 9 months, 3 weeks ago

EAP - Extensible Authentication Protocol - Handles authentication of information

DHCP - Dynamic Host Configuration Protocol - Assign IP address

IPSec - Internet Protocol Security

NAT - Network Address Translation - Used to translate address

upvoted 3 times

 **Shaman73** 1 year ago

C. IPSec

upvoted 4 times

Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

- A. Software as a service
- B. Infrastructure as code
- C. Internet of Things
- D. Software-defined networking

**Correct Answer:** B

Community vote distribution



B (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer:** B

Infrastructure as Code (IaC) is the correct answer because it provides the necessary tools and practices for automating and simplifying the deployment of infrastructure resources in a cloud environment. IaC enables efficient and repeatable resource provisioning, making it the most effective solution for the systems administrator's needs.

upvoted 15 times

  **1f2b013** Most Recent 10 months, 4 weeks ago

**Selected Answer:** B

IaC as it provides a means of automating deployment of infrastructure as a code.

upvoted 4 times

  **adderalpm** 1 year ago

Infrastructure as code (IaC) is the ability to provision and support your computing infrastructure using code instead of manual processes and settings. Any application environment requires many infrastructure components like operating systems, database connections, and storage.

upvoted 3 times

  **Shaman73** 1 year ago

B. Infrastructure as code

upvoted 3 times



After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

- A. Insider threat
- B. Email phishing
- C. Social engineering
- D. Executive whaling

**Correct Answer:** C

Community vote distribution

C (84%)

D (16%)

EXAMM3R Highly Voted 1 year ago

Executive whaling is when the CFO is one being targeted, therefore the answer is C  
upvoted 23 times

geocis Highly Voted 1 year ago

Answer is C....Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment.  
The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation.  
upvoted 10 times

edward0811 Most Recent 4 months, 1 week ago

Selected Answer: C

The answer is C - We have to read the question carefully. At the end of the question, it says, "Which of the following TOPICS". The only one that truly qualifies as a "TOPIC" is social engineering. All the others are examples of social engineering.  
upvoted 1 times

TECHBOSS 5 months, 1 week ago

Selected Answer: C

C: SOCIAL ENGINEERING. The two parties are the IT individual and the CALLER threatening AS IF they were the CFO. Whaling involves ACTULLY targeting the CFO. "IT" is the target.  
upvoted 1 times

917a0a9 7 months, 1 week ago

Selected Answer: C

"executive whaling" is a term used in cybersecurity, referring to a highly targeted phishing attack specifically aimed at high-level executives like CEOs, CFOs, or other senior leaders within an organization, essentially meaning the "whale" in this analogy is the high-value target, the executive with significant access to sensitive information

Answer is social engineering. The CFO WAS NOT the target in this scenario  
upvoted 3 times

courtr 8 months, 2 weeks ago

Selected Answer: C

voice phishing is a type of social engineering. executive whaling would only be the case if the CFO was the target receiving the call.  
upvoted 1 times

myazureexams 9 months, 2 weeks ago

Selected Answer: C

C- SOCIAL engineering

The user recognized the topic of social engineering from the security awareness training session. Executive whaling, also known as "whaling," is a

specific type of social engineering attack where the attacker impersonates a high-ranking executive. In this scenario, the user identified a social engineering attempt, even if they didn't specify executive whaling.

upvoted 1 times

🗨️ 👤 **PAWarriors** 10 months ago

**Selected Answer: C**

Correct answer is C.

The scenario described is social engineering. As mentioned by other members, "executive whaling" is a form of spear phishing that targets high-profile individuals, like CEOs or

CFOs. In this case a regular "user" is the one that received the call a not a high-profile individual.

upvoted 1 times

🗨️ 👤 **Cyber\_Texas** 10 months ago

**Selected Answer: C**

It is C because someone is pretending to be someone else that would classify as social engineering

upvoted 1 times

🗨️ 👤 **Crucible\_Bro** 10 months, 3 weeks ago

**Selected Answer: C**

someone is pretending to be someone within the company with authority. Social engineering.

upvoted 1 times

🗨️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: C**

Suspicious caller impersonated someone with authority (CFO) to trick the user into providing credit card information. This is a classic example of social engineering, where the attacker exploits trust and urgency to extract sensitive data. The scenario matches the characteristics of a social engineering attack, as it involves manipulating the victim through a phone call rather than using technological methods or digital communication channels.

upvoted 5 times

🗨️ 👤 **Dlove** 11 months, 1 week ago

**Selected Answer: C**

C. Social Engineering

We have to pay attention to the question because they can be very tricky. They didn't specifically target the CFO they simply mentioned the person and said they wanted credit card info. Based on the question that we have the correct answer is C

upvoted 5 times

🗨️ 👤 **Bimbo\_12** 11 months, 1 week ago

**Selected Answer: C**

C. Social engineering

Explanation:

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In this scenario, the suspicious caller was attempting to deceive the user into providing credit card information by falsely claiming to be acting on behalf of the Chief Financial Officer. This tactic is a classic example of social engineering, where the attacker uses social manipulation rather than technical hacking methods to obtain sensitive information.

It is not D because this is a type of phishing attack that specifically targets high-profile executives (also known as "whales") to steal sensitive information. While the scenario does involve the mention of a high-ranking executive, it is broader in scope and fits under the general category of social engineering rather than a specific whaling attack through email.

upvoted 4 times

🗨️ 👤 **TheMichael** 11 months, 2 weeks ago

**Selected Answer: C**

How I understand it is Whaling is when they impersonate an executive, executive whaling is when they target an executive (spearfishing in a sense), and social engineering is a broad form of trickery to deceive whoever the target is (not specific) to divulge information.

upvoted 3 times

🗨️ 👤 **78fcd3e** 11 months, 2 weeks ago

**Selected Answer: C**

In CompTIA's lessons for 701, the only reference I could find for "whaling" is a definition of "targeting employees that have influential roles."

I'm going with C. Social engineering

upvoted 2 times

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

C Whaling is send email to the Ceo

upvoted 3 times

🗨️ 👤 **b3a128a** 11 months, 3 weeks ago

It has to be C because the caller is stating the CFO wants the information, he is not saying he is the CFO.. also the term is whaling, not executive whaling

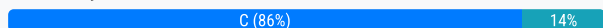
upvoted 3 times

A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

- A. Block access to cloud storage websites.
- B. Create a rule to block outgoing email attachments.
- C. Apply classifications to the data.
- D. Remove all user permissions from shares on the file server.

**Correct Answer: C**

Community vote distribution



**dbrowndiver** Highly Voted 11 months ago

**Selected Answer: C**

Apply classifications to the data is the correct first step because it establishes a foundational understanding of what data is sensitive and needs protection. By classifying the data, the security administrator can ensure that subsequent DLP policies are effectively tailored to prevent the exfiltration of sensitive customer data, while minimizing unnecessary restrictions on non-sensitive data.

upvoted 12 times

**Anyio** Most Recent 5 months, 1 week ago

**Selected Answer: C**

The NIST (National Institute of Standards and Technology) Risk Management Framework (RMF) is a seven-step process that helps organizations manage security and privacy risks. The steps are:

Prepare: Prepare the organization to manage security and privacy risks

Categorize: Classify the system to be evaluated for risk

Select: Choose controls

Implement: Put the controls in place

Assess: Evaluate the controls

Authorize: Get approval for the system

Monitor: Continuously monitor the controls

Categorize == Classification

upvoted 1 times

**G30** 6 months ago

**Selected Answer: C**

• C. Apply classifications to the data.

First Action

upvoted 1 times

**MaxiPrince** 6 months, 2 weeks ago

**Selected Answer: C**

Apply classifications to the data

upvoted 1 times

**Laura5859** 9 months, 2 weeks ago

**Selected Answer: C**

You must apply classifications to the data, so the DLP will be able to identify sensitive data.

upvoted 1 times

**nyyankee718** 11 months, 1 week ago

**Selected Answer: C**

its asking what to do FIRST/ How would users know what not to send out if data is not classified

upvoted 2 times

**ccamarada** 11 months, 2 weeks ago

**Selected Answer: C**

first classify the information

upvoted 2 times

🗨️ 👤 **101e7ca** 11 months, 3 weeks ago

**Selected Answer: B**

Applying a DLP solution to prevent data being 'leaked' out of the company, usually through email, USB or tools like Steganography.

Once installed the first thing he should do is create a rule to either warn or block email attachments. It's nothing to do with cloud storage or server file permissions and we don't need data classification for DLP to work (although it might be a nice option).

upvoted 3 times

🗨️ 👤 **Justthereforcomptia** 10 months, 2 weeks ago

So you're gonna block all the end-users from sending attachments ? are you serious...

What should be done, is classify the files you have first then block the sensitive ones from being sent as attachments. Blocking everything doesn't make any sense in the context of this question.

Correct Answer is C

upvoted 3 times

🗨️ 👤 **adderalpm** 1 year ago

DLP (Data Loss Prevention)

upvoted 3 times

🗨️ 👤 **Shaman73** 1 year ago

C. Apply classifications to the data.

upvoted 4 times

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

- A. Compromise
- B. Retention
- C. Analysis
- D. Transfer
- E. Inventory

**Correct Answer:** B

Community vote distribution

B (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: B**

The administrator is tasked with ensuring that transaction data is archived for the appropriate duration. This task involves adhering to retention schedules that dictate how long such data must be kept to meet compliance obligations.


Retention policies are critical for legal and compliance teams, as they help avoid legal issues related to data disposal and ensure that records are available for audits, investigations, or regulatory reviews.

upvoted 8 times

  **edf622f** Most Recent 9 months, 1 week ago

Sarbanes-Oxley Act. The answer is B.

upvoted 2 times

  **1f2b013** 10 months, 4 weeks ago

**Selected Answer: B**

Retention

upvoted 1 times

  **Shaman73** 1 year ago

B. Retention

upvoted 3 times

A company is working with a vendor to perform a penetration test. Which of the following includes an estimate about the number of hours required to complete the engagement?

- A. SOW
- B. BPA
- C. SLA
- D. NDA

**Correct Answer:** A

Community vote distribution

A (100%)

MAK0hunter33333333 Highly Voted 1 year, 1 month ago

Selected Answer: A

SOW: statement of work

BPA: business partnership agreement

SLA: service level agreement

NDA: no disclosure agreement

upvoted 9 times

dbrowndiver Highly Voted 11 months ago

Selected Answer: A

In the context of a penetration test, the SOW would include an estimate of the number of hours required to conduct the test, along with detailed descriptions of the testing methodologies, deliverables, and any other project-related expectations.

upvoted 5 times

Boethius Most Recent 1 year ago

A: SOW (statement of work)

The WO (Work Order) or SOW (Statement of Work) contain the details of a project and references the general terms in the MSA (Master Services Agreement). ~ Security + Get Certified Get Ahead by Darril Gibson and Joe Shelley

upvoted 3 times

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

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

**Correct Answer:** D

*Community vote distribution*

D (100%)

MAK0hunter33333333 Highly Voted 1 year, 1 month ago

**Selected Answer: D**

Ransomware is blackmailing for monetary gain which is a CRIME. It also does not fit the criteria for any other threat actor listed.  
upvoted 13 times

dbrowndiver Highly Voted 11 months ago

**Selected Answer: D**

Organized crime is the correct answer because ransomware-as-a-service operations are primarily conducted by criminal organizations seeking to monetize cyberattacks. These groups offer ransomware tools and services to other criminals, reflecting the profit-driven, organized nature of these cybercrime enterprises.  
upvoted 5 times



Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

- A. Code scanning for vulnerabilities
- B. Open-source component usage
- C. Quality assurance testing
- D. Peer review and approval

**Correct Answer:** D

Community vote distribution

D (100%)

  **geocis** Highly Voted 1 year ago

Correct Answer: D

Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

upvoted 16 times

  **MarysSon** Most Recent 3 months, 1 week ago

**Selected Answer: D**

The key word here is prevent. Code scanning reveals vulnerabilities that are already introduced to a system. Peer reviews are intended to check code prior to introduction in a production system.

upvoted 1 times

  **dbrowndiver** 11 months ago

**Selected Answer: D**

Peer reviews help catch malicious code before it is integrated into the production environment by having multiple sets of eyes on the changes, reducing the chance of any one developer slipping harmful code through the process.

upvoted 3 times

  **Shaman73** 1 year ago

D. Peer review and approval

upvoted 1 times

Which of the following can best protect against an employee inadvertently installing malware on a company system?

- A. Host-based firewall
- B. System isolation
- C. Least privilege
- D. Application allow list

**Correct Answer:** D

*Community vote distribution*

D (100%)

  **[Removed]**  1 year ago

Correct answer is option: D  
upvoted 20 times

  **dbrowndiver**  11 months ago

**Selected Answer: D**

By using an application allow list, employees cannot inadvertently install or run unauthorized software, including malware, because only approved applications are permitted to execute. This approach minimizes the risk of malware introduction through accidental downloads or installations.  
upvoted 9 times

  **Shaman73**  1 year ago

D. Application allow list  
upvoted 1 times

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

- A. Cross-site scripting
- B. Buffer overflow
- C. Jailbreaking
- D. Side loading

**Correct Answer:** C

Community vote distribution

C (100%)

 **leedsbarber** Highly Voted 1 year ago

**Selected Answer: C**

My first thought was:

D - because jailbreaking only relates to iOS and rooting is Android. They didn't specify a device.

However...

The question relates to modifying the OS, not installing unofficial apps.

So, although no OS is specified, answer C does seem most logical.

It pays to take a little more time to dissect the wording of the question as much as possible.

upvoted 16 times

 **Burg** 6 months, 1 week ago

Definitely agree. Especially with the way CompTIA words things. It's beneficial to understand what the question is asking fully.

upvoted 3 times

 **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: C**

Jailbreaking is the correct answer because it specifically involves modifying the operating system on mobile devices, which the company's Acceptable Use Policy aims to prohibit. By addressing jailbreaking, the company seeks to maintain the security and integrity of its mobile devices, preventing vulnerabilities associated with unauthorized OS modifications.

upvoted 5 times

 **testpan** Most Recent 3 months, 4 weeks ago

**Selected Answer: C**

Keyword 'modify the operating system'

upvoted 1 times

 **ExamTopics701** 9 months, 1 week ago

It can't be A or B.


upvoted 1 times

 **Laura5859** 9 months, 2 weeks ago

**Selected Answer: C**

Jailbreaking is defined by CompTIA as gaining full access to the iOS device by removing the limitations imposed by the Apple iOS operating system.

upvoted 2 times

 **MAKOhunter33333333** 1 year, 1 month ago

**Selected Answer: C**

Jailbreaking is modding iOS and rooting is modding Android.

upvoted 5 times

Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Choose two.)

- A. Fencing
- B. Video surveillance
- C. Badge access
- D. Access control vestibule
- E. Sign-in sheet
- F. Sensor

**Correct Answer:** CD

Community vote distribution

CD (80%)

AC (20%)

🗳️ 👤 **Shaman73** Highly Voted 1 year ago

- C. Badge access
  - D. Access control vestibule
- upvoted 12 times

🗳️ 👤 **Anyio** Most Recent 5 months, 1 week ago

Selected Answer: CD

Keyword = "authorized" personnel  
upvoted 2 times

🗳️ 👤 **koala\_lay** 9 months, 2 weeks ago

Selected Answer: CD

Agree to answer C & D  
upvoted 3 times

🗳️ 👤 **Laura5859** 9 months, 2 weeks ago

Selected Answer: AC

The question asks how you can secure a facility. I feel like that refers to the entire campus, which would require physical barriers such as a fence and secure access to buildings. Secure building access can be accomplished with Badge Access.  
upvoted 2 times

🗳️ 👤 **deejay2** 5 months, 2 weeks ago

No, it asking the best way to ACCESS a secure facility.  
upvoted 4 times

🗳️ 👤 **jsmthy** 9 months ago

Fencing of this type is not in the sense of physical chain-link/picket fences, but the appliances to keep intruders out like firewalls and IPS.  
upvoted 3 times

🗳️ 👤 **chasingsummer** 10 months ago

Selected Answer: CD

C. Badge access and D. Access control vestibule.  
upvoted 3 times

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

- A. Segmentation
- B. Isolation
- C. Patching
- D. Encryption

**Correct Answer: A**

Community vote distribution

A (90%)

10%

MAKOhunter33333333 Highly Voted 1 year, 1 month ago

Selected Answer: A

Mentions the org wants to store it on the network just separate from the main network, which is segmentation.  
upvoted 15 times

MAKOhunter33333333 1 year, 1 month ago

CompTIA SY0-701 pg 13 states isolation cuts a system off from access to or from outside networks.

Segmentation places sensitive systems on separate networks where they MAY communicate with each other.  
upvoted 6 times

AutoroTink Highly Voted 1 year, 1 month ago

Further notes: Isolation is a security measure that can be used to protect sensitive data which typically involves creating a completely separate environment, such as a different physical server or a standalone network, which can be more restrictive than segmentation. The question has the data still on the network, just in a separate part. So, Option A is still the best answer.  
upvoted 7 times

Perc Most Recent 2 months, 1 week ago

Selected Answer: B

Correct Answer: B. Isolation

Isolation places systems or data in a completely separate network or environment, preventing access from the main corporate network. This is stronger than segmentation, which separates traffic but may still allow limited communication.  
upvoted 1 times

famuza77 8 months, 2 weeks ago

Selected Answer: B

it is Isolation  
upvoted 1 times

dbrowndiver 11 months ago

Selected Answer: A

Segmentation is the correct answer because it involves creating distinct network segments that control access and separate sensitive customer data from the main corporate network. Network segmentation is the most appropriate solution for ensuring that customer data is stored securely and not accessible to unauthorized users.  
upvoted 3 times

drosas84 1 year ago

Selected Answer: A

Network segmentation involves dividing a network into subnets to control access and traffic flow. Network isolation is more severe, creating a standalone network with no connectivity to other parts of the network. It's a stringent form of segregation.  
upvoted 5 times

hasquaati 1 year, 1 month ago

Selected Answer: A

Answer is A. While Isolation is a legitimate answer, that design is more relevant to machinery and manufacturing equipment.

upvoted 2 times

🗲️ 👤 **AutoroTink** 1 year, 1 month ago

**Selected Answer: A**

While isolation is a broader concept that can include segmentation, it typically refers to completely separating a system or environment from others, which might be more extreme than necessary for this purpose. Segmentation can help in isolating the customer data from the main corporate network, ensuring that it is not accessible to unauthorized users

upvoted 1 times

🗲️ 👤 **Yoez** 1 year, 1 month ago

**Selected Answer: B**

The correct answer is:

B. Isolation

Isolation involves creating separate network segments or zones that restrict access between them. By isolating the network segment where customer data is stored from the main corporate network, the organization can prevent unauthorized users on the corporate network from accessing the sensitive customer data. This helps enhance security by limiting the potential attack surface and reducing the risk of unauthorized access or data breaches.

upvoted 1 times

🗲️ 👤 **shady23** 1 year, 1 month ago

**Selected Answer: A**

A. Segmentation

upvoted 1 times

🗲️ 👤 **3056f7e** 1 year, 1 month ago

B cause A only involves dividing a network into smaller segments to improve security and performance but may still allow communication between segments.

upvoted 1 times

Which of the following is the most common data loss path for an air-gapped network?

- A. Bastion host
- B. Unsecured Bluetooth
- C. Unpatched OS
- D. Removable devices

**Correct Answer:** D

Community vote distribution

D (100%)

 **Yoez** Highly Voted 1 year, 1 month ago

**Selected Answer: D**

In an air-gapped network, which is physically isolated from other networks, the most common data loss path would typically be through removable devices (option D). These can include USB drives, external hard drives, or other storage devices that could be introduced into the network, intentionally or unintentionally, by users or external entities. This is because such devices can bypass the physical isolation of the air gap and introduce potential security vulnerabilities.

upvoted 9 times

 **jennyka76** Most Recent 3 months, 2 weeks ago

**Selected Answer: D**

The most common data loss path in an air-gapped network is through removable storage devices like USB drives, as they can be used to introduce malware or leak data by unauthorized individuals.

upvoted 1 times

 **dbrowndiver** 11 months ago

**Selected Answer: D**

Removable devices is the correct answer because they provide a direct, physical means to transfer data to and from an air-gapped network, making them the most common path for data loss. Removable devices circumvent the network's isolation by physically connecting it to other systems, posing a significant risk of data exfiltration.

upvoted 1 times

Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

- A. Impersonation
- B. Disinformation
- C. Watering-hole
- D. Smishing

**Correct Answer:** C

Community vote distribution

C (100%)

  **chasingsummer**  10 months ago

**Selected Answer: C**

The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.  
upvoted 6 times

  **dbrowndiver**  11 months ago

**Selected Answer: C**

Watering-hole is the correct answer because it describes the method used by the attacker to compromise a legitimate website frequented by the target group (in this case, the industry blog) and spread malware to visitors. This strategic targeting and delivery mechanism is characteristic of a watering-hole attack.  
upvoted 4 times

  **4ddc874** 11 months ago

**Selected Answer: C**

A watering-hole attack targets a specific group of people by compromising a website they frequently visit. In this case, the compromised industry blog acted as the "watering hole" for the employees  
upvoted 4 times

  **Shaman73** 1 year ago

• C. Watering-hole  
upvoted 4 times



An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

- A. Deploying a SASE solution to remote employees
- B. Building a load-balanced VPN solution with redundant internet
- C. Purchasing a low-cost SD-WAN solution for VPN traffic
- D. Using a cloud provider to create additional VPN concentrators

**Correct Answer: A**

Community vote distribution

A (100%)

 **geocis** Highly Voted 1 year ago

Answer is A.....SASE (Secure Access Service Edge) is a comprehensive networking and security approach that combines wide-area networking (WAN) capabilities with security features. It provides secure access to applications and data, including encrypted tunnel access to the data center, while also offering monitoring capabilities for remote employee internet traffic. By implementing a SASE solution, the organization can reduce traffic on the VPN and internet circuit by routing traffic intelligently through the cloud, closer to the users. This approach helps optimize performance and security, addressing the scaling issues effectively.

upvoted 16 times

 **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: A**

Deploying a SASE solution to remote employees is the best choice because it provides a holistic approach to secure remote access by reducing traffic, offering encrypted tunnel access, and monitoring internet traffic. SASE integrates necessary networking and security functions into a cloud-based solution, making it ideal for modern remote work environments.

upvoted 7 times

 **9149f41** Most Recent 4 months, 3 weeks ago

**Selected Answer: A**

SASE includes:

SD-WAN has capability of traffic load balancing.

SD-WAN, a core part of SASE, can dynamically route traffic across multiple connections.

SASE also included:

Firewalls,

Secure web gateways

upvoted 2 times

 **a4e15bd** 10 months, 2 weeks ago

The correct answer is A. Deploying SASE Solution..

Secure Access Service Edge (SASE) is a network architecture framework that combines cloud-based security technologies with wide area network capabilities. The goal of SASE is to securely connect users, systems, and endpoints to applications and services anywhere

upvoted 1 times

 **123456789User** 1 year, 1 month ago

**Selected Answer: A**

Deploying a SASE solution to remote employees.

upvoted 3 times

Which of the following is the best reason to complete an audit in a banking environment?

- A. Regulatory requirement
- B. Organizational change
- C. Self-assessment requirement
- D. Service-level requirement

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **Glacier88** Highly Voted 10 months, 1 week ago

**Selected Answer:** A

Financial services are heavily regulated.

upvoted 5 times

 **Shaman73** Most Recent 1 year ago

• A. Regulatory requirement

upvoted 4 times

Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Non-repudiation

**Correct Answer:** C

Community vote distribution

C (100%)

 **dbrowndiver** Highly Voted 11 months ago


**Selected Answer: C**

Human resources (HR) data typically includes sensitive information such as employee records, personal data, salaries, and other confidential details. Implementing the principle of least privilege ensures that only authorized HR personnel have access to this sensitive information, maintaining its confidentiality.

Access Control: By granting access only to those who require it to perform their job functions, the organization minimizes the risk of unauthorized access, data breaches, and information leaks.

The primary goal of applying least privilege to HR files is to protect sensitive data from unauthorized access, aligning directly with the confidentiality aspect of information security.

upvoted 9 times

 **Shaman73** Most Recent 1 year, 1 month ago

C. Confidentiality

upvoted 4 times

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Choose two.)

- A. The device has been moved from a production environment to a test environment.
- B. The device is configured to use cleartext passwords.
- C. The device is moved to an isolated segment on the enterprise network.
- D. The device is moved to a different location in the enterprise.
- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates.

**Correct Answer:** EF

Community vote distribution

EF (75%)

BE (25%)

  **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer:** EF

- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates.

These two cases justify decommissioning a network device:

- Encryption Level: If a device's encryption level cannot meet the organization's standards, it poses a significant security risk and should be decommissioned.
- Authorized Updates: If a device is unable to receive authorized updates, it becomes vulnerable to known exploits and cannot be maintained securely, thus it should also be decommissioned.

Therefore, the correct answers are:

- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates.

upvoted 8 times

  **jennyka76** Most Recent 3 months, 2 weeks ago

**Selected Answer:** EF

An engineer should recommend decommissioning a network device primarily when security risks are high, such as if the device's encryption level is insufficient for organization standards or if it cannot receive necessary security updates, or when it's no longer in active use.

upvoted 1 times

  **Innana** 5 months ago

**Selected Answer:** BE

Correct answers are B and E. While F is also a good alternative but not good enough as B and E

upvoted 1 times

  **asdfqwer1235** 4 months ago

B is not a good reason to justify decommissioning. Device is configured to use plaintext is bad configuration but instead of decommissioning device you can easily change the configuration and make sure it use encryption.

upvoted 3 times

  **Fontabest\_99a** 5 months, 3 weeks ago

**Selected Answer:** BE

B And E

upvoted 1 times

  **G30** 6 months ago

**Selected Answer:** EF

E. The device's encryption level cannot meet organizational standards

F. The device is unable to receive authorized updates

upvoted 2 times

🗨️ 👤 **41c27e6** 6 months ago

**Selected Answer: EF**

E. The device's encryption level cannot meet organizational standards

F. The device is unable to receive authorized updates

upvoted 1 times

🗨️ 👤 **ProudFather** 6 months, 4 weeks ago

**Selected Answer: BE**

B. The device is configured to use cleartext passwords.

E. The device's encryption level cannot meet organizational standards.

These two options represent situations where the device poses a significant security risk:

Cleartext passwords: Devices with cleartext passwords are vulnerable to unauthorized access and data breaches.

Insufficient encryption: Devices that cannot meet organizational encryption standards may not be able to protect sensitive data adequately.

The other options do not necessarily warrant decommissioning:

upvoted 1 times

🗨️ 👤 **Jamie888** 9 months, 2 weeks ago

**Selected Answer: BE**

Practice test in pluralsight say its B and E

upvoted 2 times

🗨️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: EF**

When evaluating whether a network device should be decommissioned, security vulnerabilities, compliance with organizational standards, and the ability to maintain the device are critical considerations. Options E and F highlight situations where a device is not able to meet these essential requirements.

E. The device's encryption level cannot meet organizational standards and F. The device is unable to receive authorized updates are the correct reasons for recommending the decommissioning of a network device. These conditions indicate significant security and compliance risks that cannot be addressed through reconfiguration alone, necessitating the removal of the device to protect the organization's network and data.

upvoted 4 times

🗨️ 👤 **Shaman73** 1 year ago

• E. The device's encryption level cannot meet organizational standards.

• F. The device is unable to receive authorized updates

upvoted 3 times

A company is required to perform a risk assessment on an annual basis. Which of the following types of risk assessments does this requirement describe?

- A. Continuous
- B. Ad hoc
- C. Recurring
- D. One time

**Correct Answer:** C

Community vote distribution

C (100%)

🗲️ 👤 **Catalyst33** 4 months, 3 weeks ago

**Selected Answer: C**

Continuous: Its not because that would mean running software continuously to evaluate risks

Ad hoc: its not because that one is as the name implies decided to be done on the spur of the moment (or as a reaction)

Recurring: yes because its something pre planned which reoccurs

One time: Per year means every year, not just one time

upvoted 1 times

🗲️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: C**

Recurring risk assessments are those that are scheduled to take place at regular intervals, such as annually, semi-annually, or quarterly. This type of assessment ensures that risks are regularly evaluated, allowing the company to stay informed about potential vulnerabilities and threats and adjust its risk management strategies accordingly. o Without the ability to receive updates, a device cannot be secured against emerging threats, making it a liability to the organization's security posture.

upvoted 4 times

🗲️ 👤 **Shaman73** 1 year ago

• C. Recurring

upvoted 2 times

After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

- A. Compensating
- B. Detective
- C. Preventive
- D. Corrective

**Correct Answer:** B

Community vote distribution

B (100%)

dbrowndiver Highly Voted 11 months ago

Selected Answer: B

Detective is the correct answer because reviewing log files after a ransomware attack is an example of a detective control. It is used to identify, analyze, and understand security incidents post-occurrence, providing valuable information for future prevention and response strategies.

upvoted 6 times

opeyemi777 Most Recent 9 months, 3 weeks ago

Selected Answer: B

Detective

upvoted 1 times

Ina22 11 months, 1 week ago

Its B : Detective

upvoted 1 times

Shaman73 1 year ago

• B. Detective

upvoted 1 times

Which of the following exercises should an organization use to improve its incident response process?

- A. Tabletop
- B. Replication
- C. Failover
- D. Recovery

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **dbrowndiver** Highly Voted 11 months ago

**Selected Answer:** A

Tabletop is the correct answer because tabletop exercises are specifically designed to evaluate and improve incident response processes by allowing teams to simulate responses to hypothetical incidents. This exercise provides valuable insights into the effectiveness of the current response plan and identifies areas for improvement, enhancing the organization's overall incident response capabilities.

upvoted 9 times

 **Shaman73** Most Recent 1 year ago

- A. Tabletop

upvoted 3 times



Which of the following best ensures minimal downtime and data loss for organizations with critical computing equipment located in earthquake-prone areas?

- A. Generators and UPS
- B. Off-site replication
- C. Redundant cold sites
- D. High availability networking

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **ProudFather** 6 months, 4 weeks ago

**Selected Answer: B**

B. Off-site replication

While all options are important for disaster recovery, off-site replication is the most effective way to ensure minimal downtime and data loss in the event of an earthquake. By replicating critical data to a remote location, organizations can quickly restore operations in the event of a disaster.  
upvoted 3 times

🗳️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: B**

Earthquake Protection: In earthquake-prone areas, having data and systems replicated off-site ensures that even if the primary site is compromised, the organization can recover its operations from the remote location with minimal downtime and data loss.

Data and System Availability: Off-site replication provides a means to restore operations quickly, as the backup data is up-to-date and can be accessed or moved to a disaster recovery site.

Off-site replication is crucial for disaster recovery planning, particularly in areas susceptible to natural disasters. It ensures business continuity by safeguarding data and systems in a secure location away from the primary site's risks.

upvoted 4 times

🗳️ 👤 **cdsu** 1 year ago

Answer B:

Copying data to a geographically distant location. This ensures that data is preserved even if the primary site is compromised by an earthquake  
upvoted 4 times

🗳️ 👤 **Shaman73** 1 year ago

• B. Off-site replication

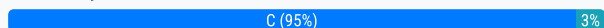
upvoted 2 times

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation
- D. Replacement

**Correct Answer:** C

Community vote distribution



**KrazyMonkey** Highly Voted 1 year, 1 month ago

**Selected Answer:** C

I've not heard of patching legacy devices... Professor Messer would be disappointed.  
upvoted 23 times

**CyberSecurity24** Highly Voted 1 year ago

**Selected Answer:** C

Patching is a common method for addressing vulnerabilities. However, in the case of legacy devices, patches may no longer be provided, or applying new patches may be difficult. Therefore, it is not suitable as a quick mitigation method, making C. Segmentation the correct answer.  
upvoted 12 times

**sentinell** Most Recent 2 weeks, 3 days ago

**Selected Answer:** D

Replacement

IoT devices are fine when segmented in the work environment. What happens when you get home and they are exposed outside the segmented network?  
upvoted 1 times

**itone3333** 2 months, 1 week ago

**Selected Answer:** C

When I see the word 'legacy', I know patching has nothing to do with it like a father that went out to get milk.  
upvoted 1 times

**Drey09** 5 months, 3 weeks ago

**Selected Answer:** C

He's telling mitigate, replace will solve the problem  
upvoted 1 times

**ProudFather** 6 months, 4 weeks ago

**Selected Answer:** D

D. Replacement

Since the vulnerability is in the OS of legacy IoT devices, patching might not be feasible due to the age of the devices and the lack of vendor support for updates. In such cases, the most effective mitigation strategy is to replace the vulnerable devices with newer models that have security updates and support.

While segmentation and insurance can be helpful, they are not the primary solution to address the vulnerability itself.  
upvoted 1 times

**bordfree** 4 weeks ago

I was on the fence with D, ended up going with C, but I came to the comments to figure out why it was one over the other. Looks like "Mitigate" is the keyword here. Segmenting will mitigate the risk immediately until you can solve the problem by replacing the devices. The long-term solution should be replacement, but the immediate mitigation practice is to segmentate.

upvoted 3 times

🗨️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: C**

Legacy IoT Devices: These devices often lack the ability to be quickly patched or replaced due to hardware limitations or operational constraints. Segmentation offers a rapid response by limiting access and isolating these devices from critical network resources.

Access Control: By segmenting the network, you can apply stricter access controls and monitoring, ensuring that any potential compromise of the IoT devices does not affect the broader network.

upvoted 6 times

🗨️ 👤 **SHADTECH123** 1 year, 1 month ago

**Selected Answer: C**

Segmentation would best mitigate the network access vulnerability in the OS of legacy IoT devices quickly. By segmenting the network, you can isolate the vulnerable devices from the rest of the network, thereby limiting potential access and reducing the risk of exploitation. This is often faster than patching or replacing the devices, especially if patches are not immediately available or replacement is not feasible in the short term.

upvoted 8 times

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

**Selected Answer: C**

I retract my previous answer. You can't do patching on legacy stuff...MY BAD!

upvoted 5 times

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

**Selected Answer: C**

Key word is legacy device. Patches may not be available. Segmentation will also be a valid solution for legacy IoT devices. Answer is C.

upvoted 3 times

🗨️ 👤 **e5c1bb5** 1 year, 1 month ago

**Selected Answer: C**

theres always trolls/mislead people. legacy devices arent supported anymore. segmentation is the way to go. theres always vulnerabilities in IOT devices. what do you do if you need to use them? SEGMENTATION.

upvoted 3 times

🗨️ 👤 **shady23** 1 year, 1 month ago

**Selected Answer: C**

Question #: 729

Topic #: 1

[All SY0-601 Questions]

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation
- D. Replacement

Patching doesn't work as it's legacy, Segregation is the quickest option of the remaining three.

upvoted 3 times

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

**Selected Answer: B**

Network segmentation could limit the potential impact of the vulnerability but does not address the vulnerability in the devices.

upvoted 1 times

🗨️ 👤 **Justthereforcomptia** 10 months, 2 weeks ago

Legacy OS doesn't receive patches, so your answer is invalid.

upvoted 1 times

🗨️ 👤 **nesquick0** 10 months, 3 weeks ago

its a legacy OS which it cannot receive updates or be patched.

upvoted 1 times

🗨️ 👤 **Yoez** 1 year, 1 month ago

**Selected Answer: B**


The option that would best mitigate the vulnerability quickly is patching (option B). Patching involves applying updates or fixes provided by the software vendor to address known vulnerabilities or weaknesses in the system. By promptly patching the OS of the legacy IoT devices, the vulnerability can be mitigated, reducing the risk of exploitation by malicious actors. This is typically the quickest and most direct way to address known vulnerabilities and enhance the security posture of the devices.

upvoted 1 times

  **festuuss** 4 months, 1 week ago

Patching is wrong because we are dealing with legacy IoT which means they may no longer provide new patches for their OS.

upvoted 1 times

  **917a0a9** 7 months, 1 week ago

legacy system means it can not be patched

upvoted 1 times

After an audit, an administrator discovers all users have access to confidential data on a file server. Which of the following should the administrator use to restrict access to the data quickly?

- A. Group Policy
- B. Content filtering
- C. Data loss prevention
- D. Access control lists

**Correct Answer:** D

Community vote distribution

D (100%)

SHADTECH123 Highly Voted 1 year, 1 month ago

**Selected Answer: D**

Access control lists (ACLs) should be used to restrict access to the data quickly. ACLs allow the administrator to specify which users or groups have permission to access certain files or directories on the file server, providing a straightforward and immediate way to enforce access controls and protect confidential data.

upvoted 10 times

Nilab Most Recent 8 months, 1 week ago

Why can't be group policy?

upvoted 2 times

3dk1 8 months, 1 week ago

Because group policy applies to broader system policies (on workstations and servers), but does not directly manage file access permissions.

upvoted 5 times

dbrowndiver 11 months ago

**Selected Answer: D**

In this scenario, D. Access control lists (ACLs) is the best choice because it provides a quick and precise way to adjust file permissions and restrict access to confidential data on a file server. ACLs allow administrators to implement immediate changes and ensure only authorized users have access to sensitive files.

upvoted 2 times

A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A. MOA
- B. SOW
- C. MOU
- D. SLA

**Correct Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **KosherKin** 3 months, 2 weeks ago

**Selected Answer:** D

At first I choose A. MOA but this is where you have to take your time and really read the question. 99.99% is similar to metrics. SLA is an agreement that involves metrics.

upvoted 2 times

🗳️ 👤 **Syl0** 9 months, 4 weeks ago

MOA - memorandum of Agreement

MOU - Memorandum of Understanding

SOW - Statement / Scope of Work

SLA - Service Level Agreement

upvoted 4 times

🗳️ 👤 **dbrowndiver** 11 months ago

**Selected Answer:** D

In this scenario, the client demands 99.99% uptime for hosted security services. The SLA is the appropriate document to specify this uptime requirement and any associated metrics.

upvoted 1 times

🗳️ 👤 **Dean1065** 1 year ago

**Selected Answer:** D

D - SLA

upvoted 2 times

🗳️ 👤 **Shaman73** 1 year ago

• D. SLA

upvoted 3 times

A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

- A. Certification
- B. Inventory list
- C. Classification
- D. Proof of ownership

**Correct Answer:** A

*Community vote distribution*

A (100%)

MAK0hunter33333333 Highly Voted 1 year, 1 month ago

**Selected Answer: A**

Third-party certificate of destruction, proof it was actually disposed  
upvoted 14 times

dbrowndiver Highly Voted 11 months ago

**Selected Answer: A**

For a classified storage array, certification is critical to ensure that sensitive data has been irretrievably destroyed, preventing unauthorized access or data breaches.

The certification serves as evidence that the company complied with legal and regulatory requirements regarding the handling and disposal of classified materials. This can be important for audits or investigations.

Certification provides assurance and documentation that the storage array was disposed of securely, mitigating risks associated with the handling of classified information.

upvoted 5 times

Oca8ee9 Most Recent 6 months, 3 weeks ago

**Selected Answer: A**

Sanitization Certification will provide proof.

upvoted 2 times

A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data. Which of the following should the company consider?

- A. Geographic dispersion
- B. Platform diversity
- C. Hot site
- D. Load balancing

**Correct Answer:** A

Community vote distribution

A (100%)

  **geocis** Highly Voted 1 year ago

Answer: A

Geographic dispersion is the practice of having backup data stored in different locations that are far enough apart to minimize the risk of a single natural disaster affecting both sites. This ensures that the company can recover its regulated data in case of a disaster at the primary site. Platform diversity, hot site, and load balancing are not directly related to the protection of backup data from natural disasters. Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 449; Disaster Recovery Planning: Geographic Diversity  
upvoted 10 times

  **ChocolateRenaissance** Most Recent 2 months ago

Selected Answer: A

In the event that the main location goes down there will be multiple other servers running  
upvoted 1 times

  **3dk1** 8 months, 1 week ago

Selected Answer: A

this one easy  
upvoted 1 times

  **dbrowndiver** 11 months ago

Natural Disaster Protection: By storing backup data in geographically dispersed locations, the company ensures that a natural disaster in one region does not affect the backup data in another region.  
Regulatory Compliance: Many regulations require companies to have disaster recovery strategies that protect data integrity and availability, which geographic dispersion effectively addresses. Geographic dispersion directly addresses the risk of complete data loss due to a natural disaster by ensuring that data is stored in multiple locations, making it the most appropriate solution for this scenario  
upvoted 2 times

  **Shaman73** 1 year ago

• A. Geographic dispersion  
upvoted 3 times



A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

- A. Obtain the file's SHA-256 hash.
- B. Use hexdump on the file's contents.
- C. Check endpoint logs.
- D. Query the file's metadata.

**Correct Answer:** D

Community vote distribution

D (100%)

  **geocis** Highly Voted 1 year ago

Answer D.....Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes. Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis.

upvoted 7 times

  **Shaman73** Highly Voted 1 year, 1 month ago

D. Query the file's metadata.

upvoted 5 times

  **dbrowndiver** Most Recent 11 months ago

**Selected Answer:** D

In this scenario, choice "D" is correct. Query the file's metadata is the correct answer because metadata provides direct information about the file's creation date and possibly the creator. This method is the most efficient and effective way to gather the required details about a potentially malicious video file. By querying the file's metadata, the security analyst can access information about when the file was created and potentially who created it, assuming the creator's details were embedded or tagged during the file's creation.

upvoted 3 times

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

- A. Red
- B. Blue
- C. Purple
- D. Yellow

**Correct Answer:** C

Community vote distribution

C (100%)

  **123456789User** Highly Voted 1 year, 1 month ago

**Selected Answer: C**

Red = offensive

Blue = defensive

Yellow = builders

Purple = mix of offensive and defensive. Also the color you get when you mix red and blue.

upvoted 29 times

  **adderallpm** Highly Voted 1 year ago

Grimace



upvoted 12 times

  **dbrowndiver** Most Recent 11 months ago

**Selected Answer: C**

Purple teams combine the strengths of both offensive and defensive approaches to provide a holistic security strategy. This integration enhances the organization's ability to identify weaknesses, improve response capabilities, and implement effective security measures.

upvoted 2 times

  **Dlove** 11 months, 2 weeks ago

**Selected Answer: C**

C. Purple

Purple teaming is a collaborative approach to cybersecurity that brings together red and blue teams to test and improve an organization's security posture.

upvoted 3 times

A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

- A. Patch availability
- B. Product software compatibility
- C. Ease of recovery
- D. Cost of replacement

**Correct Answer:** A

Community vote distribution

A (100%)

SHADTECH123 Highly Voted 1 year, 1 month ago

Selected Answer: A

The most likely security implication that the security team would document is patch availability. End-of-life operating systems no longer receive security updates or patches from the vendor, which leaves them vulnerable to newly discovered exploits and vulnerabilities. This lack of ongoing support means that any security flaws found in the operating systems will not be addressed, increasing the risk of compromise.

upvoted 8 times

Etc\_Shadow28000 Highly Voted 1 year ago

Selected Answer: A

A. Patch availability

The primary security implication of using end-of-life operating systems is the lack of patch availability. End-of-life systems no longer receive security updates or patches from the vendor, making them vulnerable to known exploits and security vulnerabilities that will not be fixed. This poses a significant risk to the security of the kiosks and the overall network.

Therefore, the correct answer is:

A. Patch availability

upvoted 7 times

9149f41 Most Recent 4 months, 3 weeks ago

Selected Answer: A

The question is not asking for a solution to the legacy system, but rather asking what information needs to be documented in this scenario.

Additionally, determining replacement costs is not a cybersecurity responsibility, as security teams can only recommend replacement while vendors provide the actual cost estimates

upvoted 2 times

dbrowndiver 11 months ago

Selected Answer: A

Patch availability is a critical concern for maintaining the security and integrity of systems. The absence of patches for EOL systems is a major security risk that the security team would likely document as a primary concern

upvoted 1 times

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

- A. A full inventory of all hardware and software
- B. Documentation of system classifications
- C. A list of system owners and their departments
- D. Third-party risk assessment documentation

**Correct Answer:** A

*Community vote distribution*

A (100%)

MAK0hunter33333333 **Highly Voted** 1 year, 1 month ago

**Selected Answer: A**

Conducting inventory is part of risk management, so knowing what is in your environment will be very helpful to track and patch  
upvoted 13 times

dbrowndiver **Most Recent** 11 months ago

**Selected Answer: A**

In this scenario, the best answer is "A". A full inventory of all hardware and software is the correct answer because it provides the essential information needed to accurately assess the risk posed by a new vulnerability. This inventory enables the security analyst to identify affected systems, prioritize responses, and measure the overall risk to the organization effectively.

upvoted 4 times

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A. Impact analysis
- B. Scheduled downtime
- C. Backout plan
- D. Change management boards

**Correct Answer:** B

*Community vote distribution*

B (100%)

MAK0hunter33333333 Highly Voted 1 year, 1 month ago

**Selected Answer: B**

Set time aside for IT to make changes, like a maintenance window, typically not during peak hours  
upvoted 9 times

dbrowndiver Most Recent 11 months ago

**Selected Answer: B**

In this scenario, the best choice is "B". Scheduled downtime is the correct answer because it specifically involves setting a designated time for changes to occur, balancing the need for system maintenance with minimizing business impacts. Scheduled downtime ensures that updates and changes are performed in a controlled and predictable manner, reducing the risk of unplanned disruptions.

upvoted 3 times

A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

- A. Hashing
- B. Tokenization
- C. Encryption
- D. Segmentation

**Correct Answer:** C

Community vote distribution

C (91%)




9%

  **SHADTECH123**  1 year, 1 month ago

**Selected Answer:** C

To ensure sensitive data at rest is rendered unreadable, the company will most likely use encryption. Encryption transforms the data into an unreadable format using an algorithm and a key, and only authorized parties with the correct decryption key can convert it back to its original readable form. This is the most effective way to protect data at rest from unauthorized access.



upvoted 8 times

  **Jedsturr**  7 months, 2 weeks ago

**Selected Answer:** D


lets EOL, keyword is Decomissioned

upvoted 1 times

  **aaebd57** 1 month, 3 weeks ago

Wrong Question...

upvoted 1 times

  **deejay2** 5 months, 3 weeks ago

Lets EOL?? What does that mean?

upvoted 1 times

  **Nilab** 8 months ago

Are these questions still reliable -lease I GOT EXAM TOMORROW

upvoted 4 times

  **Viknikpik** 4 months ago

Are they how was it?

upvoted 3 times

  **dbrowndiver** 11 months ago

**Selected Answer:** C

In this scenario option C is best. Encryption is the correct because it effectively renders sensitive data unreadable to unauthorized users while allowing authorized users to access the data with the correct decryption key. Encryption is the standard method for protecting data at rest, ensuring data security and compliance with regulatory requirements.

upvoted 3 times

  **Shaman73** 1 year, 1 month ago

C. Encryption

upvoted 2 times

A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?

- A. End of business
- B. End of testing
- C. End of support
- D. End of life

**Correct Answer:** D

Community vote distribution

D (52%)

C (48%)

🗳️ 👤 **Shaman73** Highly Voted 1 year ago

- D. End of life
- upvoted 29 times

🗳️ 👤 **MYC199** Highly Voted 11 months, 2 weeks ago

Selected Answer: C

C. From the CompTIA study guide: End of life - while the equipment or device is no longer sold, it remains supported. End of support - the last date on which the vendor will provide support and/or updates.

I'm confused.

upvoted 21 times

🗳️ 👤 **MusicEssentials12** Most Recent 3 days, 21 hours ago

Selected Answer: C

I Like Fortnite

upvoted 1 times

🗳️ 👤 **Kekeee** 5 days, 18 hours ago

Selected Answer: C

end of support

upvoted 1 times

🗳️ 👤 **JASOSA** 1 week, 5 days ago

Selected Answer: D

I am pretty sure it is EOL

upvoted 1 times

🗳️ 👤 **ef74e4b** 1 week, 6 days ago

Selected Answer: C

End of Support.

upvoted 1 times

🗳️ 👤 **geniseer** 3 weeks ago

Selected Answer: C

Follow the timeline: A product reaches its End of Life first. The company stops producing the product, but still provides support for a while, allowing customers sufficient time to update their infrastructure. Then, the product reaches its End of Support period, meaning the company no longer provides any service for that product.

upvoted 1 times

🗳️ 👤 **NRPM\_2479** 3 weeks, 1 day ago

Selected Answer: D

its D, I ran this through both chatgpt and gemini

upvoted 1 times

🗳️ 👤 **billie** 3 weeks, 2 days ago

Selected Answer: D

End of life (EOL) means the device has reached the point where the vendor no longer provides updates, patches, or support. This perfectly matches your description: decommissioned, no updates, no patches.

End of support usually refers to when a vendor officially stops providing technical assistance or updates – it's closely related but sometimes slightly earlier in the product lifecycle than EOL.

In most exam contexts, End of life is the better match for a device no longer receiving updates or patches and being decommissioned.

Summary:

If the focus is "no more updates/patches + decommissioned" → End of life (D)

If the focus is just "no longer supported/maintained" → End of support (C)

upvoted 1 times

  **sergezaza83** 3 weeks, 3 days ago

**Selected Answer: D**

D. End of life (EOL) – This is the final stage in a product's lifecycle. It means the device is being retired, no longer supported, and is no longer used.

C. End of support – This means the vendor no longer provides updates or technical help, but the device might still be in use.

upvoted 1 times

  **Baby\_Steps\_** 1 month ago


**Selected Answer: C**

Best answer is C

End of support means product is where the manufacturer stops providing support services like updates, security patches, and technical assistance, even though the product may still function.

End of life where the product is no longer being sold or actively supported by the manufacturer

upvoted 1 times


  **aaebd57** 1 month, 3 weeks ago

**Selected Answer: C**

AFAIK: CompTIA uses EOL to mean no longer being sold (hardware) or distributed (software) and EOS means no longer being updated with patches or offering support for.

So I would answer C.



upvoted 1 times

  **M4t** 3 months ago

**Selected Answer: C**

A product can reach EOL but it still can be supported by vendor for a certain period of time.

upvoted 1 times

  **Lafras23** 3 months, 1 week ago

**Selected Answer: D**

No, I read the question again, and the correct answer is End of Life!!!

upvoted 1 times

  **Lafras23** 3 months, 1 week ago

**Selected Answer: C**

End of support comes after End of life. End of life means it's not available anymore, but patches will still be provided.

upvoted 2 times

  **GeorgySid** 3 months, 2 weeks ago

**Selected Answer: C**

End of life (EOL): This is the date after which a product will no longer be sold or renewed. However, it might still receive some form of support, such as security patches

End of support (EOS): This date marks the complete cessation of all support services for the product. After this date, no new patches, updates or fixes will be released, even for critical vulnerabilities

upvoted 1 times



🗨️ 👤 **jennyka76** 3 months, 2 weeks ago

**Selected Answer: D**

had to check on this one myself twice..

my answer is - D

here is my proof for my selection

In the context of the CompTIA SY0-701 (Security+) exam, "end of life" refers to when a specific version of the exam or a related product (like a software or hardware) is no longer officially supported by CompTIA and the manufacturer respectively, meaning no further updates, patches or security fixes will be provided.

upvoted 2 times

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

- A. Encryption at rest
- B. Masking
- C. Data classification
- D. Permission restrictions

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **dbrowndiver** Highly Voted 11 months ago

**Selected Answer:** A

When a laptop is stolen, encryption at rest ensures that the data remains secure and inaccessible to the thief, as they would need the decryption key to access the files.

Data Protection: Encryption at rest provides a robust layer of security for sensitive data, making it a common requirement for organizations handling confidential information.

The primary concern with stolen laptops is unauthorized access to the data stored on them. Encryption at rest is the most effective way to prevent data loss in this scenario, as it keeps the data secure even if the device falls into the wrong hands.

upvoted 6 times

 **9149f41** Most Recent 4 months, 3 weeks ago

**Selected Answer:** A

When the device is stolen, the data will always be in rest.

So the answer is easy: Encyption at rest.

upvoted 1 times

 **Shaman73** 1 year, 1 month ago

A. Encryption at rest

upvoted 3 times

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

- A. Concurrent session usage
- B. Secure DNS cryptographic downgrade
- C. On-path resource consumption
- D. Reflected denial of service

**Correct Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **499c5c4** Highly Voted 1 year, 1 month ago

A reflected denial of service (DoS) attack occurs when an attacker sends forged requests to a server, causing the server to respond to the spoofed IP address (the target) with a large volume of traffic. In the context of DNS, this often involves DNS amplification attacks, where small DNS queries result in large responses being sent to the target. This matches the described symptoms of minimal resource usage on the DNS server but a flood of inbound traffic. The best description of the observed situation, where the DNS server is overwhelmed by inbound traffic with minimal DNS queries, is that it is experiencing a reflected denial of service attack. Therefore, the correct answer is:

D. Reflected denial of service  
upvoted 11 times

🗳️ 👤 **MAKOhunter33333333** Highly Voted 1 year, 1 month ago

**Selected Answer: D**

1. Unable to reach external websites, denial of service
2. Flooded with traffic
3. The traffic is not coming from within via verifying with network logs

DOS is best option based on those details  
upvoted 8 times

🗳️ 👤 **dbrowndiver** Most Recent 11 months ago

**Selected Answer: D**

Minimal Resource Usage: The DNS server's CPU, disk, and memory usage are minimal, indicating that the server itself is not processing a large number of queries. However, the network interface is flooded with traffic, which is a key indicator of a reflected DoS attack.

Flooded Network Interface: The flooding of the network interface with inbound traffic without a corresponding increase in actual DNS query processing suggests that the server is receiving unsolicited responses, characteristic of a reflected DoS attack.

Why this is the best choice, because the symptoms match a reflected DoS, where the server is overwhelmed by traffic that it did not initiate, preventing legitimate users from accessing external websites due to the congestion

upvoted 2 times

🗳️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

1. Unable to reach external websites, denial of service
2. Flooded with traffic
3. The traffic is not coming from within via verifying with network logs

DOS is best option based on those details  
upvoted 1 times

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

- A. RBAC
- B. ACL
- C. SAML
- D. GPO

**Correct Answer: A**

*Community vote distribution*

A (100%)

MAKOhunter33333333 **Highly Voted** 1 year, 1 month ago

**Selected Answer: A**

Role-based access control (RBAC) restricts users to only access data based on their job responsibilities.  
upvoted 13 times

AutoroTink **Highly Voted** 1 year, 1 month ago

**Selected Answer: A**

RBAC: Role-Based Access Control (Permissions based on roles. Others include: MAC, DAC, Rule-based, ABAC)  
ACL: Access Control List (Popular with configuring firewalls)  
SAML: Security Assertion Markup Language (used alongside SSO, authentication)  
GPO: Group Policy Objective (used in hardening, to dictate policies, user rights, and audit settings)  
upvoted 8 times

Syl0 **Most Recent** 9 months, 3 weeks ago

RBAC - Rule Based Access Control  
ACL - Access Control List  
SAML - Security Assertion Markup Language  
GPO - Group Policy Object  
upvoted 1 times

dbrowndiver 11 months ago

**Selected Answer: A**

In this question the best choice is "A". RBAC (Role-Based Access Control) is correct because it allows the systems administrator to prevent unauthorized access by defining roles and assigning permissions based on user responsibilities. RBAC simplifies the access management process and ensures that users only have access to the data necessary for their roles.  
upvoted 2 times

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Choose two.)

- A. Federation
- B. Identity proofing
- C. Password complexity
- D. Default password changes
- E. Password manager
- F. Open authentication

**Correct Answer:** AC

Community vote distribution

AC (100%)

 **dbrowndiver** Highly Voted 11 months ago

**Selected Answer:** AC

"A". Federation and "C". are the correct answers. Federation facilitates access to multiple systems using a single intranet profile, and password complexity ensures that the passwords used are strong and secure. These concepts work together to safeguard intranet accounts and streamline user access across various company-owned websites.

upvoted 7 times

 **1chung** Most Recent 1 month ago

**Selected Answer:** BF

Correct answer is B & F

upvoted 1 times

 **TheMichael** 11 months, 2 weeks ago

**Selected Answer:** AC

Answer: A and C

Federation establishes trust with a third-party that manages authentication, potentially providing a more secure solution for internal company systems. In this scenario the company is the third party that grants access to other company-owned websites.

The answer is not Open authentication because Open authentication allows you to log into any other company-owned websites with your password, not intranet profile. Open authentication is less secure so a company would be less likely to use it in this fashion which also makes A and C make more sense.

upvoted 4 times

 **NoobusAurelius** 11 months, 2 weeks ago

I agree with NadirM\_18 C and F makes sense because it only states Company owned websites, not company systems/apps.

upvoted 2 times

 **NadirM\_18** 11 months, 3 weeks ago

Seems like this could be CF as this is within the same company.

upvoted 1 times

 **NadirM\_18** 11 months ago

The key difference between SSO and FIM is while SSO is designed to authenticate a single credential across various systems within one organization, federated identity management systems offer single access to a number of applications across various enterprises.

upvoted 1 times

 **c80f5c5** 1 year ago

This one is tricky because federation and open auth are very similar. I think OAuth might be for third party applications (like signing into a game with your facebook account) and not multiple company owned platforms like the question asks

upvoted 3 times

  **35f7aac** 1 year ago

I guess what makes me think OAuth is because OAuth supports SSO which is what I think is being hinted at here. I wish this question was worded better.

upvoted 2 times

  **35f7aac** 1 year ago

OK. I'm going to change to Federation because i just found this on Okta's site. "SAML is independent of OAuth, relying on an exchange of messages to authenticate in XML SAML format, as opposed to JWT. It is more commonly used to help enterprise users sign in to multiple applications using a single login."

upvoted 1 times

  **35f7aac** 1 year ago

Hmm. Why not F instead of A? Question says "other company-owned websites". I thought Federation applies more to independent organizations connecting together.

upvoted 3 times

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

- A. SIEM
- B. DLP
- C. IDS
- D. SNMP

**Correct Answer:** A

*Community vote distribution*

A (100%)

adderalpm Highly Voted 1 year ago

Security information and event management  
upvoted 5 times

dbrowndiver Most Recent 11 months ago

**Selected Answer:** A

SIEM is the correct answer because SIEM systems are specifically designed to collect, centralize, and analyze logs from multiple sources, providing security alerting and monitoring capabilities essential for detecting and responding to potential threats.

upvoted 4 times

A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:

Something you know -

Something you have -

Something you are -

Which of the following would accomplish the manager's goal?

- A. Domain name, PKI, GeoIP lookup
- B. VPN IP address, company ID, facial structure
- C. Password, authentication token, thumbprint
- D. Company URL, TLS certificate, home address

**Correct Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **Shaman73** Highly Voted 👍 1 year ago

- C. Password, authentication token, thumbprint
- upvoted 7 times

🗳️ 👤 **deejay2** Most Recent 🕒 5 months, 3 weeks ago

Selected Answer: C

I get the answer is C. However, why not B?  
upvoted 1 times

🗳️ 👤 **Rafili** 5 months, 3 weeks ago

Selected Answer: C

C, because:

Something you know: In this case, it is the password that the user knows.

Something you have: This refers to the authentication token that the user has, such as a hardware or software token.

Something you are: This represents the thumbprint, which is a biometric method to verify the user's identity.

upvoted 2 times

🗳️ 👤 **nesquick0** 10 months, 3 weeks ago

Selected Answer: C

C obviously

upvoted 4 times

🗳️ 👤 **420JhonnySins69** 9 months, 2 weeks ago

But I know my VPN IP address by memory.

VPN IP address (something that I know), Company ID)

I'm my home address.

upvoted 1 times



Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Segmentation
- B. Isolation
- C. Hardening
- D. Decommissioning

**Correct Answer: A**

Community vote distribution



**Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer: A**

A. Segmentation

Segmentation is the best approach to handle a critical business application running on a legacy server. By segmenting the legacy server from the rest of the network, you can limit the potential impact of any vulnerabilities associated with the legacy system. This approach allows the critical application to continue running while minimizing the risk to the rest of the network.

Therefore, the correct answer is:

A. Segmentation  
upvoted 23 times

**AutoroTink** Highly Voted 1 year, 1 month ago

**Selected Answer: C**

Hardening involves implementing security measures to protect the application from threats while maintaining its availability. Segmentation and isolation can also be part of a security strategy, they are more about limiting access or separating the legacy system from other network segments, which might not be feasible for a critical business application that requires interaction with other systems.

upvoted 9 times

**a4e15bd** 11 months ago

hardening involves measures such as patches, removing unnecessary services, and tightening configurations to reduce vulnerabilities. While hardening is crucial, it may not be sufficient on its own for handling a legacy server due to the inherent limitations and risks of older systems. Isolation, might be better strategy because it minimizes the exposure of the lacy server to the rest of the network and reduce potential impact of any security issues on other systems.

upvoted 3 times

**Anyio** 5 months, 1 week ago

Not Isolation but Segmentation..

upvoted 1 times

**leetasaur** Most Recent 2 months ago

**Selected Answer: B**

Answer is Isolation  
upvoted 1 times

**Studytime2023** 2 months, 1 week ago

**Selected Answer: B**

Isolation (as stated in Comptia guides)  
upvoted 2 times

**JoeRealCool** 2 months, 3 weeks ago

**Selected Answer: A**

In this situation, I don't think hardening makes sense. Because it is a legacy system, it will still be vulnerable regardless of the security configuration of the system. If you add a firewall before the server, that starts to become segmentation. I also think that there is a theme here with the question

bank for these types of questions where the answer for dealing with legacy servers is either segmentation or compensating controls. Decommissioning would be the best way but I don't think it works for this particular question because it doesn't recommend what to do after decommissioning so that the critical application can still run. Isolation doesn't make sense because then the network can't access the critical application. I hate these types of questions.

upvoted 1 times

🗨️ 👤 **Konversation** 3 months ago

**Selected Answer: B**

B. Isolation

CompTIA Sec+ Student Guide - Unsupported systems and Applications: "One strategy for dealing with unsupported apps that cannot be replaced is to try to isolate them from other systems. The idea is to reduce opportunities for a threat actor to access the vulnerable app and run exploit code. Using isolation as a substitute for patch management is an example of a compensating control."

upvoted 2 times

🗨️ 👤 **93d818a** 3 months, 3 weeks ago

**Selected Answer: B**

In the context of the CompTIA Security+ (SY0-701) Exam Objectives, managing legacy systems is crucial due to their inherent security challenges. These systems often lack vendor support, making them susceptible to vulnerabilities. To mitigate risks associated with legacy systems, isolation is a recommended strategy. Isolating legacy systems involves restricting their network access to essential communications only, thereby reducing potential attack vectors

upvoted 2 times

🗨️ 👤 **test\_arrow** 4 months, 1 week ago

**Selected Answer: B**

B. Isolation

Explanation:

A legacy server running a critical business application poses security risks because it may no longer receive updates or security patches. Isolation is the best approach because it minimizes the risk of compromise while allowing the application to continue running.

upvoted 1 times

🗨️ 👤 **585402e** 4 months, 2 weeks ago

**Selected Answer: A**

For this question i choose "Segmentation" but..

Segmentation is ideal when the legacy server requires internet access through the company's web proxy. It keeps the server within a secure, isolated network segment, ensuring it can access the internet while minimizing risks to other parts of the network.

Isolation is the better approach when the legacy server only needs to be powered on for specific local operations. It provides a higher level of security by completely separating the server from other systems and network resources.

upvoted 3 times

🗨️ 👤 **Anyio** 5 months, 1 week ago

**Selected Answer: A**

A. Segmentation.

Segmentation isolates the legacy server within the network, minimizing the attack surface while still allowing necessary communication.

Other options:

B-Isolation may be too restrictive

C-Hardening is limited due to outdated systems

D-Decommissioning isn't viable for critical applications.

Segmentation provides a balanced approach, enhancing security while maintaining functionality.

upvoted 2 times

🗨️ 👤 **Stunomatic** 3 months, 4 weeks ago

in security there is nothing about balanced approach.....zero trust

upvoted 1 times

🗨️ 👤 **ITExperts** 5 months, 1 week ago

**Selected Answer: C**

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues

Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability

upvoted 1 times

🗨️ 👤 **41c27e6** 6 months ago

**Selected Answer: C**

How about patching the legacy server first?

upvoted 1 times

🗨️ 👤 **baijaba** 5 months, 2 weeks ago

you can not patch a legacy software/hardware

upvoted 1 times

🗨️ 👤 **Phatcharaphon** 6 months, 3 weeks ago

**Selected Answer: B**

Isolation is the most effective approach to ensure the legacy system is protected while continuing to support critical business functions, making B the correct choice.

upvoted 3 times

🗨️ 👤 **laternak26** 6 months, 4 weeks ago

**Selected Answer: B**

Given the constraints associated with legacy systems, B. Isolation is the most practical approach to mitigate security risks. By isolating the legacy server, you can protect it and the broader network from potential vulnerabilities.

upvoted 2 times

🗨️ 👤 **ProudFather** 6 months, 4 weeks ago

**Selected Answer: D**

D. Decommissioning

While segmentation, isolation, and hardening can be useful security measures, the best long-term solution for a legacy application is to decommission it and replace it with a more modern and secure alternative. Legacy systems are often difficult to patch, update, and secure, making them prime targets for cyberattacks. By decommissioning the legacy server, the organization can reduce its attack surface and improve its overall security posture.

upvoted 1 times

🗨️ 👤 **dc\_Furious** 7 months, 2 weeks ago

A Segmentation

This is a critical business application if the system is isolated it would not function properly

segmentation would Allow the legacy server to continue operating within the network while restricting its communication to only necessary systems and users. This reduces the attack surface and helps protect the rest of the network from potential vulnerabilities associated with the legacy server.

upvoted 1 times

🗨️ 👤 **3dk1** 7 months, 3 weeks ago

**Selected Answer: A**

It is not Isolation. Isolation would mean blocking access altogether...

That means it is either A or C. I am going with A though.

upvoted 2 times

Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

- A. VM escape
- B. SQL injection
- C. Buffer overflow
- D. Race condition

**Correct Answer:** C

*Community vote distribution*

C (100%)

  **dbrowndiver**  11 months ago

**Selected Answer:** C

The scenario specifically mentions overwriting a register with a malicious address, which is a hallmark of a buffer overflow attack. This technique is commonly used to redirect the program to execute malicious instructions, making buffer overflow the most relevant vulnerability here. In a buffer overflow attack, the attacker might overwrite a register or a return address on the stack with a malicious address, redirecting the program's control flow to execute arbitrary code.

upvoted 9 times

  **Shaman73**  1 year ago

- C. Buffer overflow

upvoted 5 times

After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

- A. Retain the emails between the security team and affected customers for 30 days.
- B. Retain any communications related to the security breach until further notice.
- C. Retain any communications between security members during the breach response.
- D. Retain all emails from the company to affected customers for an indefinite period of time.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: B**

Retain any communications related to the security breach until further notice is the correct answer. This approach ensures that all relevant evidence is preserved in compliance with the legal hold, covering the full scope of communications and documents needed for the lawsuit. It aligns with the purpose of a legal hold, which is to safeguard all potential evidence until the legal proceedings are complete.

upvoted 5 times

 **Shaman73** Most Recent 1 year ago

- B. Retain any communications related to the security breach until further notice.

upvoted 3 times

Which of the following describes the process of concealing code or text inside a graphical image?

- A. Symmetric encryption
- B. Hashing
- C. Data masking
- D. Steganography

**Correct Answer:** D

*Community vote distribution*

D (100%)

  **dbrowndiver** 11 months ago

**Selected Answer: D**

Steganography is the correct answer because it specifically involves the process of concealing code or text inside a graphical image, allowing information to be hidden in plain sight. This technique is unique in its ability to embed data within another medium, making it distinct from other security and privacy techniques like encryption, hashing, or data masking.

upvoted 4 times

  **Shaman73** 1 year, 1 month ago

D. Steganography

upvoted 4 times

An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

- A. Vishing
- B. Smishing
- C. Pretexting
- D. Phishing

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **dbrowndiver** 11 months ago

**Selected Answer: B**

Smishing is the correct answer because the attack is conducted via SMS text messages, and the goal is to manipulate the employee into taking action (purchasing gift cards) based on fraudulent communication. Smishing precisely captures the medium and technique used in this type of social engineering attack.

upvoted 3 times

  **jennyka76** 1 year ago

Answer - B

Smishing, a combination of the words "SMS" and "phishing", is a type of cybercrime that uses deceptive text messages to trick people into sharing sensitive information or downloading malware. Smishing messages may appear to be from a reputable company, such as a bank, and may include a link or phone number to entice the recipient into clicking or calling. If the victim interacts with the message as intended, they may be led to a fraudulent website where they enter personal or financial information, or they may unknowingly download malicious software onto their device. If they call a number, the attacker may try to trick them into providing information verbally or incurring charges.

upvoted 3 times

Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

- A. Mitigate
- B. Accept
- C. Transfer
- D. Avoid

**Correct Answer:** A

Community vote distribution

A (100%)

  **Etc\_Shadow28000**  1 year ago

**Selected Answer:** A

A. Mitigate

When a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the first risk management strategy an enterprise should adopt is to mitigate the risks. This involves implementing measures to reduce the risk to an acceptable level. Mitigation can include steps such as patching vulnerabilities, applying compensating controls, segmenting the network, and hardening the application and its environment.

Therefore, the correct answer is:

A. Mitigate  
upvoted 14 times

  **Syl0**  9 months, 4 weeks ago

**Selected Answer:** A

Mitigate 1st since it is a legacy application and is critical  
upvoted 2 times

  **dbrowndiver** 11 months ago

**Selected Answer:** A

Critical Legacy Application: The application is crucial for business operations, so removing it (avoiding) or accepting the risk without any action could have severe implications.

Preventative Controls Needed: Since preventative controls are not yet implemented, mitigation would involve applying these controls to enhance security and reduce risk exposure.

This why it is the best choice: Mitigation is the most appropriate strategy for addressing risks associated with critical applications, especially when controls can be applied to minimize potential threats.

upvoted 3 times

  **Shaman73** 1 year ago

A. Mitigate  
upvoted 3 times



Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule. Which of the following best describes this form of security control?

- A. Physical
- B. Managerial
- C. Technical
- D. Operational

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **d4a5620** Highly Voted 9 months, 3 weeks ago

**Selected Answer: A**

A) Physical: This is a physical security control because it involves physical barriers and measures to control access to the facility, such as checking photo IDs and using an access control vestibule.

B) Managerial: Managerial controls are policies, procedures, and guidelines established by an organization to ensure security compliance and oversight. This scenario is more focused on physical actions than managerial oversight.

C) Technical: Technical controls involve systems and software (e.g., firewalls, encryption) that secure data and systems electronically. The scenario here involves people and physical infrastructure, not technology.

D) Operational: Operational controls are implemented by people in their day-to-day activities, such as security training or incident response. While the scenario involves operational tasks, the primary focus is on physical security measures.

In summary, physical controls like ID checks and vestibules are examples of barriers to control access to secure areas, making A) Physical the best choice.

upvoted 6 times

 **Shaman73** Most Recent 1 year, 1 month ago

A. Physical

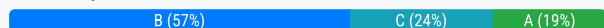
upvoted 3 times

The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface. Which of the following would have most likely prevented this from happening?

- A. Using least privilege
- B. Changing the default password
- C. Assigning individual user IDs
- D. Reviewing logs more frequently

**Correct Answer:** B

Community vote distribution



**d4a5620** Highly Voted 9 months, 3 weeks ago

idk if it's my ADHD or what but I had to re-read this question like 5 times and I still don't completely understand what they're asking lol  
upvoted 23 times

**famuza77** 8 months, 2 weeks ago

I had to read it like 10 times and choosed A lol  
upvoted 5 times

**Shaman73** Highly Voted 1 year ago

B. Changing the default password  
upvoted 9 times

**Linaz312** Most Recent 2 months, 3 weeks ago

**Selected Answer: C**

None really, the answer here is likely B, but in this scenario C is the only thing that makes sense as preventive action:

A: irrelevant, admin should have access

B: This presumes the admin is left with a default password which isnt stated.. the question worded doesn't say anything about misconfiguration, it can't just expect you to assume thats the case

C: only preventive action, maybe if localadmin was USER10 , it can prevent the account from being a target.

D. not preventive action

If answer is B, it should be a different scenario or at least worded differently. nothing to say there was no configuration  
upvoted 2 times

**MarysSon** 3 months, 1 week ago

**Selected Answer: A**

I'm sorry but B is possible, but it isn't the obvious answer. There is no indication that the system's default password was used or any nefarious activity occurred. Sometimes system administrators use their privileged accounts when their normal accounts will accomplish a specific task: in that case, A would be a better answer.

upvoted 1 times

**Anyio** 5 months, 1 week ago

**Selected Answer: B**

B. Changing the default password

Explanation:

Default administrator accounts often come with weak or widely known credentials, making them an easy target for attackers. Changing the default password to a strong, unique one is a fundamental security practice that would have likely prevented unauthorized access.

Other Options:

A. Using least privilege: This is important but doesn't address the issue if the default password is still in use.

C. Assigning individual user IDs: While useful for tracking and accountability, it doesn't prevent unauthorized access if the default admin account remains active.

D. Reviewing logs more frequently: Log reviews can help detect incidents but won't prevent them.

Changing the default password directly addresses the vulnerability.

upvoted 2 times

🗳️ 👤 **chavers93** 6 months, 3 weeks ago

**Selected Answer: B**

Keyword "unexpectedly" and "logged in". if expected it would be with privilege. But not known Somebody could have cracked an easy password.

My choice is B

upvoted 5 times

🗳️ 👤 **ProudFather** 6 months, 4 weeks ago

**Selected Answer: C**

C: By assigning individual user IDs, the company can track who is accessing the remote management interface and hold individuals accountable for their actions. This helps prevent unauthorized access and makes it easier to identify potential security threats.

upvoted 2 times

🗳️ 👤 **fmeox567** 7 months, 1 week ago

**Selected Answer: B**

The most likely action that would have prevented the local administrator account from being used unexpectedly to log in to the remote management interface is:

B. Changing the default password

Here's why:

- Changing the default password: Many VPN appliances come with default usernames and passwords. If these are not changed, anyone with knowledge of the default credentials (which are often easily found online) can gain access to the appliance. Changing the default password to something strong and unique would make it much more difficult for unauthorized users to log in.

- A. Using least privilege: While this is a good security practice, it typically refers to ensuring users have only the minimum level of access needed to perform their tasks. In the case of an administrator account being used, the issue is more likely related to the strength of the password rather than inappropriate access rights being assigned.

upvoted 2 times

🗳️ 👤 **9ef4a35** 7 months, 1 week ago

I will go for C, this will help to track the exact user that logged in

upvoted 1 times

🗳️ 👤 **KelvinYau** 7 months, 4 weeks ago

**Selected Answer: C**

Nowadays, there are not much systems that allow you to log in with a default password. In 2024, the answer should be either A or C. The best option is to disable local admin accounts and assign individual users with least privilege. So C & A is correct

upvoted 1 times

🗳️ 👤 **famuza77** 8 months, 2 weeks ago

I would choose A

upvoted 2 times

🗳️ 👤 **Ty13** 9 months ago

**Selected Answer: B**

Answer is B.

It's the \*local\* admin account. A and C wouldn't work here because those are talking specifically about non-local accounts.

To put it another way, go check your home router - if it's old enough, there's like a 99% chance the default username/password is just admin/admin. It's hard-coded so if you ever physically reset the device then the creds will always default back.

upvoted 1 times

🗳️ 👤 **Fhaddad81** 9 months, 2 weeks ago

I will select C since its local administrator with default permission and should not be used remotely and best practice to assign individual user for each IT admin should manage this device

upvoted 1 times

🗳️ 👤 **chasingsummer** 9 months, 2 weeks ago

**Selected Answer: C**

I think you need to have separate account for VPN and separate account for management.

Option C makes the most sense; Assigning individual user IDs

upvoted 1 times

🗲️ 👤 **420JhonnySins69** 9 months, 2 weeks ago

**Selected Answer: A**

I'm just want to vote for A, because it seems the most reasonable.

upvoted 4 times

🗲️ 👤 **internslayer** 10 months, 2 weeks ago

This is why I hate Sec+ questions. It should be assumed that part of assigning individual user accounts would be to disable a shared local admin account. Using shared accounts is bad practice!!

upvoted 2 times

🗲️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: B**

Many devices and applications come with default administrator credentials that are intended to be changed immediately after installation. Failure to change these passwords leaves systems vulnerable to unauthorized access. By changing the default password for the local administrator account, the company would significantly reduce the risk of unauthorized access. Attackers often attempt to use default credentials to gain entry, so ensuring these are changed is a fundamental security practice.

upvoted 3 times

Which of the following is the best way to secure an on-site data center against intrusion from an insider?

- A. Bollards
- B. Access badge
- C. Motion sensor
- D. Video surveillance

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ **fuckifiknow** 5 months, 1 week ago

**Selected Answer: B**

Wouldn't an insider have a badge?

upvoted 1 times

🗳️ **MarysSon** 3 months, 1 week ago

Yes, an insider would have an access badge, but the badge is associated with assigned permissions and restrictions or PKI certificates. When properly configured, the badges prevent insiders from accessing unauthorized systems or data. B is correct.

upvoted 2 times

🗳️ **bordfree** 4 weeks ago

I think everyone is correct with B, but I think the problem I had that made me hesitant is that access by an insider doesn't have to be unauthorized to cause damage, sometimes the insider has authorization to access the systems they are causing damage with, which is why they can cause so much damage. I re-read the question though, and the keyword here is "intrusion" which implies that they are unauthorized to enter. Therefore, having badge access would keep them out and they wouldn't be able to access it.

upvoted 1 times

🗳️ **dbrowndiver** 11 months ago

**Selected Answer: B**

Access badge is the correct answer because it provides a direct method of controlling and monitoring access to the data center, ensuring that only authorized personnel can enter. Access badges are an effective way to prevent insider threats by restricting access based on roles and permissions, making them the best choice for securing an on-site data center against intrusion from insiders.

upvoted 3 times

🗳️ **jem003** 11 months, 2 weeks ago

**Selected Answer: B**

Access Badge: This allows for controlled and monitored entry into the data center. Only authorized personnel with a valid badge can enter, which helps to prevent unauthorized access. Access badges can be integrated with identity management systems, providing a log of who accessed the data center and when, which is crucial for auditing and accountability.

upvoted 2 times

🗳️ **Shaman73** 1 year ago

**Selected Answer: B**

B. Access badge

upvoted 3 times

An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group. Which of the following access controls is most likely causing the lack of access?

- A. Role-based
- B. Discretionary
- C. Time of day
- D. Least privilege

**Correct Answer:** A

*Community vote distribution*



A (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: A**

Role-based is the correct answer because the issue arises from the engineer's account not being updated to include the new role associated with the new team's shared folders. Role-Based Access Control is the framework in place that determines access based on roles assigned to users, making it the most relevant explanation for the engineer's access issue.

upvoted 6 times

  **ITExperts** 5 months, 1 week ago

why not least privilege?

upvoted 1 times

  **Shaman73** Most Recent 1 year ago

**Selected Answer: A**

A. Role-based

upvoted 3 times

  **Shaman73** 1 year ago

• A. Role-based

upvoted 1 times

Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Choose two.)

- A. Channels by which the organization communicates with customers
- B. The reporting mechanisms for ethics violations
- C. Threat vectors based on the industry in which the organization operates
- D. Secure software development training for all personnel
- E. Cadence and duration of training events
- F. Retraining requirements for individuals who fail phishing simulations

**Correct Answer:** CE

Community vote distribution

CE (100%)

 **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer:** CE


- C. Threat vectors based on the industry in which the organization operates
- E. Cadence and duration of training events

When formulating a training curriculum plan for a security awareness program, it is crucial to focus on:

- Threat vectors based on the industry in which the organization operates (C): Understanding the specific threats that are most relevant to the industry helps tailor the training content to address the most pressing risks and vulnerabilities that employees might face.
- Cadence and duration of training events (E): Establishing an appropriate schedule and duration for training ensures that employees receive regular, ongoing education to keep security top-of-mind and adapt to evolving threats.

Therefore, the correct answers are:

- C. Threat vectors based on the industry in which the organization operates
  - E. Cadence and duration of training events
- upvoted 11 times

 **Th3irdEye** Highly Voted 1 year, 1 month ago

**Selected Answer:** CE

- C you need to know what to train against
- E training schedule is one of the most important aspects of the curriculum

The chosen answer with talking about ethics violations is unrelated to security training.  
Retraining requirements are important too but less so than C and E.

upvoted 5 times

 **Jacket** Most Recent 9 months, 2 weeks ago

- C. Threat vectors based on the industry in which the organization operates:

Understanding the specific threats that are relevant to your industry is critical. Different industries face unique risks (e.g., phishing attacks in finance, insider threats in healthcare). Training should be tailored to address these industry-specific threats to ensure the most relevant and effective education for employees.

- E. Cadence and duration of training events:

The frequency and length of training sessions are essential to ensure that the training is both effective and engaging. Regular, well-timed training helps reinforce security principles, ensuring employees are constantly aware of evolving threats and practices without feeling overwhelmed.

upvoted 1 times

🗨️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: CE**

opt C. Threat vectors based on the industry in which the organization operates and opt E. Cadence and duration of training events are the correct answers. These factors ensure that the training is relevant, engaging, and effective by focusing on the specific threats the organization faces and maintaining consistent reinforcement through well-planned training sessions.

upvoted 1 times

🗨️ 👤 **Shaman73** 1 year ago

**Selected Answer: CE**

C. Threat vectors based on the industry in which the organization operates Most Voted

E. Cadence and duration of training events Most Voted

upvoted 1 times

🗨️ 👤 **edmondme** 1 year ago

**Selected Answer: CE**

ethics issues are unrelated to security trainings. Also setting a cadence is another important factor

upvoted 2 times

🗨️ 👤 **c80f5c5** 1 year ago

**Selected Answer: CE**

Threat vectors and training schedule sounds more important to me than the others

upvoted 1 times

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

**Selected Answer: CE**

If I was to make a curriculum, I'd want to know the biggest "what" that we would teach, and "when" and "how often" we'd be teaching it. The others are great, but not as important as these two things.

upvoted 4 times



A network administrator is working on a project to deploy a load balancer in the company's cloud environment. Which of the following fundamental security requirements does this project fulfil?

- A. Privacy
- B. Integrity
- C. Confidentiality
- D. Availability

**Correct Answer:** D

*Community vote distribution*

D (100%)

🗳️ 👤 **dbrowndiver** 11 months ago

**Selected Answer: D**

Availability is the correct answer because deploying a load balancer enhances the availability of applications and services by distributing traffic, providing redundancy, and ensuring continued access to resources even in the event of server failures. This project directly supports the availability aspect of the security triad.

upvoted 4 times

🗳️ 👤 **Dlove** 11 months, 2 weeks ago

D. Availability

Load balancing in cloud computing distributes traffic and workloads to ensure that no single server or machine is under-loaded, overloaded, or idle. Load balancing optimizes various constrained parameters such as execution time, response time, and system stability to improve overall cloud performance. Therefore it allows the systems more availability.

upvoted 3 times

🗳️ 👤 **Shaman73** 1 year, 1 month ago

D. Availability

upvoted 2 times



A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible. Which of the following operating system security measures will the administrator most likely use?

- A. Deploying PowerShell scripts
- B. Pushing GPO update
- C. Enabling PAP
- D. Updating EDR profiles

**Correct Answer:** B

Community vote distribution

B (100%)

  **adderalpm**  1 year ago

Group Policy Objects (GPOs) provides an infrastructure for centralized configuration management of the Windows operating system and applications that run on the operating system. GPOs are a collection of settings that define what a system will look like and how it will behave for a defined group of computers or users.

upvoted 12 times

  **dbrowndiver**  11 months ago

**Selected Answer: B**

Pushing GPO update is the correct answer because it allows the systems administrator to implement a new password policy across all systems quickly and efficiently through centralized management. GPOs provide the necessary tools to enforce security settings consistently throughout the enterprise environment.

upvoted 3 times

  **Shaman73** 1 year ago

**Selected Answer: B**

B. Pushing GPO update

upvoted 1 times

Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

- A. ARO
- B. RTO
- C. RPO
- D. ALE
- E. SLE

**Correct Answer:** D

Community vote distribution


D (100%)

 **SHADTECH123** Highly Voted 1 year, 1 month ago

**Selected Answer: D**

ALE (Annual Loss Expectancy) represents the expected monetary loss for an asset due to a risk over a year. It is calculated by multiplying the Annual Rate of Occurrence (ARO) by the Single Loss Expectancy (SLE). This provides a clear picture of the financial impact of a risk over time.

upvoted 21 times

 **NinjaTrain** Highly Voted 11 months ago

ARO: Annual Rate of Occurrence

RTO: Recovery Time Objective

RPO: Recovery Point Objective

ALE: Annual Loss Expectancy

SLE: Single Loss Expectancy

upvoted 16 times

 **dbrowndiver** Most Recent 11 months ago

**Selected Answer: D**

ALE (Annualized Loss Expectancy) is the correct answer because it combines both the potential impact of a single event and the frequency of that event occurring to provide a comprehensive financial estimate. This allows an organization to effectively compare the long-term costs of risk transfer strategies against the expected impact of the risk.

upvoted 4 times

 **Shaman73** 1 year ago

**Selected Answer: D**

D. ALE

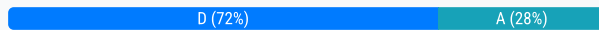
upvoted 1 times

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

- A. Key stretching
- B. Tokenization
- C. Data masking
- D. Salting

**Correct Answer:** D

Community vote distribution



**dbrowndiver** Highly Voted 11 months ago

**Selected Answer: D**

Salting is the correct answer because it involves adding a random string to a password before hashing to strengthen security. This technique effectively prevents precomputed hash attacks, making it a critical component of modern password protection strategies.

upvoted 13 times

**VincentvdS** Most Recent 4 months, 3 weeks ago

**Selected Answer: D**

Salting is correct. Read the difference between Salting and Key Stretching on : <https://library.mosse-institute.com/articles/2023/07/key-stretching-and-saltingm.html>

It explains a lot.

upvoted 2 times

**Eracle** 6 months, 2 weeks ago

**Selected Answer: A**

Why not A?

From CompTIA Security+ SY0-601 Certification Guide :

"Key stretching is where you append a random set of characters to a password to increase the size of the password and its hash, ensuring that a brute-force attack needs more compute time to crack the password."

upvoted 3 times

**Eracle** 5 months, 4 weeks ago

CORRECTION: cannot be D, because lengthening the key does not add a causal string to the password. Key stretching involves applying a cryptographic function repeatedly (thousands or millions of times) on the password and salt to make the hashing process much slower and computationally expensive.

CORRECT ANSWER: A.

upvoted 4 times

**\_tips** 6 months, 3 weeks ago

**Selected Answer: A**

Salting

Adds a random string of characters, called a "salt", to a password before hashing it. This makes each password unique and prevents attackers from:

Using dictionary lookups to see how popular passwords are hashed

Guessing the hash function to unlock a database of passwords

Key stretching

Lengthens the password by iterating the hash of the salted password. This makes it much more difficult for attackers to crack passwords using brute-force or precomputed tables.

upvoted 1 times

**chalaka** 7 months, 1 week ago


**Selected Answer: D**

D. Salting

Explanation:

Salting involves adding a random string (called a salt) to a password before it is hashed to prevent attackers from using precomputed hash databases (like rainbow tables) to crack the password. The random string (in this case, 36 characters) is unique and makes the password significantly harder to guess because it ensures that even if two users have the same password, their hashes will be different.

upvoted 2 times

  **jsmthy** 9 months ago

**Selected Answer: A**

Key stretching techniques are used to make a possibly weak key, typically a password or passphrase, more secure against a brute-force attack by increasing the resources it takes to test each possible key.

Salting does not add to the length of the password and does not stop attackers from brute-forcing the key as the salt is added after the password is submitted.

Tokenization and Data masking will not prevent brute-force attacks for the same reason. They are processes that don't alter a weak password.

upvoted 4 times

  **Shaman73** 1 year ago

**Selected Answer: D**

D. Salting

upvoted 2 times

A technician is deploying a new security camera. Which of the following should the technician do?

- A. Configure the correct VLAN.
- B. Perform a vulnerability scan.
- C. Disable unnecessary ports.
- D. Conduct a site survey.

**Correct Answer:** D

Community vote distribution

D (88%)

9%

  **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer: D**



D. Conduct a site survey.

Before deploying a new security camera, conducting a site survey is crucial. A site survey helps determine the optimal placement of the camera, assesses environmental factors, ensures there are no blind spots, and verifies that the camera will effectively cover the desired area. It also helps in planning for network connectivity, power supply, and other logistical considerations.

Therefore, the correct answer is:

D. Conduct a site survey.

upvoted 8 times

  **AutoroTink** Highly Voted 1 year, 1 month ago

**Selected Answer: D**



A site survey is essential to determine the best locations for camera installation, ensuring optimal coverage and signal strength. It involves assessing the physical environment to identify any potential issues that could affect the camera's performance, such as obstructions, lighting conditions, and power source availability.

A. Configure the correct VLAN: While important for network segmentation, it's not the first step in physical deployment.

B. Perform a vulnerability scan: This is more relevant for assessing the security of existing systems, not the initial placement of a camera.

C. Disable unnecessary ports: This is a security measure for network devices, but it doesn't address the physical aspects of camera deployment.

upvoted 6 times

  **MarysSon** Most Recent 3 months, 1 week ago

**Selected Answer: B**

The question does not describe the scenario adequately. If you're installing a new video security system with multiple cameras, that would point towards D – conduct a site survey. When installing one, new camera, you need to ensure it contains no vulnerabilities or malicious firmware. Based on the question, the better answer is B.

upvoted 1 times

  **3dk1** 7 months, 3 weeks ago

I thought a site survey had to do with setting up Access Points for wireless networks, not setting up a security camera?

upvoted 1 times

  **Ty13** 9 months ago

Are they deploying a new camera to replace an old one? If so, it's C, because they wouldn't need to conduct a site survey if they already have optimal locations set.

Is it just the thought of "Hey, I want to get a camera in the parking garage."? Then it would be D.

upvoted 1 times

  **93a09c9** 10 months, 3 weeks ago

**Selected Answer: D**

A site survey is ALWAYS the first step before installing any system or component.

upvoted 2 times

  **dbrowndiver** 11 months ago

**Selected Answer: D**

Conduct a site survey is the correct answer because it is the critical first step in deploying a new security camera. It ensures that the camera is installed in the right location and covers the necessary areas effectively. Once the site survey is completed, other actions such as VLAN configuration, vulnerability scanning, and port management can follow to ensure optimal performance and security.

upvoted 2 times

  **cdsu** 1 year ago

Answer: D

...physical placement first

upvoted 3 times

  **Shaman73** 1 year ago

**Selected Answer: D**

D. Conduct a site survey.

upvoted 2 times

  **f71cbb0** 1 year, 1 month ago

**Selected Answer: C**

C should be better answer than D. Deploying is not the same installing.

If a technician were "installing" a new security camera, then the best answer would be (D) conduct a site survey.



upvoted 3 times

  **SHADTECH123** 1 year, 1 month ago

**Selected Answer: D**

Conducting a site survey involves assessing the physical environment where the security camera will be installed. This includes identifying optimal camera placement, ensuring sufficient coverage, assessing lighting conditions, and identifying potential sources of interference. It helps ensure that the security camera is deployed effectively to meet the organization's surveillance requirements.

upvoted 3 times

  **Yoez** 1 year, 1 month ago

**Selected Answer: D**

I would say D

upvoted 3 times

  **shady23** 1 year, 1 month ago

**Selected Answer: D**

D. Conduct a site survey.

The keyword in the question that makes option D correct is "deploying a new security camera."

Conducting a site survey is crucial when deploying new security cameras because it allows the technician to assess various factors such as the physical environment, potential obstacles, optimal camera placement, coverage areas, and lighting conditions. This ensures that the security camera is installed in the most effective location to fulfill its surveillance objectives.

upvoted 4 times

A company is experiencing a web services outage on the public network. The services are up and available but inaccessible. The network logs show a sudden increase in network traffic that is causing the outage. Which of the following attacks is the organization experiencing?

- A. ARP poisoning
- B. Brute force
- C. Buffer overflow
- D. DDoS

**Correct Answer:** D

Community vote distribution

D (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: D**

DDoS is the correct answer because the sudden increase in network traffic leading to a web services outage is characteristic of a Distributed Denial of Service attack. This type of attack overwhelms the target's resources, making services inaccessible, even though they are still operational. DDoS attacks specifically aim to disrupt access by flooding the target with excessive traffic, matching the symptoms described in the scenario.

upvoted 7 times

  **danielbadasu** Most Recent 2 weeks, 2 days ago

**Selected Answer: D**

inaccessible = Denial

hence D.

upvoted 1 times

  **Shaman73** 1 year ago

**Selected Answer: D**

D. DDoS

upvoted 4 times



Which of the following threat actors is the most likely to be motivated by profit?

- A. Hacktivist
- B. Insider threat
- C. Organized crime
- D. Shadow IT

**Correct Answer:** C

*Community vote distribution*

C (100%)

  **dbrowndiver** 11 months ago

**Selected Answer: C**

Profit is the main driver for organized crime, making them the most likely threat actor motivated by financial incentives. They are structured to exploit opportunities that result in monetary rewards. Therefore, Organized crime is the correct answer because organized crime groups are primarily driven by the pursuit of financial gain. They engage in cyber activities designed to steal, extort, or otherwise generate profit, making them the most profit-motivated threat actor in this context.

upvoted 4 times

  **Shaman73** 1 year, 1 month ago

C. Organized crime

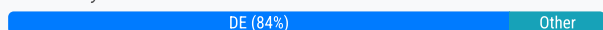
upvoted 1 times

An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Choose two.)

- A. Application
- B. Authentication
- C. DHCP
- D. Network
- E. Firewall
- F. Database

**Correct Answer:** DE

Community vote distribution



**Shaman73** Highly Voted 1 year ago

**Selected Answer:** DE

- D. Network
- E. Firewall

upvoted 12 times

**VincentvdS** Most Recent 4 months, 3 weeks ago

**Selected Answer:** DE

In the context of a command-and-control (C2C) server, analyzing network and firewall logs is more effective for identifying the impacted host. These logs provide detailed information about network traffic, including connections to and from the C2C server, which can help pinpoint the affected devices.

The two most relevant logs to analyze in this scenario would be:

- D. Network

Network logs can provide insights into the traffic patterns and connections related to the C2C server.

- E. Firewall

Firewall logs can help identify any unusual or unauthorized connections to the C2C server, aiding in the identification of the impacted host.

upvoted 3 times

**Aces155** 5 months, 1 week ago

**Selected Answer:** CD

Bing copilot is saying C and D.

The best two logs to analyze for identifying the impacted host in a command-and-control incident would be:

Network logs: These provide detailed information about network traffic, including connections to and from the command-and-control server.

DHCP logs: These help map IP addresses to specific devices at given times, which is crucial for identifying the impacted host.

While firewall logs are valuable for security information, network and DHCP logs together provide the most comprehensive data needed to pinpoint the specific host involved.

upvoted 1 times

**Aces155** 5 months, 1 week ago

It wouldn't let me comment without entering answers. I just wanted to provide this explanation

upvoted 1 times

**41c27e6** 6 months ago

**Selected Answer:** DE

Network Logs (D):



Network logs are crucial for identifying communication between the compromised host and the command-and-control server. These logs will typically

include details of network traffic, including IP addresses, ports, protocols, and patterns of communication. By analyzing network logs, you can track outbound connections that may have been initiated by the infected host to communicate with the command-and-control server.

Firewall Logs (E):

Firewall logs are useful for identifying inbound and outbound traffic that is blocked or allowed by the firewall. They can help pinpoint suspicious traffic patterns, such as attempts to connect to known malicious IP addresses (such as the command-and-control server). Firewall logs will also show if the infected host tried to bypass any restrictions to communicate with external servers.

upvoted 2 times

  **c7b3ff0** 8 months, 2 weeks ago

**Selected Answer: BE**

Since this is specifically asking about identifying the impacted host, I chose B and E.

B. Authentication - This log helps identify any unauthorized access or unusual login attempts related to compromised hosts.

E. Firewall - provide insights into incoming and outgoing traffic patterns, detecting comms with the C2 server to help identify the affected host.

upvoted 1 times

  **dbrowndiver** 11 months ago

**Selected Answer: CE**

C. DHCP and E. Firewall logs are the correct answers because they provide essential information to trace network communications and identify the specific host(s) impacted by the command-and-control server connection. Firewall logs help pinpoint unusual outbound connections, such as those from internal hosts to a suspicious external server, thus identifying potential breaches. DHCP logs map IP addresses to devices, while firewall logs reveal the network traffic patterns, making them both crucial for this analysis. DHCP logs are crucial for linking IP addresses seen in network activity to actual devices, especially in dynamic environments where IP addresses frequently change.

upvoted 2 times

  **101e7ca** 11 months, 1 week ago

**Selected Answer: DE**

"command-and-control server" is the problem, attacker has accessed the network and taken control of a machine. We should check the inbound and outbound traffic logs. These will be on the Router(Network) and network Firewall.

upvoted 4 times

  **Bimbo\_12** 11 months, 1 week ago

**Selected Answer: DE**

To identify the impacted host in a cybersecurity incident involving a command-and-control server, the most relevant logs to analyze would be:

C. DHCP and E. Firewall

: Firewall logs capture network traffic and can show which internal hosts communicated with external IP addresses, including the command-and-control server.

By analyzing firewall logs, you can identify the internal IP addresses that initiated or received communication with the command-and-control server, helping to pinpoint the impacted host.

If you have already identified suspicious network traffic (e.g., connections to a C2 server) in firewall or network logs, the next step is often to determine which device was responsible for that traffic.

DHCP logs are necessary for this step because they map IP addresses to specific devices. Without this mapping, knowing the IP address alone is insufficient, especially in environments where IP addresses are dynamically assigned.

By consulting DHCP logs, you can quickly identify the physical or virtual device behind the suspicious activity.

upvoted 3 times

  **cdsu** 1 year ago

Answer:

C. DHCP

E. Firewall

C: Impacted host. To trace back any suspicious network activity to a specific device

E: Firewall logs contain records of all incoming and outgoing traffic

upvoted 2 times

During a penetration test, a vendor attempts to enter an unauthorized area using an access badge. Which of the following types of tests does this represent?

- A. Defensive
- B. Passive
- C. Offensive
- D. Physical

**Correct Answer:** D

Community vote distribution

D (100%)

🗲️ 👤 **baguttebandit** 1 month, 3 weeks ago

**Selected Answer:** C

Isn't this both physical and offensive?  
upvoted 2 times

🗲️ 👤 **Cyber24** 6 months, 2 weeks ago

**Selected Answer:** D

using an access badge is a Physical  
upvoted 2 times

🗲️ 👤 **96bc5c8** 7 months, 2 weeks ago

kjgjhkg  
upvoted 1 times

🗲️ 👤 **dbrowndiver** 11 months ago

**Selected Answer:** D

o The scenario specifically involves testing the ability to physically enter a secure area, which aligns perfectly with the definition of a physical penetration test.  
upvoted 2 times

🗲️ 👤 **Shaman73** 1 year ago

**Selected Answer:** D

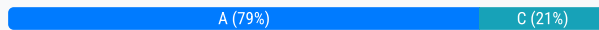
D: Physical  
upvoted 1 times

A systems administrator uses a key to encrypt a message being sent to a peer in a different branch office. The peer then uses the same key to decrypt the message. Which of the following describes this example?

- A. Symmetric
- B. Asymmetric
- C. Hashing
- D. Salting

**Correct Answer:** A

Community vote distribution



🗳️ 👤 **shady23** Highly Voted 1 year, 1 month ago

**Selected Answer:** C

Symmetric Encryption

In this type of encryption, there is only one key, and all parties involved use the same key to encrypt and decrypt information.

upvoted 6 times

🗳️ 👤 **drosas84** 1 year ago

then why did you choose C when it should be A?

upvoted 3 times

🗳️ 👤 **SHADTECH123** 1 year, 1 month ago

You stated your Selected Answer to be "C" - Hashing, but explained Symmetric encryption, I guess it's a typo

upvoted 4 times

🗳️ 👤 **Dlove** Highly Voted 11 months, 2 weeks ago

**Selected Answer:** A

A. Symmetric same key to encrypt and decrypt

upvoted 5 times

🗳️ 👤 **nesquick0** Most Recent 10 months, 3 weeks ago

**Selected Answer:** A

A. Symmetric

upvoted 4 times

🗳️ 👤 **c80f5c5** 1 year ago

**Selected Answer:** A

symmetric

upvoted 4 times

🗳️ 👤 **Shaman73** 1 year, 1 month ago

A. Symmetric

upvoted 4 times

🗳️ 👤 **MAKOhunter33333333** 1 year, 1 month ago

**Selected Answer:** A

The same key for both processes

upvoted 5 times

🗳️ 👤 **123456789User** 1 year, 1 month ago

**Selected Answer:** A

Symmetric: Same key is used to encrypt as is used to decrypt.

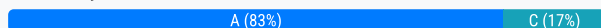
upvoted 4 times

A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network. Which of the following should be configured on the existing network infrastructure to best prevent this activity?

- A. Port security
- B. Web application firewall
- C. Transport layer security
- D. Virtual private network

**Correct Answer: A**

Community vote distribution



**dbrowndiver** Highly Voted 11 months ago

**Selected Answer: A**

Port security is a feature available on network switches that helps secure access to the physical network by restricting which devices can connect to each network port based on their MAC address.

Port Security: This is a network security feature that restricts input to an interface by limiting and identifying MAC addresses of the devices allowed to access the port. It can be configured to block devices that do not match the allowed list.

-Control Over Physical Access: By enabling port security on the network jacks, the organization can ensure that only authorized devices with specific MAC addresses are allowed to connect. Any unauthorized devices, such as a visitor's laptop, would be blocked from accessing the network.

-Dynamic or Static Configuration: Port security can dynamically learn and store allowed MAC addresses or use a predefined list, providing flexibility in securing physical network ports.

This why it is the best answer: Port security directly addresses the issue of unauthorized access through physical network connections by controlling which devices can use the network ports. It prevents unauthorized devices from gaining network access, making it the most appropriate solution for this scenario.

upvoted 6 times

**41c27e6** Most Recent 6 months ago

**Selected Answer: A**

Port security is a feature that can be configured on network switches to limit which devices can connect to specific ports

upvoted 2 times

**Andrewyounan** 11 months, 1 week ago

**Selected Answer: C**

I go more for TLS which is part of EAP-TLS used with 802.1X on the NAC to authenticate.

On the other hand, Port Sec. you'll need to either identify the MAC address or Sticky MAC address, so it makes sense to go with C. ### Maybe I'm over-thinking ### :D

upvoted 3 times

**deejay2** 5 months, 3 weeks ago

I understand why you say TLS. However, the question is asking about preventing the ability to connect to the network, not protecting the data as it flows through the network.

upvoted 4 times

**tamdod** 10 months, 1 week ago

On Port security, you shut the port off so no one can use it.

upvoted 1 times

**Shaman73** 1 year ago

**Selected Answer: A**

A. Port security

upvoted 4 times

**MAKOhunter33333333** 1 year, 1 month ago

**Selected Answer: A**

Port security / 802.1x / NAC

upvoted 4 times

A security administrator is reissuing a former employee's laptop. Which of the following is the best combination of data handling activities for the administrator to perform? (Choose two.)

- A. Data retention
- B. Certification
- C. Destruction
- D. Classification
- E. Sanitization
- F. Enumeration

**Correct Answer:** BE

Community vote distribution



**cf83993** Highly Voted 11 months ago

**Selected Answer: BE**

Bro you don't reissue something after you destroy it do you? We're talking about a laptop here not an ex ;) upvoted 32 times

**MikelMiguel** 7 months, 2 weeks ago

Reissue doesn't mean to the same employee. It could be to another employee in Shipping department. So why not destroy and sanitize account department laptop before reissuing. upvoted 2 times

**Russell15** 3 months, 1 week ago

You cant reuse something after destroying it? upvoted 2 times

**Th3irdEye** Highly Voted 1 year, 1 month ago

**Selected Answer: AE**

Destruction would make the device not usable again. Certification might make sense here if a third party was being used to sanitize the drive but usually third parties are used to destroy drives and certification is given for destruction.

I think Data retention and Sanitization makes the most sense. You want to make sure you save any critical data before you erase the drive. upvoted 23 times

**1chung** Most Recent 1 month ago

**Selected Answer: CE**

Correct Answer is CE upvoted 1 times

**Konversation** 3 months ago

**Selected Answer: AE**

Since the question does not refer a third-party but to the "internal" administrator and following the CompTIA theoretical questions it's A & E.

E. Sanitization. This is clear.

A. Data retention.

The CompTIA Student Guide and WBT refer to the "Data retention" in the "Secure Data Destruction" chapter.

B. Certification is used by CompTIA only for third-party "Asset Disposal". But a third-party is not mentioned in the question.

"certification - An asset disposal technique that relies on a third party to use sanitization or destruction methods for data remnant removal, and provides documentary evidence that the process is complete and successful."

C. Destruction - CompTIA defines this as "Physical destruction methods include shredding, crushing ..." This is also not the case for this question.



upvoted 3 times

🗄️ 👤 **adderalp** 3 months ago

**Selected Answer: AE**

Destruction renders the device unusable does it no? And you only need a certification after destruction from a third-party? So in reality, you would just want to back up the data and then make sure to overwrite the hard drive a couple times so that, that data can't be recovered. ☐☐

upvoted 2 times

🗄️ 👤 **d2087a6** 4 months ago

**Selected Answer: CE**

To safely reissue the laptop, the administrator should sanitize the device to remove all data securely. If sanitization isn't sufficient for highly sensitive data, destruction of the storage medium may be required.

upvoted 2 times

🗄️ 👤 **dbrowndiver** 5 months, 1 week ago

**Selected Answer: BE**

Data destruction involves securely deleting sensitive information so it cannot be recovered. Before reissuing a laptop, it is critical to ensure that any residual data from the previous user is permanently removed to prevent unauthorized access to sensitive information.

upvoted 2 times

🗄️ 👤 **Oca8ee9** 6 months, 3 weeks ago

**Selected Answer: BE**

Sanitization - cleaning the laptop memory

Certification - proving that the laptop is clean.

upvoted 4 times

🗄️ 👤 **ProudFather** 6 months, 4 weeks ago

**Selected Answer: CE**

To ensure the security of the data, the administrator should:

Destruction: Physically destroy any storage media that cannot be sanitized.

Sanitization: Thoroughly erase or overwrite all data on the storage media to prevent data recovery.

The other options are not relevant to the scenario:

Data retention: This involves keeping data for a specific period. It's not applicable in this case as the data needs to be removed.

Certification: This is a process of verifying that a system or process meets specific standards. It's not relevant to data handling in this context.

Classification: This involves assigning security labels to data based on its sensitivity. It's not necessary in this case as the data is being removed.

Enumeration: This involves identifying and cataloging assets. It's not relevant to data handling in this context.

upvoted 4 times

🗄️ 👤 **AndyK2** 7 months ago

**Selected Answer: CE**

C. Destruction > ensures physical media is rendered unrecoverable

E. Sanitization > removes and overwrites sensitive data to prevent unauthorized access.

Both used to protect data security when repurposing hardware.

upvoted 2 times

🗄️ 👤 **MikelMiguel** 7 months, 2 weeks ago

Its Destruction and Sanitation. This is because the laptop is been reissued and because they question did not say reissued to the "same employee" then we have to assume is been intended to be reissued for a new or another employee. therefore D&E is the answer

upvoted 2 times

🗄️ 👤 **3dk1** 7 months, 3 weeks ago

**Selected Answer: AE**

Th3irdEye explains my thinking

upvoted 3 times

🗄️ 👤 **Emmyraj** 7 months, 3 weeks ago

**Selected Answer: CE**

C. Destruction

E. Sanitization

Explanation:

1. Destruction: This involves permanently destroying any sensitive data on the laptop that is no longer needed. This ensures that no residual data from the previous user remains on the device, reducing the risk of unauthorized data access.
2. Sanitization: This involves securely wiping the laptop's storage to remove all data and ensure that it cannot be recovered. Sanitization is critical when reissuing devices to prevent accidental disclosure of sensitive information.

upvoted 1 times

  **nillie** 9 months ago

**Selected Answer: CE**

The best combination of data handling activities for the administrator to perform when reissuing a former employee's laptop are:

C. Destruction and E. Sanitization

Destruction: Ensures that any sensitive or personal data from the previous user is permanently removed and cannot be recovered.

Sanitization: Refers to thoroughly cleaning the device by securely wiping the data to prevent unauthorized access. This prepares the laptop for safe reissue to a new user.

These two activities are critical for preventing any sensitive data leakage from the former employee while ensuring that the device is clean and secure for the next user.

upvoted 2 times

  **ETQ** 8 months, 1 week ago

"Hey user, here's your laptop that I just destroyed, now chopchop, get to work!"

upvoted 3 times

  **Ty13** 9 months ago



**Selected Answer: AE**

Retention and Sanitize.

Think about it. An employee leaves - you backup any pertinent company data (Retention) and reimage the computer (Sanitize).

- You would not Certify it, because that's only if the drive needed to be destroyed.
- You would not Destroy it because that's really only important for sensitive things, not Judy the Customer Service agent.
- You would not Enumerate it (gathering info for vulnerabilities)
- Classification is typically more important for data rather than devices.

upvoted 6 times

  **ImpactTek** 9 months, 1 week ago

The answer is C&E. Destruction here refers to destroying data not the laptop.

upvoted 2 times



  **ETQ** 8 months, 1 week ago

No, it doesn't mean that at all. If it did, sanitizing after "destroying the data" would be useless.

Destruction refers to destroying the drive, which you do when you actually dispose of the machine, not when you reissue it.

You need to sanitize the drive and certify that you did.

upvoted 4 times

  **koala\_lay** 9 months, 2 weeks ago

**Selected Answer: BE**

Agree to answer B E

upvoted 3 times

A systems administrator would like to deploy a change to a production system. Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

- A. Backout plan
- B. Impact analysis
- C. Test procedure
- D. Approval procedure

**Correct Answer:** A

Community vote distribution

A (100%)

Abcd123321 Highly Voted 1 year, 1 month ago

Selected Answer: A

What is a backout plan?

A backout plan is a predefined strategy to reverse and recover from changes made to a system if the changes produce undesirable results. It's a safety measure that ensures data integrity and system availability. See also: backup, recovery time objective, mean time to recovery.

upvoted 10 times

dbrowndiver Most Recent 11 months ago

Selected Answer: A

Backout plan is the correct answer because it provides a detailed strategy for reverting changes in the event of a performance issue. This document ensures that the system can be restored to its working state, addressing the critical need for a reliable rollback mechanism during change management.

upvoted 2 times

Shaman73 1 year ago

Selected Answer: A

A. Backout plan

upvoted 2 times

A company is redesigning its infrastructure and wants to reduce the number of physical servers in use. Which of the following architectures is best suited for this goal?

- A. Serverless
- B. Segmentation
- C. Virtualization
- D. Microservices

**Correct Answer:** C

Community vote distribution

C (100%)

MAK0hunter33333333 Highly Voted 1 year, 1 month ago

Selected Answer: C

Remove physical servers > transition to virtualization for services like the cloud.  
upvoted 7 times

Exemplary Most Recent 8 months, 3 weeks ago

Proud of all of you for not taking the bait!  
upvoted 4 times

Anyio 5 months ago  
I took the bait, sorry mate!  
upvoted 3 times

Syl0 9 months, 3 weeks ago

It only says reduce the number of physical servers, it didn't say it doesn't want servers....  
upvoted 3 times

dbrowndiver 11 months ago

Selected Answer: C

Virtualization is the correct answer because it enables the reduction of physical servers by allowing multiple virtual servers to operate on a single physical machine. Virtualization optimizes resource usage and simplifies management, aligning perfectly with the company's goal of minimizing physical infrastructure.  
upvoted 3 times

Etc\_Shadow28000 1 year ago

Selected Answer: C

C. Virtualization

Virtualization is the architecture best suited for reducing the number of physical servers in use. It allows multiple virtual machines (VMs) to run on a single physical server, maximizing the utilization of hardware resources and reducing the need for multiple physical servers.

Therefore, the correct answer is:

C. Virtualization  
upvoted 4 times

Shaman73 1 year ago

Selected Answer: C

C. Virtualization  
upvoted 2 times

A bank set up a new server that contains customers' PII. Which of the following should the bank use to make sure the sensitive data is not modified?

- A. Full disk encryption
- B. Network access control
- C. File integrity monitoring
- D. User behavior analytics

**Correct Answer:** C

Community vote distribution

C (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: C**

File Integrity Monitoring is the correct answer because it specifically addresses the need to monitor and detect unauthorized modifications to sensitive data. FIM ensures that any changes to files containing PII are identified and alerted, maintaining data integrity and protecting against unauthorized alterations.

upvoted 5 times

  **Dlove** Most Recent 11 months, 2 weeks ago

**Selected Answer: C**

C. File Integrity Monitoring

File integrity monitoring is an internal control or process that performs the act of validating the integrity of operating system and application software files using a verification method between the current file state and a known, good baseline.

upvoted 2 times

  **Shaman73** 1 year ago

**Selected Answer: C**

C. File integrity monitoring

upvoted 2 times

Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked. Which of the following changes would allow users to access the site?

- A. Creating a firewall rule to allow HTTPS traffic
- B. Configuring the IPS to allow shopping
- C. Tuning the DLP rule that detects credit card data
- D. Updating the categorization in the content filter

**Correct Answer:** D

Community vote distribution

D (100%)

  **dbrowndiver**  11 months ago

**Selected Answer: D**



Updating the categorization in the content filter is the correct answer because it directly addresses the misclassification of the retail website as a gambling site. By correcting the categorization, users will be able to access the site without further issues, resolving the problem efficiently and effectively.

upvoted 9 times

  **3dk1**  8 months, 1 week ago

they went easy on us with this one

upvoted 2 times

  **ezmoney** 11 months, 3 weeks ago

D. Updating the categorization in the content filter

By updating the categorization in the content filter to accurately reflect the nature of the retail website (shopping instead of gambling), the content filter will allow users to access the site without being blocked.

upvoted 4 times

  **Shaman73** 1 year ago

**Selected Answer: D**

Updating the categorization in the content filter

upvoted 3 times

Which of the following most impacts an administrator's ability to address CVEs discovered on a server?

- A. Rescanning requirements
- B. Patch availability
- C. Organizational impact
- D. Risk tolerance

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **Etc\_Shadow28000** Highly Voted 1 year ago

**Selected Answer:** B

B. Patch availability

Patch availability most impacts an administrator's ability to address Common Vulnerabilities and Exposures (CVEs) discovered on a server. If patches are not available to fix the vulnerabilities, the administrator cannot remediate the issues, regardless of other factors.

Therefore, the correct answer is:

B. Patch availability  
upvoted 11 times

 **dbrowndiver** Most Recent 11 months ago

**Selected Answer:** B

Patch availability is the most critical factor in an administrator's ability to address CVEs on a server because it directly determines whether a known vulnerability can be fixed through updates or patches provided by software vendors. Patch Availability refers to whether a vendor has released a software update or patch that addresses a specific vulnerability identified by a CVE. Without a patch, the administrator cannot remediate the vulnerability through standard update processes.

upvoted 3 times

 **Shaman73** 1 year ago

**Selected Answer:** B

B. Patch availability  
upvoted 2 times

Which of the following describes effective change management procedures?

- A. Approving the change after a successful deployment
- B. Having a backout plan when a patch fails
- C. Using a spreadsheet for tracking changes
- D. Using an automatic change control bypass for security updates

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **dbrowndiver** Highly Voted 11 months ago

**Selected Answer: B**

o When applying patches or making system changes, there's always a risk of unforeseen issues. An effective backout plan allows for a quick and organized response, ensuring that systems can be returned to their last known good state, thereby maintaining business continuity and reducing the potential impact on operations.

upvoted 6 times

  **9149f41** Most Recent 4 months, 3 weeks ago

**Selected Answer: B**

Check if the backup or rollback to the previous setup option is available for the particular application.  
Then decide whether to update/patch the application.

upvoted 1 times

  **Shaman73** 1 year ago

**Selected Answer: B**

Having a backout plan when a patch fails

upvoted 2 times



The CIRT is reviewing an incident that involved a human resources recruiter exfiltrating sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server. Which of the following security infrastructure devices could have identified and blocked this activity?

- A. WAF utilizing SSL decryption
- B. NGFW utilizing application inspection
- C. UTM utilizing a threat feed
- D. SD-WAN utilizing IPSec

**Correct Answer:** B

Community vote distribution

B (100%)

  **dbrowndiver** Highly Voted 11 months ago

NGFW utilizing application inspection is the correct answer because it provides the necessary application-level awareness to detect and block HTTP traffic over non-standard ports, such as port 53. The NGFW's advanced inspection capabilities allow it to enforce security policies that prevent unauthorized data exfiltration, making it an essential component of modern network security infrastructure.

upvoted 7 times

  **Syl0** Highly Voted 9 months, 3 weeks ago

WAF - Web App Firewall

NGFW - Next Generation Firewall

UTM - Unified Threat Management

SD-WAN - Software defined Wide area network

upvoted 6 times

  **dbrowndiver** Most Recent 11 months ago

NGFW utilizing application inspection is the correct answer because it provides the capability to identify and block unauthorized applications and traffic using non-standard ports, such as HTTP traffic over port 53. Its advanced inspection capabilities make it well-suited to detect and prevent data exfiltration methods that involve protocol and port misuse.

upvoted 2 times

  **Etc\_Shadow28000** 1 year ago

Selected Answer: B

B. NGFW utilizing application inspection

A Next-Generation Firewall (NGFW) utilizing application inspection could have identified and blocked the use of HTTP over port 53. NGFWs have advanced capabilities that allow them to inspect and identify traffic based on the application layer, not just the port and protocol, enabling them to detect and prevent non-standard use of ports for malicious activities.

Therefore, the correct answer is:

B. NGFW utilizing application inspection

upvoted 5 times

  **Shaman73** 1 year ago

Selected Answer: B

B. NGFW utilizing application inspection

upvoted 2 times

An enterprise is working with a third party and needs to allow access between the internal networks of both parties for a secure file migration. The solution needs to ensure encryption is applied to all traffic that is traversing the networks. Which of the following solutions should most likely be implemented?

- A. EAP
- B. IPSec
- C. SD-WAN
- D. TLS

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **edmondme** Highly Voted 1 year ago

**Selected Answer:** B

If you need to secure communication between networks or remote sites, IPsec is a suitable choice. On the other hand, if you are primarily concerned with securing web-based communication, TLS is the preferred option.

upvoted 12 times

  **dbrowndiver** Highly Voted 10 months, 4 weeks ago

**Selected Answer:** B

IPSec is the correct answer because it provides comprehensive encryption for all IP traffic between the internal networks of both parties, ensuring secure file migration. IPSec's ability to encrypt, authenticate, and ensure the integrity of all data packets makes it the most suitable solution for protecting communications between the enterprise and the third party.

upvoted 7 times

  **Shaman73** Most Recent 1 year ago

**Selected Answer:** B

B. IPSec

upvoted 2 times

An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization. Which of the following best describes the tool the administrator is using?

- A. DLP
- B. SNMP traps
- C. SCAP
- D. IPS

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗳️ 👤 **Syl0** 9 months, 3 weeks ago

SNMP - Simple Network Management Protocol is for network devices.

SCAP - Security Content Automation Protocol

IPS - Intrusion Prevention System

DLP would be the one that focuses on Data because it is Data Loss Prevention

upvoted 3 times

🗳️ 👤 **dbrowndiver** 10 months, 4 weeks ago

**Selected Answer: A**

DLP is the correct answer because it is specifically designed to detect, monitor, and prevent the unauthorized transfer of sensitive data, such as fingerprinted files, outside the organization. DLP solutions provide the necessary tools to ensure data security by generating alerts and blocking unauthorized data exfiltration attempts.

upvoted 4 times

🗳️ 👤 **adderalpm** 1 year ago

Data Loss Prevention

upvoted 3 times

🗳️ 👤 **Shaman73** 1 year ago

**Selected Answer: A**

A. DLP

upvoted 2 times

A software developer released a new application and is distributing application files via the developer's website. Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?

- A. Hashes
- B. Certificates
- C. Algorithms
- D. Salting

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗳️ 👤 **dbrowndiver** 10 months, 4 weeks ago

**Selected Answer: A**

Hashes is the correct answer because they provide a straightforward and reliable method for verifying the integrity of downloaded files. By comparing the hash of a downloaded file with the hash provided on the website, users can ensure that the file has not been altered, confirming its integrity and authenticity.

upvoted 4 times

🗳️ 👤 **Dlove** 11 months, 2 weeks ago

**Selected Answer: A**

A. Hashes

Since hashes provide a way to verify that a file has not been altered by comparing the hash of the downloaded file with the hash provided by the developer, they are the correct choice.

upvoted 2 times

🗳️ 👤 **Shaman73** 1 year ago

**Selected Answer: A**

A. Hashes

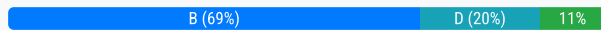
upvoted 3 times

An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?

- A. Tokenization
- B. Hashing
- C. Obfuscation
- D. Segmentation

**Correct Answer: B**

Community vote distribution



**dbrowndiver** Highly Voted 10 months, 4 weeks ago

**Selected Answer: B**

When passwords are hashed, the database stores only the hash values instead of the actual passwords. This means that even if the database is breached, the attackers cannot easily obtain the original passwords.

Hashing is a one-way function, meaning it is computationally infeasible to reverse-engineer the original input from the hash. This ensures that password data is secure even if exposed.

Hashing significantly mitigates the risk of credential theft by ensuring that password data remains protected, making it the most effective choice for securing a log-in database against potential breaches.

Hashing is the correct answer because it effectively limits the impact of a database breach by storing only hashed versions of passwords, thereby protecting sensitive credential information. Hashing ensures that even if the log-in database is compromised, the passwords remain secure and difficult for attackers to reverse-engineer.

upvoted 9 times

**a4e15bd** 10 months, 2 weeks ago

What about other information that is stored in a login database like User IDs or emails, security questions and answer, MFA, account status etc. Hashing isn't going to protect those. The only thing hashing protects in case of a breach is passwords only. This is why it can not be the best choice here. Tokenization is the correct answer.

upvoted 1 times

**test7n1** 1 week, 3 days ago

Simply because the questing is about potential impact to its "log-in database".

That's mean Usernames and Passwords.

upvoted 1 times

**35f7aac** Highly Voted 1 year ago

Why not C? What if they do get the data?

Data obfuscation is the process of disguising confidential or sensitive data to protect it from unauthorized access. Data obfuscation tactics can include masking, encryption, tokenization, and data reduction. Data obfuscation is commonly used to protect sensitive data such as payment information, customer data, and health records.

upvoted 6 times

**jsmthy** 9 months ago

Obfuscation is the generally correct, but when it comes to passwords and log-in information, it is best to store it in a non-reversible method. Therefore, hashing is the best choice out of the options presented.

upvoted 4 times

**9149f41** Most Recent 4 months, 3 weeks ago

**Selected Answer: B**

When a network is breached, segmentation makes other parts of the network safer. However, gaining access to the database by breaking the log-in password will not be of any assistance.

Instead, password hashing makes it more difficult for hackers to crack.

upvoted 1 times

🗋️ 👤 **braveheart22** 5 months ago

**Selected Answer: D**

The correct answer is D. This is because, referencing the CompTIA study guide, Segmentation is a method of securing data by dividing networks, data, and applications into isolated components to improve sensitive data protection, limit the impact of a breach, and improve network security

upvoted 2 times

🗋️ 👤 **Vinceooy** 2 months, 4 weeks ago

The question is trying to say that if the database is already breached. If the attacker is already inside the log-in database how do you limit their potential damage/impact

so the correct answer is B - Hashing so that the attacker couldn't retrieve the actual login credentials, just the random value hashes

upvoted 1 times

🗋️ 👤 **deejay2** 5 months, 3 weeks ago

**Selected Answer: D**

Segmentation. It deals with separating the data, to store in different locations, to make it harder for the attacker during a breach.

upvoted 1 times

🗋️ 👤 **Xezita** 7 months, 1 week ago

A - It talks about limiting the potential impact.

upvoted 1 times

🗋️ 👤 **deejay2** 8 months ago

D is the answer

upvoted 2 times

🗋️ 👤 **Ty13** 9 months ago

**Selected Answer: B**

B. Hashing

Use Tokenization for payments and credit cards - the data needs to be retrievable, so you'd replace the sensitive info (your CC numbers) with a non-sensitive token to act as a dummy. If you use Apple/Android Pay, the CC you save on your phone is tokenized so the actual numbers can't be stolen.

Hashing is for log-in databases and such where you need to secure the info.

upvoted 2 times

🗋️ 👤 **RIDA\_007** 9 months, 1 week ago

The answer is Hashing! The key is Log in and hashing is used for Authentication.

During login, the system combines the entered password with the stored hashes. If the result matches the stored hash, the login is successful

upvoted 1 times

🗋️ 👤 **SpikeyOG** 9 months, 2 weeks ago

**Selected Answer: D**

The correct answer is segmentation. From the CompTIA study guide, Segmentation is a method of securing data by dividing networks, data, and applications into isolated components to improve sensitive data protection, limit the impact of a breach, and improve network security

upvoted 4 times

🗋️ 👤 **nyyankee718** 9 months, 3 weeks ago

**Selected Answer: B**

log-in database is the key in the question, which is related to hashing

upvoted 3 times

🗋️ 👤 **17f9ef0** 10 months ago

**Selected Answer: A**

Answer is A

upvoted 2 times

🗋️ 👤 **a4e15bd** 10 months, 2 weeks ago

A. Tokenization

Here is why: Tokenization replaces sensitive information with token that has no meaningful value outside the tokenization system. The original data is stored securely elsewhere. If the a database with tokenized data is breached, the sensitive information remains protected. Keep in mind, hashing only protects stored passwords which is by converting them into a fixed size string of characters that are irreversible, but what about all the other data that is also stored in a login database like username or emails, security questions and answers, multi factor authentication, account status or

last login information. Hashing is not going to protect all that.

This is why although hashing is a great choice for securing passwords, it is not the best option considering the context of a login database and hence tokenization is the correct answer!

upvoted 3 times

  **mr.sgtan** 11 months ago

**Selected Answer: A**

For "log-in" database, using tokenization to replace sensitive data with non-sensitive placeholder can secure the log-in data information.

upvoted 2 times

  **mr.sgtan** 11 months ago

**Selected Answer: D**

For "log-in" database, using tokenization to replace sensitive data with non-sensitive placeholder can secure the log-in data information.

upvoted 1 times

  **mr.sgtan** 11 months ago

I mean "A. Tokenization". I mis-checked it.

upvoted 1 times

  **Andrewyounan** 11 months, 1 week ago

**Selected Answer: B**

Just for clarification "log-in database" means username and password. Because it took me a minute to process it's not database-SQL

upvoted 2 times

  **Etc\_Shadow28000** 1 year ago

**Selected Answer: B**

B. Hashing

Hashing is the most likely recommendation for protecting a log-in database. By hashing passwords, the organization ensures that even if the database is breached, the actual passwords are not exposed in plaintext. Hashing converts passwords into a fixed-size string of characters, which is not reversible, thus protecting user credentials.

Therefore, the correct answer is:

B. Hashing

upvoted 3 times

An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

- A. Virus
- B. Trojan
- C. Spyware
- D. Ransomware

**Correct Answer:** D

Community vote distribution

D (100%)

MAK0hunter33333333 Highly Voted 1 year, 1 month ago

Selected Answer: D

Files are populating a message, nothing else would except ransomware to let the victim know. Also, .ryk is a file extension for Ransomeware Ryuk upvoted 10 times

dbrowndiver Highly Voted 10 months, 4 weeks ago

Selected Answer: D

Ransomware encrypts files on a victim's system and displays a message demanding payment to decrypt the files or restore access. It often renames files with specific extensions to indicate encryption. File Extension (.ryk): The presence of a .ryk extension on files is indicative of the Ryuk ransomware, which is known to encrypt files and append this extension to indicate they have been affected. Display Message: Ransomware usually displays a message (ransom note) informing victims of the encryption and providing instructions for paying the ransom. The symptoms described (files with a .ryk extension and a ransom message) strongly suggest a ransomware infection, as this pattern matches known ransomware behaviors, especially related to Ryuk. upvoted 7 times

Shaman73 Most Recent 1 year ago

Selected Answer: D

D. Ransomware  
upvoted 2 times



A systems administrator is advised that an external web server is not functioning properly. The administrator reviews the following firewall logs containing traffic going to the web server:

```

Date      |      Time      | SourceIP | SPort | Flag | DestIP | DPort
2023-01-25 01:45:09.102 98.123.45.100 4560 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 95.123.45.101 3361 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 99.123.45.102 3662 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 89.123.45.103 5663 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 98.123.45.104 4064 SYN 100.50.20.7 443
2023-01-25 01:45:09.102 80.123.45.105 4365 SYN 100.50.20.7 443
  
```

Which of the following attacks is likely occurring?

- A. DDoS
- B. Directory traversal
- C. Brute-force
- D. HTTPS downgrade

**Correct Answer: A**

Community vote distribution

A (100%)

 **dbrowndiver** Highly Voted 10 months, 4 weeks ago

**Selected Answer: A**

(100.50.20.7) on port 443. This pattern is typical of a SYN flood DDoS attack, where attackers overwhelm a server with SYN requests to deplete its resources.

Simultaneous Connections: All requests occur simultaneously (01:45:09.102), suggesting a coordinated attack, which is a hallmark of DDoS attacks. DDoS is the correct answer because the logs display multiple SYN requests from different IP addresses to the same server in a short time, indicative of a SYN flood DDoS attack aimed at overwhelming the server and causing disruption.


upvoted 7 times

 **MAKOhunter3333333** Highly Voted 1 year, 1 month ago

**Selected Answer: A**

DDOS via syn attack

upvoted 5 times

 **itone3333** Most Recent 3 weeks, 6 days ago

**Selected Answer: A**

Multiple sources, SYN, one destination IP at the same time..

upvoted 1 times

 **ezmoney** 11 months, 3 weeks ago

all of those SYN messages prove this is a DDos attack.

upvoted 3 times

 **Shaman73** 1 year ago

**Selected Answer: A**

A. DDoS

upvoted 2 times

An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?

- A. Recovery point objective
- B. Mean time between failures
- C. Recovery time objective
- D. Mean time to repair

**Correct Answer:** D

*Community vote distribution*

D (100%)

🗳️ 👤 **dbrowndiver** 10 months, 4 weeks ago

**Selected Answer: D**

Mean Time to Repair (MTTR) is the correct answer because it directly relates to calculating the time needed to resolve hardware issues and restore the server to full functionality. MTTR is a critical metric for understanding and improving maintenance processes, ensuring efficient recovery from hardware failures.

upvoted 4 times

🗳️ 👤 **Shaman73** 1 year ago

**Selected Answer: D**

D. Mean time to repair

upvoted 2 times

A security engineer is installing an IPS to block signature-based attacks in the environment.

Which of the following modes will best accomplish this task?

- A. Monitor
- B. Sensor
- C. Audit
- D. Active

**Correct Answer:** D

Community vote distribution

D (100%)

🗲️ 👤 **a4e15bd** Highly Voted 10 months, 3 weeks ago

D. Active

In active mode, an intrusion prevention system not only monitors network traffic for suspicious activity but also take immediate action to block or mitigate detected threats based on its signatures. This proactive approach ensures that identified threats are automatically blocked or neutralized providing a real-time protection for the environment.

upvoted 6 times

🗲️ 👤 **deejay2** Most Recent 6 months, 3 weeks ago

Selected Answer: D

It's either active or passive. If it's a current attack (real time), which it appears to be, the answer is active.

upvoted 1 times

🗲️ 👤 **45bfb97** 10 months, 3 weeks ago

Selected Answer: D

Active

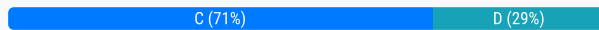
upvoted 1 times

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

- A. XDR
- B. SPF
- C. DLP
- D. DMARC

**Correct Answer:** C

Community vote distribution



🗳️ 👤 **March2023** 9 months, 3 weeks ago

**Selected Answer: C**

C for sure

upvoted 1 times

🗳️ 👤 **Syl0** 9 months, 3 weeks ago

XDR - Extended Detection and Response

SPF - Sender Policy Framework - for Email to identify who can send to the domain

DLP - Data Loss Prevention

DMARC - similar as SPF, helps with email

upvoted 4 times

🗳️ 👤 **Glacier88** 10 months, 1 week ago

**Selected Answer: C**

DLP solutions are specifically designed to identify and prevent the unauthorized movement of sensitive data within and outside an organization. They can monitor data in real-time, detect suspicious activity, and take actions like blocking data transfers or alerting administrators.

upvoted 2 times

🗳️ 👤 **Ina22** 10 months, 2 weeks ago

DLP is the answer

upvoted 2 times

🗳️ 👤 **Justthereforcomptia** 10 months, 3 weeks ago

**Selected Answer: C**

DLP is the right option, it stops data from being exfiltrated from your environment.

upvoted 1 times

🗳️ 👤 **TheDorse** 10 months, 3 weeks ago

**Selected Answer: C**

DLP solutions are specifically designed to monitor, detect, and prevent unauthorized data transfers or leaks outside the organization. DLP can identify sensitive data and enforce policies to prevent it from being exfiltrated, making it the most effective solution for mitigating the risk of data exfiltration.

upvoted 1 times

🗳️ 👤 **RoRoRoYourBoat** 10 months, 3 weeks ago

**Selected Answer: D**

Answer D: EDR is used designed to detect, investigate, and respond to advanced threats to prevent them from spreading across the network.

upvoted 2 times

🗳️ 👤 **Dunbahhh** 10 months, 3 weeks ago

I think you meant to say question 182 is EDR. EDR isn't an option for this question.

upvoted 7 times

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

- A. IDS
- B. ACL
- C. EDR
- D. NAC

**Correct Answer:** C

*Community vote distribution*

C (100%)

🗳️ 👤 **Syl0** 9 months, 3 weeks ago

IDS - Intrusion Detection System

ACL - Access Control List

EDR - Endpoint Detection and Response

NAC - Network Access Control

upvoted 1 times

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: C**

C. EDR (Endpoint Detection and Response) is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network.

EDR solutions provide advanced threat detection, response, and mitigation capabilities for endpoints. They monitor endpoint activities for signs of malicious behavior, provide visibility into threats, and can respond to and contain security incidents.

upvoted 2 times

🗳️ 👤 **Muhammad\_Umair** 10 months, 3 weeks ago

Endpoint Detection and Response (EDR) is an integrated, layered approach to endpoint protection that combines real-time continuous monitoring and endpoint data analytics with rule-based automated response. D

upvoted 4 times

Client files can only be accessed by employees who need to know the information and have specified roles in the company. Which of the following best describes this security concept?

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Non-repudiation

**Correct Answer:** B

*Community vote distribution*

B (100%)

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: B**

B. Confidentiality is the security concept that ensures client files are only accessible to employees who need to know the information and have specified roles in the company. It focuses on protecting information from unauthorized access and ensuring that only those with proper authorization can view or handle the data.

upvoted 2 times

🗳️ 👤 **RoRoRoYourBoat** 10 months, 3 weeks ago

**Selected Answer: B**

Confidentiality. This security concept ensures that sensitive information is only accessible to those who are authorized and have a legitimate need to know.

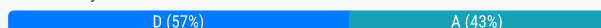
upvoted 4 times

Which of the following describes the category of data that is most impacted when it is lost?

- A. Confidential
- B. Public
- C. Private
- D. Critical

**Correct Answer:** D

Community vote distribution



**laternak26** Highly Voted 6 months, 2 weeks ago

**Selected Answer:** A

A. Confidential:

Confidential data refers to information that is intended to be kept private within an organization or a specific group of individuals. Losing confidential data can have serious consequences, including reputational damage, financial losses, legal penalties, and regulatory violations. This is because confidential data often includes sensitive business information, trade secrets, personal identifiable information (PII), and other critical elements that could cause significant harm if exposed or lost.

Why not D. Critical:

Critical data refers to information necessary for the operation of a business or system. While critical data loss can be very disruptive, "confidential" is typically the term used for the most sensitive information, making it the category most directly impacted when lost.

upvoted 8 times

**Linus312** 2 months, 3 weeks ago

its D, the question is what data is most impacted , I suppose they mean impactful which is definitely Critical

upvoted 1 times

**jbmac** Highly Voted 6 months ago

**Selected Answer:** D

D. Critical

Explanation:

Critical data is the category of data that is most impacted when it is lost because it is essential to the organization's operations, mission, or business continuity. Loss of critical data can lead to:

Severe disruptions in business processes.

Financial loss.

Regulatory non-compliance.

Irreparable damage to the organization's reputation.

Other Options:

A. Confidential: Refers to data that must be protected from unauthorized access, but its loss may not always disrupt critical operations.

B. Public: Refers to information intended to be openly shared, so its loss typically has little to no impact.

C. Private: Refers to sensitive personal information (e.g., PII), where its loss could result in privacy violations but may not always have operational impact.

Thus, critical data is the most impacted when lost, as it is essential for the organization's core functions.

upvoted 7 times

**8f23125** Most Recent 2 months ago

**Selected Answer:** A

Confidential data: Loss results in severe legal, financial, and reputational consequences.

Critical data: Loss may disrupt operations, but the focus is on functionality rather than privacy or legal violations.

upvoted 1 times

**b0cfac** 4 months, 1 week ago

**Selected Answer: D**

Comptia sec+ exam tip "The difference between critical and confidential is the level of damage"

Took me a while to confirm this in the comptia sec books under: privacy- data types - classifications.

upvoted 4 times

  **TmNvrWts** 4 months, 2 weeks ago

**Selected Answer: D**

Why not the others?

A. Confidential – Sensitive but not necessarily the most impactful if lost; unauthorized access is the bigger concern.

B. Public – Already accessible by anyone, so its loss has minimal impact.

C. Private – Personal or sensitive data, but its loss typically affects individuals more than organizations.

upvoted 2 times

  **Rackup** 5 months ago

**Selected Answer: A**

Answer: A. Confidential

Explanation: Confidential data is the most impacted when it is lost because it often includes sensitive information such as trade secrets, financial records, personal identifiable information (PII), and other data that can cause significant harm to the organization or individuals if exposed. Loss of this data can lead to legal penalties, reputational damage, and financial losses. While private and critical data can also be important, confidential data specifically refers to information that requires strict access control and protection. Public data is typically less sensitive and less impactful if lost.

upvoted 1 times

  **agp2684** 5 months ago

**Selected Answer: A**

That's a tricky question, . It should be classified confidential. According to the CompTIA material, the data classifications are: public, sensitive, private, and confidential. Critical is not mentioned.

upvoted 2 times

  **ITExperts** 5 months, 1 week ago

**Selected Answer: D**

crazy! it is critical

upvoted 3 times

  **Cocopqr** 6 months, 3 weeks ago

**Selected Answer: A**

Confidential data refers to sensitive information that, if lost or exposed, could result in significant harm to individuals or organizations. This could include personal data, financial information, trade secrets, or any data that requires protection due to its sensitive nature.

upvoted 2 times

  **3b1fd98** 6 months, 4 weeks ago

**Selected Answer: A**

A. Confidential

Explanation:

Confidential data refers to sensitive information that, if lost or exposed, could result in significant harm to individuals or organizations. This could include personal data, financial information, trade secrets, or any data that requires protection due to its sensitive nature.

Why not Critical?

Critical data refers to data that is essential to the functioning of a system or business. While critical data loss is highly impactful, it is not necessarily classified by its sensitivity, which is why confidential data is often seen as more directly impactful when lost.

upvoted 2 times

  **baronvon** 10 months, 1 week ago

**Selected Answer: D**

D. Critical data is the category most impacted when it is lost. Critical data is essential for the core operations of an organization, and its loss can lead to significant operational disruptions, financial losses, or damage to the organization's reputation.

upvoted 4 times

  **nesquick0** 10 months, 3 weeks ago

**Selected Answer: D**

D. Critical, because critical data must be always available.



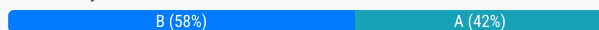
upvoted 3 times

A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?

- A. Business email
- B. Social engineering
- C. Unsecured network
- D. Default credentials

**Correct Answer:** B

Community vote distribution



**c80f5c5** Highly Voted 10 months, 3 weeks ago

**Selected Answer:** A

Business email compromise (BEC) is an email-based social engineering attack

Social engineering refers to all the techniques used to coerce or talk a victim into revealing information that someone can use to perform malicious activities and render an organization or individual vulnerable to further attacks

Answer: A- Business email  
upvoted 17 times

**Twphill** Highly Voted 9 months, 3 weeks ago

**Selected Answer:** B

Social engineering is an attack vector, while Business email is an attack surface. If it said Business Email Compromise, that would be an attack vector.

upvoted 12 times

**Kekeee** Most Recent 5 days, 17 hours ago

**Selected Answer:** B

the only reason it wouldnt be A is that A doesnt have the full BEC to it. C is still a Vector. Think of Surfaces like categories or neighborhoods and Vectors as pathways or streets. Humans are a Surface and Social engineering is a Vector

upvoted 1 times

**Zeez3377** 2 months, 1 week ago

**Selected Answer:** B

I originally thought A. Business Email, but after some research I switched to B. Social Engineering

According to CloudFlare "Business email compromise (BEC) is a type of social engineering attack that takes place over email. In a BEC attack, an attacker falsifies an email message to trick the victim into performing some action – most often, transferring money to an account or location the attacker controls. BEC attacks differ from other types of email-based attacks in a couple of key areas:

They do not contain malware, malicious links, or email attachments

They target specific individuals within organizations

They are personalized to the intended victim and often involve advance research of the organization in question"

This email includes a bad link so I dont think it can be Business Email  
upvoted 3 times

**Linas312** 2 months, 3 weeks ago

**Selected Answer:** B

Typical bad wording.. IF its a hr compromised account then could be A? but even a is it BEC they are referring to? vague for no reason, they can really blindly pick either A or B and decide which they will accept..

upvoted 3 times

**WifiWan** 3 months, 2 weeks ago

Selected Answer: A

biz email

upvoted 1 times

🗨️ 👤 **mejestique** 3 months, 3 weeks ago

Selected Answer: B

The correct answer is:

B. Social engineering

Explanation:

This scenario describes a phishing attack, a type of social engineering where an attacker sends fraudulent emails pretending to be from a trusted source (in this case, human resources). The mismatched links suggest an attempt to deceive the employee into clicking a malicious link, possibly leading to credential theft or malware installation.

Other options explained:

A. Business email – Likely refers to Business Email Compromise (BEC), which involves targeted attacks on executives or finance personnel rather than generic phishing.

C. Unsecured network – There is no indication that the employee is on an insecure network; the issue is the deceptive email content.

D. Default credentials – This applies to systems left with manufacturer-set passwords, which is unrelated to phishing emails.

Since the attacker is attempting to manipulate human behavior to gain access, this is a social engineering attack.

upvoted 1 times

🗨️ 👤 **TmNvrWts** 4 months, 2 weeks ago

Selected Answer: B

Why not the others?

A. Business email (compromise) – This involves an attacker gaining control of a legitimate business email account, but in this case, the email appears to be a fake rather than a compromised real account.

C. Unsecured network – An unsecured network could allow data interception, but it wouldn't cause misleading links in an email.

D. Default credentials – This refers to using factory-set usernames and passwords, which is unrelated to this phishing attempt.

upvoted 1 times

🗨️ 👤 **pindinga1** 5 months, 2 weeks ago

Selected Answer: A

Business email compromise (BEC) is an email-based social engineering attack

upvoted 2 times

🗨️ 👤 **esko636** 5 months, 2 weeks ago

Selected Answer: B

This is a social engineering attack done through phishing. Phishing typically involves sending mass emails to a large number of recipients, aiming to trick them into clicking on malicious links or providing sensitive information. The email in this scenario seems to fit this pattern, as it contains suspicious links that do not correspond to the company's legitimate links. Business Email Compromise (BEC), on the other hand, is more targeted. It often involves attackers gaining access to a legitimate business email account and using it to send fraudulent emails to specific individuals within the organization. These emails usually request actions like transferring funds or sharing confidential information. BEC attacks are generally more sophisticated and personalized compared to phishing.

upvoted 1 times

🗨️ 👤 **Damique** 6 months, 2 weeks ago

Selected Answer: B

It is not business email because this term refers to emails sent using an organization's domain and infrastructure, not necessarily indicative of an attack.

upvoted 1 times

🗨️ 👤 **BevMe** 7 months, 2 weeks ago

Selected Answer: B

Social Engineering is right.

upvoted 1 times

🗨️ 👤 **3dk1** 7 months, 3 weeks ago

Selected Answer: A

This lines up with A

upvoted 1 times

🗨️ 👤 **PAWarriors** 9 months, 3 weeks ago

**Selected Answer: A**

The correct answer is A.

> This is an example of Business Email Compromise (BEC). BEC is a type of phishing attack that usually targets businesses by using one of their internal email accounts to get other employees to perform some kind of malicious actions on behalf of the attacker.

In this scenario the email came from human resources, indicating that this is a BEC.

upvoted 4 times

🗨️ 👤 **Ambaj** 10 months ago

**Selected Answer: B**

B. Social engineering

upvoted 3 times

🗨️ 👤 **ofolan** 10 months ago

**Selected Answer: B**

B. Social engineering

Social engineering involves manipulating individuals into divulging confidential information or performing actions that compromise security. In this case, the email containing suspicious links is an example of a phishing attempt, where attackers try to deceive the employee into clicking on malicious links that may lead to fraudulent sites or compromise their credentials.

upvoted 5 times

🗨️ 👤 **17f9ef0** 10 months ago

**Selected Answer: B**

Answer is B

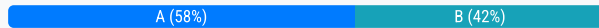
upvoted 2 times

Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

- A. SLA
- B. MOU
- C. MOA
- D. BPA

**Correct Answer: A**

Community vote distribution



**Twphill** Highly Voted 9 months, 3 weeks ago

MOU because it "describes the understanding". The question doesn't really ask for a formal document about expected levels of service.  
upvoted 12 times

**Imant14\_111** Most Recent 2 weeks, 2 days ago

**Selected Answer: A**

A Service Level Agreement (SLA) is a formal document between a service provider and a client that defines the expected level of service, including what resources will be provided and the agreed-upon time frames. It typically includes metrics to evaluate performance, uptime guarantees, and response times.

MOU (Memorandum of Understanding) and MOA (Memorandum of Agreement) are less formal and may not specify the exact level of service.

BPA (Business Partners Agreement) focuses more on the long-term relationship between partners.  
upvoted 1 times

**1chung** 4 weeks, 1 day ago

**Selected Answer: A**

I go with A  
upvoted 1 times

**aaebd57** 1 month, 3 weeks ago

**Selected Answer: A**

Even though the question uses the word "understanding," the details of that understanding are what point to the correct answer:

"what will be provided" (Scope of Service -> SLA)

"the accepted time needed" (Performance Metrics, Timelines -> SLA)

"accepted time needed to provide the company with the resources [by the client]" (Client Obligations/Responsibilities -> SLA)

upvoted 2 times

**Zeez3377** 2 months, 1 week ago

**Selected Answer: A**

At first I thought MOU, but I think the keyword is "ACCEPTED TIME" an MOU isn't an agreed upon document, but SLA is.  
upvoted 3 times

**prabh1251** 3 months, 3 weeks ago

**Selected Answer: A**

SLA (Service Level Agreement)

Defines services, performance expectations, and timelines.

Clearly outlines what will be provided and the timeframe (which matches the question).

Typically used in business and IT services to ensure service commitments are met.

MOU (Memorandum of Understanding)

A general agreement that expresses intent between two parties.

Does NOT specify detailed service expectations or timelines.  
Often used for partnerships or informal agreements rather than service delivery  
upvoted 3 times

🗨️ 👤 **prabh1251** 3 months, 2 weeks ago  
its b MOU because it "describes the understanding".  
upvoted 1 times

🗨️ 👤 **mejestique** 3 months, 3 weeks ago

**Selected Answer: A**

The correct answer is:

A. SLA (Service Level Agreement)

Explanation:

A Service Level Agreement (SLA) is a formal contract between a service provider and a client that defines the expected level of service, including:

What will be provided (e.g., services, resources)

Performance metrics (e.g., uptime, response time)

Timeframes for delivery

Responsibilities of both parties

SLAs are commonly used in IT services, cloud computing, and outsourcing agreements to ensure that services are delivered as expected.

upvoted 3 times

🗨️ 👤 **SimDecker** 4 months ago

**Selected Answer: B**

Describes understanding between 2 parties

upvoted 2 times

🗨️ 👤 **test\_arrow** 4 months, 2 weeks ago

**Selected Answer: B**

this should be B

An MOU (Memorandum of Understanding) is a formal agreement between two or more parties that outlines the mutual understanding and expectations, including what will be provided and the time required for resources. It is often used to establish the terms of cooperation before a more detailed contract is signed.

upvoted 2 times

🗨️ 👤 **kambam** 6 months, 4 weeks ago

**Selected Answer: B**

Answer is B:

Question is saying what will be provided and how much time it will take to get the resources needed. SLA refers to metrics that have been agreed upon. This states nothing about metrics being met or not met.

upvoted 4 times

🗨️ 👤 **Bkstballchic** 7 months, 3 weeks ago

B. It's asking for an understanding, not an agreement. I originally thought A, but im pretty certain it's B.

upvoted 2 times

🗨️ 👤 **famuza77** 8 months, 2 weeks ago

I would say its SLA

upvoted 1 times

🗨️ 👤 **Syl0** 9 months, 4 weeks ago

MOU - Memorandum of Understanding

MOA - Memorandum of Agreement

SLA - Service Level Agreement

BPA - Business Partner Agreement

upvoted 2 times

🗨️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: A**

A. SLA (Service Level Agreement)

An SLA is a formal document that outlines the expected level of service between a company and a client. It specifies the agreed-upon performance metrics, such as response times, service availability, and other key aspects of service delivery, including the time needed to provide resources and meet service expectations.

upvoted 2 times

  **RoRoRoYourBoat** 10 months, 3 weeks ago

**Selected Answer: A**

A. SLA (Service Level Agreement). An SLA is a formal agreement between a service provider and a client that outlines the specific services to be provided, the expected level of service, and the time frame for delivery

upvoted 2 times

A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations. Which of the following is the best type of site for this company?

- A. Cold
- B. Tertiary
- C. Warm
- D. Hot

**Correct Answer:** D

Community vote distribution

D (100%)

🗲️ 👤 **rbidev** 2 months, 2 weeks ago

**Selected Answer:** D

D is the answer but the wording is misleading here because, after they mentioned hurricanes, I initially thought they were asking about what climate to geolocate the new center.

upvoted 1 times

🗲️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer:** D

D. Hot

A hot site is a fully operational backup facility that mirrors the company's primary site and is ready to take over operations immediately in the event of a disaster. It includes all necessary hardware, software, and network configurations, allowing the company to quickly resume normal business activities with minimal downtime.

upvoted 2 times

🗲️ 👤 **Rj99** 10 months, 2 weeks ago

D. Hot is the answer

upvoted 2 times

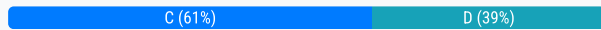


Which of the following security controls is most likely being used when a critical legacy server is segmented into a private network?

- A. Deterrent
- B. Corrective
- C. Compensating
- D. Preventive

**Correct Answer:** C

Community vote distribution



**RoRoRoYourBoat** Highly Voted 10 months, 3 weeks ago

**Selected Answer:** C

C, compensating.  
upvoted 8 times

**1chung** Most Recent 4 weeks, 1 day ago

**Selected Answer:** C

I go with C  
upvoted 1 times

**Burnboy** 2 months, 1 week ago

**Selected Answer:** C

C. Compensating  
upvoted 1 times

**EngAbood** 4 months, 1 week ago

**Selected Answer:** D

Chatgpt said D. Preventive : ( , and when ever i see legacy i chose compensating :(  
upvoted 2 times

**fc040c7** 5 months ago

**Selected Answer:** C

there have been multiple questions with legacy items being compensated for with segmentation. this is no different. I am going with C.  
upvoted 3 times

**esko636** 5 months, 2 weeks ago

**Selected Answer:** C

Compensating controls provide alternative measures to mitigate risk when the primary control is not feasible. If the legacy server cannot be patched or upgraded, segmenting it into a private network acts as a compensating control by restricting access and reducing the risk posed by its vulnerabilities.  
upvoted 1 times

**d06e2b4** 6 months, 3 weeks ago

**Selected Answer:** C

Segmentation of a critical legacy server into a private network is a compensating control because it addresses security risks when the legacy system cannot be updated or secured using standard measures, like patches or modern preventive controls.  
upvoted 4 times

**5787808** 6 months, 4 weeks ago

**Selected Answer:** D

D. Preventive  
upvoted 2 times

**viktorrdlyi** 7 months ago

**Selected Answer:** D

Preventive because we aint compensating anything!! Nothing mentioned in the question to compensate!  
upvoted 3 times

fc040c7 5 months ago

wouldn't "segmenting into a private network" to be further used by the compensation control as opposed to taking the legacy software off service  
upvoted 2 times

fmeox567 7 months ago

**Selected Answer: D**

D. Preventive

Preventive controls are designed to stop or mitigate unwanted actions or events before they happen. By segmenting a critical legacy server into a private network, the organization is aiming to prevent unauthorized access and potential threats, thus isolating the server from the broader network and reducing the risk of compromise.

upvoted 1 times

famuza77 8 months, 2 weeks ago

C, Compensating

upvoted 1 times

BluezClues 9 months ago

**Selected Answer: C**

The correct answer is C. Compensating.

When a critical legacy server is segmented into a private network, the security control being used is likely **compensating**. This is because the legacy server may not support modern security features, and network segmentation is implemented as a workaround to mitigate risks and protect it from external threats. A compensating control is used to achieve a level of security equivalent to the one required when it is not possible to implement the primary control.

The other options:

- A. Deterrent is designed to discourage malicious actions, such as warning signs or legal warnings.
- B. Corrective is aimed at fixing issues after an incident has occurred.
- D. Preventive is used to stop attacks from happening in the first place, but in this case, segmentation is compensating for the server's inherent vulnerabilities.

Thus, network segmentation is a "compensating" control.

upvoted 1 times

goku5786 9 months ago

**Selected Answer: D**

D. Preventive

upvoted 1 times

nillie 9 months ago

**Selected Answer: C**

The most likely security control being used when a critical legacy server is segmented into a private network is:

C. Compensating

A compensating control is implemented when the primary control (such as patching or updating a legacy server) is not feasible. Segmenting the legacy server into a private network is a compensating control because it mitigates risk by limiting the server's exposure without requiring changes to the server itself, which might not be possible due to its legacy status.

upvoted 2 times

a0bfa81 9 months ago

**Selected Answer: D**

Segmenting a critical legacy server into a private network is a preventive security control. It helps to protect the server from unauthorized access and potential attacks by isolating it from the rest of the network, thereby reducing the risk of security breaches. Preventive controls are designed to stop security incidents before they occur.



upvoted 1 times

jsmthy 9 months ago

**Selected Answer: C**

compensating, because the best preventative action is to remove the server altogether. You are mitigating the risk by segmenting a vulnerable legacy server.

upvoted 1 times

  **chasingsummer** 9 months, 2 weeks ago

**Selected Answer: D**

D. Preventive

upvoted 1 times

Which of the following best describes the practice of researching laws and regulations related to information security operations within a specific industry?

- A. Compliance reporting
- B. GDPR
- C. Due diligence
- D. Attestation

**Correct Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **9149f41** 4 months, 3 weeks ago

**Selected Answer:** C

Due diligence refers to conducting a thorough investigation and appropriate response to a situation  
upvoted 2 times

🗳️ 👤 **nillie** 9 months ago

**Selected Answer:** C

The best term to describe the practice of researching laws and regulations related to information security operations within a specific industry is:

C. Due diligence

Due diligence refers to the process of thoroughly investigating and ensuring that an organization's practices, especially in information security, comply with applicable laws, regulations, and industry standards. It involves identifying and understanding the legal requirements to avoid risks and ensure proper adherence to security policies.  
upvoted 1 times

🗳️ 👤 **Kingamj** 10 months, 2 weeks ago

**Selected Answer:** C

C. Due diligence.

Due diligence in the context of information security operations involves researching and understanding the laws, regulations, and standards that apply to a specific industry to ensure compliance and manage risks effectively. It's a key practice for identifying and addressing legal and regulatory requirements related to information security.  
upvoted 1 times

Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?

- A. Reporting structure for the data privacy officer
- B. Request process for data subject access
- C. Role as controller or processor
- D. Physical location of the company

**Correct Answer:** C

Community vote distribution

C (83%)

B (17%)

🗳️ 👤 **Murtuza** Highly Voted 8 months, 2 weeks ago

**Selected Answer: C**

Between the two options, C. Role as controller or processor remains the most important consideration. This distinction fundamentally shapes the organization's responsibilities and compliance requirements under data protection laws.

However, the request process for data subject access is also crucial, as it directly impacts how the organization responds to individuals' rights regarding their personal data. Both aspects are important, but understanding the role as a controller or processor is foundational.

upvoted 6 times

🗳️ 👤 **User92** Most Recent 8 months, 3 weeks ago

**Selected Answer: C**

Role as controller or processor is crucial because it fundamentally shapes the organization's responsibilities and obligations under data protection laws like the GDPR.

upvoted 2 times

🗳️ 👤 **nillie** 9 months ago

**Selected Answer: C**

The most important consideration for an organization to evaluate as it establishes and maintains a data privacy program is:

C. Role as controller or processor

Understanding whether the organization is acting as a data controller or a data processor is crucial because it determines the organization's responsibilities under various data privacy regulations, such as the GDPR. Controllers are responsible for deciding how and why personal data is processed, while processors handle data on behalf of controllers. Each role has different obligations regarding data protection, subject access requests, and overall compliance.

upvoted 2 times

🗳️ 👤 **Glacier88** 10 months, 1 week ago

**Selected Answer: C**

Controller or processor: This is a fundamental distinction in data protection law. Controllers are responsible for determining the purposes and means of processing personal data, while processors process data on behalf of controllers. The organization's role as a controller or processor will significantly impact its data privacy obligations and responsibilities.

Reporting structure for the data privacy officer: While this is important, it's not as crucial as understanding the organization's role as a controller or processor. The reporting structure can be adjusted as needed, but the fundamental legal obligations will remain the same.

Request process for data subject access: This is a critical aspect of data privacy compliance, but it should be established based on the organization's role as a controller or processor and the applicable laws and regulations.

Physical location of the company: While geographic location can be relevant, it's not the most important factor. The organization's role as a controller or processor and the applicable laws and regulations will have a greater impact on its data privacy obligations.



upvoted 2 times

🗳️ 👤 **Yoming** 10 months, 2 weeks ago

**Selected Answer: B**

B. This answer is at the heart of the matter. What is an approved, secure process for accessing data. All other answers are secondary or irrelevant

upvoted 1 times

  **nesquick0** 10 months, 3 weeks ago

**Selected Answer: B**

B. Request Process for data access

upvoted 1 times

  **a4e15bd** 10 months, 3 weeks ago

B. Request process for data subject access.

This is one of the most important considerations because it involves how individuals can access, correct or delete their personal data as required by data protection regulations such as GDPR.

upvoted 4 times

A security analyst is investigating a workstation that is suspected of outbound communication to a command-and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted. Which of the following logs would the analyst most likely look at next?

- A. IPS
- B. Firewall
- C. ACL
- D. Windows security

**Correct Answer:** B

Community vote distribution

B (100%)

Kingamj Highly Voted 10 months, 2 weeks ago

**Selected Answer: B**

Since the logs on the endpoint were deleted, the security analyst would likely turn to firewall logs. Firewall logs can provide information about network traffic, including outbound connections that may indicate communication with a command-and-control server. These logs can help the analyst identify suspicious traffic patterns or unauthorized communication that bypassed endpoint defenses.

upvoted 5 times

Glacier88 Most Recent 10 months, 1 week ago

**Selected Answer: B**

While the endpoint logs themselves are deleted, the firewall logs might still provide valuable information. Firewalls typically record network traffic, including outbound connections, which could help the analyst identify the destination of the suspicious communication. By examining the firewall logs, the analyst might be able to determine the IP address of the command-and-control server and gather other relevant information about the incident.

upvoted 1 times

1edea48 10 months, 3 weeks ago

This isn't correct. The answer has to be C. In the question, it specifically states that the logs on the endpoint were deleted. That tells me that someone had access to those logs, which means there might have very well been tampering on the endpoint. The ACL has the ability to show us who was able to access those logs and when they were deleted.

upvoted 2 times

850bc48 9 months, 2 weeks ago

I agree with this, if there's an issue at the endpoint, why wouldn't I check the access logs associated.

upvoted 1 times

3dk1 8 months ago

To add onto this, what am I going to see in the ACL? A compromised user? At least the firewall will give us information about the command-and-control servers traffic and attack vector.

upvoted 2 times

a4e15bd 10 months, 3 weeks ago

B. Firewall

upvoted 1 times

An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident. Which of the following plans is the IT manager creating?

- A. Business continuity
- B. Physical security
- C. Change management
- D. Disaster recovery

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗳️ 👤 **a0bfa81** 9 months ago

**Selected Answer: A**

A business continuity plan describes how an organization will maintain its operations and continue functioning in the event of a significant disruption or global incident. It covers strategies for ensuring that critical business functions remain operational despite various types of emergencies or disasters. therefore the answer is A.

upvoted 2 times

🗳️ 👤 **Yoming** 10 months, 2 weeks ago

**Selected Answer: A**

This comprehensive document analyzes risks to business operations. The BCP considers the impact, recovery and mitigation options from a natural disaster.

upvoted 1 times



A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the best option?

- A. Hot
- B. Cold
- C. Warm
- D. Geographically dispersed

**Correct Answer:** C

*Community vote distribution*

C (100%)

🗨️ 👤 **a4e15bd** 10 months, 2 weeks ago

**Selected Answer: C**

c. warm

upvoted 1 times

🗨️ 👤 **Yoming** 10 months, 2 weeks ago

**Selected Answer: C**

A warm site serves as a compromise between an immediate failover resource and an empty shell that must be built

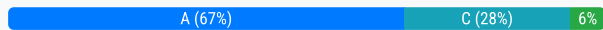
upvoted 3 times

A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?

- A. Virtualization and isolation of resources
- B. Network segmentation
- C. Data encryption
- D. Strong authentication policies

**Correct Answer:** A

Community vote distribution



**nillie** Highly Voted 9 months ago

**Selected Answer: A**

The security team should ensure that all of the following are in place, but the most comprehensive answer that addresses cloud-based services is:

A. Virtualization and isolation of resources

In a cloud-based environment, virtualization and isolation of resources are critical to maintaining security best practices. Virtualization allows multiple workloads to run on the same physical infrastructure while keeping them isolated from each other, which is a foundational practice in cloud environments to prevent data leakage or unauthorized access between different tenants or applications.

upvoted 7 times

**585402e** Most Recent 4 months, 2 weeks ago

**Selected Answer: C**

Since it is in the Cloud and theoretically can be compromised at some point, in my opinion, the first thing that needs to be ensured is the confidentiality of the data. Therefore, the data should always be encrypted.

upvoted 1 times

**fd91c58** 4 months, 3 weeks ago

**Selected Answer: C**

The best answer is C. Data encryption. Here's why:

Virtualization and isolation of resources: While important for resource management and security, it doesn't directly address the protection of data in transit or at rest.

Network segmentation: This helps in limiting the spread of potential breaches but doesn't directly protect the data itself.

Data encryption: This is crucial for protecting data both in transit and at rest, ensuring that even if data is intercepted or accessed without authorization, it remains unreadable.

Strong authentication policies: These are essential for controlling access to the cloud environment but don't directly protect the data once it is accessed.

this makes sense to me data encryption is the basic level of security best practices.

upvoted 1 times

**Glacier88** 10 months, 1 week ago

**Selected Answer: A**

Virtualization and isolation of resources: This ensures that each application or tenant within the cloud environment is running in its own isolated virtual environment, preventing unauthorized access or interference from other users.

Network segmentation: While network segmentation is a valuable security measure, it's not as directly related to the security of the on-premises software application itself. It's more about protecting the overall network infrastructure.

Data encryption: Data encryption is crucial for protecting sensitive data both at rest and in transit, but it's not the primary concern for ensuring a secure cloud-based environment.

Strong authentication policies: Strong authentication policies are essential for controlling access to the cloud environment, but they don't address the isolation and protection of resources within that environment.

upvoted 2 times

🗨️ 👤 **Yoming** 10 months, 2 weeks ago

**Selected Answer: B**

Network segmentation would provide a barrier between the hosting software and internal company resources

upvoted 1 times

🗨️ 👤 **RobJob** 9 months, 1 week ago

I'm not sure how network segmentation can be applicable when it is a cloud environment.

upvoted 4 times

🗨️ 👤 **EfaChux** 10 months, 2 weeks ago

**Selected Answer: C**

Setting up a private cloud means your data will be traveling over the internet, encryption seems like a best practice to me when compared to virtualization and isolation which could already be in place for the on-premise architecture

upvoted 3 times

🗨️ 👤 **Crucible\_Bro** 10 months, 3 weeks ago

**Selected Answer: A**

I'm not overly smart about this type of thing, but I \*feel\* like this is one of those trick questions. In order to get any sort of cloud services up you'll need virtualization. The isolation of resources may be part of the security aspect but I am not entirely sure. D is probably a stronger answer but I don't necessarily disagree with A.

upvoted 4 times

🗨️ 👤 **a4e15bd** 10 months, 3 weeks ago

D. Strong authentication policies. Ensuring a strong user authentication is crucial to prevent unauthorized access to the cloud environment. This forms the first line of defense in securing the system.

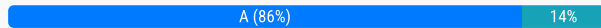
upvoted 3 times

A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link. Which of the following security practices helped the manager to identify the attack?

- A. End user training
- B. Policy review
- C. URL scanning
- D. Plain text email

**Correct Answer:** A

Community vote distribution



🗳️ 👤 **chalaka** 7 months, 1 week ago

**Selected Answer:** A

A. End user training

Explanation:

The manager identified the suspicious link by recognizing a discrepancy in the domain's URL. This ability likely comes from end-user training on phishing and other cybersecurity threats. Such training teaches employees to carefully examine links, avoid clicking on unknown or suspicious URLs, and recognize common red flags of phishing attacks.

upvoted 3 times

🗳️ 👤 **3dk1** 8 months ago

**Selected Answer:** A

A, User training

upvoted 1 times

🗳️ 👤 **Murtuza** 8 months, 2 weeks ago

**Selected Answer:** A

The correct answer is A. End user training.

End user training helps employees recognize phishing attempts and other security threats by teaching them to look for signs such as suspicious URLs. This training empowers users to identify and avoid potential security risks effectively

upvoted 1 times

🗳️ 👤 **nillie** 9 months ago

**Selected Answer:** A

The security practice that helped the manager identify the attack is:

A. End user training

End user training teaches employees how to recognize phishing attempts and other malicious activities. In this case, the manager's awareness of hovering over links to check for suspicious URLs before clicking is a direct result of effective security awareness training. This is a key aspect of preventing social engineering attacks, like phishing.

upvoted 2 times

🗳️ 👤 **jsmthy** 9 months ago

**Selected Answer:** C

The manager is scanning a URL. End-user training may make the practice of checking URLs more prevalent, but it is not the security practice being demonstrated.

upvoted 1 times

🗳️ 👤 **ChillingSpree** 9 months ago

URL Scanning is something you'd typically set up with a NGFW. It is a technology and not something a human does in the context of this subject.

upvoted 5 times

  **rabid\_adobo** 10 months ago

A. GPT

upvoted 1 times

  **Ina22** 10 months, 3 weeks ago

A. End user training

upvoted 2 times

A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

- A. Validate the code signature.
- B. Execute the code in a sandbox.
- C. Search the executable for ASCII strings.
- D. Generate a hash of the files.

**Correct Answer:** A

Community vote distribution

A (100%)

🗲️ 👤 **a4e15bd** Highly Voted 👍 10 months, 3 weeks ago

A. Validate the code signature

Code signing is a process where the software vendor signs the executable code with a digital certificate. This certificate verifies the identity of the software vendor and ensures that the code has not been altered with since it was signed. By validating the code signature, the company can confirm the authenticity and integrity of the software.

upvoted 9 times

🗲️ 👤 **ProudFather** Most Recent 🕒 6 months, 3 weeks ago

Selected Answer: A

A code signature is a digital signature that verifies the authenticity and integrity of software. By validating the code signature, the company can confirm that the software came from the intended vendor and has not been tampered with.

upvoted 1 times

🗲️ 👤 **nillie** 9 months ago

Selected Answer: A

The best way for the company to confirm that the software came from the vendor is:

A. Validate the code signature.

Code signing uses digital signatures to confirm the identity of the software publisher and ensure that the code has not been altered since it was signed. By validating the code signature, the company can verify that the software is authentic and comes from the trusted vendor.

upvoted 3 times

A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which of the following techniques would increase enterprise security?

- A. Installing HIDS on the system
- B. Placing the system in an isolated VLAN
- C. Decommissioning the system
- D. Encrypting the system's hard drive

**Correct Answer:** B

Community vote distribution

B (61%)

C (39%)

🗳️ **a4e15bd** Highly Voted 10 months, 3 weeks ago

B. Placing the system in an isolated VLAN

Give that the system is critical for processing customer transactions, decommissioning immediately might impact business continuity. The next best approach is to place the system in an isolated VLAN.

upvoted 15 times

🗳️ **Migzz** Highly Voted 10 months, 3 weeks ago

Why would you "Decommission the system" when it is critical for transitions? The answer is B, Isolate it until you're ready to make the relevant changes or ready to replace it.

upvoted 9 times

🗳️ **ProudFather** Most Recent 6 months, 3 weeks ago

Selected Answer: C

C. Decommissioning the system

The most secure option is to decommission the system entirely. End-of-life systems are no longer supported by the vendor, meaning they will not receive security patches. This makes them highly vulnerable to attacks. By decommissioning the system, the organization can eliminate the risk associated with it.

While the other options may provide some level of security, they do not address the fundamental issue of the system being end-of-life.

upvoted 2 times

🗳️ **nyyankee718** 7 months, 3 weeks ago

Selected Answer: C

Yes it is critical so it should be replaced soon, VLAN can be short term

upvoted 3 times

🗳️ **nillie** 9 months ago

Selected Answer: B

The best technique to increase enterprise security in this situation is:

B. Placing the system in an isolated VLAN

By placing the system in an isolated VLAN, the organization can reduce the risk of the outdated system being exploited by limiting its network exposure and controlling access to and from the critical system. This helps to minimize the impact that vulnerabilities in the end-of-life operating system could have on the broader network.

upvoted 2 times

🗳️ **Glacier88** 10 months, 1 week ago

Selected Answer: B

Placing the system in an isolated VLAN: This will physically separate the critical system from the rest of the network, reducing the risk of unauthorized access or attacks.

Installing HIDS on the system: While an HIDS can detect and alert on suspicious activity, it might not be enough to mitigate the risks associated with an end-of-life operating system, which lacks security updates and patches.

Decommissioning the system: This is a potential solution if the system can be replaced with a more secure alternative. However, if the system is critical for business operations, decommissioning it might not be feasible.

Encrypting the system's hard drive: Encryption can protect the data stored on the system, but it doesn't address the security vulnerabilities associated with an end-of-life operating system.



upvoted 1 times

  **Dharmesh16** 10 months, 3 weeks ago

**Selected Answer: B**

techniques would increase "enterprise" security. you can use system but system can't connect with other devices on network

upvoted 8 times

  **qacollin** 10 months, 3 weeks ago

**Selected Answer: C**

Yes, decommissioning the system is generally the most effective approach for addressing the security risks associated with running an end-of-life operating system.

GPT

upvoted 2 times

  **Justthereforcomptia** 10 months, 3 weeks ago

You cannot do this as it's business critical

upvoted 6 times



The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators. Which of the following should the CISO use?

- A. Penetration test
- B. Internal audit
- C. Attestation
- D. External examination

**Correct Answer:** B

Community vote distribution



01a4c2e Highly Voted 8 months, 2 weeks ago

Selected Answer: B

Ty13 2 weeks, 2 days ago

Selected Answer: B

B. Internal Audit

I know people want to select D because... it sounds right. External audit to compare against external regulations. But there's a part being overlooked: 'would like to gain an understanding'. Which you don't NEED a third party to confirm, because the company already KNOWS those regulations. But you WOULD need an external audit if there was a large breach and the regulatory agencies wanted to know how it happened.

What is being asked, effectively, is "Can an internal audit team verify that we meet external regulations?"

upvoted 7 times

ETQ 8 months, 1 week ago

This literally doesn't make any sense. Then you can say the same for pentests and everything else. Oh, why hire an external person to check on your security, just do an internal pentest!

If you want to actually check and be sure about regulations, you'll always hire a company that specializes in it.

"Can an internal audit team verify that we meet external regulations?" The answer is maybe, but you'll never be sure. If they overlook something, your audit will be useless.

upvoted 5 times

Rackup Most Recent 5 months ago

Selected Answer: D

Answer: D. External examination

Explanation: An external examination is the best approach for the CISO to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators. This process typically involves an external party, such as a third-party auditor or regulatory body, reviewing the company's security policies and controls to ensure they align with industry regulations and standards.

While internal audits (B) assess the company's internal controls and practices, external examinations provide an unbiased review from an external perspective, which is essential for understanding compliance with external regulatory requirements.

upvoted 1 times

ijia\_Ai0823 5 months ago

Selected Answer: B

In my opinion, it's Internal audit.

It's more likely to be a sequential things (Based on an ISO-9001 external audit I experienced before). A company usually do an internal audit before proceeding to an external audit, because external audit must have a authorized third-party auditors and can be quite costly to be certified that your company is qualified by the auditors. In most cases, the auditors may conclude some corrective actions(like CAR) that need your company to finish. After the correction report is submitted and validated by the auditors, your company can receive the approved certification.

upvoted 1 times

🗨️ 👤 **Suga\_1** 5 months, 3 weeks ago

The correct answer is: C. Attestation.

Explanation:

Attestation: This involves an independent third party verifying that the company's security policies, processes, or systems meet the requirements imposed by external regulations. Attestations are often used to demonstrate compliance with regulatory frameworks and standards such as SOC 2, ISO 27001, or GDPR.

upvoted 1 times

🗨️ 👤 **laternak26** 6 months, 2 weeks ago

**Selected Answer: B**

An internal audit is a comprehensive evaluation of a company's operations, processes, and policies to ensure they are compliant with internal standards as well as external regulations. In the context of comparing the company's security policies to external regulatory requirements, an internal audit would be the most appropriate tool. It involves reviewing and assessing the security measures and procedures in place and determining how well they align with legal and regulatory requirements, ensuring that the company meets compliance standards.

Why not D. External examination:

An external examination is typically performed by third-party auditors or regulators to assess compliance with external standards and regulations. While it can provide valuable insights into regulatory adherence, it is not the best tool for an internal review by the CISO. An internal audit allows the CISO to assess the company's own security policies and their alignment with external regulations before seeking an external review.

upvoted 2 times

🗨️ 👤 **ProudFather** 6 months, 3 weeks ago

**Selected Answer: D**

D. External examination

An external examination by a qualified third-party auditor can provide an objective assessment of the company's security practices against industry standards and regulatory requirements. This can help the CISO identify any gaps or weaknesses in the company's security posture and take corrective action.

The other options are not as suitable:

upvoted 2 times

🗨️ 👤 **e2ba0ff** 7 months ago

**Selected Answer: B**

vendor's self-assessment of practices against industry or organizational requirement

upvoted 2 times

🗨️ 👤 **Murtuza** 8 months, 2 weeks ago

**Selected Answer: D**

Between the two options, D. External examination is the most suitable for understanding how the company's security policies compare to external regulatory requirements.

An external examination involves an independent review by an external party, providing an objective assessment of the company's compliance with regulatory standards. This ensures that the evaluation is unbiased and thorough, which is crucial for regulatory compliance.

upvoted 2 times

🗨️ 👤 **nillie** 9 months ago

**Selected Answer: B**

The CISO should use:

B. Internal audit

An internal audit is a structured assessment of the company's security policies, processes, and controls to ensure they meet both internal standards and external regulatory requirements. This will help the CISO understand how well the company's security policies align with the requirements imposed by regulators.

upvoted 2 times

🗨️ 👤 **Ty13** 9 months ago

**Selected Answer: B**

## B. Internal Audit

I know people want to select D because... it sounds right. External audit to compare against external regulations. But there's a part being overlooked: 'would like to gain an understanding'. Which you don't NEED a third party to confirm, because the company already KNOWS those regulations. But you WOULD need an external audit if there was a large breach and the regulatory agencies wanted to know how it happened.

What is being asked, effectively, is "Can an internal audit team verify that we meet external regulations?"

upvoted 2 times

🗳️ 👤 **RIDA\_007** 9 months, 1 week ago

**Selected Answer: D**

An external examination (also known as an external audit or external review)

upvoted 1 times

🗳️ 👤 **NONS3c** 9 months, 2 weeks ago

**Selected Answer: B**

even GPT Said

upvoted 1 times

🗳️ 👤 **Cyber\_Texas** 10 months ago

D external examination is best here

upvoted 1 times

🗳️ 👤 **myazureexams** 10 months ago

**Selected Answer: D**

It is D period. And for the exam, make the association "External with External" DONE

upvoted 4 times

🗳️ 👤 **Glacier88** 10 months, 1 week ago

**Selected Answer: D**

External examination: An external examination, conducted by an independent third party, can provide an objective assessment of the company's security policies and practices against external regulatory requirements. This can help the CISO identify any gaps or areas for improvement.  
Penetration test: While penetration tests can identify vulnerabilities in the company's security infrastructure, they don't directly assess compliance with external regulations.

Internal audit: Internal audits can assess the company's adherence to internal policies and procedures, but they might not provide a comprehensive view of compliance with external regulations.

Attestation: Attestation is a formal process of providing assurance about a specific claim or assertion. While it might involve compliance with regulations, it doesn't necessarily provide a full assessment of the company's security policies and practices.

upvoted 1 times

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: B**

B. Internal audit

An internal audit allows the CISO to assess how the company's security policies align with the requirements imposed by external regulators. This process involves reviewing and evaluating the company's policies, procedures, and controls to ensure compliance with regulatory standards.

upvoted 3 times

🗳️ 👤 **Dlove** 10 months, 2 weeks ago

**Selected Answer: D**

D. External Examination

An external examination involves a review or assessment conducted by an independent third party, often to evaluate how an organization's policies, procedures, and practices align with regulatory requirements or industry standards. This process is crucial for identifying gaps between the company's internal security policies and the requirements imposed by external regulators. It provides the CISO with an unbiased understanding of the organization's compliance status.

upvoted 1 times

A systems administrator notices that the research and development department is not using the company VPN when accessing various company-related services and systems. Which of the following scenarios describes this activity?

- A. Espionage
- B. Data exfiltration
- C. Nation-state attack
- D. Shadow IT

**Correct Answer:** D

Community vote distribution

D (85%)

B (15%)

  **nillie**  9 months ago




**Selected Answer:** D

The scenario described is:

D. Shadow IT

Shadow IT refers to the use of technology, systems, or services by employees without the approval or knowledge of the IT department. In this case, the research and development department is bypassing the company's VPN, potentially using unauthorized methods to access company-related services and systems. This can pose security risks, as these systems may not adhere to the company's security policies and protocols.


upvoted 8 times

  **ITExperts**  5 months, 1 week ago

**Selected Answer:** D

D, espionage given here is crazy lmao

upvoted 2 times



  **gingergroot** 6 months, 4 weeks ago

**Selected Answer:** B

B. Data exfiltration

From the official CompTIA SY0-701 study guide - "Data exfiltration is the unauthorized transfer of data outside an organization and is a significant concern."

upvoted 2 times

  **gingergroot** 6 months, 4 weeks ago

\*concern



upvoted 2 times

  **Honeybadge** 7 months, 1 week ago

**Selected Answer:** B

This question is worded terribly as it isn't noted that the department is using shadow IT. One shouldn't just assume they are using unauthorized software or hardware. Or I could assume since they aren't using a VPN to provide them a secure tunnel when accessing company resources, they were compromised causing data to be exfiltrated. They are just simply not using their VPN to access authorized company services and systems. This seems to be more of a policy enforcement issue than anything.

upvoted 1 times

  **917a0a9** 7 months, 1 week ago

The question makes no mention to doing anything with the data, especially exfiltrating it or moving the data elsewhere. It's D

upvoted 4 times



  **jsmthy** 9 months ago

**Selected Answer:** D

Using unauthorized software, eh Dave? The scenario may imply the use of an unofficial VPN for the sake of carrying out Espionage or Data Exfiltration, but there is no sign of it. The threat is the VPN rather the user or the data. Additionally, it doesn't seem like the nation-state attack would

fit since the hallmarks of such an attack aren't present (lots of funding, firmware-level bugs, unique spyware, social engineering).

upvoted 4 times

  **MarDog** 10 months, 2 weeks ago

Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization.

upvoted 4 times

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

- A. Shadow IT
- B. Insider threat
- C. Data exfiltration
- D. Service disruption

**Correct Answer:** A

*Community vote distribution*

A (100%)


 **Dlove** Highly Voted 10 months, 3 weeks ago

**Selected Answer: A**

A. Shadow IT

Shadow IT is when an employee uses information technology (IT) systems without the approval of an organization's IT department.

upvoted 10 times

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

Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization.

upvoted 3 times

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

- A. To track the status of patching installations
- B. To find shadow IT cloud deployments
- C. To continuously the monitor hardware inventory
- D. To hunt for active attackers in the network

**Correct Answer:** A

*Community vote distribution*

A (100%)

  **a4e15bd** Highly Voted 10 months, 3 weeks ago



Answer A is correct:

Daily vulnerability scans help ensure that all the endpoints are up to date with security patches and identify any vulnerabilities that may have been introduced due to unpatched software. This regular scanning helps in monitoring and verifying the effectiveness of patch management process.  
upvoted 9 times

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

**Selected Answer: A**

Results of vulnerability scans are CVEs.  
upvoted 2 times

  **qacollin** 10 months, 3 weeks ago

**Selected Answer: A**

A. GPT  
upvoted 1 times

Which of the following is classified as high availability in a cloud environment?

- A. Access broker
- B. Cloud HSM
- C. WAF
- D. Load balancer

**Correct Answer:** D

*Community vote distribution*

D (100%)

  **a4e15bd**  10 months, 3 weeks ago

D

Load balancer distributes incoming network traffic across multiple servers or instances ensuring that no single server becomes overwhelmed and helps maintain the availability of applications and services.


upvoted 5 times

  **FrozenCarrot**  9 months, 3 weeks ago

**Selected Answer: D**

Load balancer distribute traffic between servers, guarantee availability.

upvoted 2 times

  **qacollin** 10 months, 3 weeks ago

**Selected Answer: D**

D. GPT!

upvoted 2 times



Which of the following security measures is required when using a cloud-based platform for IoT management?

- A. Encrypted connection
- B. Federated identity
- C. Firewall
- D. Single sign-on

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **a4e15bd** Highly Voted 10 months, 3 weeks ago

A

IOT devices often transmit sensitive data over networks and encryption ensures that this data is securely transmitted and protected from interception or tampering.

upvoted 6 times

🗳️ 👤 **billie** Most Recent 1 month ago

Selected Answer: A

omg chatgpt actually got it right

upvoted 1 times

🗳️ 👤 **test\_arrow** 4 months, 1 week ago

Selected Answer: A

A. Encrypted Connection

Why?

When using a cloud-based platform for IoT management, data is transmitted over the internet, making encryption critical to protect sensitive information.

Encrypted connections (e.g., TLS/SSL, VPN, or IPSec) ensure that data remains secure in transit and prevent eavesdropping or man-in-the-middle (MitM) attacks.

Many IoT devices are vulnerable due to weak security implementations, making encryption a fundamental security measure.

Why Not the Others?

B. Federated Identity – Useful for authentication across multiple systems but not specifically required for IoT cloud management.

C. Firewall – Important for network security but doesn't protect data in transit between IoT devices and the cloud.

D. Single Sign-On (SSO) – Enhances authentication convenience but does not directly secure IoT data transmission.

upvoted 1 times

🗳️ 👤 **qacollin** 10 months, 3 weeks ago

Selected Answer: A

A. GPT

upvoted 1 times


Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?

- A. Unidentified removable devices
- B. Default network device credentials
- C. Spear phishing emails
- D. Impersonation of business units through typosquatting

**Correct Answer: A**

*Community vote distribution*

A (100%)

  **qacollin** 10 months, 3 weeks ago

**Selected Answer: A**



A. GPT

upvoted 3 times

  **Lykkefcode\_111** 9 months, 2 weeks ago

I think is incorrect. The question refers to an 'attack vector,' but option A describes an 'attack surface.' In my opinion, the correct answer should be option C. Spear phishing emails.

upvoted 3 times

  **TmNvrWts** 4 months, 2 weeks ago

Phishing is also an external stuff so +1 on answer A side :D

upvoted 1 times

  **ETQ** 8 months, 1 week ago

A definitely describes a threat vector, as in for example using a USB to install malware to gain access to systems, or simply used to copy data.

upvoted 4 times

  **Lykkefcode\_111** 8 months ago

Sorry for the confusion. You are right.

upvoted 3 times

Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

- A. Encryption
- B. Hashing
- C. Masking
- D. Tokenization

**Correct Answer:** C

Community vote distribution

C (89%)

11%

🗳️ 👤 **ProudFather** Highly Voted 6 months, 3 weeks ago

**Selected Answer: C**

Masking involves hiding sensitive information by replacing it with a specific character, such as an asterisk (\*). In the case of credit card numbers, masking would typically involve displaying only the last four digits, while the rest of the numbers are replaced with asterisks. This allows for partial visibility of the card number while protecting the sensitive information.

upvoted 5 times

🗳️ 👤 **63f8be6** Most Recent 2 months, 2 weeks ago

**Selected Answer: C**

i will go for masking.

upvoted 1 times

🗳️ 👤 **pindinga1** 5 months, 2 weeks ago

**Selected Answer: D**

Tokenizacion is Right

upvoted 1 times

🗳️ 👤 **famuza77** 8 months, 2 weeks ago

It is Tokenization

upvoted 1 times

🗳️ 👤 **rrynzon** 9 months, 2 weeks ago

this is wrong, the correct answer is "tokenization"

upvoted 2 times

🗳️ 👤 **850bc48** 9 months, 2 weeks ago

no because tokenization is basically when a randomly generated number is created in lieu of you actual card number, so that if your card is intercepted during a transaction, the attack doesn't get your actual number.

upvoted 3 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

C. Masking - is used to protect sensitive information while still allowing authorized users to view a portion of the data like a credit card number.

upvoted 4 times

🗳️ 👤 **Sol\_tyty** 10 months, 1 week ago

GPT!!!

upvoted 2 times

🗳️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: C**

C . GPT

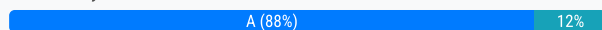
upvoted 2 times

The Chief Information Security Officer (CISO) has determined the company is non-compliant with local data privacy regulations. The CISO needs to justify the budget request for more resources. Which of the following should the CISO present to the board as the direct consequence of non-compliance?

- A. Fines
- B. Reputational damage
- C. Sanctions
- D. Contractual implications

**Correct Answer: A**

Community vote distribution



**pindinga1** Highly Voted 5 months, 2 weeks ago

**Selected Answer: A**

Why not e: "All to Above" jajajaj  
upvoted 7 times

**Eracle** Most Recent 5 months, 4 weeks ago

**Selected Answer: C**

Why not Sanctions?  
upvoted 2 times

**BevMe** 7 months, 2 weeks ago

**Selected Answer: A**

Regulatory fines are usually significant and have a clear financial impact on the company, making them a compelling reason to allocate more resources for compliance.

Reputational damage is also a serious consequence, but its effect is a bit indirect, resulting from, say, data breaches or public knowledge of non-compliance. It can be harder to quantify and justify immediately compared to direct financial penalties.

upvoted 2 times

**jsmthy** 9 months ago

**Selected Answer: A**

Hit the executives where it hurts most.  
upvoted 4 times

**Glacier88** 10 months, 1 week ago

**Selected Answer: A**

Fines: Under GDPR, fines can be substantial, reaching up to 4% of a company's global annual turnover. This makes them a very direct and immediate consequence of non-compliance, emphasizing the financial risk associated with it.

Reputational damage: While this remains a significant concern, it may not be as immediately quantifiable as fines. Fines can serve as a concrete measure of the financial impact of non-compliance.

Sanctions: Sanctions are typically imposed by governments as a result of serious violations of laws or international agreements. They are not directly related to data privacy compliance.

Contractual implications: While non-compliance may have contractual implications, especially if there are specific data privacy clauses in contracts with customers or partners, it's not necessarily the most immediate or significant consequence.

upvoted 4 times

**jafyyy** 10 months, 1 week ago

A. Fines are financial consequence of non-compliance with data privacy regulations  
upvoted 1 times

**qacollin** 10 months, 3 weeks ago

A. GPT  
upvoted 2 times

Which of the following alert types is the most likely to be ignored over time?

- A. True positive
- B. True negative
- C. False positive
- D. False negative

**Correct Answer:** C

*Community vote distribution*

C (100%)

🗨️ 👤 **jafyyy** 10 months, 1 week ago

C. False Positive - triggered when an event is NOT actually a threat.

True Positive - an actual threat

True Negative - no threat

False Negative - an actual threat isn't detected, dangerous type since threats go unnoticed.

upvoted 4 times

🗨️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: C**

C. GPT

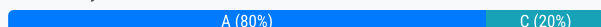
upvoted 2 times

A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports. Which of the following vulnerabilities has likely been exploited in this software?

- A. Memory injection
- B. Race condition
- C. Side loading
- D. SQL injection

**Correct Answer: A**

Community vote distribution



🗳️ 👤 **a4e15bd** Highly Voted 10 months, 3 weeks ago

A is correct.

Memory injection allows the attackers to inject malicious code directly into the memory of a running process which can then be used to execute arbitrary commands or generate unauthorized network traffic.

Race Condition refers to two processes competing to modify the same resource which can lead to unpredictable behavior but is less likely to cause abnormal outbound traffic.

Side Loading refers to loading a malicious DLL into a legitimate process.

SQL injection involves injecting malicious SQL code into a database and is primarily concerned with database manipulation rather than generating outbound network traffic.

upvoted 19 times

🗳️ 👤 **Exemplary** 8 months, 3 weeks ago

Just a quick note: Your definition of side loading is incorrect. Side loading involves installing software from third party or unauthorized sources, typically involving mobile devices. What you described is actually a DLL Injection.

upvoted 17 times

🗳️ 👤 **JoeRealCool** Most Recent 2 months, 3 weeks ago

**Selected Answer: A**

Side loading would make sense if the question referenced changes made to the files the software uses to run. That's my understanding of the difference between side loading and memory injection. For it to be side loading, an attacker would have to place a malicious file in storage that the software unintentionally loads and runs code off of.

upvoted 1 times

🗳️ 👤 **test\_arrow** 4 months, 2 weeks ago

**Selected Answer: A**

The abnormal behavior—unexpected outbound traffic over random high ports—suggests that malicious code has been injected into the application's memory. Memory injection attacks allow an attacker to execute arbitrary code within the memory space of a legitimate process, often leading to unauthorized network activity, data exfiltration, or the deployment of additional malware.

upvoted 1 times

🗳️ 👤 **jbmac** 6 months ago

**Selected Answer: C**

The correct answer is:

C. Side loading

Explanation:

Side loading involves the unauthorized loading or execution of malicious code alongside legitimate software. In this scenario:

The software is behaving abnormally and generating unexpected outbound traffic, which suggests it may have been compromised to execute additional, malicious code.

Random high-port outbound traffic is a common indicator of malware or other unauthorized processes attempting to exfiltrate data or communicate with a command-and-control (C2) server.

upvoted 1 times

🗨️ 👤 **chalaka** 7 months, 1 week ago

**Selected Answer: A**

A. Memory injection

Memory injection vulnerabilities allow an attacker to manipulate the memory of a running application. This can lead to malicious behavior, such as executing arbitrary code or altering the application's normal operation. In this scenario, the abnormal behavior (outbound traffic over random high ports) suggests that the software has been compromised to execute unauthorized operations, which is characteristic of a memory injection exploit.

upvoted 2 times

🗨️ 👤 **Habbiti** 7 months, 3 weeks ago

The correct answer is C, side loading

Side loading refers to a situation where software loads a malicious or unauthorized component or library (often from an untrusted source) instead of a legitimate one. In this case, the abnormal behavior (outbound traffic over random high ports) suggests that the application may have been compromised, and a malicious payload has been introduced, causing the software to behave unexpectedly. The random outbound traffic could indicate that the compromised software is now communicating with a command-and-control server or exfiltrating data.

upvoted 1 times

🗨️ 👤 **jafyyy** 10 months, 1 week ago

A. Memory Injection

upvoted 1 times

An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

- A. Asset inventory
- B. Network enumeration
- C. Data certification
- D. Procurement process

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗳️ 👤 **Luswepo** 7 months, 3 weeks ago

**Selected Answer: A**

The best answer is: A. Asset inventory

An asset inventory is essential for ensuring that all systems requiring the patch are updated. By maintaining a comprehensive inventory of all systems, the administrator can identify which devices have the critical application installed and require the patch. An accurate asset inventory helps ensure that no systems are overlooked during the patching process.

- Network enumeration focuses on identifying devices on the network but does not necessarily provide information about the applications running on those devices.
- Data certification relates to validating the integrity and accuracy of data, which is unrelated to identifying systems needing patches.
- Procurement process involves acquiring hardware or software but does not help track existing systems for patching needs.

Therefore, an asset inventory is the best choice for maintaining awareness of all systems that require patching.

upvoted 2 times

🗳️ 👤 **PAWarriors** 9 months, 3 weeks ago

**Selected Answer: A**

Asset inventory is a list of all hardware, software, and systems within the organization. Maintaining an up-to-date asset inventory allows the systems administrator to easily identify which systems are running the critical application and need the patch

upvoted 3 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

A. Asset Inventory provides complete list of assets that need to be managed.

upvoted 1 times



Which of the following should a security operations center use to improve its incident response procedure?

- A. Playbooks
- B. Frameworks
- C. Baselines
- D. Benchmarks

**Correct Answer: A**

*Community vote distribution*

A (100%)

  **jafyyy** Highly Voted 10 months, 1 week ago

A. Playbooks



Its a step by step procedure outlining how to respond to specific types of incidents.

upvoted 8 times

  **StringerBarksdale** Most Recent 10 months, 2 weeks ago

The answer is B

upvoted 2 times

  **qacollin** 10 months, 3 weeks ago

**Selected Answer: A**

A. GPT

upvoted 3 times

Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?

- A. Continuity of operations
- B. Capacity planning
- C. Tabletop exercise
- D. Parallel processing

**Correct Answer:** C

*Community vote distribution*

C (100%)

🗲️ 👤 **Adelsola** 3 months, 1 week ago

**Selected Answer: C**

C. Tabletop exercise  
upvoted 2 times

🗲️ 👤 **jafyyy** 10 months, 1 week ago

C. Tabletop exercise  
upvoted 1 times

🗲️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: C**

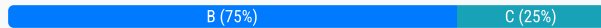
C . GPT  
upvoted 2 times

A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies. Which of the following is the most important consideration during development?

- A. Scalability
- B. Availability
- C. Cost
- D. Ease of deployment

**Correct Answer:** B

Community vote distribution



ServerBrain **Highly Voted** 9 months, 3 weeks ago

**Selected Answer: B**

to report report health emergencies...  
upvoted 5 times

Brian\_Douglas **Most Recent** 3 months, 2 weeks ago

**Selected Answer: B**

They don't want the page to crash due to high traffic/use.  
upvoted 1 times

Chickenbuttbrown 6 months, 1 week ago

**Selected Answer: C**

i dont see how its not cost for a healthcare org thats all they care about  
upvoted 2 times

fc040c7 5 months ago

I get what you're saying but for test purposes the keywords were "healthcare emergencies" which would indicate an importance of availability.  
Answer B  
upvoted 5 times

jafyyy 10 months, 1 week ago

B. Availability is crucial for patient safety in health emergencies.  
upvoted 2 times

qacollin 10 months, 3 weeks ago

B. GPT  
upvoted 2 times

Which of the following agreement types defines the time frame in which a vendor needs to respond?

- A. SOW
- B. SLA
- C. MOA
- D. MOU

**Correct Answer:** B

*Community vote distribution*

B (100%)

🗳️ 👤 **AndyK2** 7 months ago

**Selected Answer: B**

A Service Level Agreement (SLA) defines the specific levels of service that a vendor is expected to provide, including:

Response time frames: The time within which the vendor must respond to issues, requests, or incidents.

Uptime guarantees: Commitments to service availability.

Performance metrics: Quantifiable goals for the service.

An SLA ensures accountability and sets clear expectations for the relationship between the organization and the vendor.

Why not the other options?

A. SOW (Statement of Work):

A Statement of Work outlines the deliverables, project scope, and timelines but does not define service levels or response times.

C. MOA (Memorandum of Agreement):

An MOA is a formal agreement between parties, often used for partnerships or collaborations, but it lacks the detailed operational metrics found in an SLA.

D. MOU (Memorandum of Understanding):

An MOU is an informal document that expresses intent between parties but does not contain enforceable terms like response times.

upvoted 4 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

B. SLA (Service Level Agreement)

upvoted 2 times

🗳️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: B**

B. GPT

upvoted 3 times

Which of the following is a feature of a next-generation SIEM system?

- A. Virus signatures
- B. Automated response actions
- C. Security agent deployment
- D. Vulnerability scanning

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **FrozenCarrot** Highly Voted 9 months, 3 weeks ago

**Selected Answer: B**



next-gen SIEM platforms can dynamically analyze vast datasets in real time, enabling the identification of subtle, evolving threats that traditional systems might overlook.

upvoted 5 times

  **jafyyy** Most Recent 10 months, 1 week ago

B. Automated Response Actions

upvoted 2 times

  **qacollin** 10 months, 3 weeks ago

**Selected Answer: B**

B. GPT

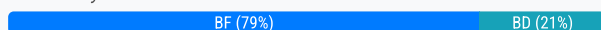
upvoted 2 times

To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed. Which of the following best describe these types of controls? (Choose two.)

- A. Preventive
- B. Deterrent
- C. Corrective
- D. Directive
- E. Compensating
- F. Detective

**Correct Answer:** BF

Community vote distribution



internslayer **Highly Voted** 10 months, 2 weeks ago

**Selected Answer: BF**

I believe it is B and F because the CCTV will give you the ability to monitor the data center and its presence and signs are a deterrent.  
upvoted 12 times

itone3333 **Most Recent** 2 months ago

**Selected Answer: BF**

ComTIA 701 training categorizes the CCTV as a deterrent but I'll take your word for it.  
upvoted 1 times

laternak26 6 months, 2 weeks ago

**Selected Answer: BD**

B. Deterrent:

The CCTV system and the signs warning of surveillance are deterrent controls because they are designed to discourage malicious or unauthorized actions. The idea is that people will be less likely to engage in inappropriate behavior if they know they are being watched or recorded.

D. Directive:

The signs informing people that they may be filmed are also directive controls. Directive controls are intended to communicate policies, rules, or expectations to individuals, in this case, warning them about the surveillance and informing them of the monitoring policy. This sets a clear guideline for behavior in the area.

Why not F. Detective:

Detective controls are designed to detect incidents or breaches, such as intrusion detection systems (IDS) or security cameras for identifying events. The CCTV system could be considered a detective control if it is used to record and analyze activities for incidents, but the signs are more related to deterrence and direction.  
upvoted 1 times

User92 8 months, 4 weeks ago

**Selected Answer: BF**

Deterrent: The signs serve as a deterrent by discouraging potential intruders or malicious activities through the awareness of surveillance.  
Detective: The CCTV system itself acts as a detective control by monitoring and recording activities, which can be reviewed to detect and investigate incidents.  
upvoted 2 times

baronvon 10 months, 1 week ago


**Selected Answer: BD**

It's B and D  
upvoted 2 times

Hayder81 10 months, 1 week ago

I believe it is B and F

upvoted 1 times

  **CJfromVA** 10 months, 3 weeks ago



**Selected Answer: BD**

I believe and what I will go with.

B. Deterrent: The CCTV system and signs serve to deter potential unauthorized activities or behavior by making individuals aware that they are being monitored. The idea is that the possibility of being recorded will discourage malicious or inappropriate actions.



D. Directive: Posting signs about being filmed can also be considered a directive control. It communicates rules or policies to individuals about their behavior and the monitoring system in place, guiding how they should act within the data center.

upvoted 1 times

  **EfaChux** 10 months, 2 weeks ago

CCTV is detective, its there to detect incidents. Some CCTV are hidden so people may not even know its there so it doesn't stop them but it can see them and alert the security team.

upvoted 2 times

  **baronvon** 10 months, 1 week ago

The question says that they posts several signs about the possibility of being filmed, people may not know but they will act differently knowing they are being recorded

upvoted 1 times

  **fc040c7** 5 months ago

The CCTV is the detective control and the signs are a deterrent control. Like you said people would act differently if they know they are being watched. A sign telling them that they are being watched/filmed will “deter” them from doing unauthorized activities.

upvoted 2 times

Which of the following examples would be best mitigated by input sanitization?

- A. `<script>alert("Warning!");</script>`
- B. nmap - 10.11.1.130
- C. Email message: "Click this link to get your free gift card."
- D. Browser message: "Your connection is not private."

**Correct Answer:** A

Community vote distribution

A (100%)

  **CJfromVA** Highly Voted 10 months, 3 weeks ago

**Selected Answer:** A

This question is the same on exam topics 601 #604 - The answer is in fact A and it shows "A. `<script>alert("Warning!");</script>`"  
upvoted 22 times

  **3dk1** Highly Voted 8 months ago

huh, so thats why my browser showed "warning!" when opening this page's questions.

hahahaha

upvoted 21 times

  **TonyStarChillingFromHeaven** Most Recent 7 months ago


**Selected Answer:** A

A. `<script>alert("Warning!");</script>`  
upvoted 1 times

  **jsmthy** 9 months ago

**Selected Answer:** A

Your browser is like Ron Burgundy. Whatever shows up on the HTML file, it is going to read it and execute it.  
upvoted 11 times

  **Sole\_tone** 10 months, 3 weeks ago

the Answer is A but it doesn't show anything but what it should be showing is something like this.  
`<script>alert("Warning!");</script>`  
If you look in the 601 study guide that's what it shows  
upvoted 11 times



An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

- A. Smishing
- B. Disinformation
- C. Impersonating
- D. Whaling

**Correct Answer:** C

Community vote distribution



**BugG5** Highly Voted 10 months, 2 weeks ago

**Selected Answer: C**

Impersonating involves pretending to be someone else, in this case, the Chief Executive Officer (CEO), to deceive the employee into taking a specific action (buying gift cards). The attacker is leveraging the authority and trust associated with the CEO's position to manipulate the employee.

Whaling: This phishing attack targets high-profile individuals, such as executives.

An attacker is 'posing' and not 'targeting' a CEO. Therefore its C

upvoted 12 times

**Abas2** Most Recent 1 month, 2 weeks ago

**Selected Answer: C**

Impersonating involves pretending to be someone else, in this case, the Chief Executive Officer (CEO), to deceive the employee into taking a specific action (buying gift cards). The attacker is leveraging the authority and trust associated with the CEO's position to manipulate the employee.

Whaling: This phishing attack targets high-profile individuals, such as executives.

An attacker is 'posing' and not 'targeting' a CEO. Therefore its C

upvoted 1 times

**Emmyraj** 7 months, 3 weeks ago

**Selected Answer: D**

The correct answer is:

D. Whaling

Explanation:

Whaling is a type of social engineering attack that specifically targets high-profile individuals such as executives, or in this case, impersonates them to deceive others. The attacker is posing as the CEO to manipulate an employee into performing an action, such as buying gift cards. This is a targeted attack that leverages the authority and influence of a senior executive.

upvoted 1 times

**kambam** 6 months, 4 weeks ago

It is not targeting a high profile individual so it cannot be whaling. It is targeting an employee while pretending to be a high profile individual. C - Impersonating is correct

upvoted 3 times

**Nilab** 8 months, 2 weeks ago

**Selected Answer: C**

Impersonation

upvoted 1 times

**Glacier88** 10 months, 1 week ago

**Selected Answer: C**

Smishing: Phishing via SMS messages.

Disinformation: Spreading false information.

Impersonating: Pretending to be someone else.

Whaling: Targeting high-profile individuals.

Given that the attacker is posing as the CEO, impersonating is the most accurate answer.

upvoted 2 times

🗨️ 👤 **Hayder81** 10 months, 1 week ago

Impersonating C

upvoted 1 times

🗨️ 👤 **jafyyy** 10 months, 1 week ago

C. Impersonating -

Given the target is an employee rather than a high-profile executive, most accurate technique used is Impersonating.

upvoted 1 times

🗨️ 👤 **ExamTopics2040** 10 months, 2 weeks ago

Whaling targets high-profile individuals within an organization, such as executives, CEOs, CFOs, or other senior management. so C is best answer

upvoted 2 times

🗨️ 👤 **Migzz** 10 months, 3 weeks ago

Answer is D whaling. Only because it involves a high-profile executive. If you look up the definition of whaling and compare it to C., whaling is a more suitable answer from a security plus exam standpoint.

upvoted 3 times

🗨️ 👤 **rbidev** 2 months, 2 weeks ago

Whaling would be pretending to be the CEO and targeting another high level employee...both players need to be "whales" for whaling. Therefore, C: Impersonating is the right answer.

upvoted 1 times

🗨️ 👤 **RIDA\_007** 9 months, 1 week ago

Posing as "CEO" the attacker pretending to be the CEO. Hence it's C.

upvoted 1 times

🗨️ 👤 **RobJob** 9 months, 1 week ago

Whaling is targeting high-profile executives not impersonating the,

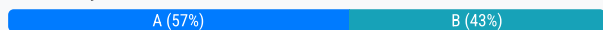
upvoted 1 times

After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned. Which of the following describes this example?

- A. False positive
- B. False negative
- C. True positive
- D. True negative

**Correct Answer:** A

Community vote distribution



test\_arrow Highly Voted 4 months, 1 week ago

Selected Answer: A

the vulnerability was NOT present after the scan indicates a false positive  
upvoted 7 times

1chung Most Recent 4 weeks ago

Selected Answer: B

Correct answer is B  
upvoted 1 times

Ekim149 1 month, 3 weeks ago

Selected Answer: A

After the scan, the result stated that there is a vulnerability, but it was identified that that vulnerability was not actually on the system, which is False Positive  
upvoted 2 times

781f0b4 2 months ago

Selected Answer: A

it is a  
upvoted 1 times

Burnboy 2 months, 1 week ago

Selected Answer: A

A. False positive  
upvoted 1 times

9ce65e3 2 months, 2 weeks ago

Selected Answer: A

False Positive = flagged issue but not really there.  
upvoted 1 times

timotei 2 months, 2 weeks ago

Selected Answer: A

Ans A - Scanned, identified but not found = False positive

False negative is identified, scanned but not found.  
upvoted 2 times

TommyPel 2 months, 2 weeks ago

Selected Answer: B

False negative  
upvoted 1 times

c3bb5b6 2 months, 2 weeks ago

Selected Answer: B

Its false negative. a test result which incorrectly indicates that a particular condition or attribute is absent.

upvoted 1 times

🗨️ 👤 **SAM0678** 3 months ago

**Selected Answer: B**

Its a false negative

upvoted 3 times

🗨️ 👤 **mejestique** 3 months, 3 weeks ago

**Selected Answer: B**

Its a false negative

upvoted 1 times

🗨️ 👤 **tomahawk117** 4 months ago

**Selected Answer: B**

This one is a false negative. Why? A known vulnerability has been found but the scanner failed to see it. False Positive means the scanner incorrectly identified a vulnerability

upvoted 3 times

🗨️ 👤 **TmNvrWts** 4 months, 2 weeks ago

**Selected Answer: A**

The correct answer is:

A. False positive

Explanation:

A false positive occurs when a security system incorrectly flags a vulnerability or threat that does not actually exist on the system. In this case, the vulnerability scan reported an issue, but upon further investigation, the administrator confirmed that the vulnerability is not present.

Why not the other options?

B. False negative – This would mean a vulnerability is present but was not detected, which is the opposite of what happened here.

C. True positive – This would mean the vulnerability was correctly identified and is actually present on the system.

D. True negative – This would mean the system was correctly identified as not having the vulnerability, but in this case, the scan incorrectly reported it.

upvoted 3 times

🗨️ 👤 **ijja\_Ai0823** 5 months ago

**Selected Answer: B**

B. False negative. Because it is an "identified" vulnerabilities but not reported by a scan.

upvoted 2 times

🗨️ 👤 **rrynzon** 9 months, 2 weeks ago

False Positive - Normal or expected activity is incorrectly identified as abnormal or unexpected. False Negative - Abnormal or unexpected activity is incorrectly identified as normal or expected. Therefore, B is the correct answer.

upvoted 3 times

🗨️ 👤 **jafyyy** 10 months, 1 week ago

A. False Positive - an alert for an event that is not a threat.

upvoted 2 times

🗨️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: A**

A. GPT

upvoted 1 times

A recent penetration test identified that an attacker could flood the MAC address table of network switches. Which of the following would best mitigate this type of attack?

- A. Load balancer
- B. Port security
- C. IPS
- D. NGFW

Correct Answer: B

🗨️ 👤 **Muhammad\_Umair** Highly Voted 🍎 10 months, 2 weeks ago

Port security is a feature on network switches that allows you to limit the number of MAC addresses that can be learned on a specific port. If the limit is exceeded, the switch can take predefined actions such as shutting down the port, restricting traffic, or generating alerts. This effectively prevents attackers from overwhelming the switch with a large number of MAC addresses, which could otherwise cause the switch to behave like a hub, sending traffic to all ports and potentially exposing sensitive data. (B)

upvoted 30 times

🗨️ 👤 **CISUMPATR** 2 months, 2 weeks ago

If this answer is correct, and the port shuts down from MAC address flooding, that is another form of DDOS right? Please let me know if you think this is true or not. I think the answer should be NGFW!

upvoted 1 times

🗨️ 👤 **ChocolateRenaissance** Most Recent 🔍 2 months ago

Selected Answer: B

The attack described, flooding the MAC address table of network switches, is known as a MAC flooding attack or CAM table overflow attack. The best mitigation for this specific type of attack among the choices is:

B. Port security

upvoted 2 times

A user would like to install software and features that are not available with a smartphone's default software. Which of the following would allow the user to install unauthorized software and enable new features?

- A. SQLi
- B. Cross-site scripting
- C. Jailbreaking
- D. Side loading

**Correct Answer:** C

Community vote distribution



🗳️ 👤 **2fd1029** Highly Voted 9 months, 2 weeks ago

**Selected Answer:** C

I think the answer is C, even though I first thought D. The reason I changed my mind is because at the end they also mention enabling new features, which sideloading doesn't necessarily let you do. Jailbreaking does.

upvoted 6 times

🗳️ 👤 **prabh1251** Most Recent 3 months, 2 weeks ago

**Selected Answer:** C

While side loading could allow a user to install software from unofficial sources, the key part of the question is about installing software and enabling new features that aren't part of the default software. Jailbreaking goes beyond just installing unauthorized apps — it gives the user deeper access to the device, allowing new features and system modifications that aren't possible with side loading alone.

upvoted 1 times

🗳️ 👤 **deejay2** 6 months, 3 weeks ago

**Selected Answer:** C

It's either Jailbreaking(Apple) or Rooting (Android). Both deal with not having access to the device's operating system. Since Rooting is not an option, the answer is Jailbreaking.

upvoted 4 times

🗳️ 👤 **NONS3c** 9 months, 2 weeks ago

**Selected Answer:** C

keyword said "enable new feature " for doing this action you should jailbreaking the mobile or root

upvoted 3 times

🗳️ 👤 **MsZrogas** 10 months ago

You must jailbreak the phone first before you can sideload apps.

upvoted 2 times

🗳️ 👤 **FrozenCarrot** 9 months, 3 weeks ago

No, you dont have to, for example, you can sideload apps by ADB on an android phone

upvoted 3 times

🗳️ 👤 **FrozenCarrot** 9 months, 2 weeks ago

Sideloading can also allow the installation of unauthorized apps, but jailbreaking typically provides deeper access to the system for more extensive modifications.

So i will go for C

upvoted 1 times

🗳️ 👤 **Sama001** 10 months ago

**Selected Answer:** D

Side Loading: The process of installing applications on a device without the use of official software distribution channels.

upvoted 1 times

🗳️ 👤 **850bc48** 9 months, 2 weeks ago

to enable this you would need to jail break the device first.

upvoted 2 times

🗨️ 👤 **jafyyy** 10 months, 1 week ago

Jailbraking

upvoted 1 times

🗨️ 👤 **Neno232** 10 months, 2 weeks ago

**Selected Answer: C**

Jailbreaking is the answer.

upvoted 2 times

Which of the following phases of an incident response involves generating reports?

- A. Recovery
- B. Preparation
- C. Lessons learned
- D. Containment

**Correct Answer:** C

*Community vote distribution*

C (100%)

🗲️ 👤 **jafyyy** 10 months, 1 week ago

C. Lessons Learned - focused on documentation and learning from the incident to improve future responses.  
upvoted 4 times

🗲️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: C**

C. GPT  
upvoted 3 times



Which of the following methods would most likely be used to identify legacy systems?

- A. Bug bounty program
- B. Vulnerability scan
- C. Package monitoring
- D. Dynamic analysis

**Correct Answer:** B

Community vote distribution

B (100%)

🗨️ 👤 **Murtuza** 8 months, 2 weeks ago

**Selected Answer: B**

The method most likely used to identify legacy systems is:

B. Vulnerability scan.

A vulnerability scan assesses systems for known vulnerabilities, outdated software versions, and unsupported systems. This makes it an effective way to identify legacy systems that may no longer be receiving security updates or support.

A. Bug bounty program: This focuses on crowdsourcing the identification of specific vulnerabilities but is not primarily aimed at identifying legacy systems.

C. Package monitoring: Tracks software packages for updates, but it doesn't specifically target legacy systems.

D. Dynamic analysis: Involves testing software during runtime for vulnerabilities but is not typically used to identify legacy systems.

A vulnerability scan is the most effective approach for identifying legacy systems in an environment

upvoted 4 times

🗨️ 👤 **jafyyy** 10 months, 1 week ago

C. Vulnerability Scan - can identify legacy systems as it can include outdated software versions and unpatched systems.

upvoted 1 times

🗨️ 👤 **Cyberity** 10 months, 2 weeks ago

Shouldnt the answer be Package Monitoring ?

upvoted 1 times

🗨️ 👤 **jafyyy** 10 months, 1 week ago

Package monitoring is more focused on the status of individual software packages rather than identifying entire systems that are outdated or considered legacy.

upvoted 2 times

Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns. Which of the following best describes this solution?

- A. Proxy server
- B. NGFW
- C. VPN
- D. Security zone

**Correct Answer:** C

  **jafyyy**  10 months, 1 week ago

C. VPN - provides secure remote access assuring data transmitted between remote employees and company resources is encrypted and protected from interception.

upvoted 5 times

A company allows customers to upload PDF documents to its public e-commerce website. Which of the following would a security analyst most likely recommend?

- A. Utilizing attack signatures in an IDS
- B. Enabling malware detection through a UTM
- C. Limiting the affected servers with a load balancer
- D. Blocking command injections via a WAF

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **a4e15bd** Highly Voted 10 months, 3 weeks ago

B

PDFs can be used to deliver malware such as embedded scripts or exploits. Enabling malware detection through a UTM helps to scan and block malicious content within uploaded files before they reach the server.

upvoted 15 times

🗳️ 👤 **JoeRealCool** Most Recent 2 months, 3 weeks ago

**Selected Answer: B**

I chose WAF initially and had to do some research. I'm not a big fan of this question because both a WAF and a UTM will scan .pdf files for malware, but I guess the UTM is better at it and that's why it's correct? ChatGPT said WAF and Grok said UTM.

upvoted 1 times

🗳️ 👤 **9149f41** 5 months ago

**Selected Answer: B**

Popular UTM (Unified Threat Management) tools:

Fortinet FortiGate, Sophos UTM, Cisco Meraki, WatchGuard, Palo Alto Networks, Check Point

upvoted 1 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

B. Enabling malware detection through a UTM - can scan uploaded files for malicious content.

upvoted 3 times

A security analyst developed a script to automate a trivial and repeatable task. Which of the following best describes the benefits of ensuring other team members understand how the script works?

- A. To reduce implementation cost
- B. To identify complexity
- C. To remediate technical debt
- D. To prevent a single point of failure

**Correct Answer:** D

Community vote distribution

D (100%)

🗲️ 👤 **Sol\_tyty** Highly Voted 👍 10 months, 1 week ago

NO GPT COMMENT!!!! HALLELUJAH!!!!!!

upvoted 28 times

🗲️ 👤 **Sama001** Highly Voted 👍 10 months ago

Selected Answer: D

D. To prevent a single point of failure

Other team members knowing how it works eliminates reliance on a single employee in case of script failure.

upvoted 5 times

🗲️ 👤 **c469c8e** Most Recent 🕒 10 months, 1 week ago

Script is still single point of failure

upvoted 3 times

🗲️ 👤 **jafyyy** 10 months, 1 week ago

D. To prevent a single point of failure - ensures continuity and reduces reliance on any single individual.

upvoted 2 times

🗲️ 👤 **a4e15bd** 10 months, 1 week ago

Selected Answer: D

D. Prevent Single Point of Failure

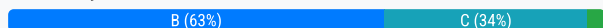
upvoted 1 times

A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems. Which of the following strategies should the company use to achieve this security requirement?

- A. Microservices
- B. Containerization
- C. Virtualization
- D. Infrastructure as code

**Correct Answer:** B

Community vote distribution



**a4e15bd** Highly Voted 10 months, 3 weeks ago

B

Containerization allows multiple applications or services to run in isolated environments on the same underlying OS. Unlike, virtualization where each VM runs its own OS, containers share the host OS kernel but keep the applications isolated from one another. This significantly reduces the number of operating systems required while maintaining security and isolation between applications.

upvoted 21 times

**1chung** Most Recent 3 weeks, 6 days ago

Selected Answer: B

B is correct

upvoted 1 times

**b0cfacf** 4 months ago

Selected Answer: B

B) Containerization is a type of virtualization, but runs on a shared operating system.

upvoted 4 times

**TmNvrWts** 4 months, 2 weeks ago

Selected Answer: B

The correct answer is:

B. Containerization

Why not the other options?

A. Microservices – Microservices is an architectural design approach that structures an application as a collection of smaller, independent services, but it does not inherently reduce the number of OS instances.

C. Virtualization – Virtualization still requires multiple OS instances (one per VM), whereas containerization shares a single OS kernel.

D. Infrastructure as Code (IaC) – IaC automates infrastructure deployment but does not specifically reduce the number of operating systems.

upvoted 2 times

**9149f41** 5 months ago

Selected Answer: B

Before Containerization:

5 Physical Servers:

Web Server (Windows OS)

Application Server (Linux OS)

Database Server (Linux OS)

Email Server (Windows OS)

File Server (Windows OS)

After Containerization:

1 Physical Server running Docker:

CopySingle Host OS

└─ Docker Engine

└─ Web Container

└─ App Container

└─ Database Container

└─ Email Container

└─ File Service Container

upvoted 3 times

🗄️ 👤 **fc040c7** 5 months ago

**Selected Answer: B**

The key phrase in this question is "reduce the number of individual operating systems" thus making containerization the better choice between virtualization and containerization. Answer B.

upvoted 3 times

🗄️ 👤 **9149f41** 5 months, 1 week ago

**Selected Answer: A**

A.

Microservices. Reasons: The company is decommissioning the physical servers and replacing them with an architecture which aligns with our answer. Containerization still requires physical servers. Even though virtualization reduces physical servers, it still requires physical servers."

upvoted 1 times

🗄️ 👤 **jbmacc** 6 months ago

**Selected Answer: B**

The correct answer is:

B. Containerization

Explanation:

Containerization allows multiple applications to run on the same operating system kernel while isolating them in separate containers. This approach:

Reduces the need for multiple individual operating systems by running applications within lightweight containers.

Improves resource efficiency and scalability.

Enhances security by isolating containers, limiting the potential impact of a compromised application.

upvoted 2 times

🗄️ 👤 **9024d4b** 6 months ago

**Selected Answer: C**

Decommissioning physical servers leads me to believe this is C

upvoted 1 times

🗄️ 👤 **a484b2b** 6 months, 3 weeks ago

**Selected Answer: B**

If the goal is reducing OS instances and enhancing application-level isolation, containerization is the better answer.

If the focus is on replacing physical servers with virtual ones, virtualization might seem plausible but doesn't fully address the isolation and security benefits containerization provides.

upvoted 1 times

🗄️ 👤 **3b1fd98** 6 months, 3 weeks ago

**Selected Answer: C**

While containers are an excellent solution for reducing infrastructure overhead, virtualization is more directly focused on consolidating physical servers into fewer operating systems, which matches the question more precisely.

upvoted 4 times

🗄️ 👤 **bctester** 6 months, 4 weeks ago

**Selected Answer: C**

Virtualization involves creating virtual versions of hardware platforms, operating systems, and storage devices. By implementing virtualization, a company can run multiple operating systems or applications on the same physical server, each in its own virtual machine (VM). This allows for: Reduced number of physical servers needed.

Centralized management of multiple OS environments.

Efficient use of hardware resources.

Isolation of applications for security purposes.

upvoted 4 times

🗲️ 👤 **Honeybadge** 7 months, 1 week ago

**Selected Answer: B**

"reduce the number of individual operating systems"

upvoted 3 times

🗲️ 👤 **braveheart22** 7 months, 2 weeks ago

**Selected Answer: C**

The correct answer is C. Virtualization.

Virtualization involves running multiple virtual machines (VMs) on a single physical server, allowing an organization to consolidate multiple operating systems and workloads onto fewer physical servers. This reduces the number of physical machines needed while still providing isolated environments for different applications, services, or operating systems.

upvoted 2 times

🗲️ 👤 **jsmthy** 9 months ago

**Selected Answer: B**

Containerization allows fewer Operating Systems.

Sometimes this question comes with fewer physical servers, resulting in virtualization.

Take steps to ensure you read the question carefully.

upvoted 3 times

🗲️ 👤 **jafyyy** 10 months, 1 week ago

B. Containerization - is more appropriate as it allows multiple applications to run on a single OS, whereas virtualization involves running multiple OS on same physical hardware.

upvoted 1 times

🗲️ 👤 **scoobysnack209** 10 months, 1 week ago

B. Containerization like "docker" container.

upvoted 1 times

An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Choose two.)

- A. Disable default accounts.
- B. Add the server to the asset inventory.
- C. Remove unnecessary services.
- D. Document default passwords.
- E. Send server logs to the SIEM.
- F. Join the server to the corporate domain.

**Correct Answer:** AC

*Community vote distribution*

AC (100%)

🗲️ 👤 **tripletripe805692** 5 months, 2 weeks ago

**Selected Answer:** AC

AC is correct. both actions make the server less vulnerable.

upvoted 1 times

🗲️ 👤 **jafyyy** 10 months, 1 week ago

AC - these options ensure the server is secure before deployment.

upvoted 3 times

🗲️ 👤 **a4e15bd** 10 months, 1 week ago

**Selected Answer:** AC

A&C are correct

upvoted 3 times



A Chief Information Security Officer would like to conduct frequent, detailed reviews of systems and procedures to track compliance objectives. Which of the following will be the best method to achieve this objective?

- A. Third-party attestation
- B. Penetration testing
- C. Internal auditing
- D. Vulnerability scans

**Correct Answer:** C

Community vote distribution

C (100%)

🗲️ 👤 **MarysSon** 2 months, 4 weeks ago

**Selected Answer: C**

It's important to read and consider all adjectives contained in the questions. Here, a key word is frequent. A and B would not be done frequently. D would not capture all compliance objectives. Only C remains, and it covers stated objectives.

upvoted 3 times

🗲️ 👤 **jafyyy** 10 months, 1 week ago

C. Internal Auditing

upvoted 2 times

🗲️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: C**

C. GPT

upvoted 2 times

Which of the following security concepts is accomplished with the installation of a RADIUS server?

- A. CIA
- B. AAA
- C. ACL
- D. PEM

**Correct Answer:** B

Community vote distribution

B (100%)

  **a4e15bd**  10 months, 3 weeks ago

B

Other being a server, RADIUS is a networking protocol that provides centralized authentication, authorization and accounting for users who connect and use a network service.



upvoted 11 times

  **Glacier88**  10 months, 1 week ago

**Selected Answer: B**

RADIUS (Remote Authentication Dial-In User Service) is a network access server protocol that provides Authentication, Authorization, and Accounting (AAA) services.

upvoted 3 times

  **jafyyy** 10 months, 1 week ago

B. Remote Authentication Dial-In User Service protocol is used for AAA (Authentication, Authorization & Accounting)

upvoted 2 times

  **examreviewer** 10 months, 2 weeks ago

**Selected Answer: B**

RADIUS is a networking protocol that provides centralized authentication, authorization and accounting - AAA

upvoted 3 times

  **examreviewer** 10 months, 2 weeks ago

RADIUS is a networking protocol that provides centralized authentication, authorization and accounting - AAA

upvoted 3 times

  **internslayer** 10 months, 2 weeks ago

**Selected Answer: B**

B. AAA

upvoted 3 times

After creating a contract for IT contractors, the human resources department changed several clauses. The contract has gone through three revisions. Which of the following processes should the human resources department follow to track revisions?

- A. Version validation
- B. Version changes
- C. Version updates
- D. Version control

**Correct Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **Dlove** Highly Voted 10 months, 3 weeks ago

**Selected Answer: D**

D. Version Control

Version control involves maintaining a record of changes made to the document, including details such as who made the changes, when they were made, and what was modified. This process ensures that all revisions are documented, and the most current version of the contract is clearly identified.

upvoted 10 times

🗳️ 👤 **kamax5400** Most Recent 4 months ago

**Selected Answer: D**

Version Control is the correct answer.

upvoted 1 times

🗳️ 👤 **PAWarriors** 9 months, 3 weeks ago

**Selected Answer: D**

Version Control tracks and manages changes in documents, software, and other files and ensures that changes do not create chaos and helps with track of it.

upvoted 2 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

D. Version Control

upvoted 1 times

The executive management team is mandating the company develop a disaster recovery plan. The cost must be kept to a minimum, and the money to fund additional internet connections is not available. Which of the following would be the best option?

- A. Hot site
- B. Cold site
- C. Failover site
- D. Warm site

**Correct Answer:** B

*Community vote distribution*

B (100%)

🗲️ 👤 **Mitch717** 7 months, 1 week ago

**Selected Answer: B**

The lowest cost solution is a Cold Site.

upvoted 4 times

🗲️ 👤 **jafyyy** 10 months, 1 week ago

B. Cold Site is a facility with minimal infrastructure used as a backup location

upvoted 1 times

🗲️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: B**

B. GPT

upvoted 2 times

An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website. Which of the following should the administrator do?

- A. Deploy multifactor authentication.
- B. Decrease the level of the web filter settings.
- C. Implement security awareness training.
- D. Update the acceptable use policy.

**Correct Answer:** C

Community vote distribution

C (100%)

Anyio 5 months ago

**Selected Answer: C**

C. Implement security awareness training.

Explanation:

The increase in blocked page messages indicates employees are attempting to visit spoofed or malicious websites, possibly due to phishing attempts. Security awareness training can educate employees on recognizing phishing attempts, spoofed websites, and other social engineering tactics to reduce the likelihood of future incidents.

Other Options:

- A. Deploy multifactor authentication: While MFA is essential for account security, it does not address the issue of employees unknowingly attempting to access spoofed websites.
- B. Decrease the level of the web filter settings: This would make the organization more vulnerable to threats by allowing access to malicious sites.
- D. Update the acceptable use policy: Updating policies is good practice but won't directly address the root cause of employees falling for spoofed sites.

upvoted 3 times

jafyyy 10 months, 1 week ago

C. Implement security awareness training

This helps employees recognize and avoid phishing & spoofed websites.

upvoted 4 times

qacollin 10 months, 3 weeks ago

C. GPT

upvoted 3 times

abrarnd825 7 months, 2 weeks ago

There is no way you can use GPT during actual exam, so please study if you don't know the answer.

upvoted 5 times

fd4ea1a 7 months, 1 week ago

No but my teacher literally says that you should use both Exam topics and Chat GPT to verify. Because Exam Topics has wrong answers also. So verifying with Chat GPT is good. Go to question 77 and you'll see one of the answers says Virus but its WORM.

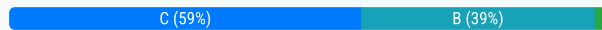
upvoted 5 times

Which of the following teams is best suited to determine whether a company has systems that can be exploited by a potential, identified vulnerability?

- A. Purple team
- B. Blue team
- C. Red team
- D. White team

**Correct Answer:** C

Community vote distribution



**jbmacc** Highly Voted 6 months ago

**Selected Answer: B**

The correct answer is:

B. Blue team

Explanation:

The blue team is responsible for defending the organization's systems, monitoring for vulnerabilities, and ensuring that systems are secure against potential threats. They:

Conduct vulnerability assessments to identify exploitable weaknesses.

Evaluate the impact of identified vulnerabilities on the organization's systems.

Work to mitigate risks and patch vulnerabilities.

upvoted 6 times

**jennyka76** Highly Voted 3 months, 3 weeks ago

**Selected Answer: C**

A red team is best suited to determine if a company has systems that can be exploited by a potential, identified vulnerability.

Explanation:

Red team role:

Red teams simulate attacks from a malicious attacker's perspective. They actively probe systems and networks to find and exploit vulnerabilities.

This allows them to identify weaknesses in an organization's security posture.

Blue team role:

Blue teams focus on defending the organization by monitoring for threats, identifying vulnerabilities, and implementing security measures to mitigate risks. While they may identify vulnerabilities during their monitoring process, their primary goal is to protect the system, not actively exploit them.

upvoted 5 times

**27035bb** Most Recent 2 weeks, 3 days ago

**Selected Answer: C**

The answer is C

upvoted 1 times

**1chung** 3 weeks, 6 days ago

**Selected Answer: C**

Correct answer is C

upvoted 1 times

**TmNvrWts** 4 months, 2 weeks ago

**Selected Answer: C**

Blue team does not exploit systems. They def

upvoted 2 times

**test\_arrow** 4 months, 2 weeks ago

**Selected Answer: C**

The Red team is responsible for simulating real-world attacks to identify vulnerabilities that could be exploited by attackers. They act as ethical hackers, attempting to exploit weaknesses in a company's systems to assess security risks. Since the question asks about determining whether systems can be exploited by a potential vulnerability, the Red team is the best choice.

upvoted 3 times

🗳️ 👤 **Whiskey\_** 4 months, 3 weeks ago

**Selected Answer: A**

While the Blue Team knows the insides of the system and thus it's weaknesses against identified vulnerabilities, the Red Team is capable of testing and confirming the potential exploit.

The combination of both is the Purple Team.

upvoted 1 times

🗳️ 👤 **AriGarcia** 5 months ago

**Selected Answer: C**

Red teams specifically focus on offensive security tactics, which includes exploiting vulnerabilities to demonstrate security weaknesses. They are trained to think and act like attackers, making them ideal for this particular task.

upvoted 2 times

🗳️ 👤 **Anyio** 5 months ago

**Selected Answer: B**

B. Blue team

Explanation:

The blue team is responsible for the organization's defensive security measures. They monitor, detect, and respond to threats, as well as assess vulnerabilities in systems. In this case, the blue team is best suited to determine whether the company has exploitable systems related to a specific, identified vulnerability.

Other Options:

A. Purple team: A collaboration between red and blue teams to improve overall security, but they don't focus specifically on identifying exploitable systems.

C. Red team: Focused on offensive security and simulating attacks but not tasked with vulnerability assessment or mitigation.

D. White team: Typically oversees the rules of engagement for red and blue team activities, but they are not directly involved in technical vulnerability analysis.

upvoted 4 times

🗳️ 👤 **pindinga1** 5 months, 1 week ago

**Selected Answer: B**

Blue team defend organization and evaluate risk

upvoted 1 times

🗳️ 👤 **tripletripe805692** 5 months, 2 weeks ago

**Selected Answer: C**

C is correct.

One of the main reasons Red-Team exists is to test an organization's security posture.

The Blue-Team will use the report/findings provided by the Red Team to harden the security infrastructure.

upvoted 3 times

🗳️ 👤 **amccert** 5 months, 2 weeks ago

**Selected Answer: C**

Red Team would be assessing if its a vector to take advantage of offensively

upvoted 1 times

🗳️ 👤 **laternak26** 6 months, 2 weeks ago

**Selected Answer: B**

The Blue team performs vulnerability scanning as part of its defensive responsibilities to identify and mitigate risks.

The Red team goes a step further by exploiting the vulnerabilities identified by the Blue team (or discovered through other means) to see if they can be used to successfully compromise the organization.

upvoted 4 times

🗳️ 👤 **Oca8ee9** 6 months, 3 weeks ago

**Selected Answer: C**

Red Team conducts offensive penetration testing mimicking what an intrusion will do.

upvoted 1 times

🗨️ 👤 **kambam** 6 months, 4 weeks ago

**Selected Answer: C**

Red Team is the correct choice since it is asking to identify weak points and vulnerabilities in the systems. Red team will simulate a real-world attack to test the systems and see where vulnerabilities are.

upvoted 1 times

🗨️ 👤 **AndyK2** 7 months ago

**Selected Answer: B**

Interesting - both Claude and ChatGPT suggest Blue Team.

Blue Team:

Focuses on defensive security

Identifies vulnerabilities in existing systems

Conducts internal vulnerability assessments

Proactively searches for potential weaknesses

Aims to protect and strengthen organizational systems

Red Team:

Focuses on offensive security

Simulates external attack scenarios

Attempts to exploit vulnerabilities

Tries to breach system defenses

Approaches systems from an attacker's perspective

While both teams deal with vulnerabilities, the Blue team is specifically responsible for identifying and determining whether systems can be exploited.

They assess vulnerabilities systematically and work to remediate them before they can be used maliciously.

The Red team would be more likely to actually exploit those vulnerabilities to test defenses, but they aren't primarily responsible for the initial identification and assessment of potential system exploits.

upvoted 3 times

🗨️ 👤 **3b6be6b** 7 months ago

**Selected Answer: B**

B. Blue team

Here's why:

Blue team is responsible for defensive security. Their main role is to monitor, detect, and respond to threats and vulnerabilities within the organization's systems. This includes assessing the company's systems to identify weaknesses that could be exploited by a known vulnerability and implementing measures to address them.

upvoted 4 times



A company is reviewing options to enforce user logins after several account takeovers. The following conditions must be met as part of the solution:

- Allow employees to work remotely or from assigned offices around the world.
- Provide a seamless login experience.
- Limit the amount of equipment required.

Which of the following best meets these conditions?

- A. Trusted devices
- B. Geotagging
- C. Smart cards
- D. Time-based logins

**Correct Answer:** A

*Community vote distribution*

A (100%)

  **a4e15bd**  10 months, 3 weeks ago

A

Trusted devices allow users to log in seamlessly from devices that are already recognized and trusted by the system. It supports remote and global access as the device does not need to be in a specific location or equipped with extra hardware. It minimizes the need for additional equipment and provides for a streamlined login experience.

upvoted 11 times

  **Glacier88**  10 months ago

**Selected Answer: A**

Trusted devices.

Remote work: Trusted devices allow employees to work from any location, including remotely or from assigned offices.

Seamless login: Once a device is trusted, users can log in without requiring additional authentication factors, providing a seamless experience.

Limited equipment: Trusted devices typically require minimal additional equipment, such as a mobile app or a hardware token.

Other options don't meet all the conditions:


Geotagging: While it can provide location-based restrictions, it might not be practical for a company with employees working from various locations worldwide.

Smart cards: These require physical cards and readers, which might be inconvenient for remote workers and could increase the amount of equipment required.

Time-based logins: While they can add a layer of security, they might not be ideal for a company with employees working in different time zones.

Trusted devices offer a balance between security and convenience, making them the most suitable solution for the company's requirements.

upvoted 3 times

  **jafyyy** 10 months, 1 week ago

A. Trusted Devices - allows users to log in from various location using their own trusted devices without requiring additional hardware.

upvoted 1 times

Which of the following methods can be used to detect attackers who have successfully infiltrated a network? (Choose two.)

- A. Tokenization
- B. CI/CD
- C. Honeypots
- D. Threat modeling
- E. DNS sinkhole
- F. Data obfuscation

**Correct Answer:** CE

Community vote distribution

CE (100%)

  **a4e15bd**  10 months, 3 weeks ago

C&E

Honeypot attracts and traps attacker and DNS sinkhole redirects malicious domain name queries to a controlled server to detect and block communication between compromised host and their C2 servers.

upvoted 17 times

  **Anyio**  5 months ago

**Selected Answer:** CE

C. Honeypots and E. DNS sinkhole

Explanation:

Honeypots: These are decoy systems set up to lure attackers and observe their behavior once they've infiltrated the network. They help detect unauthorized activity and gather intelligence about the attack.

DNS sinkhole: This redirects malicious traffic (e.g., communication with command-and-control servers) to a controlled environment, allowing detection of compromised systems within the network.

Other Options:

- A. Tokenization: Focuses on replacing sensitive data with tokens for security but doesn't help in detecting attackers.
- B. CI/CD: Refers to Continuous Integration/Continuous Deployment processes, which are unrelated to intrusion detection.
- D. Threat modeling: Identifies potential risks during system design but doesn't detect attackers already in the network.
- F. Data obfuscation: Hides sensitive data but does not help with detecting network intrusions.

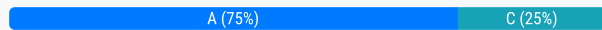
upvoted 2 times

A company wants to ensure that the software it develops will not be tampered with after the final version is completed. Which of the following should the company most likely use?

- A. Hashing
- B. Encryption
- C. Baselines
- D. Tokenization

**Correct Answer:** A

Community vote distribution



🗳️ **laternak26** 6 months, 2 weeks ago

**Selected Answer: A**

A. Hashing:

Hashing is a technique used to generate a unique, fixed-size value (hash) based on the contents of a file, such as a software application. After the final version of the software is completed, the company can create a hash of the software file and store it securely. Whenever the software is accessed or distributed, the company can recalculate the hash and compare it to the original hash. If the hashes match, the file has not been tampered with. This provides a way to verify the integrity of the software and ensure that it has not been altered after the final version.

Why not C. Baselines:

Baselines refer to a set of standards or configurations for systems and software that are considered secure. While baselines can be useful for ensuring that systems meet security standards, they do not directly address ensuring that the software has not been tampered with after it is finalized. Baselines help with ongoing security practices rather than tamper detection.

upvoted 2 times

🗳️ **3b1fd98** 6 months, 3 weeks ago

**Selected Answer: C**

C. Baselines refer to a reference point or a final version of a system or software that is used as a standard for comparison. Once a baseline is established, any changes to the software can be detected by comparing it against the baseline version. This is crucial for ensuring that the software has not been tampered with after the final version is completed. The baseline provides a known and trusted version of the software, making it easier to spot any unauthorized modifications or tampering.

upvoted 1 times

🗳️ **jafyyy** 10 months, 1 week ago

A

Hashing ensures integrity of software by detecting any unauthorized changes or tampering after its final version.

upvoted 2 times

🗳️ **qacollin** 10 months, 3 weeks ago

**Selected Answer: A**

A. GPT

upvoted 3 times

An organization completed a project to deploy SSO across all business applications last year. Recently, the finance department selected a new cloud-based accounting software vendor. Which of the following should most likely be configured during the new software deployment?

- A. RADIUS
- B. SAML
- C. EAP
- D. OpenID

**Correct Answer:** B

Community vote distribution

B (100%)

 **a4e15bd** Highly Voted 10 months, 3 weeks ago

B

SAML is widely used protocol for enabling SSO across different applications and systems, particularly in enterprise environments. It allows users to authentication once and gain access to multiple application, including cloud based services.

RADIUS is typically used for network access authentication and is not generally used for SSO with cloud based applications.

EAP is used for network authentication protocols particularly in wireless networks and does not apply to SSO.


OpenID is an identity layer on top of OAuth 2.0 for authentication but is less commonly used in enterprise environments compared to SAML for SSO.  
upvoted 10 times

 **Robuste7** Most Recent 4 months, 3 weeks ago

**Selected Answer: B**

SAML (Security Assertion Markup Language).

SAML is an open standard used in cybersecurity for authentication and authorization  
upvoted 2 times

 **jafyyy** 10 months, 1 week ago

B

SAML

upvoted 2 times

A user, who is waiting for a flight at an airport, logs in to the airline website using the public Wi-Fi, ignores a security warning and purchases an upgraded seat. When the flight lands, the user finds unauthorized credit card charges. Which of the following attacks most likely occurred?

- A. Replay attack
- B. Memory leak
- C. Buffer overflow attack
- D. On-path attack

**Correct Answer:** D

Community vote distribution

D (100%)


 **Kingamj** Highly Voted 10 months, 2 weeks ago

**Selected Answer: D**

ChatGPT

An on-path attack, also known as a man-in-the-middle (MITM) attack, occurs when an attacker intercepts the communication between two parties (in this case, the user and the airline's website). Since the user was on a public Wi-Fi network and ignored security warnings, it's possible that the attacker was able to intercept the credit card information during the transaction, leading to unauthorized charges.

upvoted 7 times

 **Glacier88** Highly Voted 10 months ago

**Selected Answer: D**

On-path attack.

Public Wi-Fi: Public Wi-Fi networks are often unsecured and can be easily compromised by attackers.

Man-in-the-middle: An on-path attack involves an attacker intercepting communication between the user and the airline website, potentially capturing sensitive information like credit card details.

Security warning: The ignored security warning likely indicated that the connection was not secure, making the user vulnerable to an on-path attack.

Replay attacks, memory leaks, and buffer overflow attacks are less likely in this scenario. Replay attacks involve reusing captured data, but it's not clear how that would have led to unauthorized charges. Memory leaks and buffer overflow attacks are typically associated with software vulnerabilities, not network-based attacks.


upvoted 6 times

 **test\_arrow** Most Recent 4 months, 2 weeks ago

**Selected Answer: D**

on-path is the new man in the middle

upvoted 1 times

 **jafyyy** 10 months, 1 week ago

D

This attack results from an attacker's interception of data sent over public WI-FI.

upvoted 1 times

A network engineer deployed a redundant switch stack to increase system availability. However, the budget can only cover the cost of one ISP connection. Which of the following best describes the potential risk factor?

- A. The equipment MTBF is unknown.
- B. The ISP has no SLA.
- C. An RPO has not been determined.
- D. There is a single point of failure.

**Correct Answer:** D

Community vote distribution

D (100%)

  **a4e15bd**  10 months, 3 weeks ago

D

Since the budget only allows for one ISP connection, this create a single point of failure for the network connectivity.

upvoted 8 times

  **dhewa**  8 months, 3 weeks ago

**Selected Answer: D**

Even though the switch stack is redundant, having only one ISP connection means that if the ISP connection fails, the entire network could go down, creating a single point of failure. This undermines the redundancy provided by the switch stack.

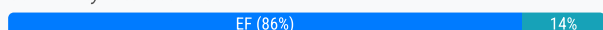
upvoted 6 times

A network team segmented a critical, end-of-life server to a VLAN that can only be reached by specific devices but cannot be reached by the perimeter network. Which of the following best describe the controls the team implemented? (Choose two.)

- A. Managerial
- B. Physical
- C. Corrective
- D. Detective
- E. Compensating
- F. Technical
- G. Deterrent

**Correct Answer:** EF

Community vote distribution



**a4e15bd** **Highly Voted** 10 months, 3 weeks ago

EF

Technical controls involve the use of technology to manage or mitigate risks. By segmenting the server into VALN and restricting access to specific devices, the network team has employed a technical control here.

Compensating controls are alternative measures in place to address a risk when the primary control is not feasible which in these case segmenting the server into VLAN and limiting access can be seen as compensating control.

upvoted 8 times

**ProudFather** **Most Recent** 6 months, 3 weeks ago

**Selected Answer:** BF

The network team implemented two types of controls:

Physical: Segmenting the server to a VLAN is a physical control, as it restricts network access to the server.

Technical: Limiting access to the VLAN only to specific devices is a technical control, as it involves configuring network devices to enforce access rules.

The other options are not applicable

upvoted 1 times

**Eracle** 6 months, 1 week ago

I don't think it is a physical control, it seems more logical because of the definition of VLAN, Virtual LAN.

upvoted 2 times

**Glacier88** 10 months ago

**Selected Answer:** EF

E. Compensating and F. Technical.

Compensating: The segmentation serves as a compensating control, mitigating the risk associated with using an end-of-life server by isolating it from the perimeter network.

Technical: The VLAN configuration is a technical control, implementing a network-based security measure to restrict access to the critical server.

The other options are not applicable in this scenario:

Managerial: Managerial controls are policies, procedures, and guidelines established by management.

Physical: Physical controls are physical barriers or safeguards, such as locks, fences, or security guards.

Corrective: Corrective controls are implemented to address a security incident or vulnerability after it has occurred.

Detective: Detective controls are designed to detect security incidents or vulnerabilities.

Deterrent: Deterrent controls are designed to discourage unauthorized access or malicious activity.

upvoted 3 times

**b82faaf** 10 months, 3 weeks ago

**Selected Answer: EF**

E. Compensating and

F. Technical (aka technological)

upvoted 3 times

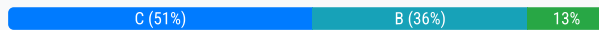


A threat actor was able to use a username and password to log in to a stolen company mobile device. Which of the following provides the best solution to increase mobile data security on all employees' company mobile devices?

- A. Application management
- B. Full disk encryption
- C. Remote wipe
- D. Containerization

**Correct Answer:** C

Community vote distribution



**a4e15bd** Highly Voted 10 months, 3 weeks ago

I would go with B. Here is the reasoning, for an immediate response to a compromised device, remote swipe may be the best option. But the question asks "What is the best solution to increase mobile data security on all employee's devices?" Implementing FDE across all company devices raises the baseline security for the entire organization ensuring that data on all devices is protected. With compromised credentials a remote swipe might even be too late, if you don't find out fast enough that the device has been stolen.

upvoted 24 times

**EfaChux** 10 months, 2 weeks ago

Threat actor already has accessed the device using username and password, encryption is useless at this point.

upvoted 18 times

**TmNvrWts** 4 months, 2 weeks ago

EfaChux is sooo right. Encryption is only useful if the device is in "rest" state which means its turned off or logged out. In this case the attacker has everything, the last thing we can do is to prevent the attacker afterwards from owning everything with wipein.

upvoted 4 times

**jafyyy** 10 months, 1 week ago

The data on the device remains protected by encryption even if the threat actor has gained access to the username/password.

upvoted 4 times

**jsmthy** 9 months ago

This is wrong. Full disk encryption does not protect against malicious access if the attacker has a password. Otherwise, the user would not have access to their own files since they don't have the password.

A remote wipe is the only way out for a stolen device with stolen credentials.

upvoted 6 times

**b82faaf** Highly Voted 10 months, 3 weeks ago

**Selected Answer: B**

B. Full disk encryption (FDE).

The question was not asking about the single phone that was stolen (in which case a remote wipe may work after the fact); rather, it asks for "the best solution to increase mobile data security on all employees' company mobile devices".

upvoted 13 times

**1chung** Most Recent 3 weeks, 6 days ago

**Selected Answer: B**

Correct answer is B

upvoted 1 times

**9ce65e3** 2 months, 2 weeks ago

**Selected Answer: B**

Analysis: The threat actor's ability to log in suggests the device's data was accessible post-authentication. Full disk encryption (B) is the best solution, as it ensures all data (corporate and personal) is encrypted and inaccessible without the encryption key, even if credentials are compromised. Containerization (D) is strong but limited to specific data, remote wipe (C) is reactive, and application management (A) doesn't address data protection directly. For broader mobile data security, encryption is proactive and comprehensive.

Final Answer: B. Full disk encryption

upvoted 1 times

🗨️ 👤 **Linas312** 2 months, 3 weeks ago

**Selected Answer: D**

The actual answer is MDM, but not here

A. irrelevant

B. also irrelevant, the actor has already signed in, the encryption is useless at this point

C. is more of reaction rather than preventive.

Either its B even though technically wrong, or D which is usually paired with MDM.. too many questions like this on these "Theory" exams..

Going with D, closest to the actual answer for this situation and scenario

upvoted 1 times

🗨️ 👤 **Anyio** 5 months ago

**Selected Answer: B**

B. Full disk encryption

Explanation:

Full disk encryption ensures that all data on a mobile device is encrypted and cannot be accessed without proper authentication. Even if a device is lost or stolen, the threat actor cannot access the data without the encryption key, adding a critical layer of protection.

Other Options:

A. Application management: Manages apps on devices but does not directly secure the data stored on the device.

C. Remote wipe: Allows erasing data on lost devices but is reactive, requiring the device to be online and detected. It is not a preventative measure for data security.

D. Containerization: Segregates personal and corporate data but doesn't protect the entire device, leaving other areas vulnerable.

upvoted 1 times

🗨️ 👤 **jbmacc** 6 months ago

**Selected Answer: D**

The correct answer is:

D. Containerization

Explanation:

Containerization is the best solution to enhance mobile data security in this scenario because it:

Creates a secure, isolated environment for company data and applications on mobile devices.

Ensures that even if a device is compromised, personal and corporate data remain segregated, reducing the risk to sensitive corporate data.

Allows for secure access and management of corporate resources without impacting personal data on the device.

upvoted 3 times

🗨️ 👤 **cab08df** 4 months, 3 weeks ago

I disagree, the question said company owned device, not (BYOD) device. Hence it should already be restricted, little to no personal data should be on the device.

upvoted 1 times

🗨️ 👤 **1f2b013** 6 months, 2 weeks ago

**Selected Answer: C**

Remote wipe allows an organization to erase all data on the device remotely, ensuring that even if a threat actor gains physical access and credentials, they cannot access the company data.

upvoted 4 times

🗨️ 👤 **0ca8ee9** 6 months, 3 weeks ago

**Selected Answer: C**

Full disk encryption means nothing once the attacker logs in. Remote wipe is the most appropriate response.

upvoted 7 times

🗨️ 👤 **viktordlyi** 7 months ago

**Selected Answer: B**

The answer is B. The question is what should they do to increase the security on employees phone. The question is not saying what should they do with the stolen phone!!

upvoted 2 times

🗨️ 👤 **TriBiT** 7 months ago

**Selected Answer: C**

encryption means nothing if they are in using a username and password - remote wipe is need to protect the organization

upvoted 6 times

🗨️ 👤 **cyberWoof** 7 months, 3 weeks ago

**Selected Answer: B**

The condition is "solution to increase mobile data security on all employees' company mobile devices", and that solution is 'B' - FDE

upvoted 1 times

🗨️ 👤 **3dk1** 7 months, 4 weeks ago

**Selected Answer: D**

Even if a threat actor gains access to the device, they would still need to bypass additional authentication mechanisms to access the data within the container.

IT administrators can enforce security policies within the container, such as restricting copy/paste functions, disabling screenshots, and requiring strong authentication.

upvoted 2 times

🗨️ 👤 **3dk1** 7 months, 4 weeks ago

It could also be A. This question is rough.....

upvoted 1 times

🗨️ 👤 **e157c7c** 8 months ago

**Selected Answer: C**

To those picking FDE because you wouldn't wipe all users' phones, this is missing the boat. You are implementing a remote wipe solution, NOT wiping everyones' phones. Given the example provided, I can't see anything but C being correct here.

upvoted 2 times

🗨️ 👤 **Murtuza** 8 months, 1 week ago

**Selected Answer: B**

B makes sense

upvoted 1 times

🗨️ 👤 **paytenj10** 8 months, 1 week ago

It says "on ALL employees devices" You aren't going to full wipe every employees mobile devices when only one has been infiltrated. Full disk encryption will increase security going forward.

upvoted 1 times

🗨️ 👤 **c7b3ff0** 8 months, 2 weeks ago

**Selected Answer: C**

I'm gonna keep it short here because Ty already explained it perfectly, but it's not B.

"If someone steals a phone AND has your credentials, the device has already been pwned" and remote wiping the stolen device is pretty much your only option. You just have to hope it gets reported and the security team gets to it fast enough. There are other measures they could have taken beforehand that would make the attacker having the username and password less devastating. This would be a big "oops" moment, all you can do is damage control.

upvoted 1 times

Which of the following best describes the risk present after controls and mitigating factors have been applied?

- A. Residual
- B. Avoided
- C. Inherent
- D. Operational

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **AndyK2** 7 months ago

**Selected Answer: A**

A. Residual

Rationale:

Residual risk is the remaining risk after implementing security controls and mitigation strategies

Represents the risk that persists even after applying protective measures

Cannot be completely eliminated, only reduced to an acceptable level

Reflects the potential impact and likelihood of a risk after implementing safeguards

upvoted 1 times

🗳️ 👤 **Mitch717** 7 months, 1 week ago

**Selected Answer: A**

Residual. The amount of money in my account after my bills are paid.

upvoted 4 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

A

This is the risk that remains after controls and mitigation efforts have been applied.

upvoted 2 times

🗳️ 👤 **Ina22** 10 months, 1 week ago

A. Residual

upvoted 3 times

A software development team asked a security administrator to recommend techniques that should be used to reduce the chances of the software being reverse engineered. Which of the following should the security administrator recommend?

- A. Digitally signing the software
- B. Performing code obfuscation
- C. Limiting the use of third-party libraries
- D. Using compile flags

**Correct Answer:** B

Community vote distribution

B (100%)

  **a4e15bd**  10 months, 3 weeks ago

B Performing code obfuscation

Code obfuscation deliberately makes the code more difficult to understand. This involves renaming variables, methods etc. Altering the code structure in ways that do not affect functionality but make reverse engineering much harder. Attacker use reverse engineering to find vulnerabilities that can be exploited or remove or bypass security protections such as encryption or anti tamper mechanisms.

upvoted 11 times

  **Anyio**  5 months ago

**Selected Answer: B**

B. Performing code obfuscation

Explanation:

Code obfuscation makes the source code harder to understand by altering its structure without changing its functionality. This technique complicates the reverse engineering process, making it more difficult for attackers to analyze and exploit the software.

Other Options:

- A. Digitally signing the software: Ensures the authenticity and integrity of the software but does not prevent reverse engineering.
  - C. Limiting the use of third-party libraries: Reduces dependency risks but does not directly address reverse engineering.
  - D. Using compile flags: Can improve performance or security during compilation but is not designed to prevent reverse engineering.
- upvoted 4 times

Which of the following is a possible factor for MFA?

- A. Something you exhibit
- B. Something you have
- C. Somewhere you are
- D. Someone you know

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **EfaChux** Highly Voted 10 months, 2 weeks ago

**Selected Answer:** B

Very tricky with the the D option, which says "someone" instead of something you know, which will be the password option.  
upvoted 5 times

🗳️ 👤 **dbrowndiver** Most Recent 5 months, 1 week ago

**Selected Answer:** B

B. Something you have

Why It's Correct:

This is a standard and widely accepted MFA factor.

Examples include:

Smart cards.

Hardware tokens.

Authentication apps generating one-time codes.

"Something you have" is a definitive MFA factor and fits perfectly within the accepted categories.

upvoted 1 times

🗳️ 👤 **557641e** 6 months, 2 weeks ago

**Selected Answer:** B

MFA Factors:

1. Something you know - Password, PIN, pattern
2. Something you have - Smart card, usb security key, hardware or software tokens, phone
3. Something you are - Biometric authentication, (fingerprint, iris scan, voice print)
4. Somewhere you are - Geolocation , IP address, 802.11 network

upvoted 2 times

🗳️ 👤 **VincentvdS** 4 months, 3 weeks ago

So C is also correct than?

upvoted 3 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

B

something you have like a smartphone or card is a standard factor to verify identity with MFA.

upvoted 1 times

🗳️ 👤 **mr\_reyes** 10 months, 2 weeks ago

This is a very trick question, if this is actually how its worded on the test:

Possible factors for MFA (Multi-Factor Authentication) include:

Something you have: This could be a physical device such as a smart card, a hardware token, or a smartphone app that generates one-time codes.

Incorrect Options:

Something you exhibit: This is not a standard factor in MFA. Authentication factors generally involve items or characteristics, not behavioral traits.

Someone you know: This would be a factor if its worded as "Something you know" (such as a password), but if they actually word it as "Someone you know" its not correct.

Somewhere you are: This would be a factor if its worded as "Something you are" (such as a fingerprint or retina scan), but if they actually word it as "Somewhere you are" its not correct.

upvoted 2 times

🗨️ 👤 **mr\_reyes** 10 months, 2 weeks ago

This would only make sense if they meant to say "Which of the following is not a possible factor for MFA?". Only 1 answer fits that question. Otherwise 3 answers fit the question as its stated.

upvoted 3 times

🗨️ 👤 **Crucible\_Bro** 10 months, 3 weeks ago

Something you have and something you know are both MFA factors...

upvoted 2 times

🗨️ 👤 **f48446d** 10 months, 3 weeks ago

I don't like the wording to this question. Possible factor? All 3 (know, have, and are) are part of MFA.

upvoted 3 times

Easy-to-guess passwords led to an account compromise. The current password policy requires at least 12 alphanumeric characters, one uppercase character, one lowercase character, a password history of two passwords, a minimum password age of one day, and a maximum password age of 90 days. Which of the following would reduce the risk of this incident from happening again? (Choose two.)

- A. Increasing the minimum password length to 14 characters.
- B. Upgrading the password hashing algorithm from MD5 to SHA-512.
- C. Increasing the maximum password age to 120 days.
- D. Reducing the minimum password length to ten characters.
- E. Reducing the minimum password age to zero days.
- F. Including a requirement for at least one special character.

**Correct Answer:** AF

Community vote distribution

AF (85%)


Other

 **b82faaf** Highly Voted 10 months, 3 weeks ago

**Selected Answer:** AF

Since the issue is with the passwords being easy to guess, the solution would be one that addresses password complexity (and not password history or age necessarily). Increasing the minimum length of the password and introducing a special character would be the best options for this.

upvoted 9 times

 **Anyio** Most Recent 5 months ago

**Selected Answer:** AF

The correct answers are:

- A. Increasing the minimum password length to 14 characters
- F. Including a requirement for at least one special character

Explanation:

A. Increasing the minimum password length to 14 characters: Longer passwords are harder to guess or brute-force, making them more secure.

F. Including a requirement for at least one special character: Adding special characters increases password complexity, reducing the likelihood of successful guessing or brute-force attacks.

Other Options:

B. Upgrading the password hashing algorithm from MD5 to SHA-512: This improves how passwords are stored but doesn't directly prevent weak passwords from being used.

upvoted 2 times

 **AndyK2** 7 months ago

**Selected Answer:** AF

- A. Increasing the minimum password length to 14 characters
- F. Including a requirement for at least one special character

Rationale:

Increasing password length:

Exponentially increases password complexity

Makes brute-force attacks more difficult

Longer passwords are harder to guess

Adding special character requirement:



Increases password entropy  
Adds complexity to password creation  
Reduces predictability of password patterns

Why other options are less effective:

Upgrading hash algorithm (B) improves storage security but doesn't directly prevent weak passwords  
Increasing maximum password age (C) doesn't improve password strength  
Reducing password length (D) weakens password security  
Reducing minimum password age (E) allows more frequent password changes, which can lead to weaker passwords

The goal is to create passwords that are both complex and memorable, making them resistant to both guessing and brute-force attacks.  
upvoted 1 times

  **viktorrdlyi** 7 months ago



**Selected Answer: BF**

As mentioned below  
upvoted 1 times

  **viktorrdlyi** 7 months ago

**Selected Answer: B**

MD-5 have a collision chance!  
upvoted 1 times

  **jafyyy** 10 months, 1 week ago

AF  
These options add further complexity.  
upvoted 1 times

A user downloaded software from an online forum. After the user installed the software, the security team observed external network traffic connecting to the user's computer on an uncommon port. Which of the following is the most likely explanation of this unauthorized connection?

- A. The software had a hidden keylogger.
- B. The software was ransomware.
- C. The user's computer had a fileless virus.
- D. The software contained a backdoor.

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **jafyyy** Highly Voted 10 months, 1 week ago

D

The software contained a backdoor bypassing normal authentication method.

upvoted 6 times

 **AndyK2** Most Recent 7 months ago

**Selected Answer: D**

Backdoors are hidden access methods that allow unauthorized remote access.

upvoted 2 times

A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include:

- A starting baseline of 50% memory utilization
- Storage scalability
- Single circuit failure resilience

Which of the following best meets all of these requirements?

- A. Connecting dual PDUs to redundant power supplies
- B. Transitioning the platform to an IaaS provider
- C. Configuring network load balancing for multiple paths
- D. Deploying multiple large NAS devices for each host

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **pokii1992** Highly Voted 10 months, 1 week ago

B. Transitioning the platform to an IaaS provider

This option addresses the 50% memory utilization baseline, provides scalable storage, and typically includes built-in redundancy to handle single circuit failures. IaaS providers offer flexible resource allocation, easy scalability, and robust infrastructure with multiple layers of redundancy.

upvoted 8 times

 **Glacier88** Most Recent 10 months ago

**Selected Answer: B**

A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include:

- A starting baseline of 50% memory utilization
- Storage scalability
- Single circuit failure resilience

Which of the following best meets all of these requirements?

- A. Connecting dual PDUs to redundant power supplies
  - B. Transitioning the platform to an IaaS provider
  - C. Configuring network load balancing for multiple paths
  - D. Deploying multiple large NAS devices for each host
- upvoted 1 times

Which of the following best describes a use case for a DNS sinkhole?

- A. Attackers can see a DNS sinkhole as a highly valuable resource to identify a company's domain structure.
- B. A DNS sinkhole can be used to draw employees away from known-good websites to malicious ones owned by the attacker.
- C. A DNS sinkhole can be used to capture traffic to known-malicious domains used by attackers.
- D. A DNS sinkhole can be set up to attract potential attackers away from a company's network resources.

**Correct Answer:** C

Community vote distribution

C (100%)

  **a4e15bd** Highly Voted 10 months, 3 weeks ago

Answer C is correct

DNS sinkhole intercepts attempts to visit harmful websites and redirects them so you don't end up reaching a malicious website and keeps your computer safe.

upvoted 11 times

  **TmNvrWts** Most Recent 4 months, 2 weeks ago

**Selected Answer: C**

The correct answer is:

C. A DNS sinkhole can be used to capture traffic to known-malicious domains used by attackers.

A DNS sinkhole is a security mechanism that redirects malicious or unwanted domain requests to a controlled server, effectively preventing devices from communicating with harmful sites.

upvoted 1 times

  **scoobysnack209** 10 months, 2 weeks ago

The Answer is C, and also the same question is in Palo Alto Networks PCNSA certification.

upvoted 3 times

An incident analyst finds several image files on a hard disk. The image files may contain geolocation coordinates. Which of the following best describes the type of information the analyst is trying to extract from the image files?

- A. Log data
- B. Metadata
- C. Encrypted data
- D. Sensitive data

**Correct Answer:** B

*Community vote distribution*

B (100%)

🗲️ 👤 **Mitch717** 7 months, 1 week ago

**Selected Answer: B**

Metadata

upvoted 1 times

🗲️ 👤 **jafyyy** 10 months, 1 week ago

B

Image files contain metadata such as geolocation coordinates and other details about the image.

upvoted 1 times

🗲️ 👤 **Muhammad\_Umair** 10 months, 2 weeks ago

(B). Metadata is data about data. So, Geolocation coordinates are definitely about Metadata.

upvoted 4 times

Which of the following most likely describes why a security engineer would configure all outbound emails to use S/MIME digital signatures?

- A. To meet compliance standards
- B. To increase delivery rates
- C. To block phishing attacks
- D. To ensure non-repudiation

**Correct Answer:** D

Community vote distribution

D (100%)

  **a4e15bd**  10 months, 3 weeks ago

Answer D is correct.

S/MIME digital signatures provides a way to ensure that the email has not been altered and that it genuinely comes from the sender (Non-repudiation)  
upvoted 8 times

  **0ca8ee9**  6 months, 3 weeks ago

**Selected Answer:** D

Non-repudiation is a concept in cybersecurity that ensures a party cannot deny their actions or agreements in a transaction or communication  
upvoted 2 times

  **TrebleSmith** 10 months, 2 weeks ago

**Selected Answer:** D

Digital signatures are going to ensure non-repudiation by confirming that the email came from the user who signed it and has not been tampered with.  
upvoted 2 times

During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers. Which of the following describes an attack method that relates to printing centers?

- A. Whaling
- B. Credential harvesting
- C. Prepending
- D. Dumpster diving

**Correct Answer:** D

  **a4e15bd** Highly Voted 10 months, 3 weeks ago

D is correct.

In a printing center, sensitive documents that are improperly disposed of could be retrieved from the trash by attackers.

upvoted 10 times

Which of the following considerations is the most important regarding cryptography used in an IoT device?

- A. Resource constraints
- B. Available bandwidth
- C. The use of block ciphers
- D. The compatibility of the TLS version

**Correct Answer:** A

*Community vote distribution*

A (83%)

C (17%)

  **baronvon** Highly Voted 10 months, 1 week ago

**Selected Answer:** A

A. Resource constraints

Resource constraints are critical in IoT devices because these devices often have limited processing power, memory, and battery life. Cryptographic operations can be resource-intensive, so it's essential to choose algorithms and protocols that are efficient and suitable for the device's capabilities. Failing to consider resource constraints can lead to performance issues or even render the device unable to perform necessary cryptographic operations.

The other options are important but generally secondary to ensuring the cryptography can operate within the device's resource limitations:

B. Available bandwidth: This is relevant for data transmission but is not a primary concern for the cryptography itself.

C. The use of block ciphers: Choosing between block ciphers and stream ciphers depends on the specific use case, but resource constraints take precedence.

D. The compatibility of the TLS version: This is important for secure communications, but resource constraints must first be addressed to ensure that the device can support any chosen protocol.

upvoted 8 times

  **Gman530** Most Recent 10 months, 1 week ago

**Selected Answer:** A

IoT devices typically don't have a ton of resources to dedicate to encrypting/decrypting data.


upvoted 3 times

  **internslayer** 10 months, 2 weeks ago

**Selected Answer:** A

A: Resource Constraints



upvoted 2 times

  **nesquick0** 10 months, 2 weeks ago

**Selected Answer:** C

C. The use of block ciphers

upvoted 1 times

  **2fd1029** 9 months, 2 weeks ago

Block cipher is a concept of cryptography, not a consideration for IoT devices with regards to cryptography.



upvoted 1 times

  **nesquick0** 10 months, 2 weeks ago

**Selected Answer:** C

C. The use of block ciphers

upvoted 1 times

  **a4e15bd** 10 months, 3 weeks ago

A is correct.

IoT devices often have limited processing power, memory and battery life. This makes it crucial to choose cryptographic algorithms that are efficient and can operate within these constraints without degrading device performance.



upvoted 4 times

A coffee shop owner wants to restrict internet access to only paying customers by prompting them for a receipt number. Which of the following is the best method to use given this requirement?

- A. WPA3
- B. Captive portal
- C. PSK
- D. IEEE 802.1X

**Correct Answer:** B

Community vote distribution

B (100%)

Anyio 5 months ago

**Selected Answer: B**

B. Captive portal

Explanation:

A captive portal is a web page that users are redirected to when they connect to a network. It is commonly used in coffee shops, hotels, and other public places to enforce policies like requiring users to enter a receipt number, agree to terms of use, or log in before granting internet access.

Other Options:

- A. WPA3: A secure Wi-Fi encryption standard, but it does not offer functionality to prompt for receipt numbers or other user-specific authentication.
- C. PSK (Pre-Shared Key): Uses a shared password for network access but cannot handle individual receipt-based authentication.
- D. IEEE 802.1X: A port-based network access control protocol typically used in enterprise environments with authentication servers, but it is too complex and not suitable for this requirement.

upvoted 2 times

qacollin 10 months, 3 weeks ago

**Selected Answer: B**

B. GPT

upvoted 1 times

a4e15bd 10 months, 3 weeks ago

B Captive Portal

This will allow the coffee shop to restrict internet access by redirecting users to a web page where they must enter the receipt information to gain access.

upvoted 3 times



While performing digital forensics, which of the following is considered the most volatile and should have the contents collected first?

- A. Hard drive
- B. RAM
- C. SSD
- D. Temporary files

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **TrebleSmith** Highly Voted 10 months, 2 weeks ago

**Selected Answer: B**

When the computer powers off, anything in the RAM is going to be lost. Therefore, collecting potential evidence out of the RAM is the first thing that should be done out of these options.

upvoted 10 times

  **a4e15bd** Highly Voted 10 months, 3 weeks ago

B is correct.

You start collecting forensic contents based on the order of volatility which is from the most volatile to the least. You collect CPU, Cache and Registers first and RAM 2nd which contains active processes, open network connections, user sessions and temp data which are lost when the system is powered off. Temporary files and hard drive/SSD comes last in the order receptively.

upvoted 8 times

A hosting provider needs to prove that its security controls have been in place over the last six months and have sufficiently protected customer data. Which of the following would provide the best proof that the hosting provider has met the requirements?

- A. NIST CSF
- B. SOC 2 Type 2 report
- C. CIS Top 20 compliance reports
- D. Vulnerability report

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **ViciousAkira** Highly Voted 👍 7 months, 3 weeks ago

B. SOC 2 Type 2 report

SOC 2 stands for System and Organization Controls 2.

A SOC 2 Type 2 report provides an audit of the effectiveness of security controls over a period of time (typically 6-12 months), specifically focusing on the operating effectiveness of controls related to security, availability, processing integrity, confidentiality, and privacy. This report would demonstrate that the controls were not only in place but also effectively protecting customer data over the required period.

upvoted 7 times

🗳️ 👤 **siheom** Most Recent ⌚ 9 months, 2 weeks ago

Selected Answer: B

VOTE B

upvoted 2 times

🗳️ 👤 **a4e15bd** 10 months, 3 weeks ago

This report provides an audit of the service organization controls over a specified period of time like six months or more and assess how well those controls protect customers data according to predefined criteria.

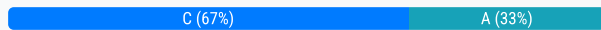
upvoted 3 times

A city municipality lost its primary data center when a tornado hit the facility. Which of the following should the city staff use immediately after the disaster to handle essential public services?

- A. BCP
- B. Communication plan
- C. DRP
- D. IRP

**Correct Answer:** C

Community vote distribution



**c7b3ff0** Highly Voted 8 months, 2 weeks ago

**Selected Answer: C**

Im going with C, because while a BCP is for helping to ensure that essential business operations continue after a disaster (such as this tornado), it is broader in scope. The DRP offers specific steps and processes to follow to recover critical IT infrastructure and systems, which is the more immediate concern "immediately after the disaster."

upvoted 9 times

**englishborn** 8 months, 2 weeks ago

The question states city staff not the IT, BCP is followed to ensure what can and cannot be supported, it is the first thing that staff members follow

upvoted 2 times

**8f23125** Most Recent 2 months ago

**Selected Answer: C**

C. DRP

Disaster recovery (DR) plans define the processes and procedures that an organization will take when a disaster occurs. Unlike a BC plan, a DR plan focuses on natural and human-made disasters that may destroy facilities or infrastructure, or otherwise prevent an organization from functioning normally. A DR plan focuses on restoration or continuation of services despite a disaster.

upvoted 1 times

**test\_arrow** 4 months, 2 weeks ago

**Selected Answer: C**

It says "After the Disaster" in the question which would be DRP Disaster recovery plan

upvoted 1 times

**fc040c7** 5 months ago

**Selected Answer: C**

What gives it away is "immediately after a disaster"

upvoted 1 times

**Anyio** 5 months ago

**Selected Answer: C**

The correct answer is:

C. DRP (Disaster Recovery Plan)

Explanation:

A Disaster Recovery Plan (DRP) is specifically designed to restore critical IT systems and infrastructure after a disaster, such as a tornado. It ensures that essential services can resume by outlining steps to recover data, applications, and systems, often leveraging backup data or alternate data centers.

Other Options:

- A. BCP (Business Continuity Plan): Focuses on maintaining critical operations during and after a disruption but works in conjunction with the DRP. DRP is the immediate focus for IT recovery.
  - B. Communication plan: Helps ensure stakeholders are informed but doesn't directly handle recovery of services.
  - D. IRP (Incident Response Plan): Deals with responding to cybersecurity incidents, such as breaches or malware, not natural disasters.
- upvoted 1 times

🗳️ 👤 **laternak26** 6 months, 1 week ago

**Selected Answer: A**

The Business Continuity Plan (BCP) would provide city staff with the necessary procedures to continue delivering essential public services during and after a disaster, ensuring that critical functions are maintained while the recovery efforts take place.

upvoted 1 times

🗳️ 👤 **fmeox567** 7 months, 1 week ago

**Selected Answer: C**

The correct answer is C. DRP (Disaster Recovery Plan). GPT

upvoted 4 times

🗳️ 👤 **8ef84bb** 7 months, 1 week ago

**Selected Answer: A**

BCP is for ensuring a business can continue operating, while DRP focuses on recovery

upvoted 1 times

🗳️ 👤 **bluray69** 6 months, 1 week ago

Incorrect.

"...AFTER the disaster"

upvoted 3 times

🗳️ 👤 **MikelMiguel** 7 months, 1 week ago

DRP is part of the BCP and DRP is specifically concerned with IT recovery, making it the immediate priority here due to Tornado disaster. Answer is DRP

upvoted 2 times

🗳️ 👤 **BevMe** 7 months, 2 weeks ago

**Selected Answer: C**

The DRP is immediately needed to restore operations of the data center.

upvoted 3 times

🗳️ 👤 **dC\_Furious** 7 months, 2 weeks ago

**Selected Answer: A**

i would say A,

Disaster Recovery Plan (DRP): Focuses on the restoration of IT systems and data following a disaster. It's all about getting the technology and data back online to support critical operations.

Business Continuity Plan (BCP): Encompasses a broader scope, ensuring that all aspects of the organization can continue to function during and after a disaster. This includes not only IT recovery but also personnel, facilities, and communication strategies to maintain essential public services.

upvoted 3 times

🗳️ 👤 **famuza77** 7 months, 2 weeks ago

**Selected Answer: C**

BCP. I mean, it is actually saying the word "Disaster"

upvoted 2 times

🗳️ 👤 **3dk1** 7 months, 3 weeks ago

**Selected Answer: A**

BCP for sure



upvoted 1 times

🗳️ 👤 **Murtuza** 8 months, 2 weeks ago

**Selected Answer: C**

DRP - While the other options might be relevant in certain contexts, they don't directly address the specific need for immediate action to restore essential public services after a disaster:


upvoted 4 times

  **709dfe4** 8 months, 2 weeks ago

**Selected Answer: A**

It s BCP

upvoted 1 times

  **User92** 8 months, 4 weeks ago

**Selected Answer: C**

Given answer is correct. An DRP, is a subset of the BCP, but DRP focuses on faster recovery after disasters

upvoted 1 times

  **BluezClues** 9 months ago

**Selected Answer: A**

A. BCP

Not DRP because...

A Disaster Recovery Plan (DRP) focuses on restoring IT infrastructure and data after a disaster. In this case, the city needs to continue running public services immediately, not just restore IT functions. A DRP will be important later in the recovery phase, but the BCP addresses the immediate need for continuing essential operations.

upvoted 3 times

Which of the following is considered a preventive control?

- A. Configuration auditing
- B. Log correlation
- C. Incident alerts
- D. Segregation of duties

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **TrebleSmith** Highly Voted 10 months, 1 week ago

**Selected Answer:** D

Segregation of duties is going to PREVENT users from having the ability to potentially manipulate processes within the business by splitting duties amongst others. Somewhat of a "checks and balances" kind of system.

upvoted 5 times

 **Muhammad\_Umair** Most Recent 10 months, 2 weeks ago

D. Segregation of duties.

upvoted 2 times



A systems administrator notices that a testing system is down. While investigating, the systems administrator finds that the servers are online and accessible from any device on the server network. The administrator reviews the following information from the monitoring system:

| Server name | IP          | Traffic sent | Traffic received | Status |
|-------------|-------------|--------------|------------------|--------|
| File01      | 10.12.14.13 | 2654812      | 23185            | Up     |
| DC01        | 10.12.15.2  | 168741       | 65481            | Up     |
| Test01      | 10.25.1.3   | 14872        | 654123168        | Down   |
| Test02      | 10.25.1.4   | 16941        | 651321685        | Down   |
| DC02        | 10.12.15.3  | 32145        | 32158            | Up     |
| Finance01   | 10.18.1.14  | 12374        | 6548             | Up     |

Which of the following is the most likely cause of the outage?

- A. Denial of service
- B. ARP poisoning
- C. Jamming
- D. Kerberoasting

**Correct Answer: A**

Community vote distribution

A (100%)

 **a4e15bd** Highly Voted 10 months, 3 weeks ago  
A Denial of Service.

This is clearly indicative of DoS attack where the two Test hosts are being overwhelmed with excessive traffic received causing them to become unresponsive and crash.

upvoted 11 times

 **TrebleSmith** Highly Voted 10 months, 3 weeks ago

**Selected Answer: A**

I do not see Kerberoasting anywhere in the exam objectives, leading me to believe the answer is A: DoS  
upvoted 6 times

 **Muhammad\_Umair** Most Recent 10 months, 2 weeks ago

A). DDOS attack.

upvoted 1 times

 **Justthereforcomptia** 10 months, 2 weeks ago

**Selected Answer: A**

DDOS attack, check the traffic received on the servers

upvoted 4 times

A security team has been alerted to a flood of incoming emails that have various subject lines and are addressed to multiple email inboxes. Each email contains a URL shortener link that is redirecting to a dead domain. Which of the following is the best step for the security team to take?

- A. Create a blocklist for all subject lines.
- B. Send the dead domain to a DNS sinkhole.
- C. Quarantine all emails received and notify all employees.
- D. Block the URL shortener domain in the web proxy.

**Correct Answer:** D

Community vote distribution



🗳️ **laternak26** Highly Voted 6 months, 1 week ago

**Selected Answer: B**

NOT D. Block the URL shortener domain in the web proxy: Blocking the URL shortener domain in the web proxy is a good idea if you suspect that the malicious URLs lead to a harmful site, but in this case, the links are redirecting to a dead domain. The malicious domain itself is no longer active, so blocking the URL shortener might not address the immediate threat. Additionally, this step doesn't prevent other similar attacks with different shorteners or domains in the future.

upvoted 13 times

🗳️ **RoRoRoYourBoat** Highly Voted 10 months, 3 weeks ago

**Selected Answer: D**

D. Block the URL shortener domain in the web proxy: By blocking the URL shortener domain, the security team can prevent users from accessing potentially malicious links, even if the domain is currently dead. This proactive measure helps mitigate the risk of future attacks using the same URL shortener.

upvoted 12 times

🗳️ **LavaBoi** Most Recent 3 days, 17 hours ago

**Selected Answer: D**

Its D: The common element across all the emails is the URL shortener. By blocking the URL shortener domain in the web proxy, you immediately prevent users from accessing any link shortened by that service. This stops the attack at its source (as far as your organization is concerned)

Not B: The dead domain is the destination of the attack, but the immediate problem is the URL shortener delivering users to that destination. Sinkholing the dead domain might be a good additional step, but it doesn't stop the initial click. The problem isn't the destination, it's the delivery mechanism (the URL shortener).

upvoted 1 times

🗳️ **Kekeee** 5 days, 15 hours ago

**Selected Answer: D**

ok for those who fell for the trap. it didnt mention enterprise but its an enterprise based on the "security team". second for a business email, url shorteners are not needed. They are mainly used for marketing campaigns. So why not block them. Its D

upvoted 1 times

🗳️ **sentinell** 1 week, 5 days ago

**Selected Answer: D**

The best step in this scenario is D. Block the URL shortener domain in the web proxy.

upvoted 1 times

🗳️ **1chung** 3 weeks, 4 days ago

**Selected Answer: B**

I go with B

upvoted 1 times

🗳️ **Arh2** 1 month ago

**Selected Answer: D**

Blocking the shortener domain prevents future access from those emails and similar ones.

upvoted 1 times

🗨️ 👤 **Abas2** 1 month, 2 weeks ago

**Selected Answer: C**

NOT D. Block the URL shortener domain in the web proxy: Blocking the URL shortener domain in the web proxy is a good idea if you suspect that the malicious URLs lead to a harmful site, but in this case, the links are redirecting to a dead domain. The malicious domain itself is no longer active, so blocking the URL shortener might not address the immediate threat. Additionally, this step doesn't prevent other similar attacks with different shorteners or domains in the future.

upvoted 1 times

🗨️ 👤 **Studytime2023** 2 months ago

**Selected Answer: D**

The description reads like a threat actor is behind this. With nothing else to go off we need to assume this is the case. Therefor blocking the URL shortener will prevent the threat actor from redirecting the URL shortener to any other domains. If we choose option B, the threat actor could simply redirect the URL shortener to a different domain. Worse yet, a different domain that might actually be working.

upvoted 1 times

🗨️ 👤 **skg01** 3 months, 3 weeks ago

**Selected Answer: D**

D. Block the URL shortener domain in the web proxy.

Explanation:

Since the attack uses URL shorteners to redirect users to potentially malicious domains, the most effective mitigation is to block the URL shortener domain in the web proxy. This prevents employees from clicking on similar links in the future, even if the attacker changes the final redirect destination.

Why not the other options?

A. Create a blocklist for all subject lines – Not effective because attackers can easily modify subject lines to bypass filters.

B. Send the dead domain to a DNS sinkhole – The domain is already dead, meaning it is no longer actively serving content. The threat lies in the URL shortener, which may redirect to different malicious sites in future attacks.

C. Quarantine all emails received and notify all employees – While notifying employees is important, quarantining all emails may cause unnecessary disruptions. Blocking the URL shortener is a more effective preventive measure.

upvoted 1 times

🗨️ 👤 **mejestique** 3 months, 3 weeks ago

**Selected Answer: D**

D. Block the URL shortener domain in the web proxy.

Explanation:

URL shorteners are often used in phishing attacks and malware distribution to obscure malicious links. Even though the current redirect domain is dead, attackers can update the shortener to point to a new malicious domain at any time.

Blocking the URL shortener domain at the web proxy ensures that:

Users cannot access any future malicious redirects coming from that shortener.

The security team prevents future attacks using the same shortener service.

It applies a broad and proactive security measure rather than reacting to just the current incident.

upvoted 1 times

🗨️ 👤 **selom1** 4 months, 2 weeks ago

**Selected Answer: D**

This provides immediate protection against current campaign

upvoted 1 times

🗨️ 👤 **DaBulls** 5 months ago

**Selected Answer: D**

The issue involves a URL shortener that redirects to a dead domain. Blocking the URL shortener domain prevents any redirection attempts, regardless of the destination domain. This measure also addresses any future malicious redirections from the same shortener.

Send the dead domain to a DNS sinkhole: While this may help if the dead domain becomes active again, it does not address the possibility of the URL shortener being used for other malicious redirections.

upvoted 1 times

🗨️ 👤 **amccert** 5 months, 2 weeks ago

**Selected Answer: C**

Jsmithy Response was on point look at his explanation

upvoted 2 times

🗨️ 👤 **Eracle** 6 months, 1 week ago

**Selected Answer: D**

Even if the domain they redirect URLs to is currently dead, the URL could be reactivated in the future for malicious purposes.

upvoted 2 times

🗨️ 👤 **gingergroot** 6 months, 4 weeks ago

**Selected Answer: B**

B. GPT

upvoted 3 times

🗨️ 👤 **Eracle** 5 months, 3 weeks ago

D. GPT in my case

upvoted 3 times

🗨️ 👤 **jsmthy** 9 months ago

**Selected Answer: C**

Quarantine is correct. The dead domain may not do anything, but there can be several layers of redirects. You can place the dead domain on the DNS sinkhole, but that won't prevent users from clicking the links. If you block the URL shortener, you could block legitimate traffic to that shortener.

upvoted 3 times

A security administrator is working to secure company data on corporate laptops in case the laptops are stolen. Which of the following solutions should the administrator consider?

- A. Disk encryption
- B. Data loss prevention
- C. Operating system hardening
- D. Boot security

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗨️ 👤 **fc040c7** 5 months ago

**Selected Answer:** A

It's funny how in this scenario it's easy picking but as soon as you apply the same scenario but with remote wipe as one of the options, you'll have a pretty even split of answers between remote wipe and disk encryption.

upvoted 2 times

🗨️ 👤 **TmNvrWts** 4 months, 2 weeks ago

remote wipe is only important when the thief has the laptops login creds aswell (is in rest state)

upvoted 1 times

🗨️ 👤 **Hayder81** 9 months, 4 weeks ago

A. Disk encryption

upvoted 1 times

🗨️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer:** A

A. GPT

upvoted 3 times


A company needs to keep the fewest records possible, meet compliance needs, and ensure destruction of records that are no longer needed. Which of the following best describes the policy that meets these requirements?

- A. Security policy
- B. Classification policy
- C. Retention policy
- D. Access control policy

**Correct Answer:** C

Community vote distribution

C (100%)

 **Glacier88** Highly Voted 10 months ago

**Selected Answer: C**

C. Retention policy.

Reasoning:

Security policy: While a security policy is important for protecting sensitive information, it doesn't specifically address the retention and destruction of records.

Classification policy: A classification policy helps categorize information based on its sensitivity and value, but it doesn't provide guidelines for how long records should be retained or when they should be destroyed.

Retention policy: A retention policy establishes rules for how long different types of records should be kept and when they can be destroyed. This is exactly what the company needs to meet compliance requirements and minimize the number of records it needs to store.

Access control policy: An access control policy governs who can access different types of information. While it's important for data protection, it doesn't directly address the retention and destruction of records.

Therefore, a retention policy is the best option for the company to meet its requirements of keeping the fewest records possible, meeting compliance needs, and ensuring destruction of records that are no longer needed.

upvoted 5 times

 **jafyyy** Most Recent 10 months, 1 week ago

C

Retention policy specifies how long a record should be kept & when it should be disposed.

upvoted 4 times

Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

- A. Code repositories
- B. Dark web
- C. Threat feeds
- D. State actors
- E. Vulnerability databases

**Correct Answer: A**

*Community vote distribution*

A (100%)

  **pokii1992** Highly Voted 10 months, 1 week ago

A. Code repositories

Code repositories often contain hardcoded credentials, API keys, or other sensitive information that developers may accidentally commit without proper security measures. This can expose these credentials when the code is shared or made public, leading to unintentional leakage of corporate credentials in cloud environments.

upvoted 8 times

  **fmeox567** Highly Voted 7 months, 1 week ago

**Selected Answer: A**

A. Code repositories

Explanation: Code repositories (such as GitHub, GitLab, or Bitbucket) are frequently used for storing and sharing code, but they are often mishandled. Developers sometimes inadvertently upload sensitive information like API keys, passwords, or private credentials into these public or even private repositories. This can lead to accidental exposure, especially if the repository is not properly secured or if access controls are misconfigured.

upvoted 5 times


Which of the following is the best reason an organization should enforce a data classification policy to help protect its most sensitive information?

- A. End users will be required to consider the classification of data that can be used in documents.
- B. The policy will result in the creation of access levels for each level of classification.
- C. The organization will have the ability to create security requirements based on classification levels.
- D. Security analysts will be able to see the classification of data within a document before opening it.

**Correct Answer:** C

Community vote distribution


C (100%)

 **pokii1992** Highly Voted 10 months, 1 week ago

The answer C is the best reason because it directly addresses the core benefit of data classification policies:

Creating security requirements based on classification levels allows organizations to implement tailored, appropriate security measures for different types of data. This approach ensures that the most sensitive information receives the highest level of protection, while less critical data may have less stringent controls. This targeted approach optimizes security efforts and resource allocation, providing a more effective and efficient way to protect an organization's information assets.

upvoted 8 times

 **laternak26** Most Recent 6 months, 1 week ago

**Selected Answer: C**

C. The organization will have the ability to create security requirements based on classification levels: A data classification policy helps the organization identify and categorize data according to its sensitivity. Once the data is classified, the organization can apply appropriate security controls based on the classification level

upvoted 2 times



An analyst is performing a vulnerability scan against the web servers exposed to the internet without a system account. Which of the following is most likely being performed?

- A. Non-credentialed scan
- B. Packet capture
- C. Privilege escalation
- D. System enumeration
- E. Passive scan

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗨️ 👤 **ViciousAkira** 7 months, 3 weeks ago

The correct answer is:

A. Non-credentialed scan

A non-credentialed scan is a vulnerability scan conducted without using login credentials. This type of scan is limited to detecting vulnerabilities that are exposed without needing privileged access. It's commonly used to assess what an external attacker could potentially see or exploit without having any system account access, which aligns with the scenario described.

upvoted 4 times

🗨️ 👤 **FrozenCarrot** 9 months, 2 weeks ago

**Selected Answer: A**

Without system account.

upvoted 1 times

🗨️ 👤 **jafyyy** 10 months, 1 week ago

A

Type of scan conducted without logging into the system

upvoted 3 times

A security administrator is hardening corporate systems and applying appropriate mitigations by consulting a real-world knowledge base for adversary behavior. Which of the following would be best for the administrator to reference?

- A. MITRE ATT&CK
- B. CSIRT
- C. CVSS
- D. SOAR

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **a4e15bd** Highly Voted 10 months, 3 weeks ago

MITRE ATT&CK is a comprehensive and widely used framework that categorizes and describes the various tactics, techniques and procedures (TTPs) employed by adversaries, it is used for threat intelligence, defensive strategy etc.

upvoted 7 times

 **3dk1** Most Recent 7 months, 3 weeks ago

**Selected Answer: A**

A. MITRE ATT&CK (answer)

B. CSIRT - a group of professionals who respond to and manage cybersecurity incidents

C. CVSS - Vulnerability scoring

D. SOAR - Security orchestration, automation and response

upvoted 3 times

An architect has a request to increase the speed of data transfer using JSON requests externally. Currently, the organization uses SFTP to transfer data files. Which of the following will most likely meet the requirements?

- A. A website-hosted solution
- B. Cloud shared storage
- C. A secure email solution
- D. Microservices using API

**Correct Answer:** D

Community vote distribution

D (100%)

  **a4e15bd** Highly Voted 10 months, 3 weeks ago

D. Microservices Using API

By using APIs will allow for increased speed of data transfer compared to file based transfer methods liker SFTP.

upvoted 8 times

  **test\_arrow** Most Recent 4 months, 2 weeks ago

**Selected Answer:** D

D. Microservices using API

Explanation:

To increase the speed of data transfer using JSON requests externally, the best solution is to use microservices with APIs. APIs allow for real-time data exchange in a structured and efficient manner, unlike SFTP, which relies on batch file transfers.

upvoted 1 times

Which of the following addresses individual rights such as the right to be informed, the right of access, and the right to be forgotten?

- A. GDPR
- B. PCI DSS
- C. NIST
- D. ISO

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **Syl0** 9 months, 4 weeks ago

GDPR - General Data Protection Regulation

NIST - Network institute of standards and technology, so doesn't have that.

PCI DSS - Payment Card Industry Data security standards

ISO - International standard for Standardisation

upvoted 3 times

🗳️ 👤 **jafyyy** 10 months, 1 week ago

A

- Addressed individual rights to be informed, access or to be forgotten among other rights.

upvoted 1 times

🗳️ 👤 **b82faaf** 10 months, 3 weeks ago

**Selected Answer: A**

A. GDPR

upvoted 2 times

An administrator is installing an LDAP browser tool in order to view objects in the corporate LDAP directory. Secure connections to the LDAP server are required. When the browser connects to the server, certificate errors are being displayed, and then the connection is terminated. Which of the following is the most likely solution?

- A. The administrator should allow SAN certificates in the browser configuration.
- B. The administrator needs to install the server certificate into the local truststore.
- C. The administrator should request that the secure LDAP port be opened to the server.
- D. The administrator needs to increase the TLS version on the organization's RA.

**Correct Answer:** B

Community vote distribution

B (100%)

  **a4e15bd**  10 months, 3 weeks ago

B is correct

The administrator needs to the server's certificate in the local trust store of the machine where LDAP browser tool is being used. This will allow the client to trust the server's certificate and establish a secure connection.

upvoted 12 times

  **test\_arrow**  4 months, 2 weeks ago

**Selected Answer: B**

B. The administrator needs to install the server certificate into the local truststore.

Explanation:

The certificate errors indicate that the LDAP browser tool does not trust the certificate presented by the LDAP server. This often happens when:

The certificate is self-signed or issued by an internal Certificate Authority (CA) not recognized by the system.

The certificate chain is incomplete or missing in the local truststore.

upvoted 2 times

Which of the following is the most important security concern when using legacy systems to provide production service?

- A. Instability
- B. Lack of vendor support
- C. Loss of availability
- D. Use of insecure protocols

**Correct Answer:** B

Community vote distribution



2fef490 Highly Voted 9 months, 2 weeks ago

Selected Answer: B

The most important security concern with legacy systems is the lack of vendor support. Without vendor support, there are no updates, security patches, or fixes for newly discovered vulnerabilities. This leaves the system exposed to potential attacks that cannot be easily mitigated, increasing the risk of security breaches.

upvoted 9 times

jbmacc Highly Voted 6 months ago

Selected Answer: D

The correct answer is:

D. Use of insecure protocols

Explanation:

Use of insecure protocols is the most critical security concern when using legacy systems to provide production services. Legacy systems often rely on outdated protocols that lack modern security features (such as encryption and secure authentication), making them vulnerable to various types of attacks (e.g., man-in-the-middle attacks, eavesdropping, etc.). These vulnerabilities can expose sensitive data and compromise the integrity of the system.

upvoted 7 times

Eracle 5 months, 3 weeks ago

A legacy system suffers from a lack of patches, but this does not necessarily translate into the use of outdated protocols. It could also happen that a legacy system uses a protocol that is still up-to-date but suffers from the lack of a patch for a known vulnerability!

upvoted 3 times

sentinell Most Recent 1 week, 5 days ago

Selected Answer: D

The most important security concern is D. Use of insecure protocols.

upvoted 1 times

8f23125 2 months ago

Selected Answer: D

D is correct, I think, use of insecure protocols is a better option because that is the reason there is no vendor support.

upvoted 2 times

Burnboy 2 months, 1 week ago

Selected Answer: D

D. Use of insecure protocols

upvoted 2 times

fc040c7 5 months ago

Selected Answer: B

Legacy items are typically unsupported. Honestly if you look through all the questions dealing with legacy items they point you toward using a compensation control (segmentation/firewall usage/isolation) because of the lack of support through patching/updates

upvoted 1 times

🗳️ 👤 **TonyStarChillingFromHeaven** 5 months, 3 weeks ago

**Selected Answer: A**

A - Lack of Vendor Support.

Insecure protocols are a major concern, but they are often a symptom of the broader issue of lack of support and updates.

upvoted 1 times

🗳️ 👤 **laternak26** 6 months, 1 week ago

**Selected Answer: D**

D. Use of insecure protocols: Legacy systems often rely on outdated protocols that are no longer considered secure by modern standards. These systems may use protocols that are vulnerable to attacks like eavesdropping, man-in-the-middle attacks, or data tampering because they do not support strong encryption or authentication methods.

upvoted 4 times

🗳️ 👤 **AndyK2** 6 months, 4 weeks ago

**Selected Answer: B**

No ongoing security updates

No patches for newly discovered vulnerabilities

upvoted 2 times

🗳️ 👤 **3dk1** 7 months, 4 weeks ago

The more I think about it, the more I realize that legacy systems could still have secure protocols.

I am going with lack of vendor support.

upvoted 1 times

🗳️ 👤 **User92** 8 months, 4 weeks ago

**Selected Answer: D**

Given answer is correct - because legacy systems often rely on outdated and insecure protocols that can be easily exploited.

upvoted 2 times

🗳️ 👤 **cyoncon** 8 months, 4 weeks ago

**Selected Answer: B**

Primary concern is vendor support.

upvoted 3 times

🗳️ 👤 **BluezClues** 9 months ago

**Selected Answer: B**

B.

Lack of Vendor Support

Why it isn't D. Use of Protocols: Many legacy systems use outdated and insecure protocols, which is certainly a concern, but insecure protocols can often be mitigated by wrapping them in secure communication channels (e.g., VPNs, encryption). The lack of vendor support to address these insecure protocols is actually a greater problem than their presence because there's no way to patch or upgrade them without vendor assistance.

upvoted 6 times

🗳️ 👤 **BluezClues** 9 months ago

B.

Lack of Vendor Support

Why it isn't D. Use of Protocols: Many legacy systems use outdated and insecure protocols, which is certainly a concern, but insecure protocols can often be mitigated by wrapping them in secure communication channels (e.g., VPNs, encryption). The lack of vendor support to address these insecure protocols is actually a greater problem than their presence because there's no way to patch or upgrade them without vendor assistance.

upvoted 3 times

🗳️ 👤 **a0bfa81** 9 months ago

**Selected Answer: B**

The most important security concern when using legacy systems is the lack of vendor support. Without vendor support, legacy systems may not receive essential security updates, patches, or technical assistance, leaving them vulnerable to known exploits and threats. This can significantly increase the risk of security breaches.


upvoted 3 times

🗳️ 👤 **nyyankee718** 9 months ago

**Selected Answer: B**

insecure protocol is an issue but would be greater without vendor support

upvoted 1 times

  **Exemplary** 9 months ago

**Selected Answer: D**

Legacy Systems - Outdated computing software, hardware, or other technologies that have been largely superseded by newer and more efficient alternatives.

Unsupported Systems - Hardware or software products that no longer receive official technical support, security updates, or patches from their respective vendors or developers.

Just because something is legacy does not mean that it's no longer supported by the vendor. However, it does mean that it is likely using outdated technologies/protocols. I vote D.

upvoted 1 times



A security investigation revealed that malicious software was installed on a server using a server administrator's credentials. During the investigation, the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?

- A. A spraying attack was used to determine which credentials to use.
- B. A packet capture tool was used to steal the password.
- C. A remote-access Trojan was used to install the malware.
- D. A dictionary attack was used to log in as the server administrator.

**Correct Answer:** B

*Community vote distribution*

B (100%)

🗳️ 👤 **FrozenCarrot** 9 months, 2 weeks ago

Telnet no encryption

upvoted 3 times

🗳️ 👤 **pokii1992** 10 months, 1 week ago

B. A packet capture tool was used to steal the password.

This is the most likely scenario given that the administrator regularly used Telnet, which transmits data in plain text. An attacker could easily capture the login credentials using a packet sniffing tool, then use those stolen credentials to install the malicious software on the server.

upvoted 1 times

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: B**

B. A packet capture tool was used to steal the password.

Telnet transmits data, including credentials, in plaintext, making it vulnerable to interception. A packet capture tool could easily capture the login credentials being transmitted, allowing an attacker to gain unauthorized access to the server.

upvoted 3 times

A user is requesting Telnet access to manage a remote development web server. Insecure protocols are not allowed for use within any environment. Which of the following should be configured to allow remote access to this server?

- A. HTTPS
- B. SNMPv3
- C. SSH
- D. RDP
- E. SMTP

**Correct Answer:** C

Community vote distribution

C (100%)

🗨️ 👤 **pokii1992** 10 months, 1 week ago

SSH is recommended because:

It provides strong encryption for all data transmitted

It's a secure protocol, meeting the requirement of avoiding insecure options

It allows secure remote access to servers, which is what you're looking for

It's widely used and supported for development environments

It can be used to set up secure tunnels for accessing web servers remotely

upvoted 3 times

🗨️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: C**

C. SSH

SSH (Secure Shell) provides encrypted remote access to servers, making it a secure alternative to Telnet, which transmits data in plaintext. SSH is commonly used for secure management of remote systems and would be the appropriate choice given the restriction on insecure protocols.

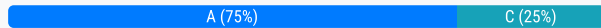
upvoted 2 times

A security administrator is working to find a cost-effective solution to implement certificates for a large number of domains and subdomains owned by the company. Which of the following types of certificates should the administrator implement?

- A. Wildcard
- B. Client certificate
- C. Self-signed
- D. Code signing

**Correct Answer: A**

Community vote distribution



🗳️ 👤 **ProudFather** 6 months, 3 weeks ago

**Selected Answer: A**

A wildcard certificate can be used to secure multiple subdomains under a single domain name. This makes it a cost-effective solution for organizations with a large number of subdomains. By purchasing a single wildcard certificate, the organization can secure all subdomains with a single certificate, reducing the need for multiple individual certificates.

upvoted 4 times

🗳️ 👤 **AndyK2** 6 months, 4 weeks ago

**Selected Answer: A**

Covers multiple subdomains with single certificate

Cost-effective for large number of domains

upvoted 1 times

🗳️ 👤 **f59f364** 7 months ago

**Selected Answer: C**

Not sure about wildcard. It can service one domain, and question says "domainS". If you by multiple wildcard certificates, it is not cost effective. I will go with C, self-signed, it doesn't say that service using certificate is public.

upvoted 2 times

🗳️ 👤 **Studytime2023** 2 months ago

You're right! It is stupid wording. One must hope the actual exam doesn't do this. For multiple domains, a SAN cert is required. Otherwise your choice of self signing which has its own drawbacks.

upvoted 1 times

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: A**

A. Wildcard

Wildcard certificates allow you to secure a domain and all of its subdomains with a single certificate. This can be a cost-effective solution for managing certificates for a large number of domains and subdomains.

upvoted 2 times

🗳️ 👤 **scholi** 10 months, 1 week ago

Wildcards are used to search for files or directories that match a certain pattern.

\* (Asterisk): Represents zero or more characters.

Example: \*.txt matches all files with a .txt extension.

? (Question Mark): Represents exactly one character.

Example: file?.doc matches file1.doc, fileA.doc, etc.

upvoted 1 times

🗳️ 👤 **scholi** 10 months, 1 week ago

A wildcard is a character or symbol used in computing to represent one or more characters in a string, allowing for flexible searching, matching, and filtering. Wildcards are commonly used in various contexts such as file searching, pattern matching, and access control.

Wildcards are used to search for files or directories that match a certain pattern.

upvoted 1 times

An auditor discovered multiple insecure ports on some servers. Other servers were found to have legacy protocols enabled. Which of the following tools did the auditor use to discover these issues?

- A. Nessus
- B. curl
- C. Wireshark
- D. netcat

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **9149f41** 5 months ago

**Selected Answer: A**

Nessus finds potential vulnerabilities  
SIEM monitors actual security events and incidents  
upvoted 1 times

🗳️ 👤 **ProudFather** 6 months, 3 weeks ago

**Selected Answer: A**

Nessus is a powerful vulnerability scanning tool that can identify a wide range of vulnerabilities, including open ports and outdated protocols. It can scan networks and individual systems to identify potential security risks.  
upvoted 1 times

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: A**

A. Nessus  
  
Nessus is a vulnerability scanner that can identify insecure ports, legacy protocols, and other security issues on servers. It is designed to detect vulnerabilities and misconfigurations in systems.  
upvoted 3 times

🗳️ 👤 **qacollin** 10 months, 3 weeks ago

**Selected Answer: A**

A. GPT  
upvoted 2 times

A security analyst received a tip that sensitive proprietary information was leaked to the public. The analyst is reviewing the PCAP and notices traffic between an internal server and an external host that includes the following:

...

```
12:47:22.327233 PPPoE [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 331) 10.5.1.1 > 52.165.16.154: IP6 (hlim E3, next-header TCP (6) payload length: 271) 2001:67c:2158:a019::ace:53104 > 2001:0:5ef5:79fd:380c:dddd:a601:24fa.13788: Flags [P.], cksum 0xd7ee (correct), seq 97:348, ack 102, win 16444, length 251
```

...

Which of the following was most likely used to exfiltrate the data?

- A. Encapsulation
- B. MAC address spoofing
- C. Steganography
- D. Broken encryption
- E. Sniffing via on-path position

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **pokii1992** Highly Voted 10 months, 1 week ago

A. Encapsulation

The PCAP shows traffic using IPv6 encapsulated within IPv4 (proto IPv6 (41)), which could be used to hide sensitive data within seemingly normal network traffic. This encapsulation technique can potentially bypass certain security controls and filters, making it an effective method for data exfiltration.

upvoted 6 times

🗳️ 👤 **sentinell** Most Recent 1 week, 5 days ago

**Selected Answer: A**

A. Encapsulation.

upvoted 1 times

🗳️ 👤 **9149f41** 5 months ago

**Selected Answer: A**

Encapsulation means hiding internal data, e.g. PW or bank balance, etc. pcap show (transmitted from IPv6 to IPv4 and it is bypass the filters.

upvoted 1 times

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer: A**

A. Encapsulation

The traffic described involves IPv6 encapsulated within IPv4, which can indicate that data is being transmitted through encapsulation to obscure the content or bypass filters. This technique could be used to exfiltrate sensitive data by embedding it within legitimate traffic patterns.

upvoted 4 times

A company wants to reduce the time and expense associated with code deployment. Which of the following technologies should the company utilize?

- A. Serverless architecture
- B. Thin clients
- C. Private cloud
- D. Virtual machines

**Correct Answer:** A

Community vote distribution

A (100%)

🗳️ 👤 **9149f41** 5 months ago

**Selected Answer:** A

AWS Lambda lets you upload code and run functions without managing servers, automatically scaling and charging only for compute time used.  
upvoted 1 times

🗳️ 👤 **pokii1992** 10 months, 1 week ago

Serverless architecture is recommended because it:

Eliminates server management tasks  
Reduces deployment time significantly  
Lowers costs by only charging for actual code execution  
Automatically scales based on demand  
Allows developers to focus solely on writing code  
Handles infrastructure and scaling automatically  
upvoted 1 times

🗳️ 👤 **baronvon** 10 months, 1 week ago

**Selected Answer:** A

A. Serverless architecture

Serverless architecture allows the company to reduce the time and expense associated with code deployment by handling the underlying infrastructure management automatically. This means the company only needs to focus on the code itself, without worrying about provisioning or managing servers. This approach can also scale automatically with demand, further reducing operational overhead and costs.  
upvoted 4 times

A security administrator is performing an audit on a stand-alone UNIX server, and the following message is immediately displayed:

(Error 13): /etc/shadow: Permission denied.

Which of the following best describes the type of tool that is being used?

- A. Pass-the-hash monitor
- B. File integrity monitor
- C. Forensic analysis
- D. Password cracker

**Correct Answer:** D

Community vote distribution

D (54%)

B (46%)

 **Cyberity** Highly Voted 10 months, 2 weeks ago

**Selected Answer: D**

Password crackers often attempt to access this file to obtain hashed passwords for cracking.

upvoted 9 times

 **Burnboy** Most Recent 2 months, 1 week ago

**Selected Answer: B**

B. File integrity monitor

upvoted 1 times

 **Foreversmall** 3 months ago

**Selected Answer: B**

both B and D could theoretically trigger the error, the context of a security audit strongly aligns with File integrity monitor (B). FIM tools are standard components of audits to ensure file integrity, whereas password crackers are more situational and less likely to be the focus of a general audit. The error reflects a permissions issue during routine integrity checks, making B the best answer.

Answer: B. File integrity monitor

upvoted 1 times

 **prabh1251** 3 months, 1 week ago

**Selected Answer: B**

password cracker was running, it would likely try to read or copy the /etc/shadow file, rather than just check permissions.

upvoted 1 times

 **prabh1251** 3 months, 3 weeks ago

**Selected Answer: D**

(Permission Denied) happens when you try to access or modify /etc/shadow, which is a highly restricted system file that stores hashed passwords for user accounts.

upvoted 3 times

 **mejestique** 3 months, 3 weeks ago

**Selected Answer: B**

B. File integrity monitor

Explanation:

The "/etc/shadow: Permission denied" error suggests that the tool is trying to access the /etc/shadow file, which stores password hashes on a UNIX system and is highly restricted.

A File Integrity Monitor (FIM) checks system files for unauthorized changes, access attempts, or modifications. Since the security administrator is conducting an audit, a FIM tool is likely being used to ensure that critical system files (like /etc/shadow) have not been altered.

upvoted 1 times



🗨️ 👤 **dbrowndiver** 5 months, 1 week ago

Selected Answer: D

The /etc/shadow file stores encrypted passwords and is protected with strict permissions to prevent unauthorized access.

• Scenario Application:

The error message (Error 13): /etc/shadow: Permission denied indicates that the tool being used attempted to access the /etc/shadow file but failed due to insufficient permissions. This behavior is consistent with a password cracker attempting to retrieve password hashes for analysis or cracking.  
upvoted 2 times

🗨️ 👤 **pindinga1** 5 months, 1 week ago

Selected Answer: D

The context based, the question says "tool" used for analysis. For my is D pssword cracker.

upvoted 2 times

🗨️ 👤 **Eracle** 5 months, 3 weeks ago

Selected Answer: B

Why not D option: a password cracker attempts to crack passwords, not read the file directly. A password cracker typically operates on a copy of the /etc/shadow file (or extracted hashes) and would not generate a "Permission denied" error during its cracking operation.

upvoted 2 times

🗨️ 👤 **laternak26** 6 months, 1 week ago

Selected Answer: D

D. Password cracker: A password cracker tool is used to attempt to recover passwords from hashed password files. In the case of UNIX-based systems, the /etc/shadow file typically stores user passwords in a hashed format. If a security administrator or attacker is trying to analyze this file, they might encounter the "Permission denied" message if they do not have sufficient privileges to access it. This suggests that the tool being used is likely attempting to crack or analyze the passwords stored in the /etc/shadow file, and it's encountering permission issues.

Why not B. File integrity monitor: A file integrity monitor typically checks whether critical system files have been modified. It wouldn't be used to crack passwords or access /etc/shadow in this way, and it wouldn't typically result in a "Permission denied" error unless there's an attempt to modify files rather than just monitor them.

upvoted 4 times

🗨️ 👤 **AndyK2** 6 months, 4 weeks ago

Selected Answer: B

Strange, Claude says it's FIM. But ChatGPT says Password Cracker.

I'd go with FIM - since it makes more sense.

upvoted 4 times

🗨️ 👤 **fmeox567** 7 months, 1 week ago

Selected Answer: D

D. Password cracker

Explanation: The message /etc/shadow: Permission denied indicates that the tool is attempting to access the /etc/shadow file, which typically contains password hashes for user accounts on a UNIX/Linux system. In a normal scenario, this file is restricted to root or privileged users to prevent unauthorized access.

This kind of message is commonly seen when a password cracker is trying to access the /etc/shadow file to extract password hashes for the purpose of cracking them (typically using brute force or dictionary attacks). The "Permission denied" error indicates that the tool lacks sufficient privileges to access the file, which is a normal security measure to protect sensitive data.

upvoted 2 times

🗨️ 👤 **BevMe** 7 months, 1 week ago

B. File Integrity Monitor

upvoted 2 times

🗨️ 👤 **cyberWoof** 7 months, 3 weeks ago

Selected Answer: B

File integrity monitor

upvoted 2 times

🗨️ 👤 **c7b3ff0** 8 months, 2 weeks ago

Selected Answer: B

I don't know why so many of you think that a security administrator would use a password cracker during an audit, but I bet there are quite a few more reasons they would use a file integrity monitor during an audit. That would probably need to be given permissions to access a restricted file like

/etc/shadow before they ran it, and if they didn't give them, I bet it would kick out a don't touch me error just like this. Answer is B.  
upvoted 4 times

🗨️ 👤 **oikj** 7 months, 3 weeks ago

While FIM could theoretically generate a "permission denied" error if misconfigured, the presence of the error immediately following access attempts on /etc/shadow is more indicative of a password-cracking attempt than standard FIM activity in this context.

upvoted 1 times

🗨️ 👤 **1798e2e** 8 months, 1 week ago

They use password crackers during audits to ensure compliance is actually being honored.

it's far easier to challenge something in an ACTIVE way than it is to defensively go through each system. Not to mention that just because something says it's working means that it actually is.

upvoted 2 times

🗨️ 👤 **User92** 8 months, 3 weeks ago

**Selected Answer: D**

Password crackers often attempt to access the /etc/shadow file to retrieve hashed passwords for cracking.

upvoted 2 times

🗨️ 👤 **Ty13** 9 months ago

**Selected Answer: B**

B. File Integrity Monitoring

The /etc/shadow file stores encrypted user passwords, and you can only access it as root. If you're checking file integrity, you're checking the permissions are still properly set and haven't been changed. You WANT to see 'Permission Denied' if you're auditing the system.

upvoted 2 times

A security administrator needs to create firewall rules for the following protocols: RTP, SIP, H.323. and SRTP. Which of the following does this rule set support?

- A. RTOS
- B. VoIP
- C. SoC
- D. HVAC

**Correct Answer:** B

Community vote distribution

B (100%)

 **baronvon** Highly Voted 10 months, 1 week ago

**Selected Answer: B**

B. VoIP

The protocols RTP (Real-time Transport Protocol), SIP (Session Initiation Protocol), H.323, and SRTP (Secure Real-time Transport Protocol) are commonly used in Voice over IP (VoIP) communications. RTP handles the transport of media streams, SIP manages call setup and control, H.323 is a standard for multimedia communication, and SRTP provides encryption for RTP. Therefore, the firewall rules for these protocols support VoIP.

upvoted 5 times

 **Syl0** Most Recent 9 months, 3 weeks ago

RTOS - Real-Time Operating system

VoIP - Voice over Internet Protocol

SoC - System on Chip

HVAC - Heat, Ventilation, Air condition

RTP - Real-Time Transport Protocol

SIP - Session initiation Protocol

SRTP - Secure Real-time Transport Protocol

upvoted 3 times

 **scoobysnack209** 10 months, 2 weeks ago

RTP Real-time Transport Protocol

SRTP Secure Real-time Transport Protocol

SIP Session Initiation Protocol

upvoted 1 times