Exam Topic Breakdown

Exam Topic	Number of Questions
Topic 1 : Exam Set 1	188
Topic 2 : Exam Set 2	195
Topic 3 : Exam Set 3	117
Topic 4 : Exam Set 4	77
TOTAL	577

Topic 1, Exam Set 1

Question #:1 - (Exam Topic 1)

During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HTTPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

A. Birthday collision on the certificate key

B. DNS hacking to reroute traffic

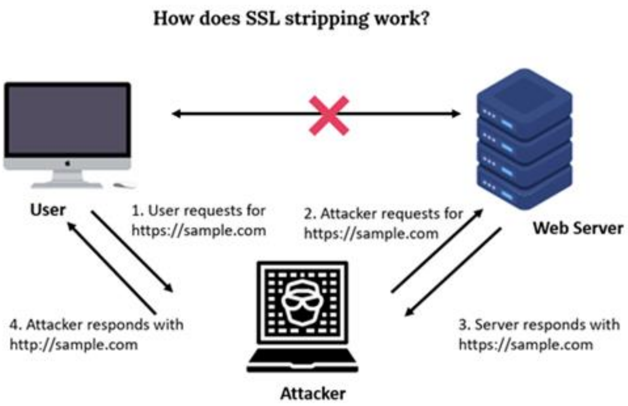
C. Brute force to the access point

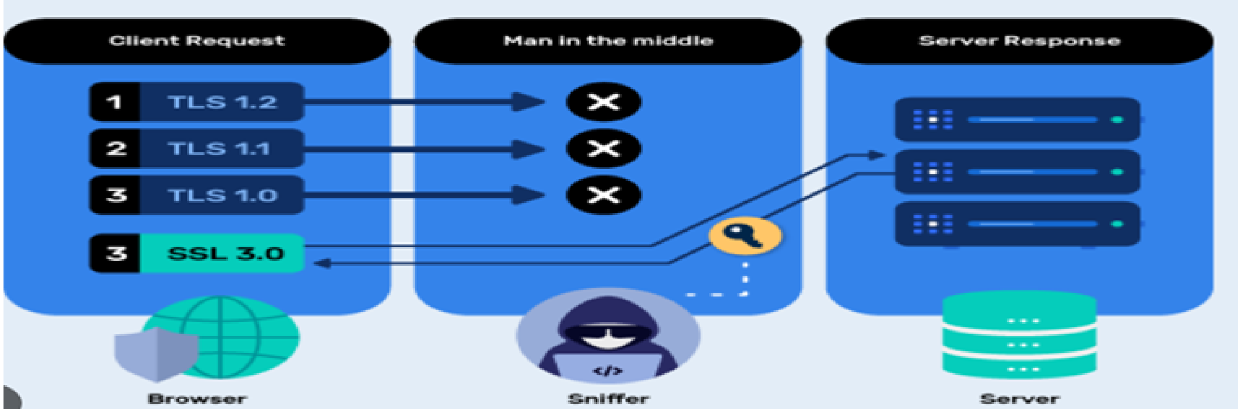
D. A SSL/TLS downgrade

Answer: D

Explanation

The scenario describes a Man-in-the-Middle (MitM) attack where the attacker intercepts traffic and downgrades the secure SSL/TLS connection to an insecure HTTP connection. This type of attack is commonly known as SSL/TLS downgrade attack or a stripping attack. The attacker is able to see and modify the communication between the client and server.


How does SSL stripping work?
User
1. User requests for https://sample.com
2. Attacker requests for https://sample.com
Web Server
4. Attacker responds with http://sample.com
3. Server responds with https://sample.com
Attacker



A. Birthday collision on the certificate key: A birthday collision in cryptography refers to a scenario where two different inputs produce the same hash output. However, this is not a typical cause for delays in connection or HTTPS to HTTP reversion. It's more related to cryptographic hash functions rather than SSL/TLS protocol issues.

B. DNS hacking to reroute traffic: DNS (Domain Name System) hacking involves unauthorized changes to DNS records, such as redirecting traffic to malicious servers. While DNS hacking can impact network traffic, it's not directly related to SSL/TLS protocol issues causing delays or HTTPS-to-HTTP downgrades.

C. Brute force to the access point: Brute force attacks involve trying all possible combinations to gain unauthorized access to a system, like a password. While brute force attacks can cause network disruptions, they typically do not result in SSL/TLS downgrades or HTTPS-to-HTTP conversions. Instead, they aim to gain unauthorized access through authentication methods.

Question #:2 - (Exam Topic 1)

A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system. Which of the following would be BEST suited for this task?

A. Social media analysis

B. Annual information security training

C. Gamification

D. Phishing campaign

Answer: D

Explanation

A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.

A phishing campaign involves sending simulated phishing emails to employees to assess their ability to recognize and respond to phishing attacks. It allows the security administrator to evaluate how well users can identify and avoid suspicious or malicious emails, which is a critical skill in preventing email-based attacks and maintaining overall cybersecurity.

A. Social media analysis: This involves monitoring and analyzing social media for security threats and vulnerabilities but is not a direct method for testing an individual user's ability to recognize email-based attacks.

B. Annual information security training: While annual information security training is essential, it typically covers a broader range of security topics and may not specifically focus on email-based attacks or the ability to recognize them.

C. Gamification: Gamification can be used as a training method to make security awareness training more engaging and interactive. However, it may not directly test a user's ability to recognize attacks in the same way as a simulated phishing campaign would. Gamification is often used in conjunction with other training methods.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 85-86.

Question #:3 - (Exam Topic 1)

A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric

B. Symmetric

C. Homomorphic

D. Ephemeral

Answer: C

Explanation

Homomorphic encryption algorithms are a type of encryption algorithm designed to allow mathematical operations to be performed on encrypted data.

Homomorphic encryption is designed specifically to perform computations on encrypted data, making it the most suitable choice for this scenario where data sensitivity is paramount, and computational overhead and speed are not primary concerns.

A. Asymmetric encryption: While it's useful for secure communication and key exchange, it doesn't typically support computations on encrypted data.

B. Symmetric encryption: Also doesn't support computations on encrypted data and is more commonly used for data confidentiality during storage and transmission.

D. Ephemeral encryption: Ephemeral encryption usually refers to the use of short-lived keys, and it doesn't directly address the requirement of performing computations on encrypted data while stored in the cloud.

References:

References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 6

https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/cryptography-concepts-2/

https://www.microsoft.com/en-us/research/wp-content/uploads/2018/01/security_homomorphic_encryptio
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/symmetric-and-asymmetric-crypt

Question #:4 - (Exam Topic 1)

The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?

A. Requiring all new, on-site visitors to configure their devices to use WPS

B. Implementing a new SSID for every event hosted by the college that has visitors

C. Creating a unique PSK for every visitor when they arrive at the reception area

D. Deploying a captive portal to capture visitors' MAC addresses and names

Answer: D

Explanation

captive portal is a web page that requires visitors to authenticate or agree to an acceptable use policy before allowing access to the network. By capturing visitors' MAC addresses and names, potential malicious activity can be traced back to a specific person.

Captive Portal: A captive portal is a web page that users must interact with before being granted access to the WiFi network. This allows the college to collect information about visitors, including their MAC addresses and names, when they log in or authenticate.

Visitor Identification: By collecting visitors' MAC addresses and names, the college can associate network activity with specific individuals. This helps in identifying potential malicious activity if it occurs, as each visitor's information is logged.

A: WPS) is not a suitable choice because WPS (Wi-Fi Protected Setup) is primarily used for simplifying the process of connecting devices to a WiFi network securely. It doesn't provide a means to collect visitor information for identification purposes.

B: (new SSID for every event) may create complexity in managing multiple SSIDs and doesn't inherently collect visitor information for identification.

C: (unique PSK for every visitor) might provide some level of security, but it doesn't necessarily associate network activity with specific individuals or capture visitor information unless additional logging and tracking mechanisms are implemented.

Question #:5 - (Exam Topic 1)

A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

A. BYOD

B. VDI

C. COPE

D. CYOD

Answer: D

Explanation

Choose Your Own Device (CYOD) is a deployment model that allows employees to select from a predefined list of devices.

It provides employees with flexibility in device preference while allowing the company to maintain control and security over company data and infrastructure. CYOD deployment model provides a compromise between the strict control provided by Corporate-Owned, Personally Enabled (COPE) deployment model and the flexibility provided by Bring Your Own Device (BYOD) deployment model.

CYOD provides:
- flexibility for employees on device preference,
- satisfies the concerns about supporting too many different types of hardware,
- provides greatest amount of control and security over company data and infrastructure.

A: BYOD (Bring Your Own Device) allows employees to use their own devices but can pose challenges in terms of data security and control, as company data may reside on a variety of unmanaged devices.

B: A VDI is a type of remote desktop virtualization because the virtual desktop is remote to the end user. For example, typically, Microsoft Windows desktops are physical machines with Microsoft Windows installed on them. However, virtualized desktops could have a Linux desktop sitting on a Windows server machine.

C: (Corporate-Owned, Personally-Enabled) provides company-owned devices to employees but may not offer the flexibility of using employees' preferred personal devices.

References: CompTIA Security+ Study Guide, Chapter 6: Securing Application, Data, and Host Security, 6.5 Implement Mobile Device Management, pp. 334-335

Mustafa Aghamirzayev — Today at 10:18 AM
honestly in this question "providing flexibility" and concerning about different types of hardware how in this case CYOD is the answer..

Question #:6 - (Exam Topic 1)

An organization wants to enable built-in FDE on all laptops. Which of the following should the organization ensure is Installed on all laptops?

A. TPM

B. CA

C. SAML

D. CRL

Answer: A

Explanation

The organization should ensure that a Trusted Platform Module (TPM) is installed on all laptops in order to enable built-in Full Disk Encryption (FDE). TPM is a hardware-based security chip that stores encryption keys and helps to protect data from malicious attacks. It is important to ensure that the TPM is properly configured and enabled in order to get the most out of FDE.

B. CA (Certificate Authority): A Certificate Authority is a trusted entity that issues digital certificates. These certificates are used in various security protocols to establish secure connections and verify the identity of parties in a communication. While a CA is essential for managing digital certificates, it's not directly related to enabling Full Disk Encryption (FDE) on laptops. CA is more relevant in the context of securing communications, web applications, and authentication processes.

C. SAML (Security Assertion Markup Language): SAML is an XML-based standard used for exchanging authentication and authorization data between parties, particularly in Single Sign-On (SSO) scenarios. SAML is not related to enabling FDE on laptops. It is used for identity and access management, allowing users to access multiple applications with a single set of credentials.

D. CRL (Certificate Revocation List): A Certificate Revocation List is a list of digital certificates that have been revoked by the Certificate Authority before their expiration date. CRL is crucial for maintaining the security of certificate-based systems, such as SSL/TLS certificates for websites and digital signatures. It is not directly related to enabling FDE on laptops.

Petra Martina Vrancic

—

Today at 10:22 AM

The primary purpose of TPM is to enhance the security of a computer by providing a secure, tamper-resistant environment for storing and processing sensitive information, such as encryption keys, digital certificates, and other security-related data.

Question #:7 - (Exam Topic 1)

The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

A. Account audits

B. AUP

C. Password reuse

D. SSO

Answer: A

Explanation

Account audits are periodic reviews of user accounts to ensure that they are being used appropriately and that access is being granted and revoked in accordance with the organization's policies and procedures. If the compliance team had been conducting regular account audits, they would have identified the users who left the company six months ago and ensured that their access was revoked in a timely manner. This would have prevented the compliance violation caused by these users still having access to the company's systems.

To prevent this compliance violation, the company should implement account audits. An account audit is a regular review of all user accounts to ensure that they are being used properly and that they are in compliance with the company's security policies. By conducting regular account audits, the company can identify inactive or unused accounts and remove access for those users. This will help to prevent compliance violations and ensure that only authorized users have access to the company's systems and data.

B. AUP (Acceptable Use Policy): An AUP is a policy that outlines acceptable behavior and usage of an organization's IT resources by employees. While it is essential for setting guidelines, it does not directly prevent users from retaining access after leaving the company.

C. Password reuse: Password reuse refers to the practice of using the same password for multiple accounts. While password policies are crucial for security, they are not directly related to users retaining access after leaving the company.

D. SSO (Single Sign-On): Single Sign-On streamlines the authentication process for users by allowing them to access multiple services with a single set of credentials. While SSO enhances user experience and security, it doesn't address the specific issue of users retaining access after leaving the company; it primarily deals with authentication and access to various services.

Annie Ercan

—

Today at 10:24 AM

Account Audits to review the accounts not in use anymore

Danut Halau

—

Today at 10:23 AM

These audits involve reviewing and evaluating user accounts, permissions, and access rights within an organization's systems, networks, and applications. The primary goals of account audits are to ensure security, compliance, and the principle of least privilege (PoLP).

Question #:8 - (Exam Topic 1)

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A spill-tunnel VPN

D. Load-balanced servers

Answer: B

Explanation

A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.

To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

A. A reverse proxy: While a reverse proxy can be part of a security architecture, it doesn't inherently provide SSL decryption or WAF functionality. Reverse proxies are often used for load balancing, caching, and enhancing security, but SSL inspection is typically a separate component.

C. A spill-tunnel VPN: A spill-tunnel VPN is not a standard component for protecting a website from malicious web requests over SSL. It's more related to secure communication between networks and remote access, rather than web application security.

D. Load-balanced servers: Load balancing can improve the availability and performance of a website, but it doesn't directly address SSL decryption or the specific security needs of a WAF. While load balancing is a valuable part of a web infrastructure, it's not the primary requirement for protecting against malicious web requests over SSL.

Osimkhon Ibrokhimov — Today at 10:27 AM

without decryption certificate waf is blind, or its vision is impaired (edited)

David Berrios — Today at 10:27 AM

sesure scoket layer

Mohammadreza Mostafaei — Today at 10:27 AM

split tunnel for send traffic on vpn

Hamza Mayoufi — Today at 10:27 AM

The decryption certificate allows the WAF to decrypt incoming SSL/TLS traffic, inspect it for malicious content or patterns, and then re-encrypt the traffic before forwarding it to the web server.

Nita Arapi — Today at 10:27 AM

a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF

1

David Berrios — Today at 10:27 AM

once see we requesrt over SSl

Petra Martina Vrancic — Today at 10:27 AM

Load balancing is a mechanism to distribute network traffic across multiple servers. While it is important for scalability and availability, it is not specifically required for SSL decryption in the context of a WAF.

Question #:9 - (Exam Topic 1)

During a security assessment, a security analyst finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?

A. 1s

B. chflags

C. chmod

D. lsof

E. setuid

Answer: C

Explanation

The chmod command is used to change the permissions of a file or directory. The analyst can use chmod to reduce the permissions for existing users and groups and remove the set-user-ID bit from the file.

The chmod command in Unix and Unix-like operating systems allows you to change file permissions. Specifically, you can use chmod to modify the file's permissions to make it less permissive and to remove the set-user-ID (setuid) or set-group-ID (setgid) bits. Here's how you can use it:

```
chmod options permissions filename
```

To remove the setuid bit from a file, you would typically run:

```
chmod u-s filename
```

This command removes the setuid bit from the user's (owner's) permission, reducing the file's permissions. To reduce the permissions for users and groups, you can adjust the permissions using the appropriate symbols and permissions settings in the chmod command. For example, to restrict read and write permissions for a file, you can use:

```
chmod go-rw filename
```

This removes read and write permissions for the group and others (users who are not the owner).

Option A (1s) and option B (chflags) are not standard commands for modifying file permissions and removing setuid bits in Unix-like operating systems.

Option D (lsof) is used for listing open files and is not related to changing file permissions.

Option E (setuid) refers to the set-user-ID (setuid) bit, which you want to remove, rather than being a tool or command to achieve this.

References:

CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

Mohammadreza Mostafaei — Today at 10:30 AM chflag is Change a file or folder's flags

1

Question #:10 - (Exam Topic 1)

Which of the following must be in place before implementing a BCP?

A. SLA

B. AUP

C. NDA

D. BIA

Answer: D

Explanation

A Business Impact Analysis (BIA) is a critical component of a Business Continuity Plan (BCP). It identifies and prioritizes critical business functions and determines the impact of their disruption.
A BIA identifies critical business functions and their dependencies, and it assesses the potential impacts of disruptions on these functions. Based on the BIA results, the BCP can be developed to ensure the continuity of critical business functions during and after a disruptive event.

A. SLA (Service Level Agreement): SLAs are agreements between a service provider and its customers and define the level of service expected. While SLAs can be relevant for outsourcing critical services, they are not a prerequisite for developing a BCP.

B. AUP (Acceptable Use Policy): An AUP outlines acceptable behavior and usage of IT resources by employees and users. While it is important for security, it's not directly related to the BCP.

C. NDA (Non-Disclosure Agreement): NDAs are legal agreements that protect confidential information. While they are important for protecting sensitive information, they are not a prerequisite for BCP development.

References: CompTIA Security+ Study Guide 601, Chapter 10

David Berrios — Today at 10:31 AM

Business Impact Analysis (BIA): In the context of business and information technology, BIA refers to the process of evaluating and quantifying the potential effects that a disruptive event (such as a natural disaster, cyberattack, or supply chain failure) might have on business operations. It helps organizations prioritize their activities, resources, and investments in business continuity planning and disaster recovery. (edited)

Question #:11 - (Exam Topic 1)

Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR

B. PCI DSS

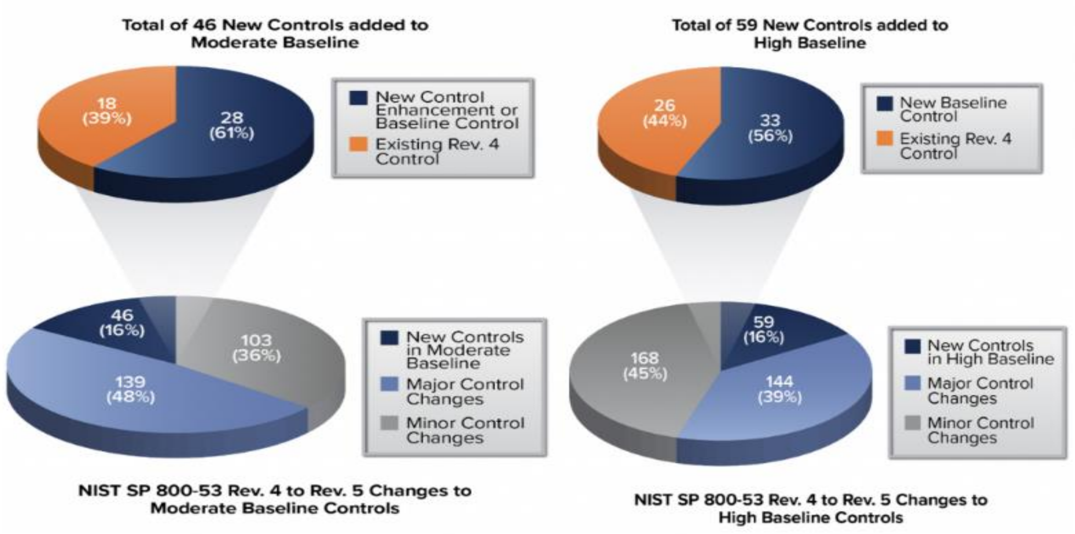
C. ISO 27000

D. NIST 800-53

Answer: D

Explanation

NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. The National Institute of Standards and Technology (NIST) Special Publication 800-53, titled "Security and Privacy Controls for Federal Information Systems and Organizations," provides a comprehensive catalog of security and privacy controls that federal agencies in the United States are required to follow. These controls are designed to protect the confidentiality, integrity, and availability of federal information systems and the data they handle.



Source: Kearney & Company, P.C. (Kearney) prepared based on NIST SP 800-53 Rev. 4 and NIST SP 800-53 Rev. 5

The other options mentioned are related to different standards and regulations:

A. GDPR (General Data Protection Regulation): GDPR is a European Union regulation that focuses on the protection of personal data and privacy rights of individuals within the EU. It does not pertain specifically to federal information systems in the United States.

B. PCI DSS (Payment Card Industry Data Security Standard): PCI DSS is a set of security standards designed to protect payment card data. It is primarily applicable to organizations that process payment card transactions and is not specific to federal information systems.

C. ISO 27000: ISO 27000 refers to a series of international standards related to information security management systems (ISMS). While these standards are widely recognized and used globally, they are not specific to United States federal information systems.

Danut Halau — Today at 10:32 AM

The catalog of security and privacy controls related to United States federal information systems is provided by the "National Institute of Standards and Technology" (NIST) through their publication called "Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations."

Petra Martina Vrancic

—

Today at 10:34 AM

The ISO 27000 series provides a framework of standards for information security management. While it is widely used globally, it is not specific to U.S. federal information systems.

Hajimurad Razagov

—

Today at 10:35 AM

USA=NIST

2

1

Osimkhon Ibrokhimov

—

Today at 10:35 AM

GDPR = EU NIST = USA ISO = GLOBAL

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

Question #:12 - (Exam Topic 1)

A retail company that is launching a new website to showcase the company’s product line and other information for online shoppers registered the following URLs:

* www.companysite.com
* shop.companysite.com
* about-us.companysite.com
* contact-us.companysite.com
* secure-logon.companysite.com

Which of the following should the company use to secure its website if the company is concerned with convenience and cost?

A. A self-signed certificate

B. A root certificate

C. A code-signing certificate

D. A wildcard certificate

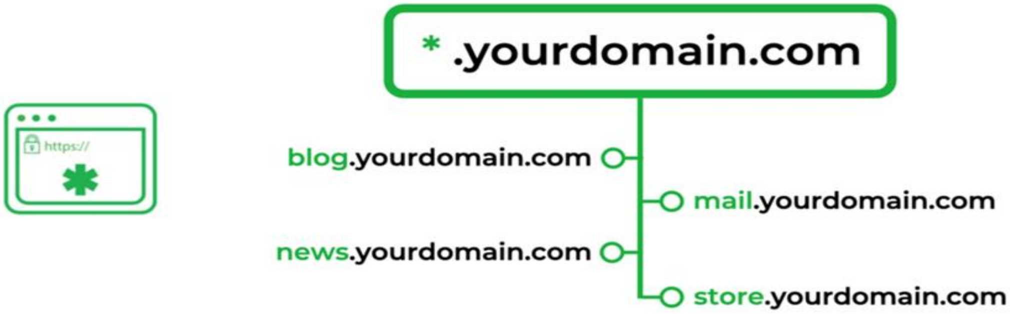
E. An extended validation certificate

Answer: D

Explanation

The company can use a wildcard certificate to secure its website if it is concerned with convenience and cost. A wildcard certificate can secure multiple subdomains, which makes it cost-effective and convenient for securing the various registered domains.

The retail company should use a wildcard certificate if it is concerned with convenience and cost. A wildcard SSL certificate is a single SSL/TLS certificate that can provide significant time and cost savings, particularly for small businesses. The certificate includes a wildcard character (*) in the domain name field, and can secure multiple subdomains of the primary domain1



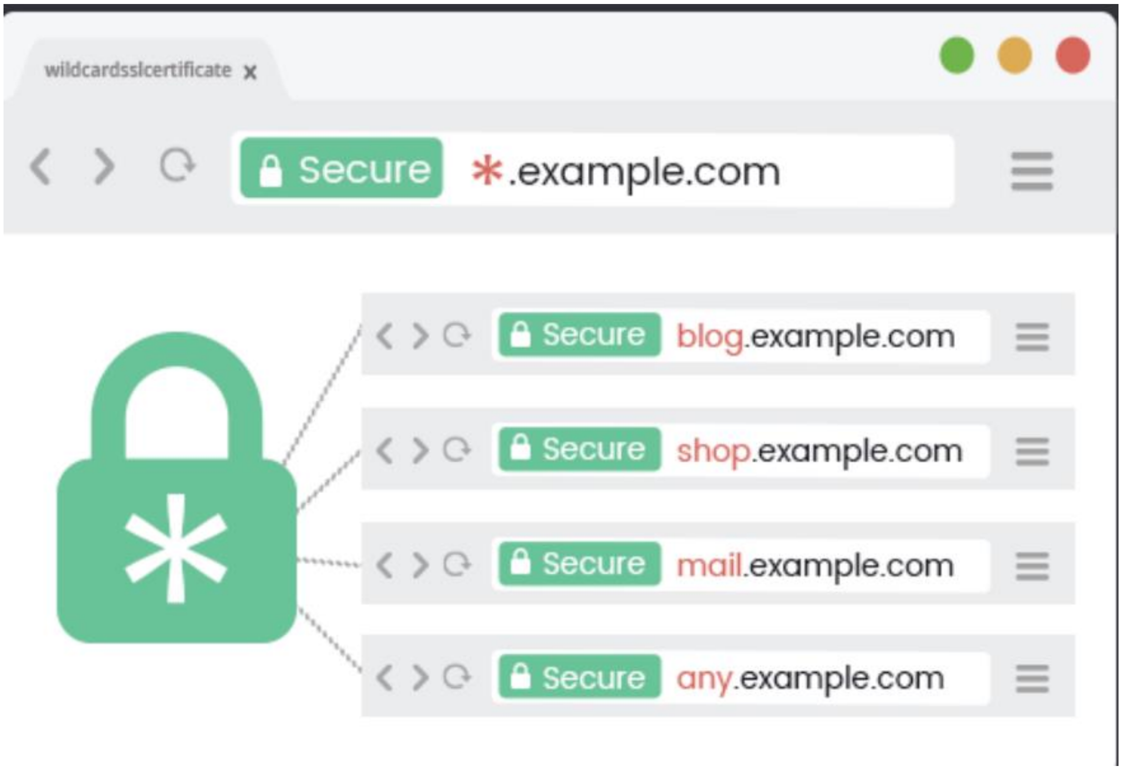
Wildcard SSL certificates secures your website URL and an unlimited number of its subdomains. For example, a single Wildcard certificate can secure www.coolexample.com, blog.coolexample.com, and store.coolexample.com.
Wildcard certificates secure the common name and all subdomains at the level you specify when you submit your request. Just add an asterisk (*) in the subdomain area to the left of the common name.
https://uk.godaddy.com/help/what-is-a-wildcard-ssl-certificate-567

A. A self-signed certificate: Self-signed certificates are not typically used for public-facing websites because they may not be trusted by users' browsers, leading to security warnings.

B. A root certificate: Root certificates are used in the context of certificate authorities (CAs) to sign other certificates. They are not used directly to secure websites.

C. A code-signing certificate: Code-signing certificates are used to digitally sign software and scripts to verify their authenticity. They are not meant for securing websites.

E. An extended validation certificate: Extended Validation (EV) certificates provide the highest level of assurance for website users but may be costlier and offer features that exceed the convenience and cost concerns mentioned in the question.



Wildcard SSL Certificates

Secure a Domain and its Unlimited Subdomains

Petra Martina Vrancic — Today at 10:37 AM

Advantages of Wildcard Certificates:

Cost-Effective: Instead of obtaining individual certificates for each subdomain, a wildcard certificate allows securing all subdomains with a single certificate, which can be cost-effective.

Convenience: Managing and renewing a single wildcard certificate is more convenient than managing multiple certificates for each subdomain.

1

David Berrios — Today at 10:37 AM

wildcard certificate is a type of SSL/TLS certificate that is used to secure a domain and all its subdomains. Unlike a standard SSL certificate, which is issued for a specific domain name (e.g., www.example.com), a wildcard certificate is issued for a domain and all its subdomains

Farid Abbasov — Today at 10:38 AM

one time purchese

2

Mohammadreza Mostafaei — Today at 10:38 AM

Wildcard notation consists of an asterisk and a period before the domain name. Secure Sockets Layer (SSL) certificates often use wildcards to extend SSL encryption to subdomains.

Question #:13 - (Exam Topic 1)

An employee's company account was used in a data breach Interviews with the employee revealed:

- The employee was able to avoid changing passwords by using a previous password again.
- The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccurring? (Select TWO)

A. Geographic dispersal

B. Password complexity

C. Password history

D. Geotagging

E. Password lockout

F. Geofencing

Answer: C F

Explanation

Two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofencing. Password history is a feature that prevents users from reusing their previous passwords. This can enhance password security by forcing users to create new and unique passwords periodically. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords.

Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device. This can enhance security by preventing unauthorized access from hostile or foreign region. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries.

A. Geographic dispersal: Geographic dispersal typically involves distributing data centers or resources across different physical locations for redundancy and disaster recovery. While it can be a useful security measure, it may not directly address the specific issue described in the scenario.

B: Complex passwords should contain a good mixture of upper/lower case letters, numbers, and symbols. Passwords should also not be based on dictionary words and should contain at least seven characters (the longer the better).

D. Geotagging: Geotagging is the process of adding geographic location data to media such as photos. It's not directly related to securing user accounts or preventing unauthorized access.

E. Password lockout: Password lockout policies can be useful to prevent brute force attacks, but they are typically used in combination with strong password complexity requirements (Option B). While they help protect against attacks, they may not directly prevent an employee from using a previous password.
mmm ok

Mamurjon Ismatov — Today at 10:43 AM
Password history policies prevent users from reusing a certain number of their previous passwords

David Berrios — Today at 10:44 AM
chose password hisotry and password complexity

Danut Halau — Today at 10:44 AM
It helps prevent brute-force attacks and unauthorized users from repeatedly trying to guess passwords until they gain access

Question #:14 - (Exam Topic 1)

A security architect is implementing a new email architecture for a company. Due to security concerns, the Chief Information Security Officer would like the new architecture to support email encryption, as well as provide for digital signatures. Which of the following should the architect implement?

A. TOP

B. IMAP

C. HTTPS

D. S/MIME

Answer: D

Explanation

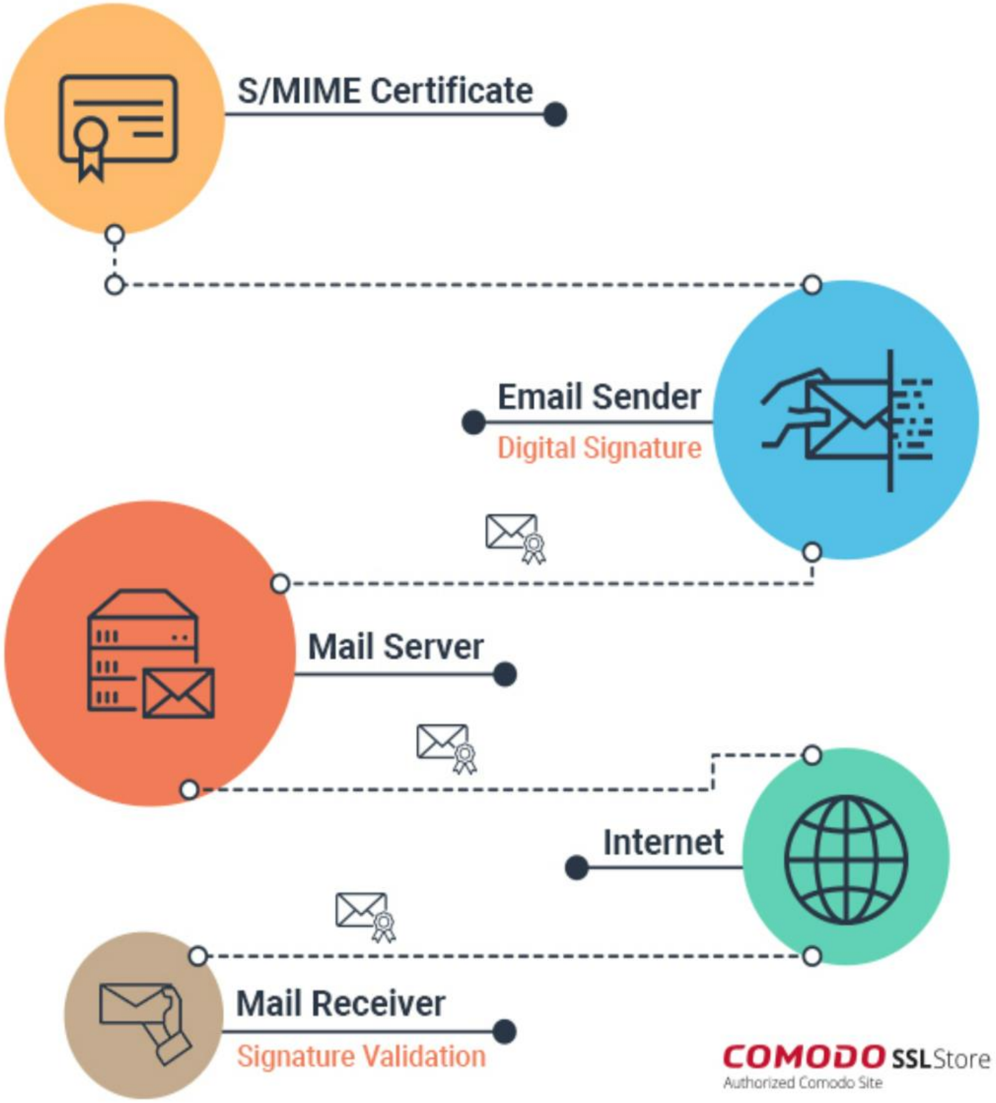
S/MIME (Secure/Multipurpose Internet Mail Extensions) is a protocol that enables secure email messages to be sent and received. It provides email encryption, as well as digital signatures, which can be used to verify the authenticity of the sender. S/MIME can be used with a variety of email protocols, including POP and IMAP.

Which clients support S/MIME?

These are some of the many desktop and mobile email clients that support email encryption certificates:

Apple Mail
CipherMail

Gmail (paid version)
IBM Notes
iPhone iOS Mail
MailMate
Microsoft Outlook and Outlook on the Web
Mozilla Thunderbird



A: TOP is not a standard email security protocol but rather a method for designating specific email messages for processing by automated systems.

B. IMAP (Internet Message Access Protocol): IMAP is a protocol used for accessing and managing email messages on a mail server. While IMAP can be used with secure connections (e.g., IMAPS), it does not provide encryption or digital signature capabilities by default.

C. HTTPS (Hypertext Transfer Protocol Secure): HTTPS is used for securing web communications, such as accessing web pages, and is not directly related to securing email communications or providing digital signatures within emails.

References:

https://www.comptia.org/content/guides/what-is-smime

CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 139

2

1

Danut Halau — Today at 10:47 AM

Secure Multipurpose Internet Mail Extensions Implement S/MIME, a widely used email encryption and digital signature standard. S/MIME requires users to have digital certificates that are used to sign and encrypt email messages.

Nita Arapi — Today at 10:47 AM

S/MIME is an encryption protocol used to digitally sign and encrypt an email to ensure that the email is authenticated and its content is not altered.

Osman Ceylan — Today at 10:48 AM

emalil s/mime

Osimkhon Ibrokhimov — Today at 10:48 AM

Email Encryption = S/MIME

Petra Martina Vrancic — Today at 10:48 AM

if the Chief Information Security Officer is looking for email encryption and digital signatures, implementing S/MIME would be a suitable choice. The other options (A. TOP, B. IMAP, and C. HTTPS) are not directly related to email encryption and digital signatures in the context of securing email communications.

Oytun Azkanar — Today at 10:48 AM

S/MIME is a set of standards and protocols that enhance the security of email communication by providing digital signatures and encryption capabilities.

Mamurjon Ismatov — Today at 10:48 AM

(Secure/Multipurpose Internet Mail Extensions) is a widely used standard for securing email communications

Question #:15 - (Exam Topic 1)

A user attempts to load a web-based application, but the expected login screen does not appear. A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC

```
user> nslookup software-solution.com
Server: rogue.comptia.com
Address: 172.16.1.250
Non-authoritative answer:
Name: software-solution.com
Address: 10.20.10.10
```

The help desk analyst then runs the same command on the local PC:

```
helpdesk> nslookup software-solution.com
Server: dns.comptia.com
Address: 172.16.1.1
Non-authoritative answer:
Name: software-solution.com
 Address: 172.16.1.10
```

Which of the following BEST describes the attack that is being detected?

A. Domain hijacking

B. DNS poisoning

C. MAC flooding

D. Evil twin

Answer: B

Explanation

In DNS poisoning (also known as DNS cache poisoning), an attacker manipulates or corrupts the DNS (Domain Name System) data stored in a DNS server's cache. The objective is to provide incorrect or malicious DNS information to clients requesting domain name resolution.

In this case:

The initial nslookup from the user's PC returns an IP address (10.20.10.10) that is likely incorrect or manipulated.

The subsequent nslookup from the help desk analyst's PC returns a different IP address (172.16.1.10) that might be the legitimate IP address for "software-solution.com."
This discrepancy between the two responses suggests that the DNS cache of the user's PC may have been poisoned with incorrect DNS data. It is possible that an attacker has tampered with the DNS responses, redirecting the user to a rogue or malicious website (rogue.comptia.com).

DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, such as an IP address. This results in traffic being diverted to the attacker's computer (or any other malicious destination).

DNS poisoning can be performed by various methods, such as:

- Intercepting and forging DNS responses from legitimate servers
- Compromising DNS servers and altering their records
- Exploiting vulnerabilities in DNS protocols or implementations
- Sending malicious emails or links that trigger DNS queries with poisoned responses

According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:

"DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record."

A. Domain hijacking: Domain hijacking typically involves unauthorized control or transfer of domain names, but it doesn't directly involve manipulating DNS cache or poisoning DNS data.

C. MAC flooding: MAC flooding is an attack against Ethernet switches and does not relate to DNS cache manipulation or the scenario described.

D. Evil twin: An evil twin attack typically involves setting up a rogue wireless access point to mimic a legitimate one. While it can redirect traffic, it doesn't directly involve DNS cache poisoning.

Farid Abbasov — Today at 10:50 AM

and also we can see all have 172.16 but one is 10.20.10 (edited)

[10:50 AM]

it is diffrent network

Oytun Azkanar — Today at 10:51 AM

DNS poisoning, also known as DNS cache poisoning or DNS spoofing, is a malicious attack that involves corrupting the Domain Name System (DNS) cache of a computer or network.

Mamurjon Ismatov — Today at 10:52 AM

DNS cache to redirect legitimate traffic to malicious or unauthorized destinations

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

Question #:16 - (Exam Topic 1)

The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?

A. CASB

B. Next-generation SWG

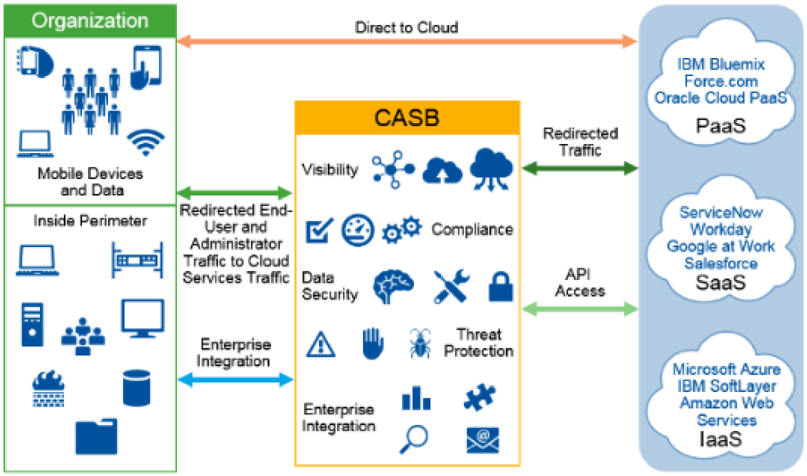
C. NGFW

D. Web-application firewall

Answer: B

Explanation

The CISO should choose a CASB (Cloud Access Security Broker) solution. CASB is a cloud-based security solution that provides URL categorization and filtering, and it can be configured to enforce security policies on corporate-owned laptops and mobile devices, even when they are away from the home office.



B: A Next-generation SWG (Secure Web Gateway) is a similar solution, but it is typically deployed on-premises, which may not provide the same level of protection for remote devices.

C: An NGFW (Next-generation Firewall) is a different type of solution that provides network traffic filtering, and a web application firewall is designed to protect web applications specifically.

D: A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

Question #:17 - (Exam Topic 1)

A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

A. Auto-update

B. HTTP headers

C. Secure cookies

D. Third-party updates

E. Full disk encryption

F. Sandboxing

G. Hardware encryption

Answer: A F

Explanation

Auto-update can help keep the app up-to-date with the latest security fixes and enhancements, and reduce the risk of exploitation by attackers who target outdated or vulnerable versions of the app.

Sandboxing can help isolate the app from other processes and resources on the system, and limit its access and permissions to only what is necessary. Sandboxing can help prevent the app from being affected by or affecting other applications or system components, and contain any potential damage in case of a breach.

- The scenario didn’t mention web applications so we took off Band C

- The scenario didn’t mention vender applications so we took of D

- The scenario didn’t mention data at rest so we took of F and G

Petra Martina Vrancic

—

Today at 10:57 AM

sandboxing is also an important security measure, especially in the context of isolating applications or processes from the rest of the system to prevent potential damage or unauthorized access. Sandboxing can be highly effective in containing and mitigating the impact of security breaches

Question #:18 - (Exam Topic 1)

Per company security policy, IT staff members are required to have separate credentials to perform administrative functions using just-in-time permissions. Which of the following solutions is the company Implementing?

A. Privileged access management

B. SSO

C. RADIUS

D. Attribute-based access control

Answer: A

Explanation

The company is implementing privileged access management (PAM) to enforce the requirement for IT staff members to have separate credentials to perform administrative functions using just-in-time permissions. PAM solutions are designed to manage and monitor privileged access to critical systems and data, including the use of administrative credentials. They often include just-in-time (JIT) access controls, which allow privileged access to be granted temporarily and only when needed, rather than continuously.

B: SSO (single sign-on) is a solution that allows users to log in once to access multiple applications and systems without needing to enter their credentials repeatedly.

C: RADIUS (Remote Authentication Dial-In User Service) is a protocol used to authenticate remote users and devices to a network,

D: (ABAC) is a method of access control that uses attributes or characteristics of users and other entities to determine access rights. While these solutions may be relevant to certain aspects of the company's security policy, they are not directly related to the requirement for separate credentials and just-in-time permissions for IT staff members.

Danut Halau

—

Today at 11:00 AM

JIT permissions involve granting temporary access to administrative privileges only when needed for specific tasks, and these permissions automatically expire after a predefined period.

Question #:19 - (Exam Topic 1)

A security analyst is running a vulnerability scan to check for missing patches during a suspected security incident. During which of the following phases of the response process is this activity MOST likely occurring?

A. Containment

B. Identification

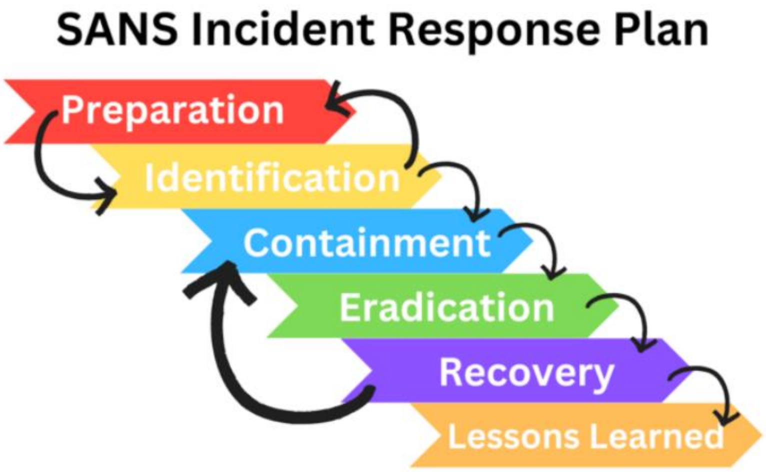
C. Recovery

D. Preparation

Answer: B

Explanation

Identification phase: This phase of the incident response process involves identifying and confirming the presence of a security incident. Part of this process may involve running various scans and assessments, such as vulnerability scans, to determine the extent of the vulnerability and potential weaknesses in the environment. Identifying missing patches is a crucial step in understanding the scope of the incident and assessing its impact.



A: Containment phase: In this phase, actions are taken to prevent the incident from spreading further and to mitigate its immediate impact.

C: Recovery phase: Once the incident is contained and mitigated, the recovery phase focuses on restoring affected systems and services to normal operation.

D: Preparation phase: This phase involves preparing the organization for potential future incidents by improving security measures, updating policies, and conducting training.

References: CompTIA Security+ Study Guide 601, Chapter 4

Question #:20 - (Exam Topic 1)

A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?

A. .pfx

B. .csr

C. .pvk

D. .cer

Answer: D

Explanation

A user should choose the .cer file format to share a public key for secure communication. A .cer file is a public key certificate that can be shared with third parties to enable secure communication.

.cer: This is a file format that stores a certificate, which is a document that binds a public key to an identity. It is also known as DER or Distinguished Encoding Rules. It is used by some applications such as OpenSSL and Java to read and write certificates

A public key is a cryptographic key that can be used to encrypt or verify data. A public key file is a file that contains one or more public keys in a specific format.

There are different formats for public key files, depending on the application and the algorithm used. Some of the common formats are:

A: .pfx: This is a file format that stores a certificate and its private and public keys. It is also known as PKCS#12 or Personal Information Exchange. It is used by some applications such as Microsoft Internet Explorer and Outlook to import and export certificates and keys

B: csr: This is a file format that stores a Certificate Signing Request, which is a message sent to a Certificate Authority (CA) to request a digital certificate. It contains the public key and some information about the identity of the requester. It is also known as PKCS#10 or Certification Request Syntax

C: .pvk: This is a file format that stores a private key for Microsoft Authenticode code signing. It is used with a .spc file that contains the certificate and public key

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Cryptography, pp. 301-302.

Question #:21 - (Exam Topic 1)

A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasionally disappears.

The task list shows the following results

Name	CPU%	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbs
Explorer	99.7%	2.15GB	0.1Mbs
Notepad	0%	3.9MB	0Mbs

Which of the following is MOST likely the issue?

A. RAT

B. PUP

C. Spyware

D. Keylogger

Answer: C

Explanation

The best available choice is PUP (Potentially Unwanted Program). Because there are no indicators for the other choices.

A potentially unwanted program (PUP) is a program that may be unwanted, despite the possibility that users consented to download it. PUPs include spyware, adware and dialers, and are often downloaded in conjunction with a program that the user wants.

In some cases PUPs can be more damaging to a computer than traditional malware by causing application freezes, crashes, and other instability.

A: RAT: A RAT (remote access Trojan) is malware an attacker uses to gain full administrative privileges and remote control of a target computer. RATs are often downloaded along with seemingly legitimate user-requested programs -- such as video games -- or are sent to their target as an email attachment via a phishing email.

Once the host system is compromised, intruders use a backdoor to control the host, or they may distribute RATs to other vulnerable computers and establish a botnet.

C: Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent. A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.

Where is spyware most commonly found?

Links or attachments. Like most other malware, spyware can be sent in a link or an email attachment.

D: Keyloggers are a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. The term keylogger, or "keystroke logger," is self-explanatory: Software that logs what you type on your keyboard.

Question #:22 - (Exam Topic 1)

A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?

A. IaC

B. MSSP

C. Containers

D. SaaS

Answer: A

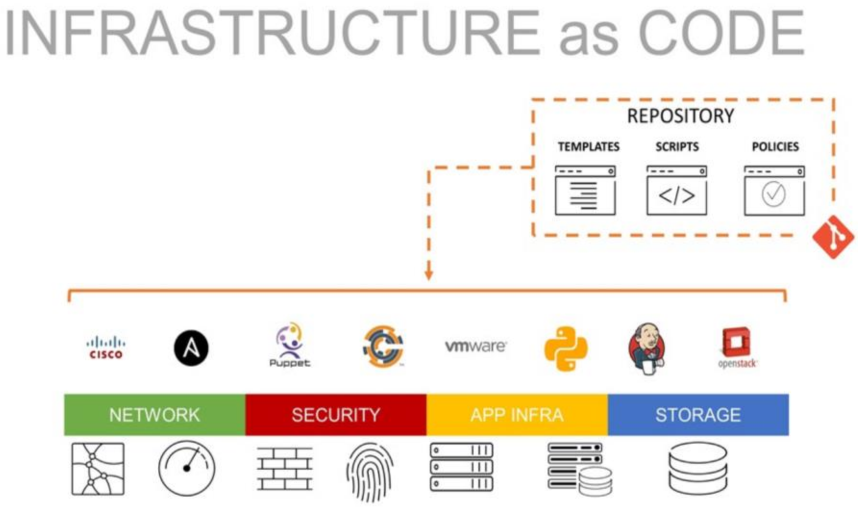
Explanation

infrastructure as Code IaC is a process of managing and provisioning infrastructure through code, typically using automation tools and scripts. This allows organizations to create and manage infrastructure resources, such as servers, networking, and storage, in a repeatable and scalable way. By using IaC, companies can reduce manual intervention and increase efficiency, as described in the example.

Containers (C) are a type of virtualization that allows applications to run in isolated environments, without the need for a separate operating system for each application.

MSSP (B) stands for "Managed Security Service Provider", which is a company that provides security services to other organizations.

SaaS (D) stands for "Software as a Service", which is a cloud computing model where software applications are provided to customers over the internet, rather than being installed on local computers. SaaS is not directly related to the example described in the question.



Question #:23 - (Exam Topic 1)

An organization is moving away from the use of client-side and server-side certificates for EAP. The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?

A. PEAP

B. EAP-FAST

C. EAP-TLS

D. EAP-TTLS

Answer: B

Explanation

EAP-FAST (Flexible Authentication via Secure Tunneling) was developed by Cisco*. Instead of using a certificate to achieve mutual authentication. EAP-FAST authenticates by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server.

802.1X EAP Types	TLS	TTLS	PEAP	FAST Flexible Authentication via Secure Tunneling
Feature / Benefit	Transport Level Security	Tunneled Transport Level Security	Protected Transport Level Security	

Client-side certificate required	yes	no	no	no (PAC)
Server-side certificate required	yes	yes	yes	no (PAC)
WEP key management	yes	yes	yes	yes
Rogue AP detection	no	no	no	yes
Provider	MS	Funk	MS	Cisco
Authentication Attributes	Mutual	Mutual	Mutual	Mutual
Deployment Difficulty	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi Security	Very High	High	High	High

References:

https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html

Question #:24 - (Exam Topic 1)

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan

B. A communications plan

C. A business continuity plan

D. A disaster recovery plan

Answer: B

Explanation

To inform the affected parties about the compromise of their sensitive data, the organization should use a communications plan. A communications plan outlines how the organization will communicate with stakeholders in the event of a security incident or breach, including affected parties, customers, employees, and the media.

The communications plan should include the following information:
1. Who will be responsible for communicating the incident to the affected parties.
2. What information will be communicated, such as the type of data that was compromised and what actions the organization is taking to address the issue.
3. When and how the information will be communicated, such as through email, phone calls, or a public announcement.
4. How the organization will handle follow-up inquiries and concerns from affected parties.

An incident response plan, business continuity plan, and disaster recovery plan are also important plans for an organization to have, but they are not specifically designed for communicating with affected parties about a security incident or breach.

Question #:25 - (Exam Topic 1)

An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes what a malicious person might be doing to cause this issue to occur?

A. Jamming

B. Bluesnarfing

C. Evil twin

D. Rogue access point

Answer: B

Explanation

Bluesnarfing is a type of Bluetooth hacking attack where an attacker gains unauthorized access to a Bluetooth-enabled device to steal data or take control of the device. In this case, the employee received multiple messages on their mobile device instructing them to pair the device to an unknown device. This could be an attempt by an attacker to trick the employee into pairing their device with the attacker's device, giving the attacker access to the employee's device and its data.

A: Jamming: Jamming involves disrupting wireless communications by emitting interference signals to interfere with legitimate transmissions. It doesn't involve pairing or accessing the victim's device.

B: Evil twin: An evil twin is a rogue wireless access point that mimics a legitimate one to trick users into connecting to it. While it can be used for various attacks, it's not directly related to Bluetooth pairing.

D: Rogue access point: A rogue access point is an unauthorized wireless access point that is set up to mimic a legitimate one. It's primarily associated with Wi-Fi networks and is not directly related to Bluetooth pairing.

Question #:26 - (Exam Topic 1)

A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?

A. Default system configuration

B. Unsecure protocols

C. Lack of vendor support

D. Weak encryption

Answer: C

Explanation

One of the risks of using legacy software is the lack of vendor support. This means that the vendor may no longer provide security patches, software updates, or technical support for the software. This leaves the software vulnerable to new security threats and vulnerabilities that could be exploited by attackers.

This is a significant risk associated with legacy software. When software reaches the end of its vendor support lifecycle, it no longer receives security updates, patches, or bug fixes. This leaves the software vulnerable to known and unknown security vulnerabilities, making it a prime target for attackers. Without vendor support, organizations have to rely solely on their own resources to secure and maintain the software, which can be challenging, especially for critical services.

A:Default system configuration: Legacy software may have default configurations that are less secure, but this risk can often be mitigated through proper configuration and security hardening.

B: Unsecure protocols: Legacy software may use outdated or unsecure communication protocols, which can pose a security risk. However, this risk can also be mitigated by using additional security measures or implementing secure gateways.

D: Weak encryption: Legacy software may use weaker encryption methods, which can impact data security. However, encryption protocols can often be upgraded or supplemented.

Question #:27 - (Exam Topic 1)

A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of (he following should the manager request to complete the assessment?

A. A service-level agreement

B. A business partnership agreement

C. A SOC 2 Type 2 report

D. A memorandum of understanding

Answer: C

Explanation

A Service Organization Control (SOC) Type 2 report **outlines a company's internal controls and details how well they safeguard customer data, specifically for cloud service providers**. Specifically, it's a third-party audit that shows if the security protocols are safe and effective.

SOC2: Evaluates the internal controls implemented by the service provider to ensure compliance with Trust Services Criteria (TSC) when storing and processing customer data.

• Type I report assesses system design

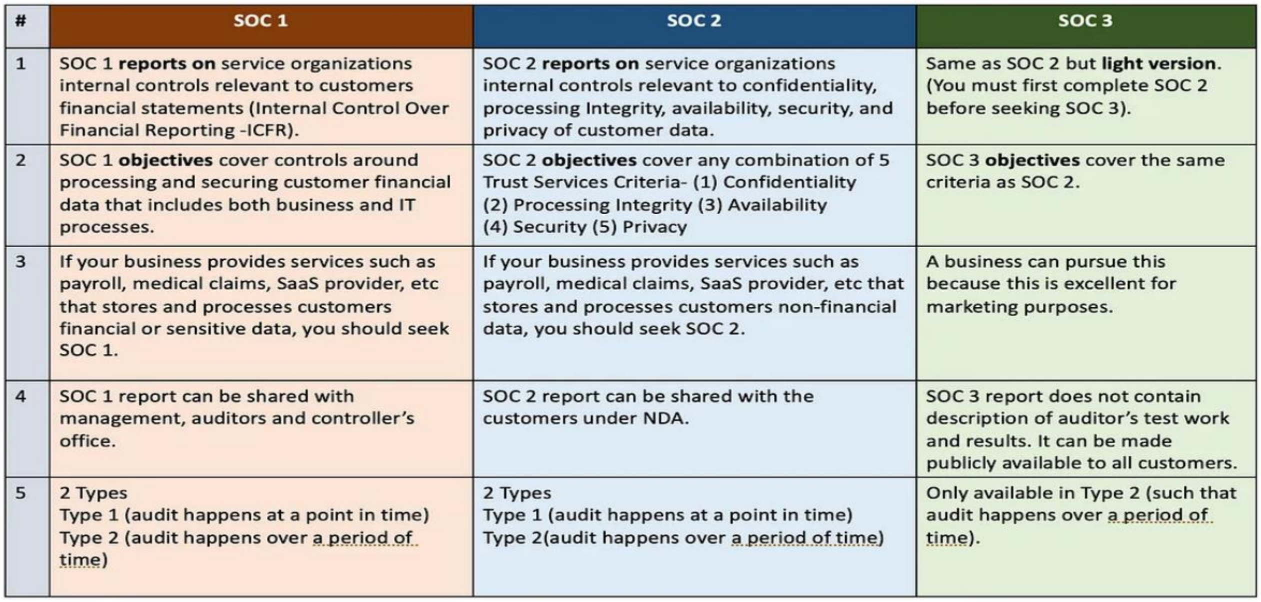
• Type II report assesses ongoing effectiveness

Note: SOC2 reports are highly detailed and designed to be restricted. They should only be shared with the auditor and regulators and with important partners under non disclosure agreement (NDA) terms.

SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a specific point in time.

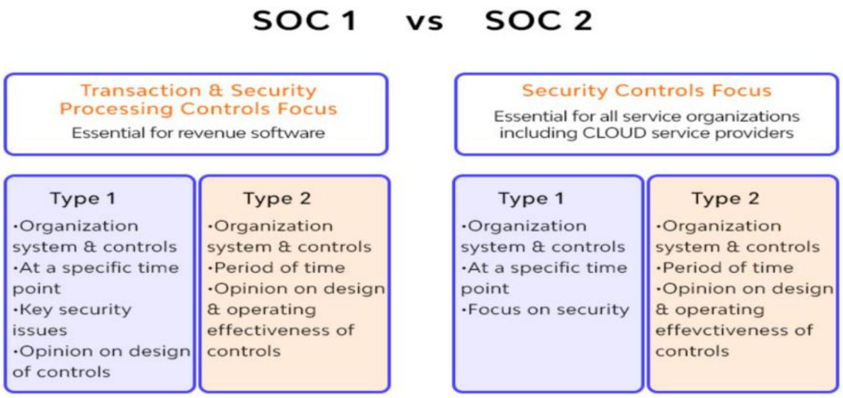
A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess the vendor's security posture despite the vendor not allowing for a direct audit.

The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor.



#	SOC 1	SOC 2	SOC 3
1	SOC 1 **reports on** service organizations internal controls relevant to customers financial statements (Internal Control Over Financial Reporting -ICFR).	SOC 2 **reports on** service organizations internal controls relevant to confidentiality, processing Integrity, availability, security, and privacy of customer data.	Same as SOC 2 but **light version**. (You must first complete SOC 2 before seeking SOC 3).
2	SOC 1 **objectives** cover controls around processing and securing customer financial data that includes both business and IT processes.	SOC 2 **objectives** cover any combination of 5 Trust Services Criteria- (1) Confidentiality (2) Processing Integrity (3) Availability (4) Security (5) Privacy	SOC 3 **objectives** cover the same criteria as SOC 2.
3	If your business provides services such as payroll, medical claims, SaaS provider, etc that stores and processes customers financial or sensitive data, you should seek SOC 1.	If your business provides services such as payroll, medical claims, SaaS provider, etc that stores and processes customers non-financial data, you should seek SOC 2.	A business can pursue this because this is excellent for marketing purposes.
4	SOC 1 report can be shared with management, auditors and controller's office.	SOC 2 report can be shared with the customers under NDA.	SOC 3 report does not contain description of auditor's test work and results. It can be made publicly available to all customers.
5	2 Types Type 1 (audit happens at a point in time) Type 2 (audit happens over a period of time)	2 Types Type 1 (audit happens at a point in time) Type 2(audit happens over a period of time)	Only available in Type 2 (such that audit happens over a period of time).

SOC 1 vs SOC 2 vs SOC 3


SOC 1 vs SOC 2
Transaction & Security Processing Controls Focus
Essential for revenue software
Security Controls Focus
Essential for all service organizations including CLOUD service providers
Type 1
·Organization system & controls
·At a specific time point
·Key security issues
·Opinion on design of controls
Type 2
·Organization system & controls
·Period of time
·Opinion on design & operating effectiveness of controls
Type 1
·Organization system & controls
·At a specific time point
·Focus on security
Type 2
·Organization system & controls
·Period of time
·Opinion on design & operating effevctiveness of controls

A. Service-level agreement: A service-level agreement defines the terms and conditions of service delivery but does not provide an independent assessment of security controls.

B. Business partnership agreement: A business partnership agreement outlines the terms and conditions of a business relationship but does not provide specific security assessment information.

D. Memorandum of understanding: A memorandum of understanding is a formal document outlining an agreement between parties, but it is not typically used to assess the security posture of a vendor

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 5

Question #:28 - (Exam Topic 1)

A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor who is not held to the same security control standards. Which of the following is the MOST likely source of the breach?

A. Side channel

B. Supply chain

C. Cryptographic downgrade

D. Malware

Answer: B

Explanation

A supply chain attack occurs when a third-party supplier or business partner is compromised, leading to an attacker gaining unauthorized access to the targeted organization's network. In this scenario, the dedicated business partner connection to a vendor was used to exfiltrate customer credit card data, indicating that the vendor's network was breached and used as a supply chain attack vector.

The breach occurred through a dedicated business partner connection to a vendor who is not held to the same security control standards as the company. This indicates a supply chain-related security issue. Here's why:

- Supply Chain: The term "supply chain" in the context of cybersecurity refers to the network of vendors, suppliers, and partners that an organization relies on for various products and services. In this case, the breach occurred through a connection to a vendor, making it a supply chain issue.
- Less Stringent Security Controls: The vendor, who is not held to the same security control standards as the company, suggests that the breach likely originated from a less secure part of the supply chain. The compromised vendor's security controls and practices may have been weaker, allowing attackers to gain access to sensitive data.

- Stolen and Exfiltrated Data: The fact that customer credit card data was stolen and exfiltrated indicates a breach of data security, which can occur when an element of the supply chain, such as a vendor, is compromised.

A. Side channel: Side-channel attacks typically involve the extraction of information from a system by analyzing physical or implementation-related characteristics, such as power consumption or timing. While side-channel attacks can be a threat, they are less likely to be the primary source of a breach involving the theft and exfiltration of customer credit card data through a vendor connection.

C. Cryptographic downgrade: Cryptographic downgrade attacks involve forcing a communication channel to use weaker cryptographic protocols or encryption methods. While these attacks can impact the security of data in transit, they are not typically associated with breaches that result in the theft and exfiltration of customer credit card data through a vendor connection.

D. Malware: Malware is malicious software that can be used to compromise systems, steal data, or perform other malicious activities. While malware can be a source of breaches, it would not be described as a dedicated business partner connection to a vendor, as implied in the scenario.

Question #:29 - (Exam Topic 1)

A help desk technician receives an email from the Chief Information Officer (C/O) asking for documents. The technician knows the CIO is on vacation for a few weeks. Which of the following should the technician do to validate the authenticity of the email?

A. Check the metadata in the email header of the received path in reverse order to follow the email’s path.

B. Hover the mouse over the CIO's email address to verify the email address.

C. Look at the metadata in the email header and verify the "From." line matches the CIO's email address.

D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents.

Answer: A

Explanation

Analyzing the email header metadata in reverse order allows the technician to trace the path of the email and verify its authenticity by examining the servers and routes it took. This can provide a technical confirmation of the email's legitimacy and origin, which is especially valuable when the CIO's identity is in question.

B. Hover the mouse over the CIO's email address to verify the email address:

- Hovering over the email address can reveal the actual email address associated with the displayed name, which can be helpful.
- This method is relatively straightforward and can quickly confirm if the email address matches the known CIO's email address.
- However, it may not provide as comprehensive a verification as examining the email header.

C. Look at the metadata in the email header and verify the "From:" line matches the CIO's email address:

- Examining the email header metadata is a standard method for email validation.
- Verifying that the "From:" line matches the CIO's known email address is a direct way to confirm the sender's authenticity.
- This method can provide assurance that the email is genuinely from the CIO, assuming the email header has not been tampered with.

D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents:

- Forwarding the email to the CIO for confirmation is a prudent step to take.
- However, it relies on a response from the CIO, which may not be immediate, especially if the CIO is on vacation.
- It's a good practice to confirm with the CIO directly, but it may not provide an immediate response for action.

Question #:30 - (Exam Topic 1)

Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

A. RTO

B. MTBF

C. MTTR

D. RPO

Answer: C

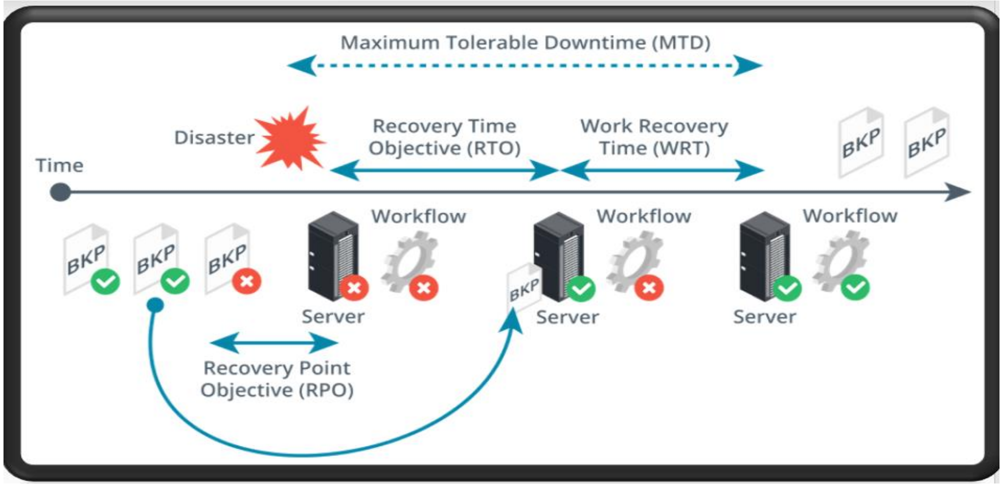
Explanation

MTTR stands for mean time to repair and is a key maintenance metric that indicates the average time taken to diagnose and rectify faulty equipment. It essentially measures an organization's efficiency in handling and resolving unplanned equipment breakdowns.

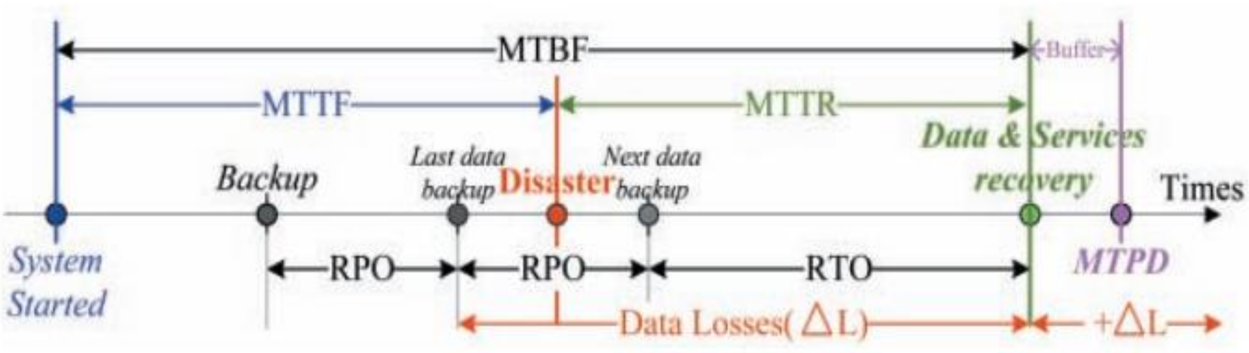
A: RTO (Recovery Time Objective): RTO specifies the maximum acceptable downtime for a particular system or process and represents the target time within which it should be restored after a failure.

B: MTBF (Mean Time Between Failures): MTBF measures the average time elapsed between consecutive failures of a system or equipment. It quantifies reliability, indicating how long a system can be expected to operate before experiencing a failure.

D: RPO (Recovery Point Objective): RPO specifies the maximum allowable data loss in the event of a failure or disaster. It represents the point in time to which data must be restored to resume normal operations.



References: CompTIA Security+ Certification Exam Objectives - 4.6 Explain the importance of secure coding practices. Study Guide: Chapter 7, page 323.



Question #:31 - (Exam Topic 1)

A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords. Which of the following should the network analyst enable to meet the requirement?

A. MAC address filtering

B. 802.1X

C. Captive portal

D. WPS

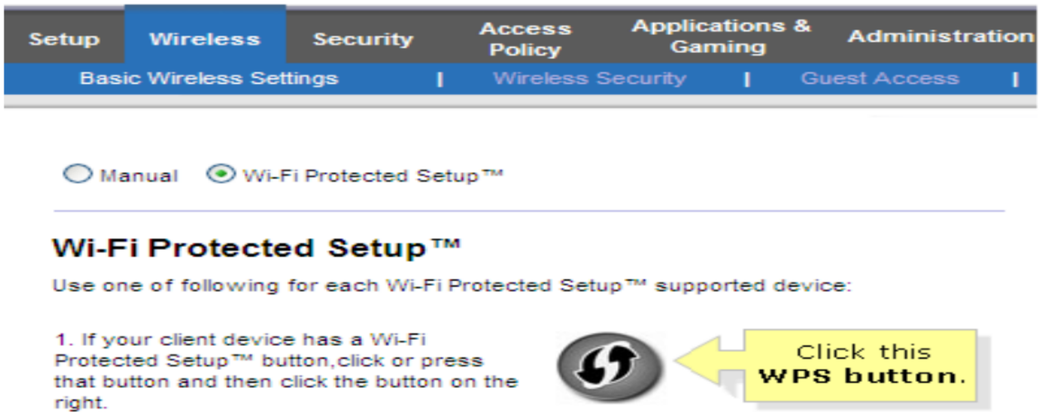
Answer: D

Explanation

The network analyst should enable Wi-Fi Protected Setup (WPS) to allow users to connect to the wireless access point securely without having to remember passwords. WPS allows users to connect to a wireless network by pressing a button or entering a PIN instead of entering a password.

Wi-Fi Protected Setup (WPS) is a feature designed to simplify the process of connecting devices to a secure wireless network. It allows users to connect to the network without manually entering a complex password. Instead, WPS typically provides two easy methods for secure connection:

- Push Button Configuration (PBC): Users can press a physical button on the router or access point and then press a corresponding button on their device (e.g., laptop, smartphone) to establish a secure connection.
- PIN Entry: Users can enter a PIN (Personal Identification Number) displayed on the router or access point into their device, and the devices will automatically exchange authentication information.



○ Manual ● Wi-Fi Protected Setup™

Wi-Fi Protected Setup™

Use one of following for each Wi-Fi Protected Setup™ supported device:

1. If your client device has a Wi-Fi Protected Setup™ button, click or press that button and then click the button on the right.

A. MAC address filtering: MAC address filtering restricts access based on the physical hardware address of devices. While it provides a layer of security, it does not eliminate the need for users to remember passwords, as devices still need to be authenticated based on their MAC addresses.

B. 802.1X: 802.1X is an authentication protocol that requires users to enter credentials to access the network. It does not eliminate the need for passwords.

C. Captive portal: A captive portal typically requires users to log in or agree to terms and conditions before gaining network access, often through a web-based interface. This method does not eliminate the need for passwords and may not align with the requirement of not needing to remember passwords.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4: Identity and Access Management

Question #:32 - (Exam Topic 1)

After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?

A. A DMZ

B. A VPN

C. A VLAN

D. An ACL

Answer: D

Explanation

Access Control Lists (ACLs) are commonly used to control and filter network traffic by permitting or denying specific types of traffic based on defined criteria. They are implemented at various points in a network, such as routers or firewalls, to manage traffic flow between network segments or subnets.

A. DMZ (Demilitarized Zone): A DMZ is a separate network segment that is typically used to host public-facing services like web servers or email servers. It is designed to provide an additional layer of security between the internal network and the internet but is not primarily used for controlling traffic between internal segments.

B. VPN (Virtual Private Network): A VPN is a technology that creates secure, encrypted connections over a public network (usually the internet). While it can be used to secure and control traffic between remote locations or users and the internal network, it is not typically used for controlling traffic between segments within the same network.

C. VLAN (Virtual Local Area Network): VLANs are used to logically segment a physical network into multiple virtual networks. While they can provide isolation between segments, VLANs themselves are not typically used for controlling traffic; they are primarily for network segmentation and management. ACLs or other security mechanisms are used to control traffic between VLANs.

References: CompTIA Security+ Certification Guide, Exam SY0-501

Question #:33 - (Exam Topic 1)

A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

A. Shadow IT

B. Credential stuffing

C. SQL injection

D. Man in the browser

E. Bluejacking

Answer: A

Explanation

Shadow IT refers to the use of unauthorized software or hardware by employees within an organization. In this case, it is possible that the sales director used an unauthorized application or service to access enterprise data, and that this access was not properly secured, allowing the thief who stole the laptop to gain access to the data.

B. Credential stuffing:Credential stuffing is a cyberattack method where attackers use username and password pairs obtained from previous data breaches to gain unauthorized access to user accounts on various online services.

- While credential stuffing can lead to unauthorized access to individual accounts, it typically does not directly lead to the compromise of enterprise data stored in the cloud.

C. SQL injection:SQL injection is a type of cyberattack where malicious SQL queries are injected into input fields of web applications to manipulate a database.

SQL injection attacks can result in unauthorized access to and manipulation of a database, but it's less likely to be the primary cause of enterprise data in the cloud being compromised due to a stolen laptop.

D. Man-in-the-browser: A Man-in-the-Browser (MitB) attack involves malware that infects a user's web browser, allowing an attacker to intercept and manipulate web transactions, including login credentials.

While a MitB attack can lead to credential theft, it typically does not directly compromise enterprise data stored in the cloud.

References:

CompTIA Security+ Certification Exam Objectives - Exam SY0-601

Question #:34 - (Exam Topic 1)

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

A. Bollard

B. Camera

C. Alarms

D. Signage

E. Access control vestibule

Answer: A

Explanation

A bollard would work best to prevent individuals from driving a car into the building. A bollard is a short, vertical post that can be used to block vehicles from entering a designated area. It is specifically designed to stop cars from crashing into buildings or other structures.

Bollards are posts designed to prevent vehicles from entering an area. They are usually made of steel or concrete and are placed close together to make it difficult for vehicles to pass through. In addition to preventing vehicles from entering an area, bollards can also be used to protect buildings and pedestrians from ramming attacks. They are an effective and cost-efficient way to protect buildings and pedestrians from unauthorized access.

Bollard: A bollard is a sturdy, vertical post typically made of metal or concrete, installed in front of entrances or areas where vehicle access needs to be restricted. They act as physical barriers and prevent vehicles from ramming into buildings or restricted areas.

B: Camera: Cameras are essential for surveillance and recording incidents, but they do not physically stop a vehicle from entering a building.

C: Alarms: Alarms can alert security personnel or law enforcement to an intrusion, but they do not physically prevent the intrusion itself.

D: Signage: Signage can provide warnings and instructions, but it is not a physical barrier to vehicle access.

E: Access control vestibule: Access control vestibules are designed to control human access through controlled entry points and may not be effective in stopping a vehicle.

Question #:35 - (Exam Topic 1)

Employees at a company are receiving unsolicited text messages on their corporate cell phones. The unsolicited text messages contain a password reset Link. Which of the attacks is being used to target the company?

A. Phishing

B. Vishing

C. Smishing

D. Spam

Answer: C

Explanation

Smishing is a type of phishing attack which begins with an attacker sending a text message to an individual. The message contains social engineering tactics to convince the person to click on a malicious link or send sensitive information to the attacker. Criminals use smishing attacks for purposes like:

Learn login credentials to accounts via credential phishing

Discover private data like social security numbers Send money to the attacker

Install malware on a phone

Establish trust before using other forms of contact like phone calls or emails

Attackers may pose as trusted sources like a government organization, a person you know, or your bank. And messages often come with manufactured urgency and time-sensitive threats. This can make it more difficult for a victim to notice a scam.

Phone numbers are easy to spoof with VoIP texting, where users can create a virtual number to send and receive texts. If a certain phone number is flagged for spam, criminals can simply recycle it and use a new one.

A: Phishing: Phishing typically involves deceptive emails that aim to trick recipients into revealing sensitive information or taking actions, such as clicking on malicious links or downloading malicious attachments.

B: Vishing: Vishing is a form of phishing conducted over voice calls (phone phishing), where attackers use social engineering techniques to impersonate legitimate entities and extract sensitive information over the phone.

D: Spam: Spam refers to unsolicited and often irrelevant or promotional messages sent via various communication channels, including email, text messages, and instant messaging. While spam can contain smishing or phishing attempts, it is a broad category of unwanted messages.

Question #:36 - (Exam Topic 1)

A company is planning to install a guest wireless network so visitors will be able to access the Internet. The stakeholders want the network to be easy to connect to so time is not wasted during meetings. The WAPs are configured so that power levels and antennas cover only the conference rooms where visitors will attend meetings. Which of the following would BEST protect the company's internal wireless network against visitors accessing company resources?

A. Configure the guest wireless network to be on a separate VLAN from the company's internal wireless network

B. Change the password for the guest wireless network every month.

C. Decrease the power levels of the access points for the guest wireless network.

D. Enable WPA2 using 802.1X for logging on to the guest wireless network.

Answer: A

Explanation

The best approach to protect the company's internal wireless network against unauthorized access by visitors is to segment the internal and guest wireless networks using VLANs (Virtual Local Area Networks) and implementing network access control (NAC) solutions.

By creating a separate VLAN for the guest wireless network, traffic between the guest and internal networks is isolated, preventing unauthorized access to company resources.

B: Changing the password for the guest wireless network every month is a security measure but might not be practical for providing easy access to visitors.

C: Decreasing the power levels of the access points for the guest wireless network can limit the network's coverage but does not necessarily prevent guests from accessing internal resources if they gain access to the network.

D: Enabling WPA2 using 802.1X for logging on to the guest wireless network is a good security measure, but it can add complexity and might not align with the goal of providing easy and hassle-free Internet access to visitors.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 4

Question #:37 - (Exam Topic 1)

Which of the following environments can be stood up in a short period of time, utilizes either dummy data or actual data, and is used to demonstrate and model system capabilities and functionality for a fixed, agreed-upon duration of time?

A. PoC

B. Production

C. Test

D. Development

Answer: A

Explanation

A POC (proof of concept) is an advanced demo project that reflects a real-world scenario. Since developing products from emerging technologies can be too risky or troublesome, POCs are often used to “prove” that a new technology, service, or idea is viable for the market.

It often uses dummy or real data to showcase how the system works in a real-world scenario. PoCs are time-limited and are used to validate whether a proposed solution meets the requirements and objectives before full-scale implementation.

B: Production: The production environment is the live, operational environment where the actual business processes and applications run. It is not typically used for testing or modeling.

C: Test: The test environment is used for testing software or system changes before they are deployed to the production environment. It is an isolated environment for quality assurance and validation.

D: Development: The development environment is where software and systems are created and developed. It is used by developers to build and code applications and solutions.

References: CompTIA Security+ Certification Guide, Exam SY0-501

Mamurjon Ismatov

—

Today at 11:44 AM

(Proof of Concept) It may use dummy data or actual data, and its purpose is to showcase the potential benefits and functionality of a solution.

Petra Martina Vrancic

—

Today at 11:44 AM

utilize dummy data or actual data and is created for a fixed, agreed-upon duration to showcase the feasibility or potential of a particular idea or solution.

Question #:38 - (Exam Topic 1)

A security assessment found that several embedded systems are running insecure protocols. These Systems were purchased two years ago and the company that developed them is no longer in business. Which of the following constraints BEST describes the reason the findings cannot be remediated?

A. inability to authenticate

B. Implied trust

C. Lack of computing power

D. Unavailable patch

Answer: D

Explanation

If the systems are running insecure protocols and the company that developed them is no longer in business, it is likely that there are no patches available to remediate the issue.

A: Inability to authenticate: While this constraint can be a security issue, it does not directly explain why the findings related to insecure protocols cannot be remediated.

B: Implied trust: Implied trust refers to situations where trust is assumed without proper authentication or verification. While it can be a security concern, it does not explain the inability to remediate insecure protocol issues.

C: Lack of computing power: A lack of computing power may affect the performance of embedded systems but is not the primary reason for the inability to remediate insecure protocol issues.

References:

CompTIA Security+ Certification Exam Objectives 1.6: Given a scenario, implement secure protocols. CompTIA Security+ Study Guide, Sixth Edition, pages 35-36

Question #:39 - (Exam Topic 1)

A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

A. Content filter

B. SIEM

C. Firewall rules

D. DLP

Answer: C

Explanation

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.

A. Content filter: Content filtering is typically used to restrict or filter specific types of content or websites. While it can be part of a security strategy, it may not directly address the issue of a high number of connections from specific IP addresses.

B. SIEM (Security Information and Event Management): SIEM solutions are used for monitoring and analyzing security events and incidents across an organization's network. They can help identify patterns and anomalies but are not typically used to address the issue described.

D. DLP (Data Loss Prevention): DLP solutions are designed to protect sensitive data from unauthorized access, sharing, or leakage. They focus on data protection and may not directly address the issue of a high number of incoming connections from specific IP addresses.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

Question #:40 - (Exam Topic 1)

A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

A. Use fuzzing testing

B. Use a web vulnerability scanner

C. Use static code analysis

D. Use a penetration-testing OS

Answer: C

Explanation

Static code analysis is when the code is examined without being executed. This analysis can be performed on both source code and object code bases. The term source code is typically used to designate the high-level language code, although, technically, source code is the original code base in any form, from high-level language to machine code. Static analysis can be performed by humans or tools, although humans are limited to the high- level language, while tools can be used against virtually any form of code base.

Using static code analysis would be the best approach to scan the source code looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. This method involves analyzing the source code without actually running the software, which can identify security vulnerabilities that may not be detected by other testing methods.

A: Fuzzing testing: Fuzzing is a dynamic testing technique that involves providing unexpected or random inputs to an application to find vulnerabilities. While it is valuable, it is typically used during dynamic testing phases, which occur after the development phase.

B: Web vulnerability scanner: Web vulnerability scanners are designed to identify vulnerabilities in web applications and websites. They are used during testing but may not cover all aspects of code analysis and may not be suitable for early detection in the development process.

D: Penetration-testing OS: A penetration-testing operating system (OS) is a specialized OS used for conducting security assessments, including penetration testing. It is not a tool for early-stage code analysis and vulnerability detection.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6: Risk Management, pp. 292-295

Question #:41 - (Exam Topic 1)

A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal data. Which of the following should the IT department implement to BEST protect the company against company data loss while still ***addressing the employees' concerns*****?**

A. Enable the remote-wiping option in the MDM software in case the phone is stolen.
B. Configure the MDM software to enforce the use of PINs to access the phone.
C. Configure MDM for FDE without enabling the lock screen.
D. Perform a factory reset on the phone before installing the company's applications.

`

Answer: B

Explanation

MDM software is a type of remote asset-management software that runs from a central server. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets. It can monitor and regulate both corporate-owned and personally owned devices to the organization’s policies.

FDE stands for full disk encryption, which is a method of encrypting all data on a device’s storage. FDE can protect data from unauthorized access in case the device is lost or stolen.

If a company decides to allow its employees to use their personally owned devices for work tasks, it should configure MDM software to enforce FDE on those devices. This way, the company can protect its data from being exposed if the device falls into the wrong hands.

However, employees may be concerned about the loss of personal data if the company also enables the remote-wiping option in the MDM software. Remote wiping is a feature that allows the company to erase all data on a device remotely in case of theft or loss. Remote wiping can also affect personal data on the device, which may not be acceptable to employees.

Therefore, a possible compromise is to configure MDM for FDE without enabling the lock screen. This means that the device will be encrypted, but it will not require a password or PIN to unlock it. This way, employees can access their personal data easily, while the company can still protect its data with encryption.

According to CompTIA Security+ SY0-601 Exam Objectives 2.4 Given a scenario, implement secure systems design:

“MDM software is a type of remote asset-management software that runs from a central server1. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets2.”

“FDE stands for full disk encryption, which is a method of encrypting all data on a device’s storage3.”

References: https://www.comptia.org/certifications/security#examdetails https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives https://www.makeuseof.com/what-is-mobile-device-management-mdm-software/

Question #:42 - (Exam Topic 1)

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations

B. It provides insurance in case of a data breach

C. It provides complimentary training and certification resources to IT security staff.

D. It certifies the organization can work with foreign entities that require a security clearance

E. It assures customers that the organization meets security standards

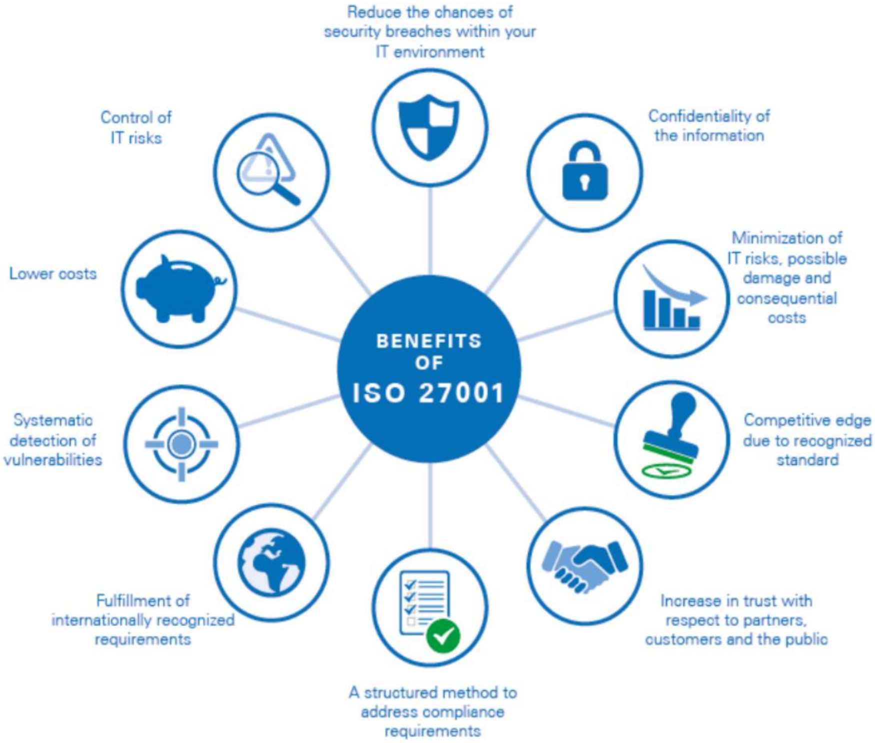
Answer: E

Explanation

ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS). It provides a framework for managing and protecting sensitive information using risk management processes. Acquiring an ISO 27001 certification assures customers that the organization meets security standards and follows best practices for information security management. It helps to build customer trust and confidence in the organization's ability to protect their sensitive information. References: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware, p. 7

The other options are not correct because:

A. ISO 27001 does not handle the sharing of forensic information between organizations.
B. ISO 27001 does not provide insurance against data breaches, it provides information on how to implement a backup solution to avoid loss of data.
C. ISO 27001 does provide general training to the staff but not specifically training towards IT security staff.
D. ISO 27001 does not provide security clearance towards an organization.


Reduce the chances of security breaches within your IT environment
Control of IT risks
Confidentiality of the information
Lower costs
Minimization of IT risks, possible damage and consequential costs
BENEFITS OF ISO 27001
Systematic detection of vulnerabilities
Competitive edge due to recognized standard
Fulfillment of internationally recognized requirements
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements

Question #:43 - (Exam Topic 1)

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

A. An air gap

B. A hot site

C. A VLAN

D. A screened subnet

Answer: D

Explanation

A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. References: CompTIA Security+ Certification Guide, Exam SY0-501

The other options are not correct because:

A. An air gapped subnet cannot receive connections from untrusted networks.
B. A hot site is an off-premises location where a company's work can resume during a disaster. A hot site has all the equipment necessary for a business to resume regular activities, including jacks for phones, backup data, computers and related peripherals.
C. A virtual local area network (VLAN) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.

Question #:44 - (Exam Topic 1)

A Chief information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?

A. DLP

B. CASB

C. HIDS

D. EDR

E. UEFI

Answer: A

Explanation

Detailed Explanation: Data Loss Prevention (DLP) can help prevent employees from stealing data by monitoring and controlling access to sensitive data. DLP can also detect and block attempts to transfer sensitive data outside of the organization, such as via email, file transfer, or cloud storage.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 10: Managing Identity and Access, p. 465

The other options are not correct because:

B. A cloud access security broker (CASB) is an on-premises or cloud-based security policy enforcement point between cloud service consumers and providers.

C. A Host-Based Intrusion Detection System, or HIDS, is a type of cybersecurity solution that monitors IT systems for signs of suspicious activity to detect unusual behaviors or patterns associated either with human users or applications that could be a sign of a security breach or attempted attack.

HIDS systems are so-named because they operate on individual host systems. In this context, a host could be a server, a PC, or any other type of device that produces logs, metrics, and other data that can be monitored for security purposes.

D:EDR (Endpoint Detection and Response): EDR solutions are similar to HIDS but provide advanced capabilities for detecting and responding to security incidents on endpoints. While they are valuable for endpoint security, they may not directly address data theft from network shares.

E. Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace basic input/output system (BIOS) but is compatible with it.

Azamat Iskakov

—

Today at 12:00 PM

here's interesting information: CompTIA has made a pile of name changes in the last 18 months: Was called > Now called Demilitarized Zone > Screened Subnet (Can't say "militarized") Man-In-The-Middle Attack > On-path attack (can't say "man") Man trap > Access control vestibule (can't say "man") Black list > block list White list > allow list

Question #:45 - (Exam Topic 1)

An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?

A. SIEM

B. SOAR

C. EDR

D. CASB

Answer: B

Explanation

Security Orchestration, Automation, and Response (SOAR) should be implemented to integrate incident response processes into a workflow with automated decision points and actions based on predefined playbooks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

The other options are not correct because:

A. Security information and event management (SIEM) is a security solution that helps organizations detect threats before they disrupt business.

C. Endpoint Detection and Response (EDR), also known as Endpoint Threat Detection and Response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

D. According to Gartner, a cloud access security broker (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Think of the CASB as the sheriff that enforces the laws set by the cloud service administrators.

Question #:46 - (Exam Topic 1)

A security analyst needs an overview of vulnerabilities for a host on the network. Which of the following is the BEST type of scan for the analyst to run to discover which vulnerable services are running?

A. Non-credentialed

B. Web application

C. Privileged

D. Internal

Answer: A

Explanation

Non-credentialed scans are also known as network scans or port scans. They are conducted by sending packets to different ports on the target host to determine which ports are open and which services are running. This type of scan is useful for discovering vulnerabilities in the network, such as outdated software or misconfigured services.

Web application scans are used to discover vulnerabilities in web applications running on a host, while privileged scans require credentials or administrative access to the target host, which may not be available to the security analyst. Internal scans are used to scan the internal network and are not specific to a single host.

Non-credentialed scans **enumerate a host's exposed ports, protocols, and services and identifies vulnerabilities and misconfigurations that could allow an attacker to compromise your network**. Ideal for large-scale assessments in traditional enterprise environments.

Credential-based vulnerability assessment, which make use of the admin account, do a more thorough check by looking for problems that cannot be seen from the network. On the other hand, **non-credentialed scans provide a quick view of vulnerabilities by only looking at network services exposed by the host**

Question #:47 - (Exam Topic 1)

Which of the following identifies the point in time when an organization will recover data in the event of an outage?

A. SLA

B. RPO

C. MTBF

D. ARO

Answer: B

Explanation

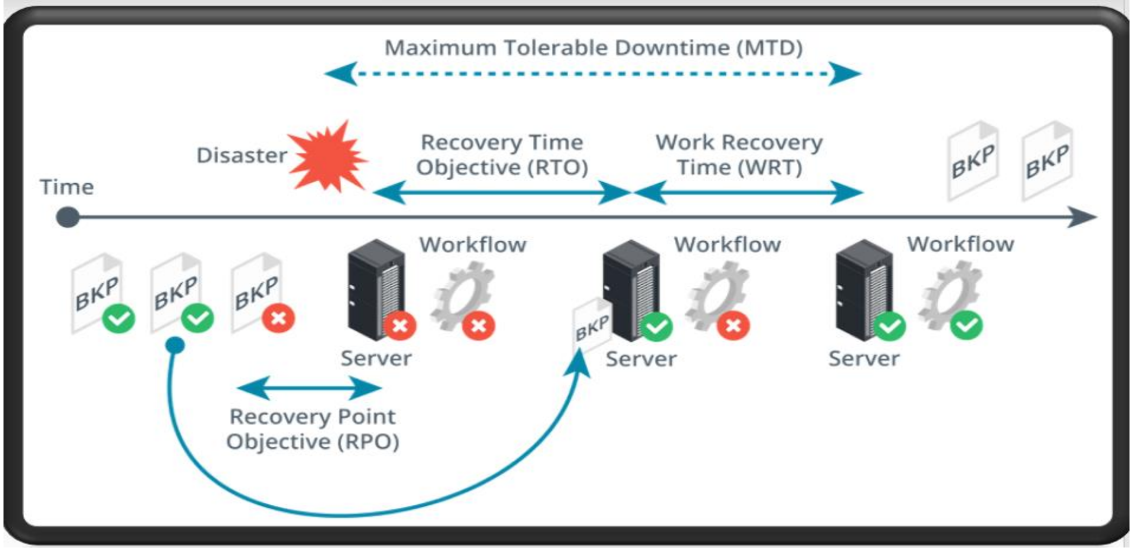
Detailed Explanation: Recovery Point Objective (RPO) is the maximum duration of time that an organization can tolerate data loss in the event of an outage. It identifies the point in time when data recovery must begin, and any data loss beyond that point is considered unacceptable.

Reference: CompTIA Security+ Certification Guide, Exam SY0-601 by Mike Chapple and David Seidl, Chapter-7: Incident Response and Recovery, Objective 7.2: Compare and contrast business continuity and disaster recovery concepts, pp. 349-350.

A. Service level agreement (SLA). An SLA is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.

C. MTBF (mean time between failures) is the average time between repairable failures of a technology product. The metric is used to track both the availability and reliability of a product. The higher the time between failure, the more reliable the system.

D. Annualized Rate of Occurrence, also known as ARO, refers to the expected frequency with which a risk or a threat is expected to occur. ARO is also commonly referred to as Probability Determination.



Question #:48 - (Exam Topic 1)

A company recently experienced an attack during which its main website was directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the company implement to prevent this type of attack from occurring in the future?

A. IPsec

B. SSL/TLS

C. DNSSEC

D. S/MIME

Answer: C

Explanation

The attack described in the scenario is a DNS hijacking attack.

To prevent this type of attack from occurring in the future, the company should implement DNSSEC (Domain Name System Security Extensions).

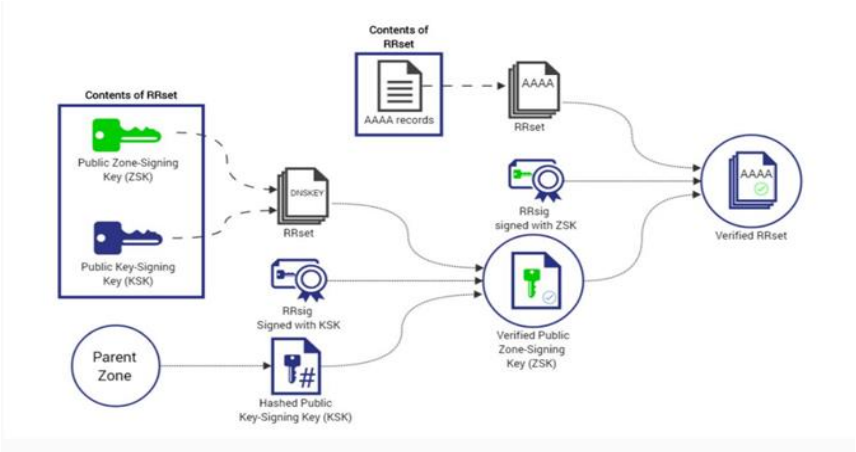
DNSSEC is a set of security extensions to the DNS protocol that provide origin authentication of DNS data, data integrity, and authenticated denial of existence.

By using DNSSEC, the company can ensure that DNS requests are not tampered with and that customers are directed to the correct web server.

IPSec is a protocol used for secure communication over IP networks.

SSL/TLS is a protocol used to secure web traffic.

S/MIME is a protocol used to secure email traffic. While these protocols are important for security, they do not address the specific issue of DNS hijacking.



Question #:49 - (Exam Topic 1)

A security analyst must enforce policies to harden an MDM infrastructure. The requirements are as follows:

* Ensure mobile devices can be tracked and wiped.

* Confirm mobile devices are encrypted.

Which of the following should the analyst enable on all the devices to meet these requirements?

A. A Geofencing

B. Biometric authentication

C. Geolocation

D. Geotagging

Answer: C

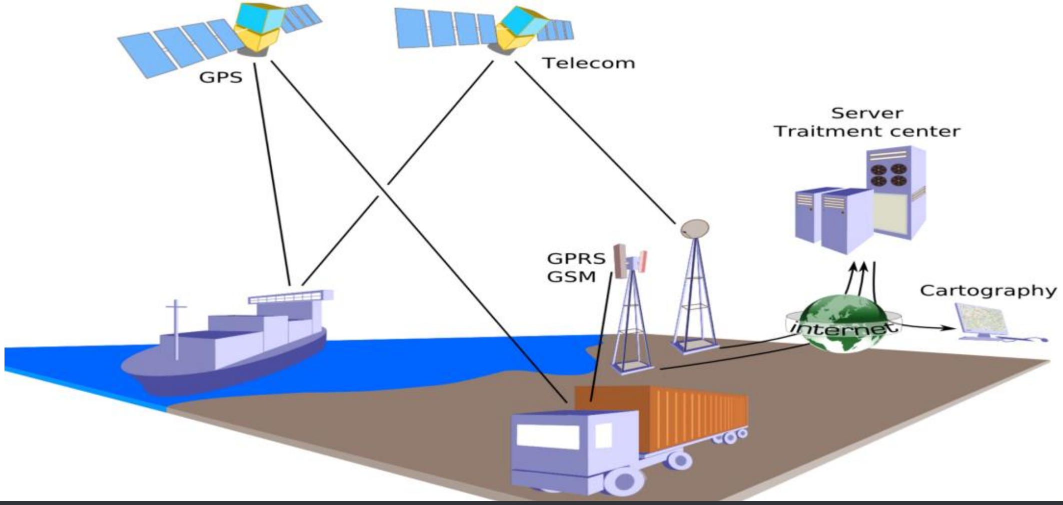
Explanation

Geolocation: Geolocation allows for the tracking and location of mobile devices. It enables the MDM system to determine the physical location of devices, which is essential for tracking and remote wiping in case a device is lost or stolen. Additionally, geolocation can provide data on device movement and can trigger actions such as remote wiping when a device goes out of a designated area (geofencing).

A: Geofencing: Geofencing is used to define geographical boundaries and trigger actions when a device enters or exits those boundaries. While it can be related to geolocation, it's not used to enforce encryption or confirm device encryption status.

B: Biometric authentication: Biometric authentication refers to methods like fingerprint or facial recognition, which are used for device access and user authentication but do not address tracking, wiping, or encryption directly.

D: Geotagging: Geotagging is the process of adding geographical information to media files like photos and videos. It is not used to track, wipe, or confirm device encryption.



Israfil Yilmaz

—

Today at 12:07 PM

encryted

Emin Gun

—

Today at 12:07 PM

it's about logging

Bilal Sevinc

—

Today at 12:07 PM

just distance realted

Alex Portnoy

—

Today at 12:07 PM

geo fancing its limiting in one particualr area

Nita Arapi

—

Today at 12:07 PM

specific location or area

Question #:50 - (Exam Topic 1)

Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).

A. Mantraps

B. Security guards

C. Video surveillance

D. Fences

E. Bollards

F. Antivirus

Answer: A B

Explanation

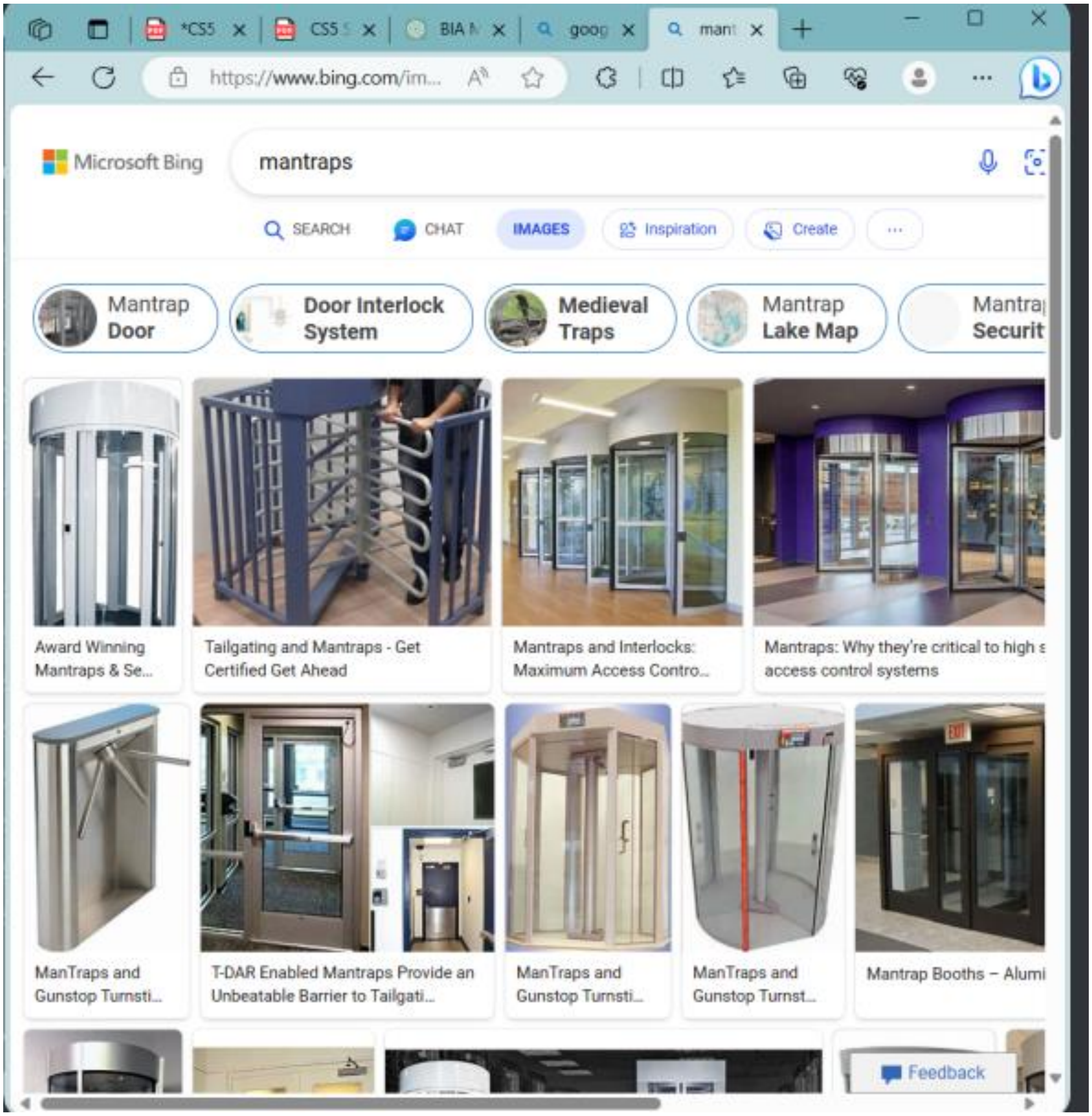
A - a mantrap can trap any personnel with bad intention (preventive), and kind of same as detecting, since you will know if someone is trapped there(detective), and it can deter those personnel from approaching as well(deterrent) B - security guards can sure do the same thing as above, preventing malicious personnel from entering(preventive+deterrent), and notice those personal as well(detective)

C. Video surveillance is the use of security cameras to monitor and record activity in a specific area or location for security, safety or monitoring purposes. Security cameras capture live footage, which can be viewed in real-time or recorded for later review. Video surveillance is also referred to as CCTV.

D. Security fencing is one of the most important forms of property protection. It can be used in industrial or commercial environments to provide maximum security for assets, storage areas as well as open spaces on the property.

E. Security bollards are also visual guides to pedestrians and traffic, but are additionally built to resist vehicle impact. These are often made of steel and filled with concrete, but can be decorated with a fine finish or a cover.

F. Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.


https://www.bing.com/im...
Microsoft Bing
mantraps
SEARCH
CHAT
IMAGES
Inspiration
Create
Mantrap Door
Door Interlock System
Medieval Traps
Mantrap Lake Map
Mantrap Securit
Award Winning Mantraps & Se...
Tailgating and Mantraps - Get Certified Get Ahead
Mantraps and Interlocks: Maximum Access Contro...
Mantraps: Why they're critical to high s access control systems
ManTraps and Gunstop Turnsti...
T-DAR Enabled Mantraps Provide an Unbeatable Barrier to Tailgati...
ManTraps and Gunstop Turnsti...
ManTraps and Gunstop Turnst...
Mantrap Booths – Alumi
Feedback

Question #:51 - (Exam Topic 1)

A security incident has been resolved. Which of the following BEST describes the importance of the final phase of the incident response plan?

A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future.//////////// Lesson learned

B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed. /////////////// Recovery

C. It identifies the incident and the scope of the breach, how it affects the production environment, and the ingress point. ////////////////////Identification

D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach. //////////////////////////Containment

Answer: A

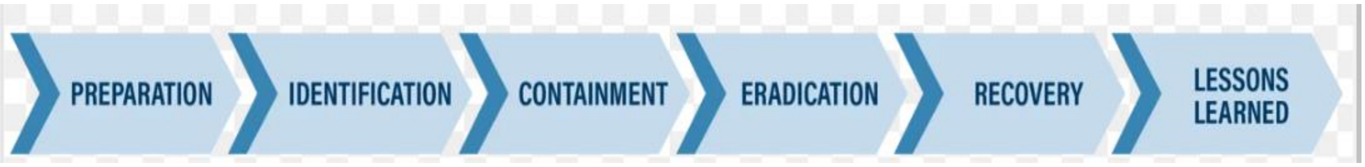
Explanation

The final phase of an incident response plan is the post-incident activity, which involves examining and documenting how well the team responded, discovering what caused the incident, and determining how the incident can be avoided in the future. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 225.

B. This is Eradication and Recovery.

C. This is Detection and Analysis

D. This is Containment



The final phase of the incident response is also called the lessons learned or remediation step.

======================

Phases of the Incident Response Plan:

1. Preparation - Preparing for an attack and how to respond

2. Identification - Identifying the threat

3. Containment - Containing the threat

4. Eradication - Removing the threat

5. Recovery - Recovering affected systems

6. Lessons Learned - Evaluating the incident response, see where there can be improvements for a future incident.

Question #:52 - (Exam Topic 1)

The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building. Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?

A. Authentication protocol

B. Encryption type

C. WAP placement

D. VPN configuration

Answer: C

Explanation

WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.

WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:

> Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.
>
> Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.
>
> Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

A. Authentication protocol is not relevant here since it should be paired with WAP.

B. Similar to A, encryption without proper placement for coverage does not cover all bases.

D. VPN stands for "virtual private network" — a service that helps you stay private online by encrypting the connection between your device and the internet. This secure connection provides a private tunnel for your data and communications while you use public networks.

Question #:53 - (Exam Topic 1)

The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

A. HIDS

B. Allow list

C. TPM

D. NGFW

Answer: D

Explanation

Next-Generation Firewalls (NGFWs) are designed to provide advanced threat protection by combining traditional firewall capabilities with intrusion prevention, application control, and other security features.

NGFWs can detect and block unauthorized access attempts, malware infections, and other suspicious activity. They can also be used to monitor file access and detect unauthorized copying or distribution of copyrighted material.

A next-generation firewall (NGFW) can be used to detect and prevent copyright infringement by analyzing network traffic and blocking unauthorized transfers of copyrighted material. Additionally, NGFWs can be configured to enforce access control policies that prevent unauthorized access to sensitive resources.

References:

CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

A. A host-based intrusion detection system is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces, similar to the way a network-based intrusion detection system operates.
B. Application allowlisting, or application control, is a security capability that reduces harmful security attacks by allowing only trusted files, applications, and processes to be run.
C. What is a Trusted Platform Module (TPM)? Why is it Important?
D. A Trusted Platform Module (TPM) is a specialized chip on a laptop or desktop computer that is designed to secure hardware with integrated cryptographic keys. A TPM helps prove a user's identity and authenticates their device. A TPM also helps provide security against threats like firmware and ransomware attacks.

Question #:54 - (Exam Topic 1)

Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company’s final software releases? (Select TWO.)

A. Unsecure protocols

B. Use of penetration-testing utilities

C. Weak passwords

D. Included third-party libraries

E. Vendors/supply chain

F. Outdated anti-malware software

Answer: D E

Explanation

The most likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases are:

1. Supply chain attacks - injecting vulnerable code into open-source components used by the company.
2. Insider threats - employees intentionally or accidentally introducing vulnerable code.
3. Unsecured third-party code - including code from untrusted sources without proper security analysis.
4. Lack of code review processes - failing to properly review code for vulnerabilities before release.
5. Poor software development practices - not following secure coding guidelines, failing to address known vulnerabilities, etc.

A. Unsecure protocols are when protocol, service, or port that introduces security concerns due to the lack of controls over confidentiality and/or integrity this has nothing to do with the inclusion of vulnerable code in software unless its included in a third party library by another vendor or supply chain.
B. Pentesting is utilized to find vulnerabilities.
C. Weak passwords can be an attack vector towards a malicious actor adding vulnerable code in a software but not likely to happen.

Petra Martina Vrancic

—

Today at 12:50 PM

These two vectors highlight the importance of scrutinizing external sources in the software development process to ensure that no vulnerable or malicious code is introduced unintentionally. It's crucial for software companies to have robust practices in place for vetting and monitoring their supply chain and third-party dependencies.

References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Supply Chain and Software Development Life Cycle

Question #:55 - (Exam Topic 1)

Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

A. Hashing

B. DNS sinkhole

C. TLS inspection

D. Data masking

Answer: C

Explanation

TLS inspection allows the IDS and WAF to decrypt and inspect the contents of HTTPS traffic. Without TLS inspection, the IDS and WAF are unable to analyze the encrypted traffic, and threats may go undetected. TLS inspection works by intercepting the HTTPS traffic, decrypting it, and inspecting it for threats or vulnerabilities. The traffic is then re-encrypted and sent to its original destination.

A: Hashing is a one-way function that transforms data into a fixed-length string of characters, typically used for data integrity verification.
B: DNS sinkhole is a technique for redirecting a domain name to a different IP address.
D: Data masking is a process of obscuring or anonymizing sensitive data to protect it from unauthorized access.
While these techniques can be used for security purposes, they are not specifically required for IDS and WAF to be effective on HTTPS traffic.

References: [1] CompTIA Security+ Study Guide Exam SY0-601 [1], Sixth Edition, Chapter 11, "Network Security Monitoring" [2] CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, Chapter 7, "Intrusion Detection and Prevention"

Question #:56 - (Exam Topic 1)

Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).

A. Page files

B. Event logs

C. RAM

D. Cache

E. Stored files

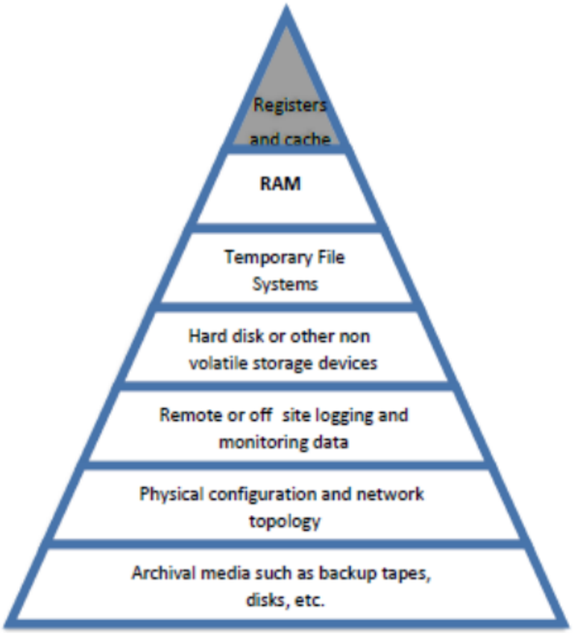
F. HDD

Answer: C D

Explanation

Order of volatility:

1. CPU, **cache**, and register contents (collect first)
2. Routing tables, ARP cache, process tables, kernel statistics
3. Live network connections and data flows
4. **Memory (RAM)**
5. Temporary file system/swap space
6. Data on hard disk
7. Remotely logged data
8. Data stored on archival media/backups (collect last)


Registers and cache
RAM
Temporary File Systems
Hard disk or other non volatile storage devices
Remote or off site logging and monitoring data
Physical configuration and network topology
Archival media such as backup tapes, disks, etc.

References: CompTIA Security+ Study Guide 601, Chapter 11

Question #:57 - (Exam Topic 1)

A security engineer needs to build a solution to satisfy regulatory requirements that state certain critical servers must be accessed using MFA. However, the critical servers are older and are unable to support the addition of MFA. Which of the following will the engineer MOST likely use to achieve this objective?

A. A forward proxy

B. A stateful firewall

C. A jump server

D. A port tap

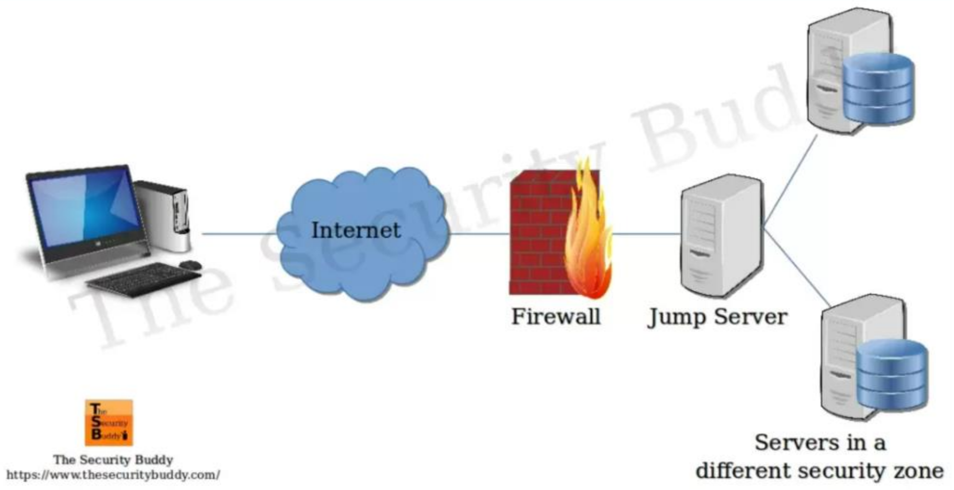
Answer: C

Explanation

A jump server is a secure host that allows users to access other servers within a network. The jump server acts as an intermediary, and users can access other servers via the jump server after authenticating with MFA.

A. A forward proxy is an intermediary that sits between one or more user devices and the internet. Instead of validating a client request and sending it directly to a web server, a forward proxy server evaluates the request, takes any needed actions, and routes the request to the destination on the client's behalf.
B. In computing, a stateful firewall is a network-based firewall that individually tracks sessions of network connections traversing it. Stateful packet inspection, also referred to as dynamic packet filtering, is a security feature often used in non-commercial and business networks.

D. A tap is typically a dedicated hardware device, which provides a way to access the data flowing across a computer network. The network tap has (at least) three ports: an A port, a B port, and a monitor port.



Question #:58 - (Exam Topic 1)

An employee receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm the employee's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing

B. Whaling

C. Phishing

D. Vishing

Answer: C

Explanation

Phishing is a type of social engineering attack that uses fraudulent emails or other forms of communication to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing emails often impersonate legitimate entities, such as banks, online services, or lottery organizations, and entice users to click on malicious links or attachments that lead to fake websites or malware downloads. Phishing emails usually target a large number of users indiscriminately, hoping that some of them will fall for the scam.

References: https://www.comptia.org/certifications/security#examdetails
https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.kaspersky.com/resource-center/definitions/what-is-phishing

A. “Spear phishing” is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.
B. Whaling is a highly targeted phishing attack - aimed at senior executives - masquerading as a legitimate email. Whaling is digitally enabled fraud through social engineering, designed to encourage victims to perform a secondary action, such as initiating a wire transfer of funds.

D. Voice phishing, or vishing, is the use of telephony to conduct phishing attacks. Landline telephone services have traditionally been trustworthy; terminated in physical locations known to the telephone company, and associated with a bill-payer.

Question #:59 - (Exam Topic 1)

A backdoor was detected in the containerized application environment. The investigation detected that a zero-day vulnerability was introduced when the latest container image version was downloaded from a public registry. Which of the following is the BEST solution to prevent this type of incident from occurring again?

A. Enforce the use of a controlled trusted source of container images

B. Deploy an IPS solution capable of detecting signatures of attacks targeting containers

C. Define a vulnerability scan to assess container images before being introduced on the environment

D. Create a dedicated VPC for the containerized environment

Answer: A

Explanation

Enforcing the use of a controlled trusted source of container images is the best solution to prevent incidents like the introduction of a zero-day vulnerability through container images from occurring again. References: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 11: Cloud Security, Container Security

B. An IPS is not capable of detecting a change in the source code of a container image.

C. The more appropriate solution is to use controlled trusted sources of container images.

D. This answer is still doesn’t solve the problem of the zero day being present.

Question #:60 - (Exam Topic 1)

A company acquired several other small companies. The company that acquired the others is transitioning network services to the cloud. The company wants to make sure that performance and security remain intact. Which of the following BEST meets both requirements?

A. High availability

B. Application security

C. Segmentation

D. Integration and auditing

Answer: C

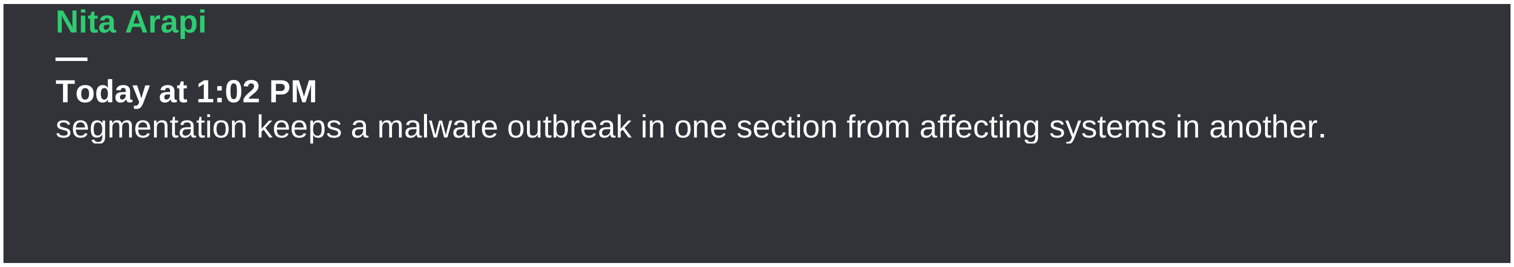
Explanation

Segmentation is a best practice in network security that can both maintain performance and enhance security. By creating separate segments for different parts of the network, you can control and limit traffic, reducing congestion (thereby potentially improving performance), and you can limit the spread of security threats.

High availability (Option A) is a concept aimed at ensuring an agreed level of operational performance, but it doesn't directly address security.

Application security (Option B) is crucial, but it doesn't encompass the entirety of network performance and security needs in a scenario like this.

Integration and auditing (Option D) are important practices, especially in a situation where several companies are being merged, but they don't directly ensure performance and security. Integration ensures that disparate systems work together, and auditing allows for review of processes, but neither directly ensures performance or security across a network.



Nita Arapi

—

Today at 1:02 PM

segmentation keeps a malware outbreak in one section from affecting systems in another.

Question #:61 - (Exam Topic 1)

A store receives reports that shoppers' credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store. The attackers are using the targeted shoppers' credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

A. Identity theft

B. RFID cloning

C. Shoulder surfing

D. Card skimming

Answer: D

Explanation

The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases. References:

CompTIA Security+ Study Guide Exam SY0-601, Chapter 5

A. Identity theft is used to apply for loans and new credit cards.
B. Credit cards work with NFC
C. The keyword is “shoppers also withdrew money from an ATM in that store” meaning the ATM probably has a skimmer.

Bezhan Safah

—

Today at 1:05 PM

Skimming occurs when devices illegally installed on ATMs, point-of-sale (POS) terminals, or fuel pumps capture data or record cardholders' PINs. Criminals use the data to create fake debit or credit cards and then steal from victims' accounts.

Question #:62 - (Exam Topic 1)

A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application.

B. The system was quarantined for missing software updates.

C. The software was not added to the application whitelist.

D. The system was isolated from the network due to infected software

Answer: C

Explanation

This is a common symptom of an application that is being blocked by an application whitelist.

To resolve the issue, the desktop support technician should add the new software program to the application whitelist to allow it to run on the computer.

Application whitelisting: is the approach of restricting the usage of any tools or applications only to those that are already vetted and approved. Organizations adopt this approach by delegating a system administrator or third-party application to manage the list of applications and enforce these restrictions.

Firewall rules determine if traffic will go through or get blocked. Because he is already installed but cant use it. in order to use it they need to approved app as a in white list

The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run.

References: https://www.techopedia.com/definition/31541/application-whitelisting

A. While this is possible the question asks for the most likely cause which is C.
B. While this is possible the question asks for the most likely cause which is C.
C. While this is possible the question asks for the most likely cause which is C.

Question #:63 - (Exam Topic 1)

Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production

B. Test

C. Staging

D. Development

Answer: D

Explanation

A development environment is the environment that is used to develop and test software. It is typically installed locally on a system that allows code to be assessed directly and modified easily with each build. In this environment, dummy data is often utilized to test the software's functionality.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 3: Architecture and Design

The environment that utilizes dummy data and is most likely to be installed locally on a system that allows it to be assessed directly and modified easily with each build is the development environment. The development environment is used for developing and testing software and applications. It is typically installed on a local system, rather than on a remote server, to allow for easy access and modification. Dummy data can be used in the development environment to simulate real-world scenarios and test the software's functionality.

References: https://www.techopedia.com/definition/27561/development-environment

A. BBIn a production environment, systems go live and your developed code is released to end-users. You deploy completed code that has endured proper vulnerability testing and risk analysis. All of the testing is complete and there's the expectation that you'll find only minor bugs, if any.
B. A test environment is where the testing teams analyze the quality of the application/program. This also allows computer programmers to identify and fix any bugs that may impact smooth functioning of the application or impair

user experience.

C. Staging environments are made to test codes, builds, and updates to ensure quality under a production-like environment before application deployment. The staging environment requires a copy of the same configurations of hardware, servers, databases, and caches.

Question #:64 - (Exam Topic 1)

A bad actor tries to persuade someone to provide financial information over the phone in order to gain access to funds. Which of the following types of attacks does this scenario describe?

A. Vishing

B. Phishing

C. Spear phishing

D. Whaling

Answer: A

Explanation

Vishing is a social engineering attack that uses phone calls or voicemail messages to trick people into divulging sensitive information, such as financial information or login credentials.

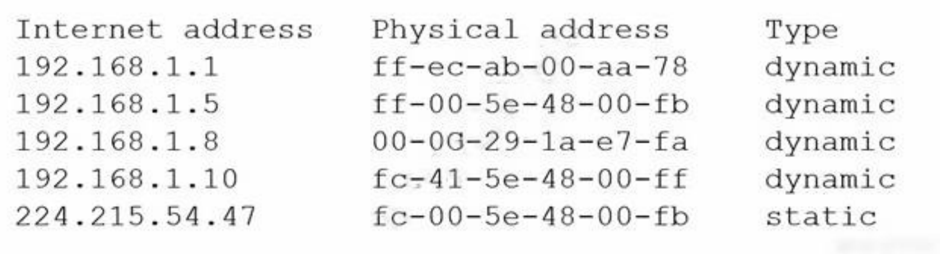
B. Phishing is a form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

C. "Spear phishing" is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents.

D. Whaling is a highly targeted phishing attack - aimed at senior executives - masquerading as a legitimate email. Whaling is digitally enabled fraud through social engineering, designed to encourage victims to perform a secondary action, such as initiating a wire transfer of funds.

Question #:65 - (Exam Topic 1)

A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:



```
Internet address     Physical address      Type
192.168.1.1          ff-ec-ab-00-aa-78     dynamic
192.168.1.5          ff-00-5e-48-00-fb     dynamic
192.168.1.8          00-0G-29-1a-e7-fa     dynamic
192.168.1.10         fc-41-5e-48-00-ff     dynamic
224.215.54.47        fc-00-5e-48-00-fb     static
```

Which of the following BEST describes the attack the company is experiencing?

A. MAC flooding

B. URL redirection

C. ARP poisoning

D. DNS hijacking

Answer: C

Explanation

Note: all links are dynamic and the static just poisoned the log. Last MAC says static, this MAC is forged and its indication of ARP poisoning.

The output of the “arp -a” command shows that there are two connections to the same IP address and port number. This indicates that there are two active sessions between the client and server.

The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client’s browser.

Based on the output of the “netstat -ano” command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as **C. ARP poisoning**.

ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

A. In computer networking, a media access control attack or MAC flooding is a technique employed to compromise the security of network switches.
B. A URL redirection attack is a form of web-based threat where the attacker manipulates URLs to redirect users from a legitimate website to a malicious one, mostly to steal sensitive information or distribute malware.

D. Domain Name Server (DNS) hijacking is a type of DNS attack. An attacker purposefully manipulates how DNS queries are resolved, thereby redirecting users to malicious websites. Hackers either install malware on user PCs, seize control of routers, or intercept or hack DNS connections to carry out the attack.

Nita Arapi

—

Today at 1:12 PM

ARP poisoning is a technique that manipulates ARP tables to redirect network traffic, while MAC flooding targets Ethernet switches to disrupt their normal operation and potentially capture network traffic

Question #:66 - (Exam Topic 1)

A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy

A. Incremental backups followed by differential backups

B. Full backups followed by incremental backups

C. Delta backups followed by differential backups

D. Incremental backups followed by delta backups

E. Full backup followed by differential backups

Answer: B

Explanation

In the event of a system failure, the amount of data lost is the smallest with incremental backup strategy, since only the data that has not yet been backed up after the most recent increment is affected.

Differential backups only back up the files that have changed since the previous full backup, while incremental backups do the same, they back up the files that have changed since the previous incremental or full backup.

Incremental backup: Backs up all files that have changed since the last backup occurred. Differential backup: Backs up only copies of all files that have changed since the last full backup.

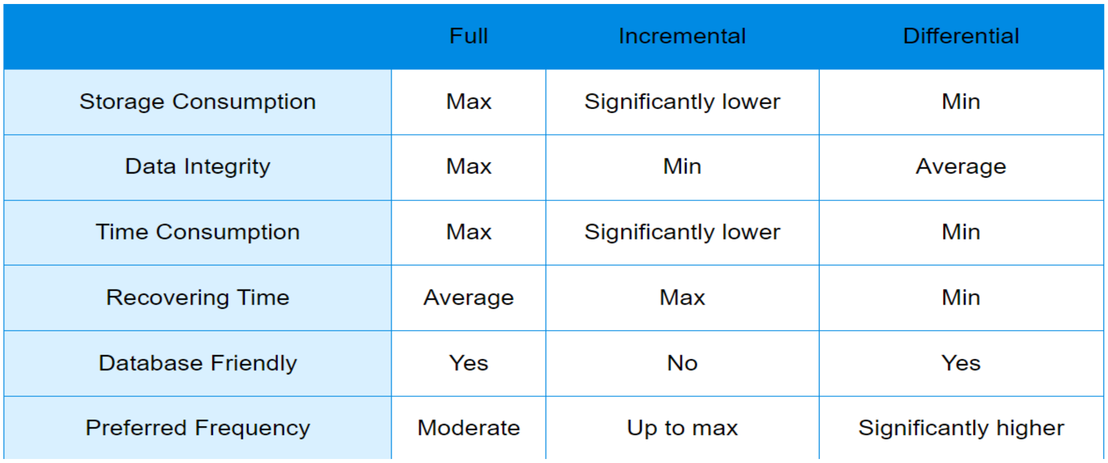
C. A delta, or incremental delta, backup image is a copy of all database data that has changed since the last successful backup (full, incremental, or delta) of the table space in question. This is also known as a differential, or noncumulative, backup image.

D. Differential backups only back up the files that have changed since the previous full backup, while incremental backups do the same, they back up the files that have changed since the previous incremental or full backup.

E. Differential backups are ideal when organizations must find a balance between backup size and restoration time. This strategy is optimal for quick data recovery, as the process involves applying the latest full backup followed by the most recent differential backup.

Reference: https://anexia.com/blog/en/the-3-best-backup-strategies-for-your-data-backup/#:~:text=Advantages%20of%20incremental%20backup&text=In%20the%20event%20of%20a%20system%20failure%2C%20the%20amount%20of,most%20recent%20increment%20is%20affected.

CompTIA Security+ Certification Guide, Third Edition (Exam SY0-601) page 126



	Full	Incremental	Differential
Storage Consumption	Max	Significantly lower	Min
Data Integrity	Max	Min	Average
Time Consumption	Max	Significantly lower	Min
Recovering Time	Average	Max	Min
Database Friendly	Yes	No	Yes
Preferred Frequency	Moderate	Up to max	Significantly higher

1. Storage Consumption: An average consumption of free storage space per a typical backup task.
2. Data Integrity: A possibility of restoring links between backup components without recovering.
3. Time Consumption: A typical task runtime for a particular type of data backup method.
4. Recovering Time: A typical runtime for a recovery task used to a particular backup method.
5. Database Friendly: An option of saving database content in a “hot” mode.

6. Preferred Frequency: A typical frequency for implementing these types of data backup.

Source: https://www.handybackup.net/backup_articles/backup-type.shtml

Question #:67 - (Exam Topic 1)

Which of the following is a risk that is specifically associated with hosting applications in the public cloud?

A. Unsecured root accounts

B. Zero day

C. Shared tenancy

D. Insider threat

Answer: C

Explanation

When hosting applications in the public cloud, there is a risk of shared tenancy, meaning that multiple organizations are sharing the same infrastructure. This can potentially allow one tenant to access another tenant's data, creating a security risk. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

Options A, B, and D are not specifically associated with hosting applications in the public cloud, although they can be potential risks in any computing environment.

Question #:68 - (Exam Topic 1)

A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

```
User account ‘JHDoe’ does not exist…
User account ‘VMAdmin’ does not exist…
User account ‘tomcat’ wrong password…
User account ‘Admin’ does not exist…
```

Which of the following MOST likely would have prevented the attacker from learning the service account name?

A. Race condition testing

B. Proper error handling

C. Forward web server logs to a SIEM

D. Input sanitization

Answer: B

Explanation

Based on the errors the attacker was able to figure out which accounts exist and which do not. This allowed the attacker to focus their attention on the existing accounts and brute force them. Therefore it is important to do proper error handling to avoid giving attackers too much information. Even when error messages don’t provide a lot of detail, inconsistencies in such messages can still reveal important clues on how a site works, and what information is present under the covers. For example, when a user tries to access a file that does not exist, the error message typically indicates, “file not found”. When accessing a file that the user is not authorized for, it indicates, “access denied”. The user is not supposed to know the file even exists, but such inconsistencies will readily reveal the presence or absence of inaccessible files or the site’s directory structure.

B. Proper error handling is the control that would have most likely prevented the attacker from learning the service account name.

Proper error handling is a crucial aspect of application security, as it helps prevent information leakage and other security issues. In this case, the logs indicate that the application is providing information about the existence or non-existence of user accounts, which could allow an attacker to learn the name of the service account.

By implementing proper error handling, the application could be configured to provide a generic error message, rather than providing information about specific user accounts. This would make it more difficult for an attacker to learn the name of the service account.

Race condition testing (A) is a technique for detecting and preventing race conditions, which occur when two or more processes or threads access shared resources in an unexpected way.

Forwarding web server logs to a SIEM (C) is a best practice for monitoring and analyzing security events, but it would not necessarily prevent the attacker from learning the service account name.

Input sanitization (D) is a technique for validating and filtering user input to prevent malicious input from being processed by an application. While input sanitization is an important control for preventing attacks such as SQL injection and cross-site scripting (XSS), it is not directly related to the issue described in the question.

How to solve the issue: **built in function to protect inputs using try-catch to solve it**

Source: https://owasp.org/www-community/Improper_Error_Handling

The other answers are not relevant to the question.

Question #:69 - (Exam Topic 1)

As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

C. HTTPS://*.app1.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022

D. HTTPS://".comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2023

Answer: C

Explanation

This certificate property will meet the requirements because it has a wildcard at the secondary subdomain level (.app1.comptia.org), which means it can be used for any subdomain under app1.comptia.org, such as test.app1.comptia.org or dev.app1.comptia.org. It also has a validity period of less than one year, which means it will need to be rotated annually. The other options do not meet the requirements because they either have a wildcard at the primary domain level (.comptia.org), which is not allowed, or they have a validity period of more than one year, which is too long.

A: This is not correct because it does not include a secondary subdomain.

B:This is not correct because it does not include the wildcard.

D: This is not correct because it does not include the wildcard and the duration is 2 years.

Question #:70 - (Exam Topic 1)

Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data. Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public. Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE

B. TPM

C. HIDS

D. VPN

Answer: A

Explanation

Based on these definitions, the best security solution to mitigate the risk of future data disclosures from a laptop would be FDE. FDE would prevent unauthorized access to the data stored on the laptop even if it is stolen or lost. FDE can also use TPM to store the encryption key and ensure that only trusted software can decrypt the data. HIDS and VPN are not directly related to data encryption, but they can provide additional security benefits by detecting intrusions and protecting network traffic respectively.

B. A Trusted Platform Module (TPM) is a specialized chip on a laptop or desktop computer that is designed to secure hardware with integrated cryptographic keys. A TPM helps prove a user's identity and authenticates their device. A TPM also helps provide security against threats like firmware and ransomware attacks.The most common task associated with a TPM is FDE, or Full-Disk Encryption.

C. A Host-Based Intrusion Detection System, or HIDS, is a type of cybersecurity solution that monitors IT systems for signs of suspicious activity to detect unusual behaviors or patterns associated either with human users or applications that could be a sign of a security breach or attempted attack.

D. A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Nigina Novruzova

—

Today at 1:23 PM

(FDE) - protects all data stored on a hard drive from unauthorized access using disk-level encryption.

Question #:71 - (Exam Topic 1)

Which of the following is the MOST secure but LEAST expensive data destruction method for data that is stored on hard drives?

A. Pulverizing

B. Shredding

C. Incinerating

D. Degaussing

Answer: B

Explanation

Degaussing is a process that uses a strong magnetic field to erase data from a hard drive. This method is considered very secure because it completely destroys the data, making it unrecoverable. Degaussing machines can be purchased for a relatively low cost, making it a cost-effective data destruction method.

Question #:72 - (Exam Topic 1)

An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files. Which of the following controls should the organization consider to mitigate this risk?

A. EDR

B. Firewall

C. HIPS

D. DLP

Answer: D

Explanation

DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, print, email, upload, or download sensitive data based on predefined policies and rules.

References: https://www.comptia.org/certifications/security#examdetails

https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives
https://www.forcepoint.com/cyber-edu/data-loss-prevention-dlp

The other answers are not relevant to the case in point.

Question #:73 - (Exam Topic 1)

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyber threat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII

B. TLP

C. TTP

D. STIX

Answer: A

Explanation

TAXII (Trusted Automated Exchange of Indicator Information): TAXII is a protocol and a set of specifications that facilitate the sharing of cyber threat intelligence data, including indicators of compromise (IOCs), with external security partners, organizations, and stakeholders. It allows for the automated exchange of structured threat information in a standardized and secure manner.

B: TLP (Traffic Light Protocol): TLP is a set of designations used to indicate the sensitivity of shared threat intelligence. It focuses on the handling and sharing guidelines for threat intelligence rather than the technical mechanisms for sharing.
C: TTP (Tactics, Techniques, and Procedures): TTPs are descriptions of how threat actors conduct attacks. While they are valuable for understanding threats, they do not directly relate to the technical means of sharing threat intelligence.
D: STIX (Structured Threat Information eXpression): STIX is a standardized language for representing structured threat information. While it is related to threat intelligence, it is primarily a format for encoding and sharing threat information rather than a transport protocol like TAXII. STIX and TAXII are often used together to share threat intelligence effectively

Bilal Sevinc

—

Today at 1:29 PM

TAXII is a protocol and standard specifically designed for sharing cyber threat intelligence and indicators of compromise (IoC) among trusted entities, such as security partners and other organizations.
.

Question #:74 - (Exam Topic 1)

Which of the following incident response steps occurs before containment?

A. Eradication

B. Recovery

C. Lessons learned

D. Identification

Answer: D

Explanation

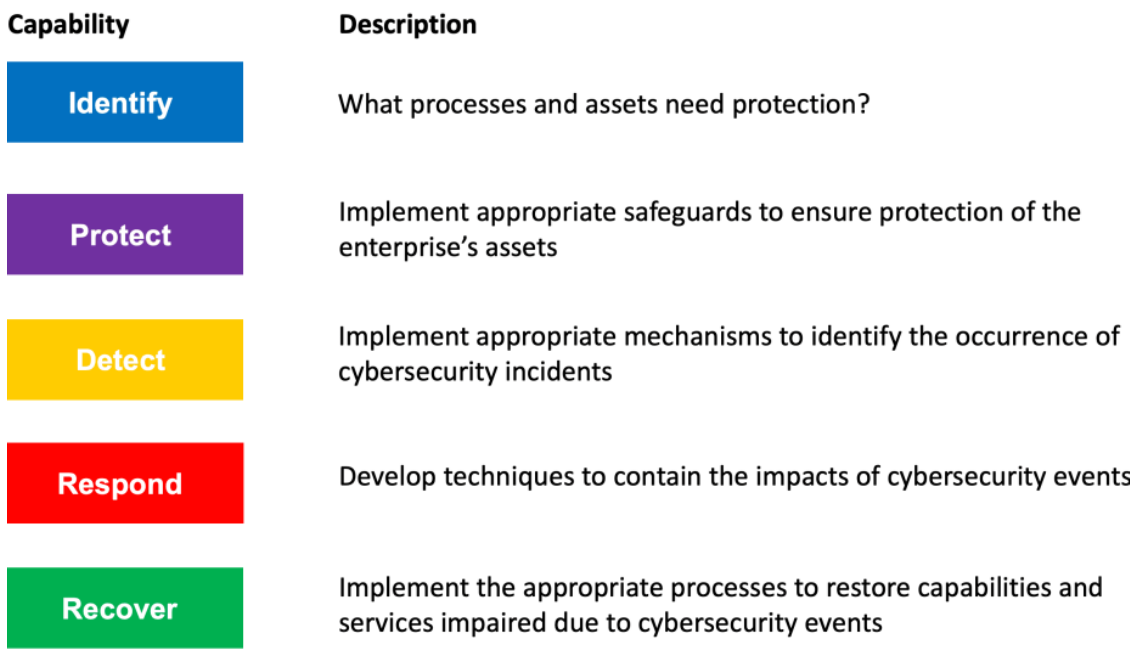
Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.

A: Eradication: Following containment, the eradication phase focuses on completely removing the root cause of the incident from the affected systems and environment.

B: Recovery: Once the threat has been eradicated, the recovery phase begins. During this phase, systems and services are restored to normal operation, and business operations are resumed.

C: Lessons Learned: Lessons learned and post-incident analysis typically occur after the incident has been fully addressed. It involves a comprehensive review of the incident, identification of weaknesses in security measures, and recommendations for improvements to prevent future incidents.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 10: Incident Response and Recovery, pp. 437-441.



Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

Question #:75 - (Exam Topic 1)

Which of the following environments would MOST likely be used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics?

A. Test

B. Staging

C. Development

D. Production

Answer: A

Explanation

The test environment is used to assess the execution of component parts of a system at both the hardware and software levels and to measure performance characteristics. References: CompTIA Security+ Study Guide 601, Chapter 2

B. Staging environments are made to test codes, builds, and updates to ensure quality under a production-like environment before application deployment. The staging environment requires a copy of the same configurations of hardware, servers, databases, and caches.

C. A development environment in software and web development is a workspace for developers to make changes without breaking anything in a live environment. The development environment is often seen as a developer's “everything-goes” workspace.

D. A production environment is a real-time setting where the latest versions of software, products, or updates are pushed into live, usable operation for the intended end users. One very common example of this would be a company updating a new version of their app and making it live for all users.

Staging Environment VS Test Environment

A staging environment mimics the production environment to perform final QA checks on application.	A test environment validates each component of application under test.
It replicates all requirements and configurations of the production environment.	It is dynamic and requires specific configurations to test each component.
It validates the complete application.	It tests the Individual components or functions.

Both testing and staging environments play a critical role in ensuring the application performs as expected in real-life scenarios. On the one hand, the testing environment ensures each application component performs its job well. On the other hand, the staging environment ensures the application’s features work well with everything connected around it.

Mohammadreza Mostafaei
—
Today at 1:32 PM
stage is befor to publish the app

Bezhan Safah
—
Today at 1:32 PM
Test > Staging > Production (LIVE)

Question #:76 - (Exam Topic 1)

A customer has reported that an organization's website displayed an image of a smiley face rather than the expected web page for a short time.Two days earlier ,a security analyst reviews log tries and sees the following around the time of the incident:

Website	Time	Name server	A record
CompTIA.org	8:10	names.comptia.org	192.168.1.10
CompTIA.org	9:00	names.comptia.org	192.168.1.10
CompTIA.org	9:30	ns.attacker.org	10.10.50.5
CompTIA.org	10:00	names.comptia.org	192.168.1.10

Which of the following is MOST likely occurring?

A. Invalid trust chain

B. Domain hijacking

C. DNS poisoning

D. URL redirection

Answer: C

Explanation

The log entry shows the IP address for "www.example.com" being changed to a different IP address, which is likely the result of DNS poisoning.

DNS poisoning occurs when an attacker is able to change the IP address associated with a domain name in a DNS server's cache, causing clients to connect to the attacker's server instead of the legitimate server.

It's redirecting traffic from server to different IP so it's DNS poisoning

DNS poisoning, also known as DNS cache poisoning, occurs when an attacker manipulates or corrupts the DNS (Domain Name System) cache to redirect domain name resolutions to malicious IP addresses. In this case, the log entries show a suspicious change in the DNS resolution for the "CompTIA.org" domain:

- At 8:10, the website's A record (IP address) is resolved to "192.168.1.10" by the nameserver "names.comptia.org," which appears legitimate.
- At 9:30, there is a change in the resolution, where the nameserver "ns.attacker.org" resolves the A record to "10.10.50.5." This change in DNS resolution is highly suspicious and indicates a possible DNS poisoning attack.
- At 10:00, the resolution reverts to the previous IP address "192.168.1.10."

The sudden change in the DNS resolution to an attacker-controlled IP address (10.10.50.5) suggests that DNS poisoning may have occurred. This could lead to the website displaying unexpected content, such as the smiley face image reported by the customer.

A: Invalid trust chain: This typically relates to SSL/TLS certificates and trust issues in certificate chains, which doesn't align with the DNS resolution changes described in the log entries.

B: Domain hijacking: Domain hijacking involves unauthorized changes to domain registrar settings or ownership, but it doesn't directly manipulate DNS cache as described here.

D: URL redirection: URL redirection is typically a legitimate configuration used for various purposes, and it doesn't involve changing DNS cache entries to malicious IP addresses.

References: CompTIA Security+ SY0-601 Exam Objectives: 3.2 Given a scenario, implement secure network architecture concepts.

Question #:77 - (Exam Topic 1)

A company recently experienced an attack during which its main website was directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers. Which of the following should the company implement to prevent this type of attack from occurring in the future?

A. IPSec

B. SSL/TLS

C. DNSSEC

D. S/MIME

Answer: C

Explanation

The attack described in the question is known as a **DNS hijacking** attack. In this type of attack, an attacker modifies the DNS records of a domain name to redirect traffic to their own server. This allows them to intercept traffic and steal sensitive information such as user credentials.

To prevent this type of attack from occurring in the future, the company should implement **C. DNSSEC**.

DNSSEC (Domain Name System Security Extensions) is a security protocol that adds digital signatures to DNS records. This ensures that DNS records are not modified during transit and prevents DNS hijacking attacks.

A. In computing, Internet Protocol Security is a secure network protocol suite that authenticates and encrypts packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks.
B. TLS/SSL provides secure (encrypted) communication between a remote client and a TCP/IP application server. Under TLS protocol, the application server is always authenticated. To participate in a TLS session, an application server must provide a certificate signed by a certificate authority (CA) to prove its identity.

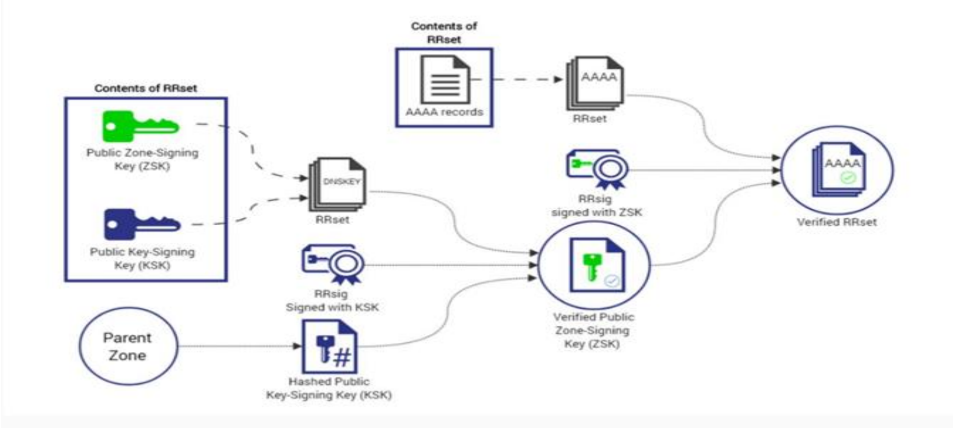
D. S/MIME (Secure/Multipurpose internet Mail Extensions) is a widely accepted protocol for sending digitally signed and encrypted messages.

Petra Martina Vrancic

—

Today at 1:36 PM

attacker manipulates the DNS resolution process to redirect traffic to a malicious server. To prevent this type of attack, implementing DNSSEC is a suitable solution.



Question #:78 - (Exam Topic 1)

A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which of the following configurations should an analysis enable to improve security? (Select TWO.)

A. RADIUS /// authorization

B. PEAP

C. WPS

D. WEP-EKIP

E. SSL

F. WPA2-PSK//// improving security

Answer: A F

Explanation

WPA2 and RADIUS can work together to provide a secure wireless network, with RADIUS providing centralized authentication and WPA2 providing encryption and authentication for the data transmitted over the air**.**

WPA2 is a security protocol that provides encryption and authentication for wireless networks. It uses Advanced Encryption Standard (AES) encryption to secure data transmission over a wireless network and 802.1X for authentication, which provides centralized management of user accounts. WPA2 is considered to be the most secure wireless security protocol and is recommended for use in all Wi-Fi networks.

RADIUS, on the other hand, is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network access. It is used for remote authentication of users who want to access a network, and it can be used to secure various types of networks, including wireless networks, VPNs, and dial-up connections. RADIUS provides several benefits in terms of security, including centralized management of user accounts, support for strong encryption, and the ability to implement two-factor authentication.

In a wireless network, WPA2 provides the encryption and authentication for the data transmitted over the air, while RADIUS provides the centralized management of user accounts and authentication of users attempting to connect to the network.

PEAP(Protected Extensible ***Authentication*** Protocol) is an 802.1X authentication method that **uses server-side public key certificate to establish a secure tunnel in which the client authenticates with server**. The PEAP authentication creates an encrypted SSL/TLS tunnel between client and authentication server

Bezhan Safah

—

Today at 1:39 PM

Wi-Fi Protected Access Pre-Shared Key or WPA-PSK is a system of encryption used to authenticate users on wireless local area networks.

Question #:79 - (Exam Topic 1)

A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promotion to production?

A. Disable unneeded services.

B. Install the latest security patches.

C. Run a vulnerability scan.

D. Encrypt all disks.

Answer: C

Explanation

Running a vulnerability scan is the final step to be performed prior to promoting a system to production. This allows any remaining security issues to be identified and resolved before the system is put into production. Final is vulnerability testing to make sure its not vulnerable to publish.

A: Disable unneeded services: This is typically done during system hardening to reduce the attack surface by disabling unnecessary services.
B: Run a vulnerability scan: Vulnerability scans are conducted to identify and remediate vulnerabilities before the system is put into production. It is often performed earlier in the system's lifecycle.
D: Encrypt all disks: Disk encryption is an important security measure but is generally implemented as part of the system's initial configuration and may not be the final step before production promotion.

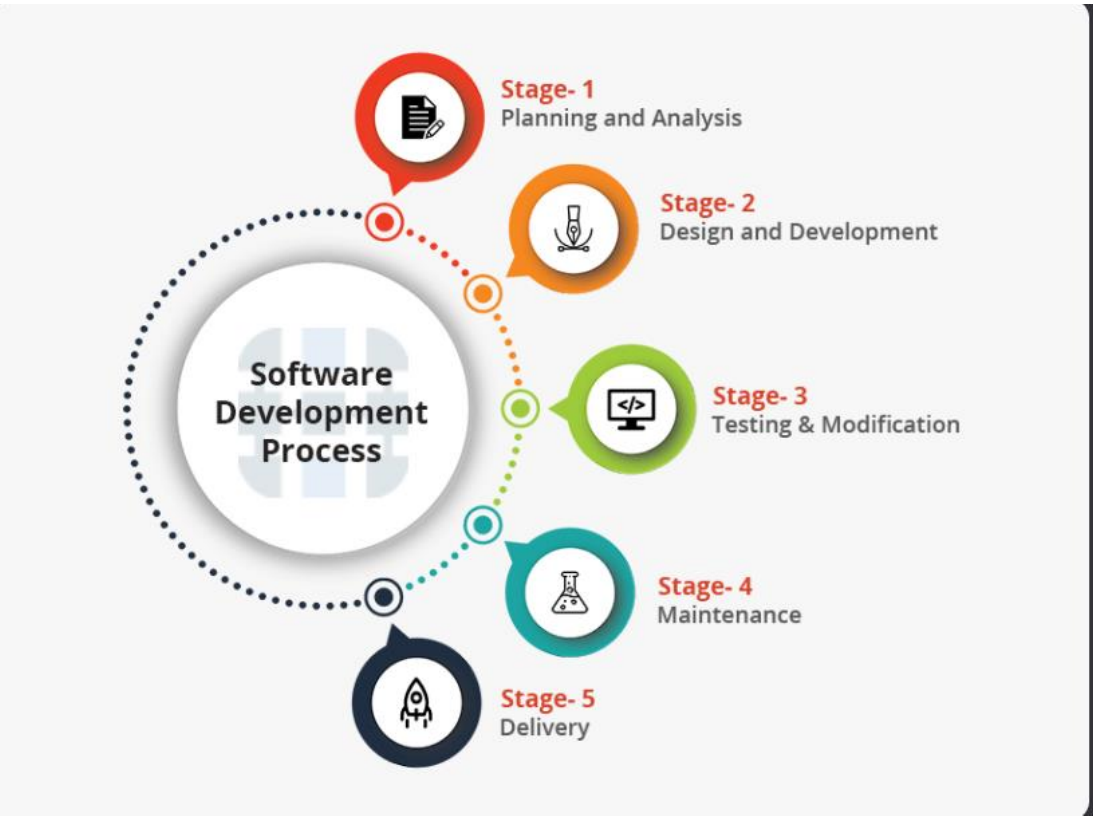
References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3

Nigina Novruzova

—

Today at 1:41 PM

Vulnerability scans - checks specific parts of your network for flaws.



Question #:80 - (Exam Topic 1)

An application owner reports suspicious activity on an internal financial application from various internal users within the past 14 days. A security analyst notices the following:

•Financial transactions were occurring during irregular time frames and outside of business hours by unauthorized users.

•Internal users in question were changing their passwords frequently during that time period.

•A jump box that several domain administrator users use to connect to remote devices was recently compromised.

•The authentication method used in the environment is NTLM.

Which of the following types of attacks is MOST likely being used to gain unauthorized access?

A. Pass-the-hash

B. Brute-force

C. Directory traversal

D. Replay

Answer: A

Explanation

Pass-the-Hash is a credential theft and lateral movement technique in which an attacker abuses the NTLM authentication protocol to authenticate as a user without ever obtaining the account’s plaintext password.

Since the attacker uses the password hash, which normally changes only when the password itself is changed, the adversary has significant time to abuse the compromised account.

NTLM providesExchange and SharePoint services,it can also be main reason

The suspicious activity reported by the application owner, combined with the recent compromise of the jump box and the use of NTLM authentication, suggests that an attacker is likely using a pass-the-hash attack to gain unauthorized access to the financial application. This type of attack involves stealing hashed passwords from memory and then using them to authenticate as the compromised user without needing to know the user's plaintext password.

B. Brute force would be detected immediately.

C. Directory traversal is not relevant to the questions.

D. Replay attack is not relevant to the question. A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a spoofing attack by IP packet substitution.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

Question #:81 - (Exam Topic 1)

A dynamic application vulnerability scan identified code injection could be performed using a web form.

Which of the following will be BEST remediation to prevent this vulnerability?

A. Implement input validations

B. Deploy MFA

C. Utilize a WAF

D. Configure HIPS

Answer: A

Explanation

A. Implement Input Validations: Input validation involves checking and sanitizing user input to ensure that it adheres to expected formats and doesn't contain malicious code. By validating and sanitizing input data, you can prevent most code injection attacks, such as SQL injection and cross-site scripting (XSS). This is considered a fundamental security practice and should be applied to all parts of your application where user input is accepted.

B. Deploy MFA (Multi-Factor Authentication): Multi-Factor Authentication is an excellent security measure, but it primarily addresses authentication and access control issues. While MFA adds an extra layer of security, it does not directly mitigate code injection vulnerabilities.

C. Utilize a WAF (Web Application Firewall): WAFs are designed to protect web applications from various types of attacks, including SQL injection and XSS. However, they are not a substitute for proper input validation. WAFs can provide an additional layer of security but should be used in conjunction with other security measures.

D. Configure HIPS (Host Intrusion Prevention System): HIPS can help monitor and protect against various forms of attacks, including some code injection attacks. However, they are typically more focused on system-level threats rather than application-level vulnerabilities. It's important to use HIPS in a comprehensive security strategy but not rely solely on it to address code injection vulnerabilities.

References: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 3, 18

Question #:82 - (Exam Topic 1)

A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?

A. Dumpster diving

B. Shoulder surfing

C. Information elicitation

D. Credential harvesting

Answer: A

Explanation

Crosscut shredders are used to destroy paper documents and reduce the risk of data leakage through dumpster diving. Dumpster diving is a method of retrieving sensitive information from paper waste by searching through discarded documents.

B: Shoulder surfing: Shoulder surfing involves attackers observing or capturing sensitive information, such as passwords or PINs, by looking over a person's shoulder as they enter the information. This is typically addressed through physical security measures and privacy screens.

C: Information elicitation: Information elicitation refers to the act of obtaining information from individuals through conversation or social engineering techniques. This risk is typically mitigated through security awareness training and policies.

D: Credential harvesting: Credential harvesting involves attackers collecting usernames and passwords, often through phishing or other malicious means. It is typically addressed through security awareness training, multi-factor authentication (MFA), and email filtering.

References:

CompTIA Security+ Study Guide, Exam SY0-601, 6th Edition, Chapter 1

Dumpster diving
This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:
1 Passwords
2 Access codes
3 Organizational charts
4 Calendars
5 Network/application diagrams
6 Credit card receipts
7 Expense reports
8 Phone numbers
9 Printed emails
10 Names

Question #:83 - (Exam Topic 1)

While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network witches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps

B. A Telnet session

C. An SSH connection

D. SFTP traffic

Answer: B

Explanation

The security analyst is likely observing a Telnet session, as Telnet transmits data in plain text format, including usernames and passwords. Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware.

Bilal Sevinc — Today at 1:48 PM

Telnet is a protocol used for remote terminal access and management of network devices. However, it is considered insecure because it sends data, including usernames and passwords, in plaintext, making it susceptible to eavesdropping and interception. When Telnet is used for communication, usernames and passwords are transmitted in an unencrypted form, allowing an observer to capture and view them in plaintext.

Mamurjon Ismatov — Today at 1:48 PM

usernames and passwords are often sent in plaintext,

Danut Halau — Today at 1:48 PM

a Telnet session refers to a network communication session established using the Telnet protocol. Telnet (short for "teletype network") is a protocol that allows users to remotely access and manage devices or systems over a network

Farid Abbasov — Today at 1:48 PM

23

volkan — Today at 1:48 PM

23

Danut Halau — Today at 1:48 PM

23

Question #:84 - (Exam Topic 1)

Which of the following authentication methods sends out a unique password to be used within a specific number of seconds?

A. TOTP

B. Biometrics

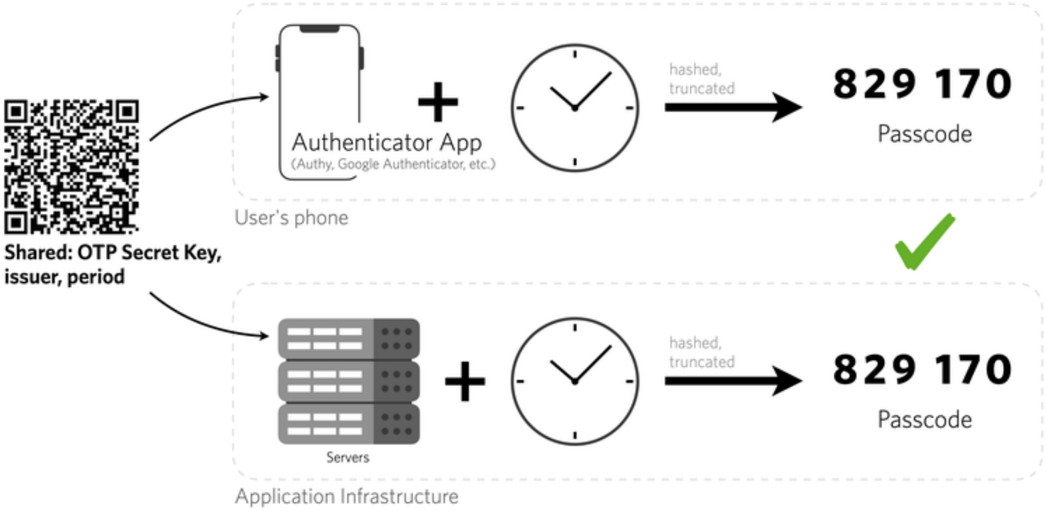
C. Kerberos

D. LDAP

Answer: A

Explanation

Time-based One-Time Password (TOTP) is a type of authentication method that sends out a unique password to be used within a specific number of seconds. It uses a combination of a shared secret key and the current time to generate a one-time password. TOTP is commonly used for two-factor authentication (2FA) to provide an additional layer of security beyond just a username and password.



Question #:85 - (Exam Topic 1)

A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

A. Disable Telnet and force SSH.

B. Establish a continuous ping.

C. Utilize an agentless monitor

D. Enable SNMPv3 With passwords.

Answer: D

Explanation

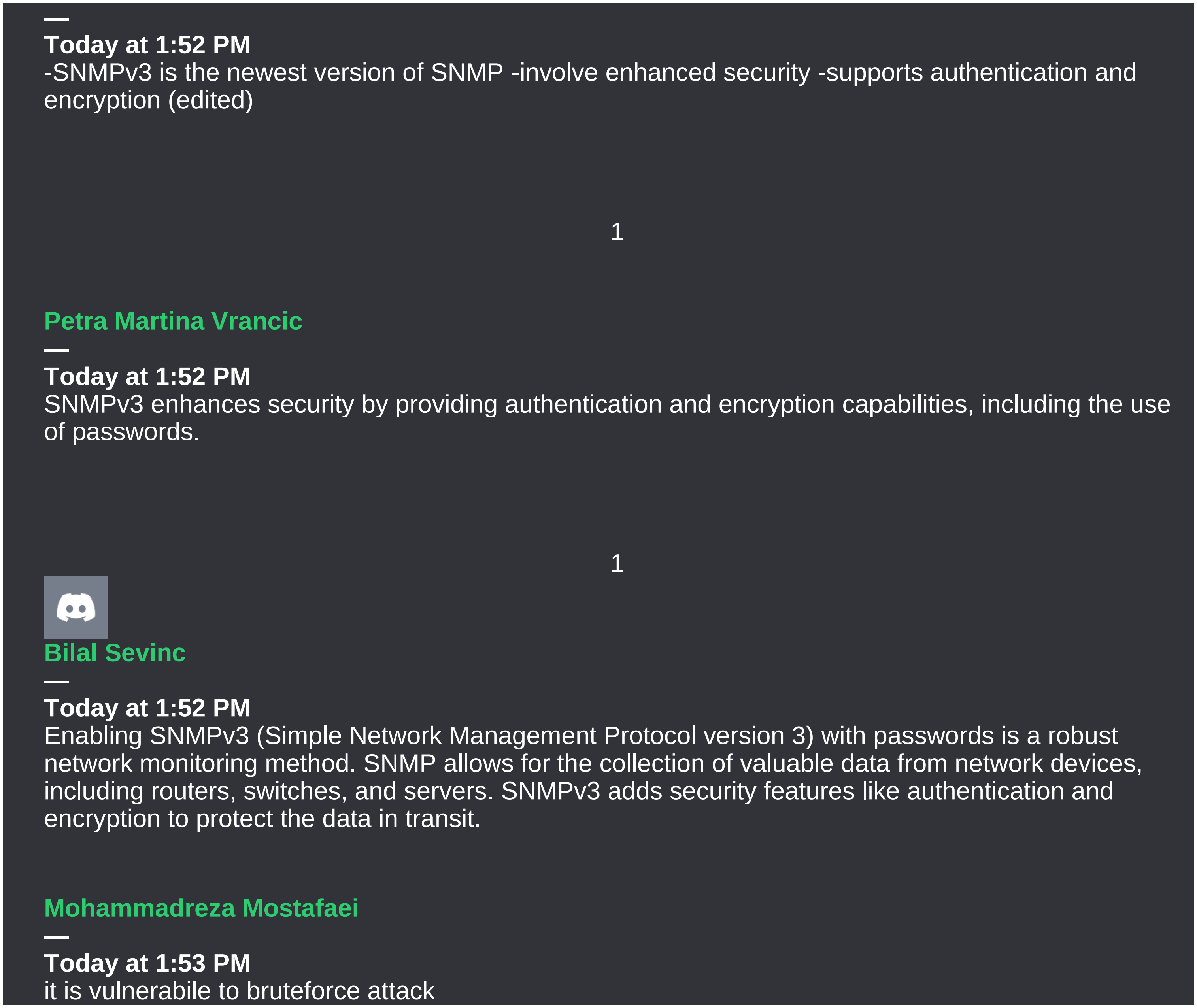
Enabling SNMPv3 (Simple Network Management Protocol Version3) provides a secure way to collect and analyze data on network performance, device status, and other important metrics.

C. Utilize an agentless monitor: Agentless monitoring tools can be effective for network monitoring as they don't require additional software (agents) to be installed on monitored devices. This option is more focused on network monitoring but doesn't specify a particular tool or method.

D. Enable SNMPv3 with passwords: SNMP (Simple Network Management Protocol) is designed for network monitoring and management. SNMPv3, with strong authentication and encryption, is a secure way to monitor network devices. This option is a strong choice for network monitoring, especially if you need to collect detailed data and statistics from network devices.

In the context of network monitoring, option D (Enable SNMPv3 with passwords) is likely the best method. SNMP allows for the collection of a wide range of network-related data, including performance metrics, error rates, and device status. SNMPv3 adds security features such as authentication and encryption, making it a secure and comprehensive choice for monitoring network operations. However, it's important to configure SNMPv3 properly with strong passwords and access control to maintain security.

Option C (Utilize an agentless monitor) is also a good choice, depending on the specific monitoring requirements and tools available. It can be effective for monitoring without the need to install additional software on devices, but it may not provide as detailed information as SNMP.



—

Today at 1:52 PM

-SNMPv3 is the newest version of SNMP -involve enhanced security -supports authentication and encryption (edited)

1

Petra Martina Vrancic

—

Today at 1:52 PM

SNMPv3 enhances security by providing authentication and encryption capabilities, including the use of passwords.

1

Bilal Sevinc

—

Today at 1:52 PM

Enabling SNMPv3 (Simple Network Management Protocol version 3) with passwords is a robust network monitoring method. SNMP allows for the collection of valuable data from network devices, including routers, switches, and servers. SNMPv3 adds security features like authentication and encryption to protect the data in transit.

Mohammadreza Mostafaei

—

Today at 1:53 PM

it is vulnerabile to bruteforce attack

Question #:86 - (Exam Topic 1)

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions

B. Multifactor authentication

C. A banned password list

D. A complex password policy

Answer: B

Explanation

In the context of mitigating unauthorized login attempts, credential theft, and brute-force attacks, the best control for the company to require from prospective vendors is Multifactor Authentication (MFA).

Here's why:

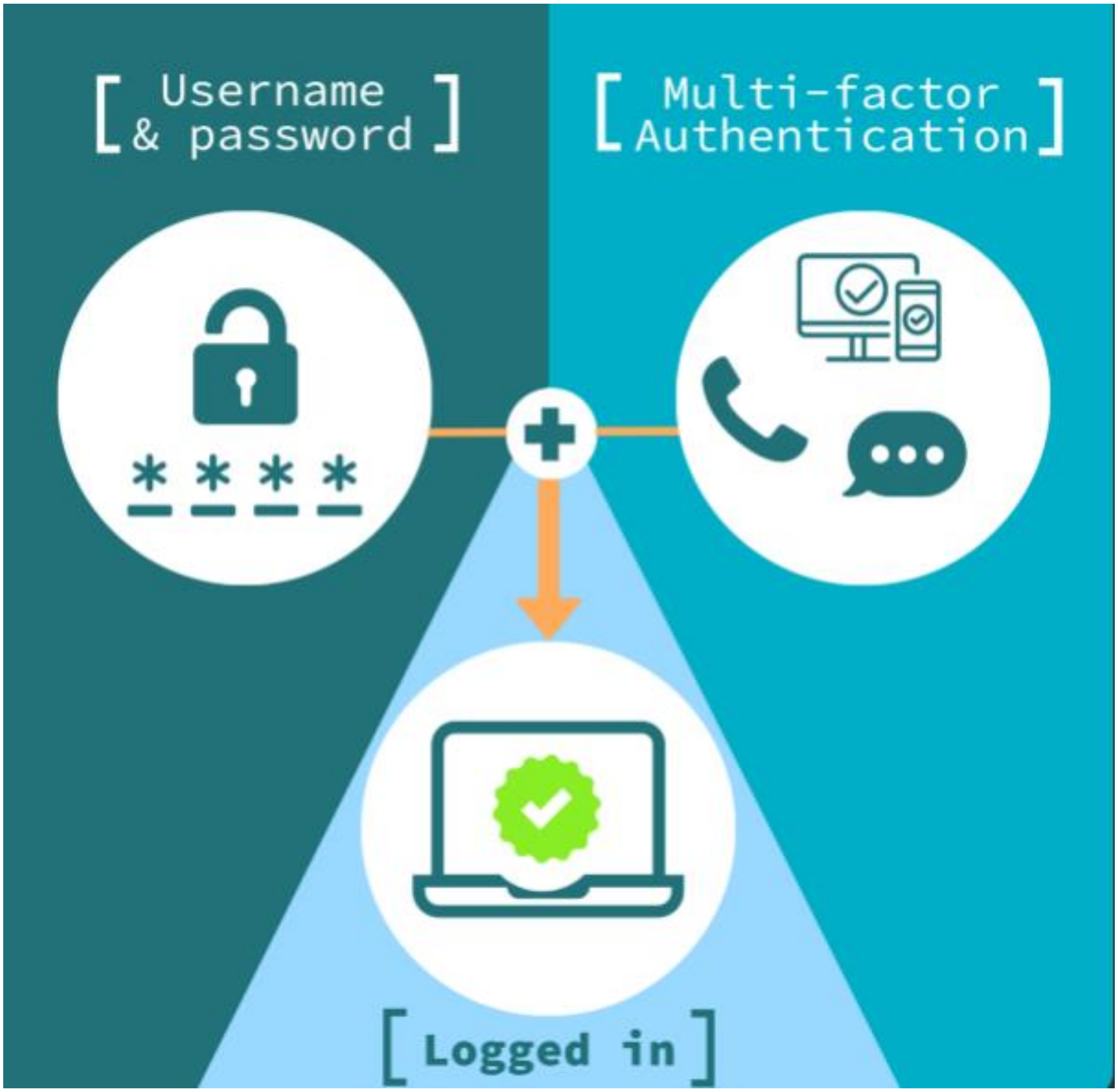
Multifactor Authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple forms of identification before gaining access to a system or application. This could include something they know (like a password) and something they have (like a smartphone with a one-time code generator). MFA significantly enhances security because even if an attacker manages to steal or guess a user's password, they would still need the second factor to gain access.

IP restrictions: IP restrictions can help limit access to specific IP addresses or ranges, which can be effective in some cases. However, they can be cumbersome for users who need to access resources from different locations, such as remote workers or employees on the go. Additionally, they may not fully protect against credential theft or brute-force attacks if the attacker is within an authorized IP range.

A banned password list: While maintaining a banned password list is a good security practice to prevent users from using easily guessable or commonly used passwords, it may not be sufficient on its own to protect against credential theft or brute-force attacks. Attackers can still attempt to guess non-banned passwords.

A complex password policy: A complex password policy is important for strong password management, but it may not be enough to prevent unauthorized access if attackers are using stolen credentials or conducting brute-force attacks.

Implementing MFA ensures that even if an attacker manages to obtain a user's password through theft or brute-force, they would still need the additional factor to gain access, making it significantly more challenging for them to succeed.



Question #:87 - (Exam Topic 1)

A Chief Information Officer receives an email stating a database will be encrypted within 24 hours unless a payment of $20,000 is credited to the account mentioned in the email. This BEST describes a scenario related to:

A. whaling

B. smishing

C. spear phishing

D. vishing

Answer: A

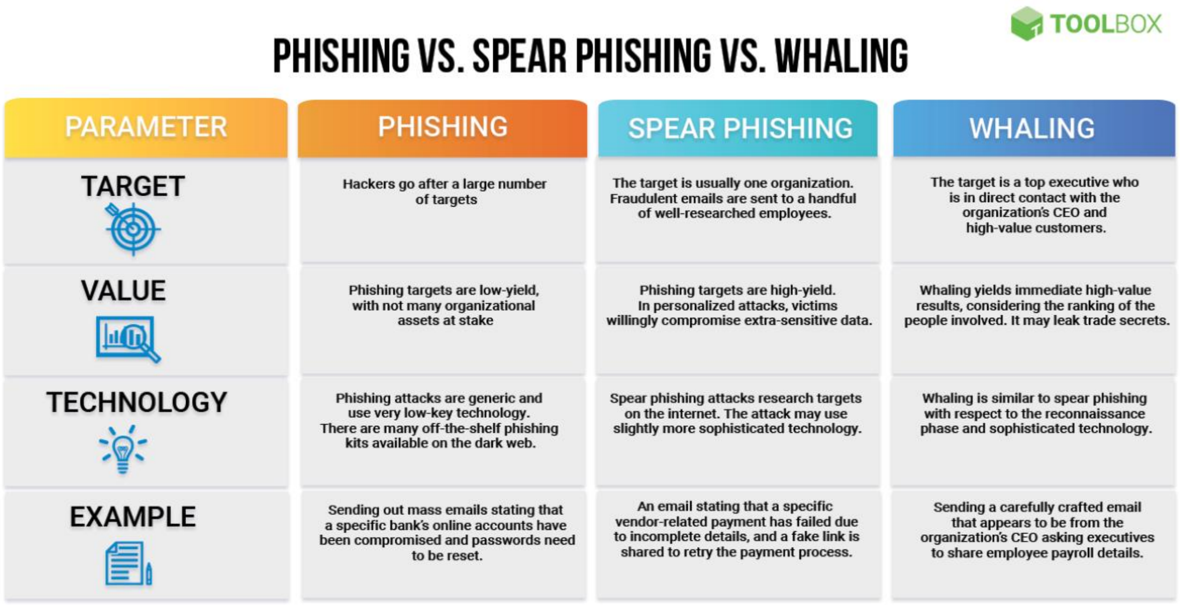
Explanation

Whaling typically refers to targeted phishing attacks aimed at high-level executives or individuals with significant authority or access within an organization. While the Chief Information Officer is an executive, the scenario does not specifically mention that they hold a high-level executive position in the email.

Smishing involves phishing attacks conducted via text messages or SMS. The scenario mentions an email, not a text message.

Vishing involves phishing attacks conducted over the phone, typically using voice calls. The scenario mentions an email communication, not a phone call.

Spear phishing is a type of phishing attack that is highly targeted and personalized.



TOOLBOX

PHISHING VS. SPEAR PHISHING VS. WHALING

PARAMETER	PHISHING	SPEAR PHISHING	WHALING
TARGET	Hackers go after a large number of targets	The target is usually one organization. Fraudulent emails are sent to a handful of well-researched employees.	The target is a top executive who is in direct contact with the organization's CEO and high-value customers.
VALUE	Phishing targets are low-yield, with not many organizational assets at stake	Phishing targets are high-yield. In personalized attacks, victims willingly compromise extra-sensitive data.	Whaling yields immediate high-value results, considering the ranking of the people involved. It may leak trade secrets.
TECHNOLOGY	Phishing attacks are generic and use very low-key technology. There are many off-the-shelf phishing kits available on the dark web.	Spear phishing attacks research targets on the internet. The attack may use slightly more sophisticated technology.	Whaling is similar to spear phishing with respect to the reconnaissance phase and sophisticated technology.
EXAMPLE	Sending out mass emails stating that a specific bank's online accounts have been compromised and passwords need to be reset.	An email stating that a specific vendor-related payment has failed due to incomplete details, and a fake link is shared to retry the payment process.	Sending a carefully crafted email that appears to be from the organization's CEO asking executives to share employee payroll details.

Question #:77 - (Exam Topic 1)

A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody.

B. Inspect the file metadata.

C. Reference the data retention policy.

D. Review the email event logs

Answer: D

Explanation

D. Review the email event logs: Reviewing the email event logs can support an investigation for fraudulent submission, as these logs can provide details about the history of emails, including the message content, timestamps, and sender/receiver information. Since the reports were claimed to have been sent via email, reviewing the email event logs can help verify whether such emails were indeed sent and whether they contain the same reports or any discrepancies in the communication history.

B. Inspect the file metadata: If the reports were submitted as plain text within the body of a new email message, then there may not be a separate document with file metadata to inspect. In such a case, reviewing the file metadata wouldn't be applicable since the reports are in the email body.

Question #:78 - (Exam Topic 1)

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again.

Which of the following is the BEST technical implementation to prevent this from happening again?

A. Configure DLP solutions

B. Disable peer-to-peer sharing

C. Enable role-based access controls

D. Mandate job rotation

E. Implement content filters

Answer: A

Explanation

Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

A. Configure DLP solutions: DLP solutions are specifically designed to monitor and prevent unauthorized data transfers, ensuring that sensitive data doesn't leave the organization without proper authorization. This is a proactive measure to prevent data loss and maintain data security.

B. Disable peer-to-peer sharing: While disabling peer-to-peer sharing can be a security measure, it's not as comprehensive as DLP. It may address one specific avenue for data loss but won't cover all potential data leakage scenarios.

C. Enable role-based access controls: Role-based access controls are essential for controlling who has access to what data within an organization. However, they won't prevent data from being accidentally or intentionally leaked by authorized users. DLP complements access controls by monitoring data movement.

D. Mandate job rotation: Job rotation is a personnel management strategy that can help with internal controls, but it's not a technical implementation to prevent data loss. It may mitigate certain risks, but it doesn't directly address the technical aspects of data protection.

E. Implement content filters: Content filters are typically used to control the types of content that can be accessed or sent through network channels. While they can be part of a security strategy, they are not as specialized as DLP solutions for preventing data loss.

David Berrios

—

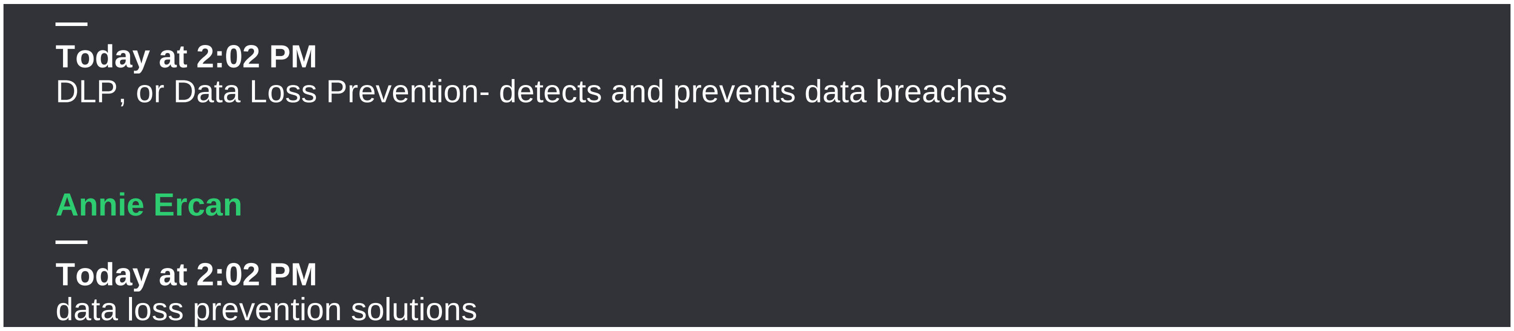
Today at 2:01 PM

was think head

[2:02 PM]

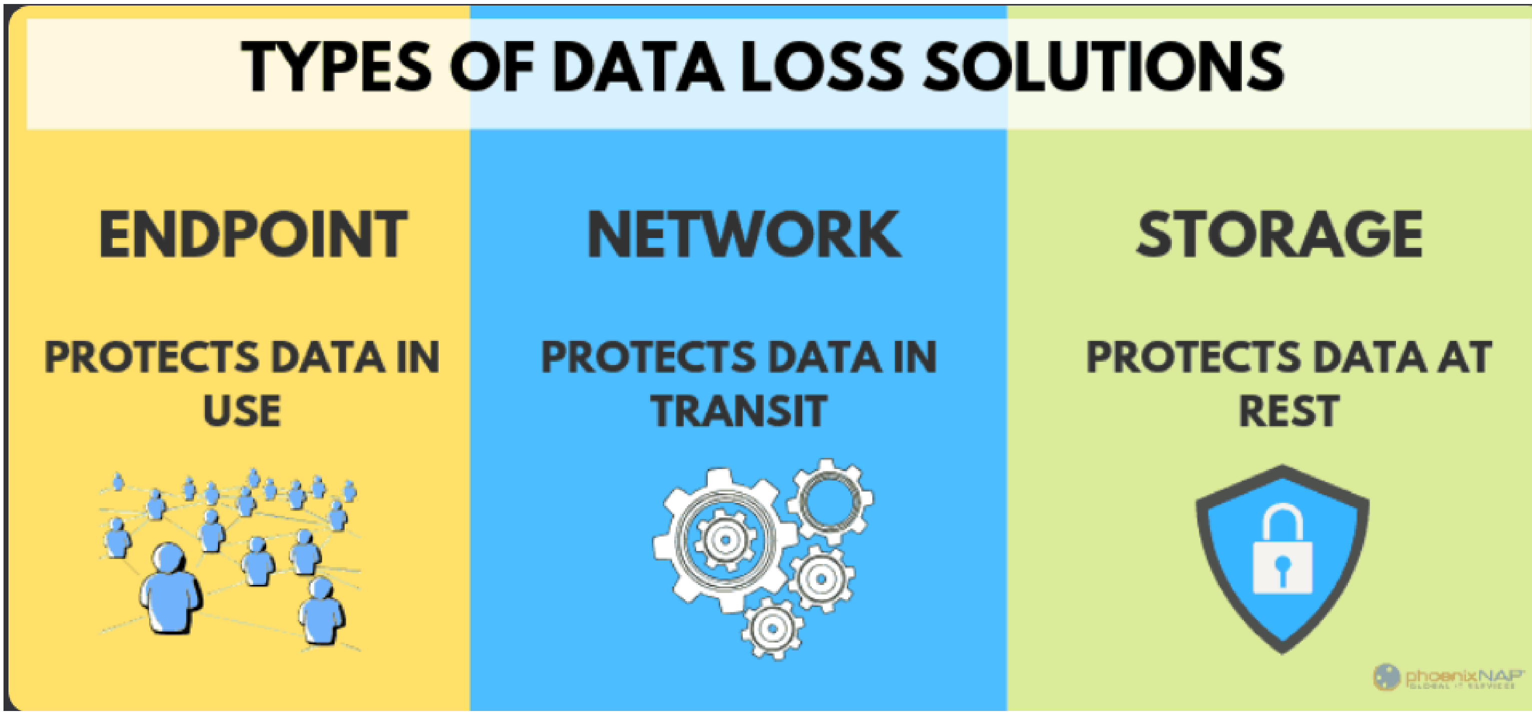
DLp

Nigina Novruzova



—
Today at 2:02 PM
DLP, or Data Loss Prevention- detects and prevents data breaches

Annie Ercan
—
Today at 2:02 PM
data loss prevention solutions



Question #:90 - (Exam Topic 1)

Which of the following involves the inclusion of code in the main codebase as soon as it is written?

A. Continuous monitoring

B. Continuous deployment

C. Continuous validation

D. Continuous integration

Answer: D

Explanation

Continuous Integration (CI) is a practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration is verified by an automated build and automated tests. CI allows for the detection of errors early in the development cycle, thereby reducing overall development costs. Continuous integration is the DevOps manner of continually updating and improving the production codebase.

B. Continuous Deployment (CD): CD is a practice that takes CI a step further. It involves automatically deploying code changes to production or staging environments after passing automated tests. Continuous Deployment aims to deliver new features or fixes to users quickly and frequently.

Nigina Novruzova

—

Today at 2:04 PM

An 'integrated security system' - 'integrating' of two or more electronic security systems

Question #:91 - (Exam Topic 1)

During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

A. User behavior analytics

B. Dump files

C. Bandwidth monitors

D. Protocol analyzer output

Answer: A

Explanation

User behavior analytics (UBA) would be the best data source to assess the accounts impacted by the attack, as it can identify abnormal activity, such as repeated brute-force attacks and logins from unfamiliar geographic locations, and provide insights into the behavior of the impacted accounts.

Advances in user behavioral analysis have provided another interesting use of the SIEM: monitoring what people do with their systems and how they do it. If every day, upon beginning work, the accountants start the same programs, then when an accountant account logs in and does something totally different, like accessing a system they have never accessed before, this indicates a behavioral change worth looking into. Many modern SIEMs have modules that analyze end-user behaviors, looking for anomalous behavior patterns that indicate a need for analysis.

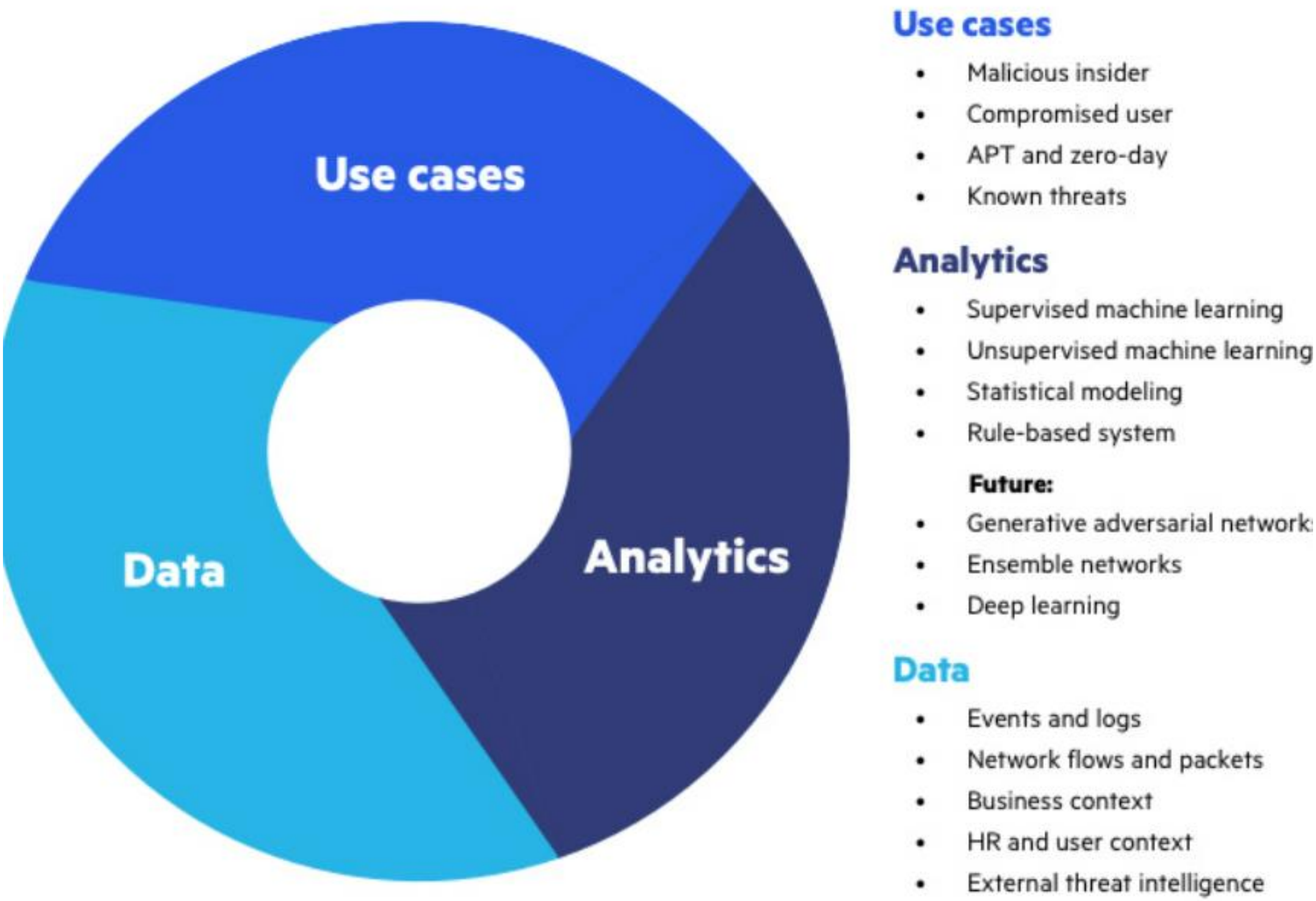
In this scenario, the incident response team is trying to assess the impact of the attack on the administrator accounts that were suspected of being compromised. User behavior analytics (UBA) is a data analysis technique that uses machine learning algorithms to detect abnormal behavior patterns that may indicate a security threat.

By analyzing the activity logs of the administrator accounts, UBA can help identify any suspicious behavior patterns, such as repeated failed login attempts or logins from unfamiliar geographic locations. This can help the incident response team identify which accounts were impacted by the attack and take appropriate action to secure them.

B:Dump files: Dump files are typically memory or system dump files and may not directly provide information about account compromise or user behavior.

C: Bandwidth monitors: Bandwidth monitors track network traffic and usage but do not specifically provide insights into user account activities or compromises.

D: Protocol analyzer output: Protocol analyzers capture and analyze network traffic at the packet level. While they can provide network-level insights, they may not directly address the assessment of compromised accounts or user behaviors.



Use cases

- Malicious insider
- Compromised user
- APT and zero-day
- Known threats

Analytics

- Supervised machine learning
- Unsupervised machine learning
- Statistical modeling
- Rule-based system

Future:

- Generative adversarial network
- Ensemble networks
- Deep learning

Data

- Events and logs
- Network flows and packets
- Business context
- HR and user context
- External threat intelligence

Question #:92 - (Exam Topic 1)

The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

A. Geofencing

B. Self-sovereign identification

C. PKl certificates

D. SSO

Answer: A

Explanation

Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.

Mamurjon Ismatov

—

Today at 2:07 PM

Geofencing is a technology that uses GPS, RFID, Wi-Fi, or cellular data to define geographical boundaries or perimeters

Question #:93 - (Exam Topic 1)

Which of the following authentication methods is considered to be the LEAST secure?

A. TOTP

B. SMS

C. HOTP

D. Token key

Answer: B

Explanation

SMS-based authentication is considered to be the least secure among the given options. This is because SMS messages can be intercepted or redirected by attackers through techniques such as SIM swapping, man-in-the-middle attacks, or exploiting weaknesses in the SS7 protocol used by mobile networks. Additionally, SMS messages can be compromised if a user's phone is lost, stolen, or infected with malware.

In contrast, TOTP (Time-based One-Time Password), HOTP (HMAC-based One-Time Password), and token keys are more secure as they rely on cryptographic algorithms or physical devices to generate one-time use codes, which are less susceptible to interception or unauthorized access.

Reference: National Institute of Standards and Technology (NIST). (2017). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Question #:94 - (Exam Topic 1)

Which of the following controls would provide the BEST protection against tailgating?

A. Access control vestibule

B. Closed-circuit television

C. Proximity card reader

D. Faraday cage

Answer: A

Explanation

Access control vestibule: An access control vestibule, also known as a mantrap, is a physical security measure that requires individuals to enter a small, enclosed area one at a time. They must undergo identity verification (e.g., using access cards or biometrics) before being granted access to the secure area. This design is highly effective at preventing tailgating because it ensures that only authorized individuals can enter the secure area.

Closed-circuit television (CCTV): CCTV systems are valuable for monitoring and recording activities in an area, including detecting tailgating incidents. However, CCTV alone doesn't prevent tailgating but can aid in identifying unauthorized access after the fact.

Proximity card reader: Proximity card readers are authentication devices that grant access based on the presentation of a valid card or badge. While they provide a level of access control, they don't inherently prevent tailgating, as an unauthorized person can follow closely behind an authorized cardholder.

Faraday cage: A Faraday cage is an enclosure designed to block electromagnetic signals, such as radio waves and electronic communications. It's not a control designed to prevent physical tailgating; instead, it's used to protect sensitive electronic equipment from external interference.

For the specific purpose of preventing tailgating, an access control vestibule is the most effective control, as it enforces strict physical access control by allowing only one person at a time to pass through and authenticate their identity before granting access to the secure area.

Question #:95 - (Exam Topic 1)

The SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC investigates the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team

B. The vulnerability management team

C. The CIRT

D. The read team

Answer: C

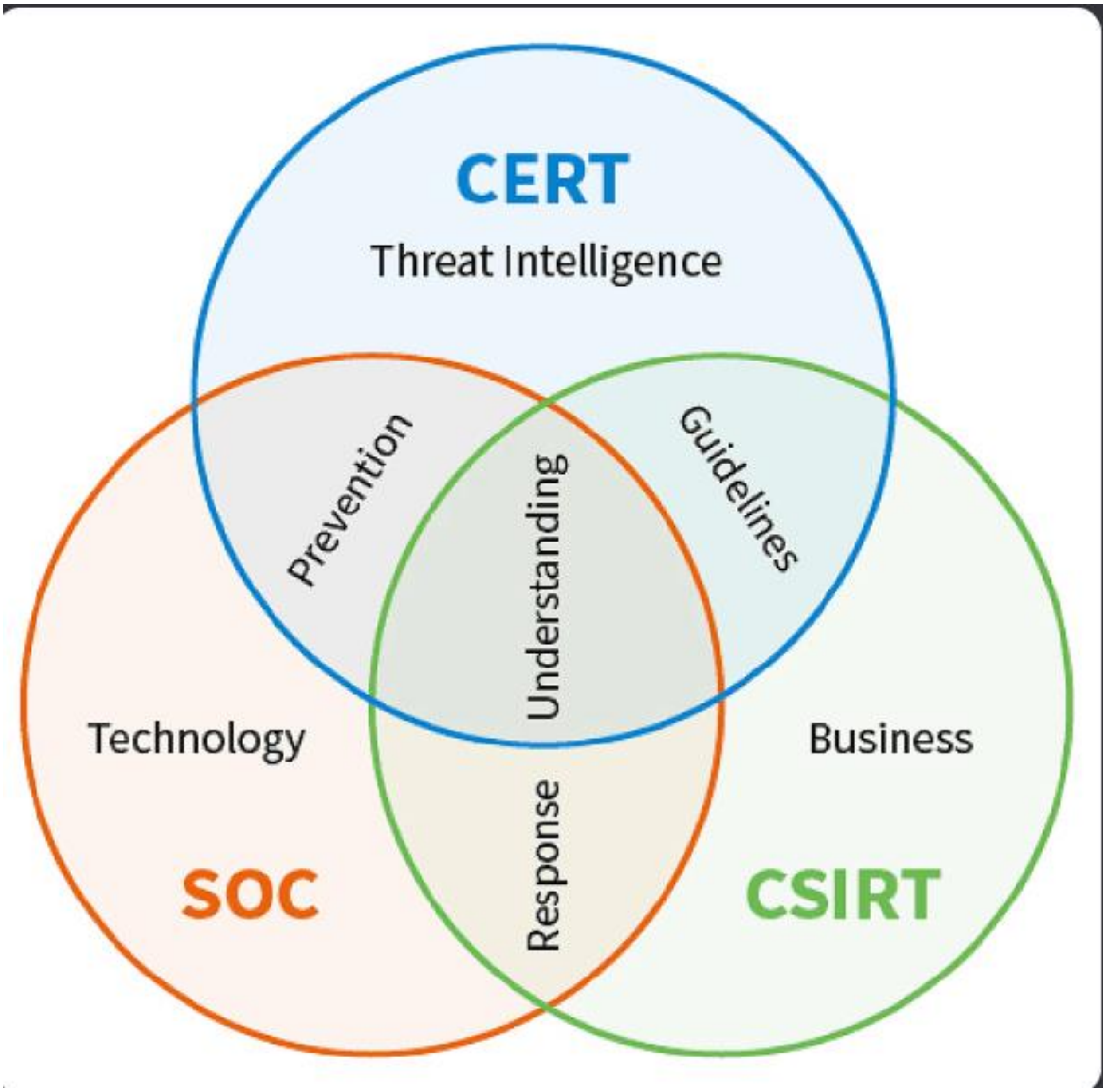
Explanation

The NOC team (Network Operations Center): The NOC team primarily focuses on the day-to-day operations of the network, ensuring network availability, performance, and monitoring. While they play a crucial role in network management, handling security incidents and malware detection typically falls under the purview of the SOC (Security Operations Center) or the CIRT.

The vulnerability management team: The vulnerability management team is responsible for identifying, assessing, and mitigating vulnerabilities in an organization's systems and applications. While the incident involves malware and privilege escalation, it may not directly relate to vulnerability management.

The CIRT (Computer Incident Response Team): Also known as **Cyber Incident Response Team**. The CIRT is specifically responsible for handling and responding to security incidents, including malware infections, breaches, and other security-related events. They have the expertise and processes in place to investigate, mitigate, and remediate such incidents. Reporting the event to the CIRT ensures that the incident is properly handled, analyzed, and contained.

The red team: The red team typically consists of security professionals who conduct simulated attacks and penetration testing to assess an organization's security posture. They are not responsible for handling real-world security incidents like the one described in the scenario.



Question #:96 - (Exam Topic 1)

Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm

B. The encryption algorithm's longevity

C. A method of introducing entropy into key calculations

D. The computational overhead of calculating the encryption key

Answer: B

Explanation

Key length of the encryption algorithm: The key length is important for the strength of the encryption but is less relevant to the length of time data needs to remain confidential. Longer key lengths generally provide stronger encryption, but the length of time data remains confidential is often determined by the algorithm's resilience over time.

A method of introducing entropy into key calculations: Entropy is important for generating strong and unpredictable encryption keys, but it primarily relates to the security of the key generation process, not the duration of confidentiality.

Computational overhead of calculating the encryption key: This is important for performance considerations but doesn't directly relate to how long data needs to remain confidential.

Encryption algorithm's longevity: The longevity of the encryption algorithm is a critical factor when selecting encryption methods for data with specific confidentiality requirements. The algorithm's longevity refers to how resistant it is to emerging cryptographic attacks and how well it will continue to protect data over an extended period. It's important to select encryption methods that are known to have long-term security and are resistant to advancements in cryptanalysis. Using outdated or vulnerable encryption algorithms can lead to data exposure if they are compromised during the data's confidentiality period.

length of time = longevity

Because they are requesting a certain length of time, longevity is the key issue

Question #:97 - (Exam Topic 1)

After a phishing scam for a user's credentials, the red team was able to craft a payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session.

Which of the following types of attacks has occurred?

A. Privilege escalation

B. Session replay

C. Application programming interface

D. Directory traversal

Answer: A

Explanation

Privilege escalation: Privilege escalation is the act of gaining higher-level access or permissions than originally granted. In this scenario, the attacker gained access to the server and was able to execute malicious software, which allowed them to initiate a new remote session with potentially higher privileges or access than they initially had. This type of attack is often a significant security breach.

Session replay: Session replay attacks involve capturing and replaying legitimate user sessions to impersonate the user. While session replay attacks can be a threat, they are not described in the scenario provided.

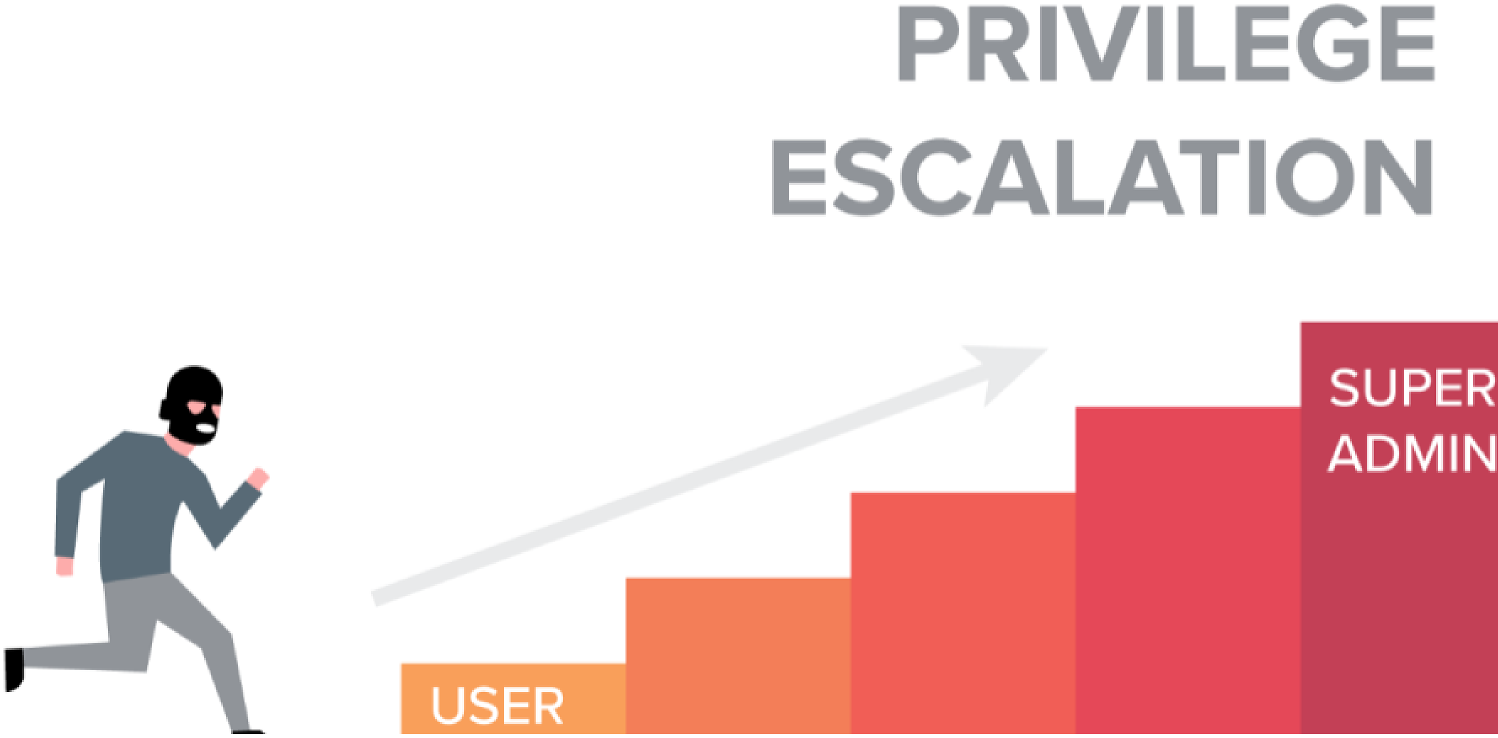
Application programming interface (API): APIs are used for communication between software components or systems. They are not directly related to the scenario described, which involves server compromise and privilege escalation.

Directory traversal: Directory traversal, also known as path traversal, is an attack in which an attacker attempts to access files or directories outside of the intended directory. It's not directly related to the scenario of initiating a new remote session after a phishing attack.

In summary, the described attack best fits the profile of privilege escalation, where the attacker gained unauthorized access to the server and escalated their privileges to execute malicious software and initiate a new remote session.

Today at 2:14 PM

Privilege escalation: -network attack used to gain unauthorized access to systems -attackers start by finding weak points



Question #:98 - (Exam Topic 1)

An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?

A. SLA

B. BPA

C. NDA

D. MOU

Answer: A

Explanation

SLA (Service Level Agreement): An SLA is a legally binding contract that defines the agreed-upon levels of service between a service provider (in this case, the cloud service provider) and the customer (the organization). It outlines various aspects of the service, including availability metrics, performance standards, response times, and penalties for non-compliance.

BPA (Business Partner Agreement): A BPA typically outlines the broader terms and conditions of a business partnership or relationship. While it may include some service-related details, it is not typically used to specify the technical or operational aspects of a service provider's performance.

NDA (Non-Disclosure Agreement): An NDA is a legal contract used to protect confidential information shared between parties. It is not related to service levels or availability metrics.

MOU (Memorandum of Understanding): An MOU is a less formal agreement that outlines the broad terms of cooperation or understanding between two parties. Like a BPA, it is not typically used to define the specific technical or operational details of a service provider's performance.

To ensure that the organization has a clear understanding of the cloud provider's obligations and commitments regarding availability, it should refer to the SLA, as it is specifically designed for this purpose and provides detailed information about service levels and performance expectations.

Question #:99 - (Exam Topic 1)

Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?

A. White team

B. Purple team

C. Green team

D. Blue team

E. Red team

Answer: A

Explanation

White team: The White team is responsible for overseeing and managing the penetration testing exercise. They act as referees and ensure that the testing is conducted according to the agreed-upon rules and scope. They also facilitate communication between the different teams involved in the exercise.

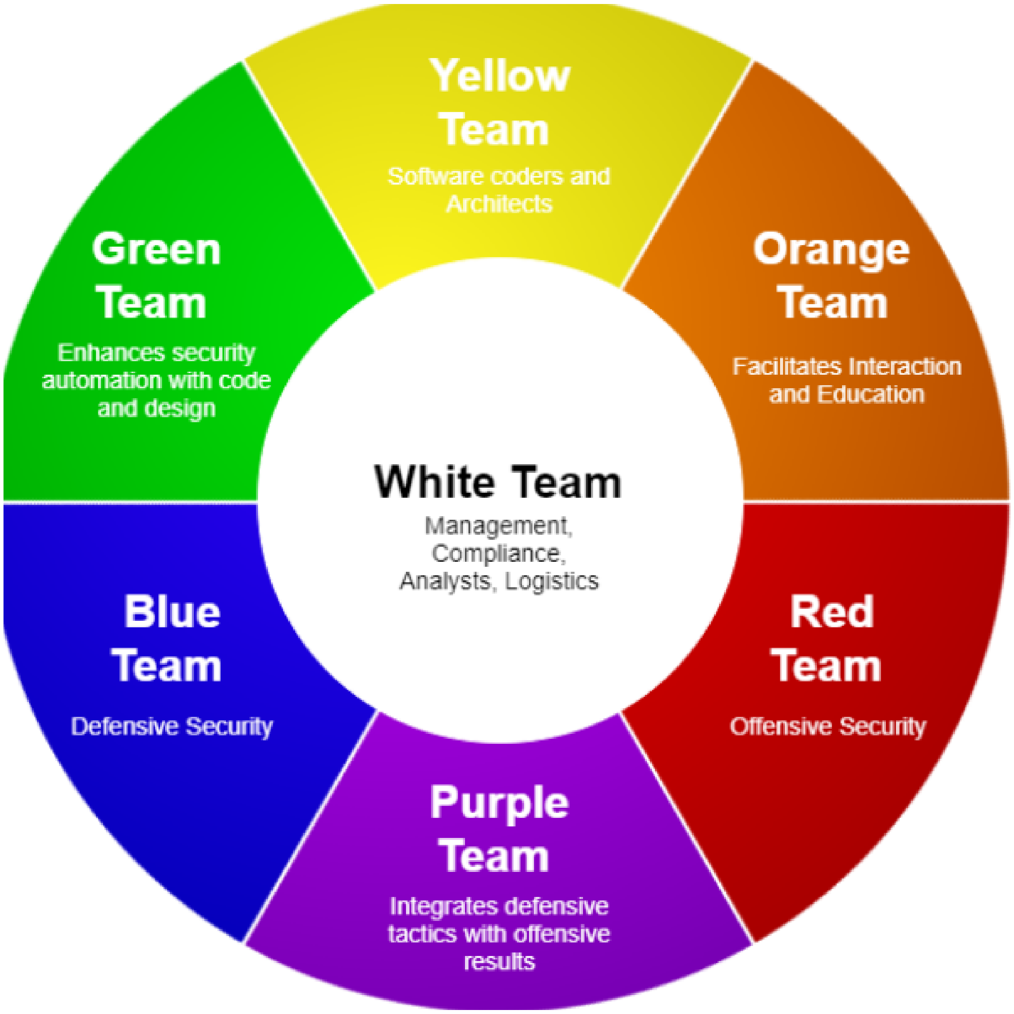
Purple team: The Purple team is a combination of both offensive (Red team) and defensive (Blue team) cybersecurity teams. They work together to simulate and improve the organization's overall security posture. Purple team exercises involve collaboration between attackers (Red) and defenders (Blue) to assess and enhance security measures.

Green team: The Green team is not as commonly used as the other colors, but in some contexts, it may refer to a team responsible for training or mentoring less-experienced individuals in cybersecurity or penetration testing.

Blue team: The Blue team represents the organization's internal defenders. They are responsible for maintaining and monitoring the organization's security infrastructure and responding to security incidents. Blue team exercises involve defending against simulated attacks, such as those conducted by the Red team.

Red team: The Red team is the offensive team in penetration testing exercises. They simulate real-world attacks to identify vulnerabilities and weaknesses in an organization's security infrastructure. Red team exercises help organizations understand their security flaws and improve their defenses.

In summary, the White team acts as a referee and overseer during a penetration testing exercise, ensuring that the testing process is conducted professionally and according to established guidelines.


Yellow Team
Software coders and Architects
Orange Team
Facilitates Interaction and Education
Green Team
Enhances security automation with code and design
White Team
Management, Compliance, Analysts, Logistics
Blue Team
Defensive Security
Red Team
Offensive Security
Purple Team
Integrates defensive tactics with offensive results

Question #:100 - (Exam Topic 1)

During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

A. Buffer overflow

B. Pass the hash

C. SQL injection

D. Replay attack

Answer: B

Explanation
The command you provided appears to be a use of the "crackmapexec" tool against an SMB (Server Message Block) service on the IP address 192.168.10.232, using the username "localadmin" and a hashed password represented as "-H 0A3CE8D07A46E5C51070F03593E0A5E6."

Based on this information, it indicates that a "Pass the Hash" (PtH) attack occurred.

In a Pass the Hash attack, an attacker uses a hashed version of a user's password (in this case, the hash "0A3CE8D07A46E5C51070F03593E0A5E6") rather than the actual plaintext password to authenticate to a system.

This allows them to gain unauthorized access to a system without needing to know the actual password. It is a common attack technique used against Windows-based systems, particularly when attackers have obtained password hashes through various means (e.g., through previous compromises).

Mimikatz, CrackMapExec (CME) and Metasploit are some of the popular tools that can potentially be used by attackers to execute a pass the hash attack.

Syntax for using CrackMapExec to perform a PtH attack is as follows:

```
        crackmapexec smb <target_IP> -u <username> -H <hash>

# Replace the following placeholders:
# - <target_IP>: The IP address of the target system.
# - <username>: The username you want to authenticate as.
# - <hash>: The NTLM hash you want to use for authentication.
```

Question #:101 - (Exam Topic 1)

The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access. Which of the following is the BEST security solution to reduce this risk?

A. CASB

B. VPN concentrator

C. MFA

D. VPC endpoint

Answer: A

Explanation

"Unsanctioned high-risk SaaS applications" refer to software-as-a-service (SaaS) applications that are used within an organization without official approval or authorization from the IT department or management. These applications are considered high-risk due to potential security, compliance, or operational concerns.

Examples of unsanctioned high-risk SaaS applications might include: file sharing and collaboration tools, project management software, communication apps, personal email services, unapproved CRM or sales tools.

The BEST security solution to reduce the risk of unsanctioned high-risk SaaS applications is a **CASB (Cloud Access Security Broker)**. A CASB provides visibility, control, and policy enforcement for cloud applications, including blocking access to unsanctioned applications.

In this scenario, using a CASB allows the organization to enforce the policy of blocking access to unsanctioned high-risk SaaS applications effectively. It provides the necessary controls and visibility to manage and secure cloud access, helping the Chief Information Security Officer achieve the goal of risk reduction in shadow IT.

Regarding the VPC endpoint, it's not a suitable solution for this scenario. VPC endpoints are used to facilitate private communication between AWS resources and certain AWS services, which is unrelated to blocking unsanctioned SaaS applications in a broader IT environment.

SaaS == Software as a Service which is Cloud Model therefore the correct answer is CASB

Cloud Access Security Broker

A cloud access security broker (CASB) is on-premises or cloud-based software that sits between a cloud service consumer and a cloud service provider. It serves as a tool for enforcing an organization's security policies through risk identification and regulation compliance whenever its cloud-residing data is accessed.

Question #:102 - (Exam Topic 1)

A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices. Which of the following is a cost-effective approach to address these concerns?

A. Enhance resiliency by adding a hardware RAID.

B. Move data to a tape library and store the tapes off-site

C. Install a local network-attached storage.

D. Migrate to a cloud backup solution

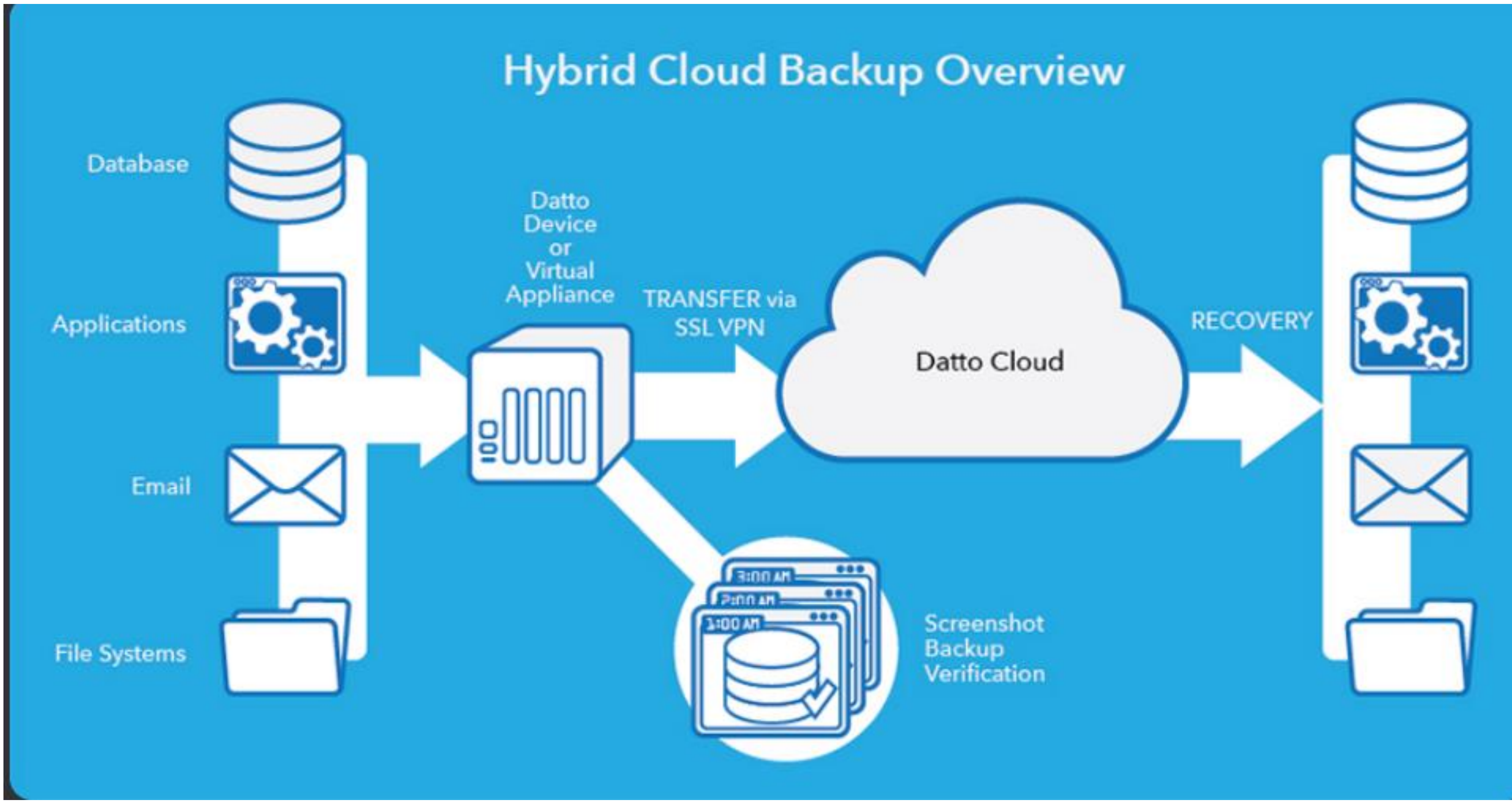
Answer: D

Explanation

The best approach to address these concerns is to migrate to a cloud backup solution. This approach will address the physical security of the backup media and the durability of the data stored on these devices. Cloud backup solutions are cost-effective and provide a secure and reliable way to store data off-site. This approach will also provide the grocery store with an automated backup process that is easy to manage and monitor.

Hardware RAID is not a cost-effective solution for addressing these concerns as it does not address the physical security of the backup media or the durability of the data stored on these devices.

Moving data to a tape library and storing tapes off-site is a good approach but it is not cost-effective as it requires additional hardware and storage space. Installing a local network-attached storage is not a good approach as it does not address the physical security of the backup media or the durability of the data stored on these devices. It also requires additional hardware and storage space which can be expensive.



Question #:103 - (Exam Topic 1)

Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix

B. Risk tolerance

C. Risk register

D. Risk appetite

Answer: D

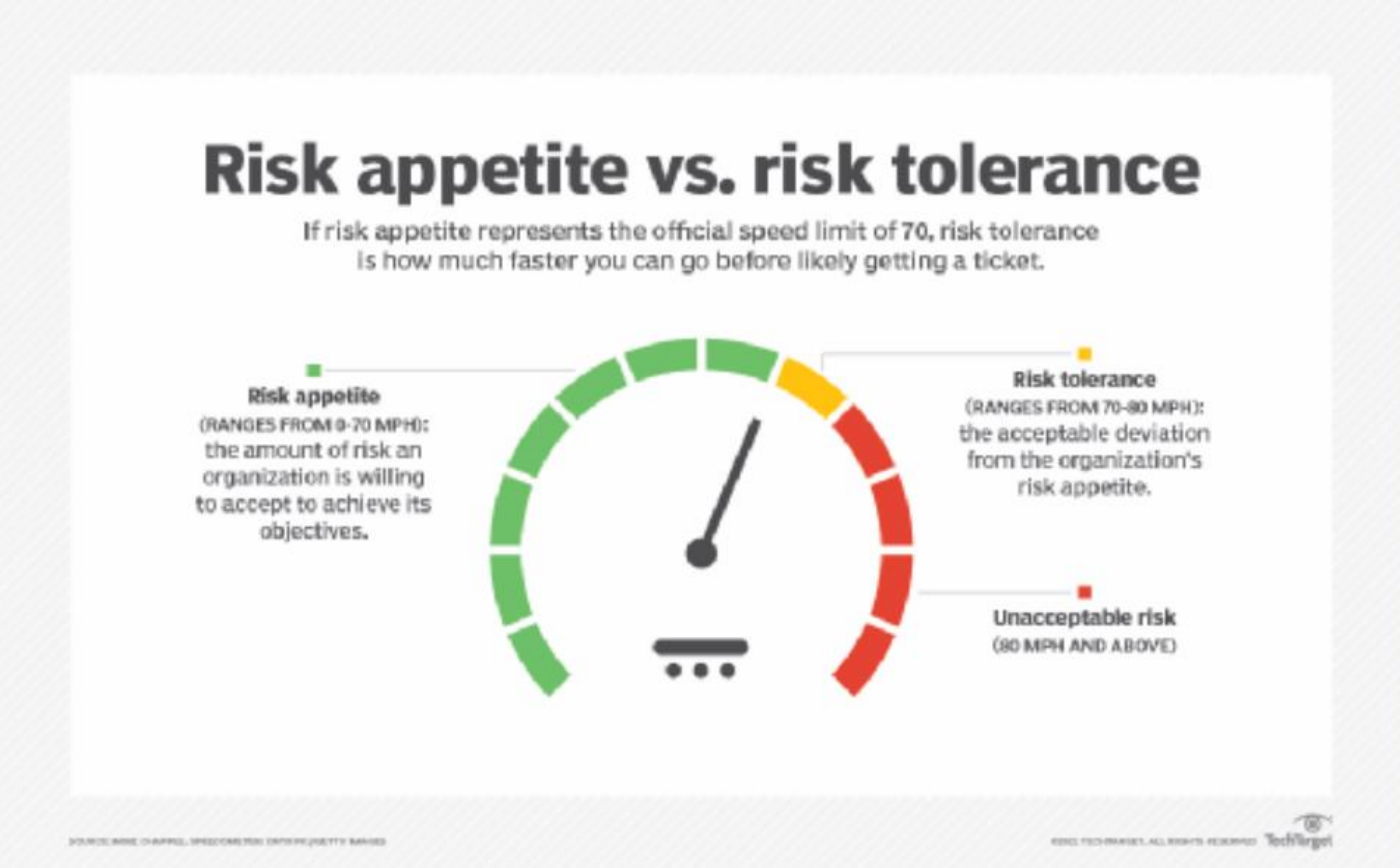
Explanation

Risk appetite refers to the amount of risk an organization is willing to accept in pursuit of its goals and objectives. It defines the organization's threshold for accepting risks and provides a basis for risk management decisions.

In the context of cloud-first adoption, reviewing the risk appetite will help the technician understand the organization's tolerance for potential security, privacy, data loss, or other risks associated with moving to a cloud-based infrastructure. With this understanding, the technician can prioritize and implement the appropriate security measures to minimize the risks to an acceptable level.

A risk matrix is a tool used in risk management to visualize and assess the likelihood and impact of potential risks. It typically consists of a two-dimensional grid or table, with likelihood of occurrence on one axis and the impact of the risk on the other axis.

This information will help determine the organization's "cloud-first" adoption strategy. References: CompTIA



Risk appetite vs. risk tolerance

If risk appetite represents the official speed limit of 70, risk tolerance is how much faster you can go before likely getting a ticket.

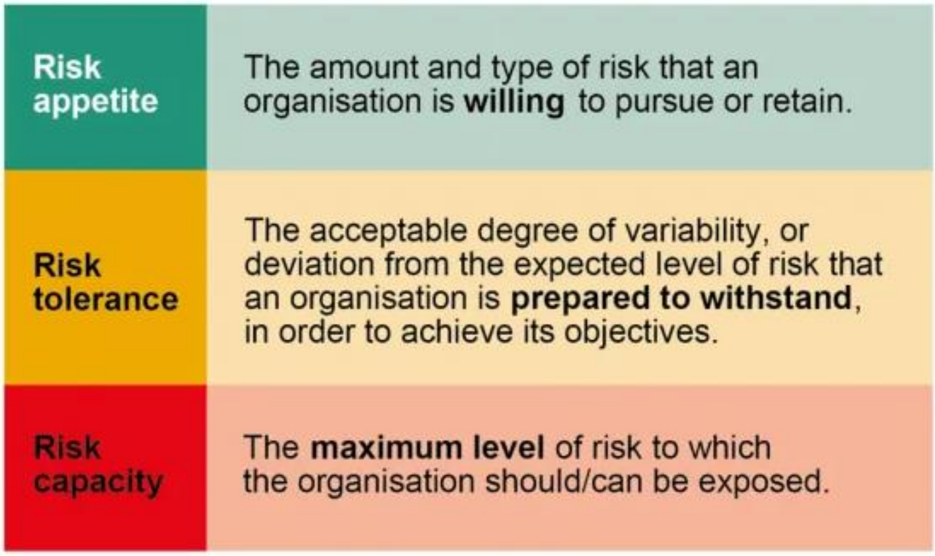
Risk appetite
(RANGES FROM 0-70 MPH):
the amount of risk an organization is willing to accept to achieve its objectives.

Risk tolerance
(RANGES FROM 70-80 MPH):
the acceptable deviation from the organization's risk appetite.

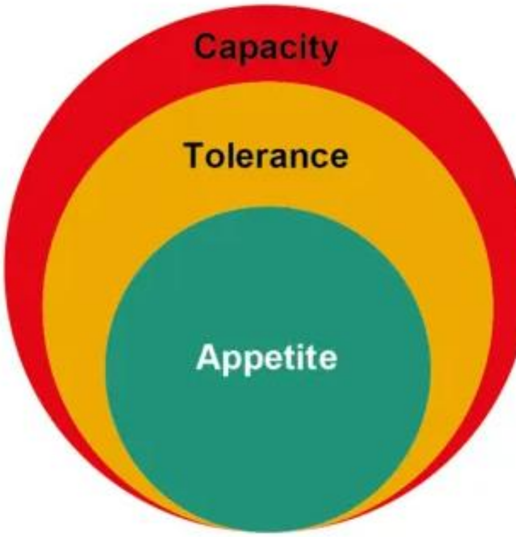
Unacceptable risk
(80 MPH AND ABOVE)

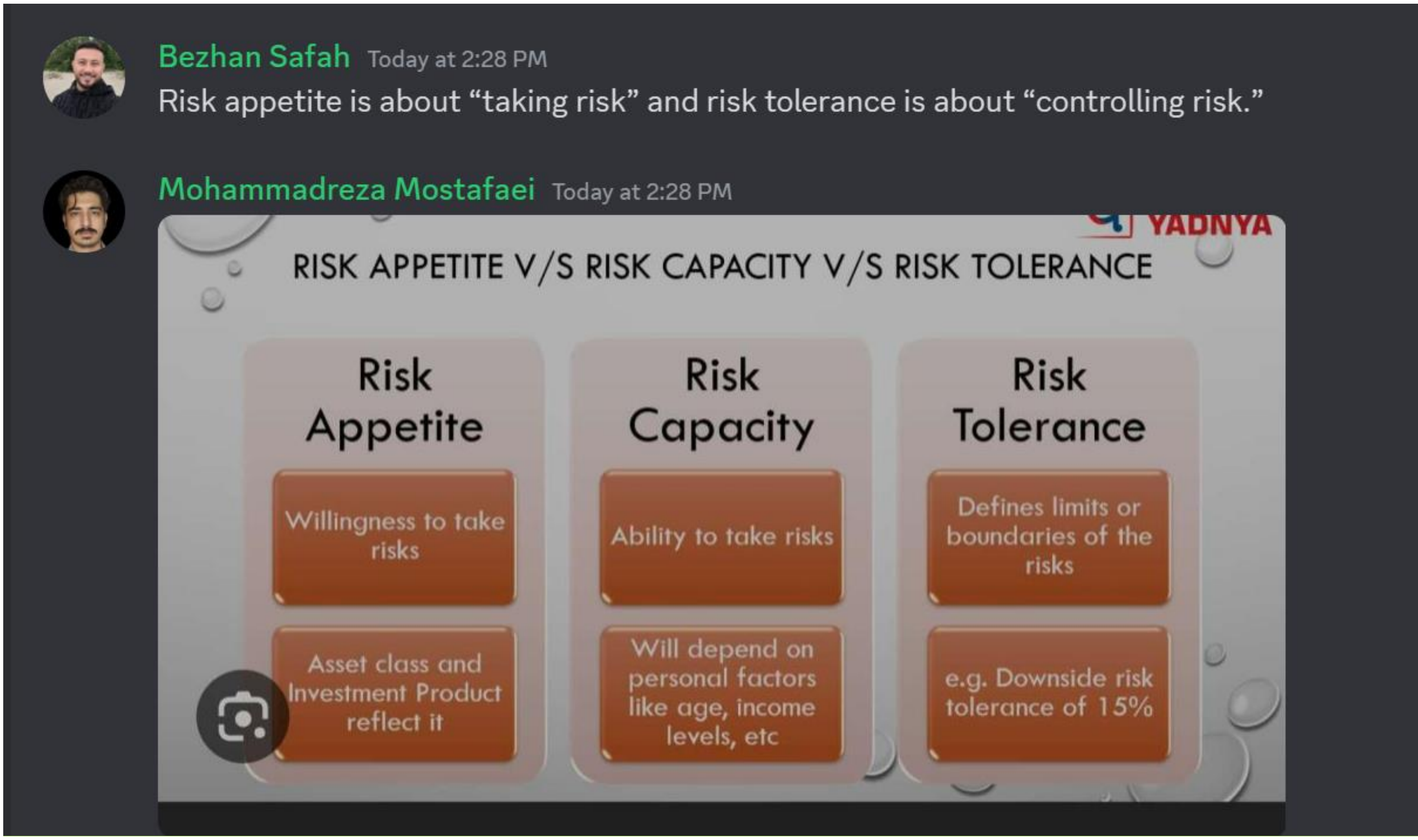
SOURCE: [illegible] SPEEDOMETER: [illegible]/GETTY IMAGES

©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget



Risk appetite	The amount and type of risk that an organisation is **willing** to pursue or retain.
Risk tolerance	The acceptable degree of variability, or deviation from the expected level of risk that an organisation is **prepared to withstand**, in order to achieve its objectives.
Risk capacity	The **maximum level** of risk to which the organisation should/can be exposed.





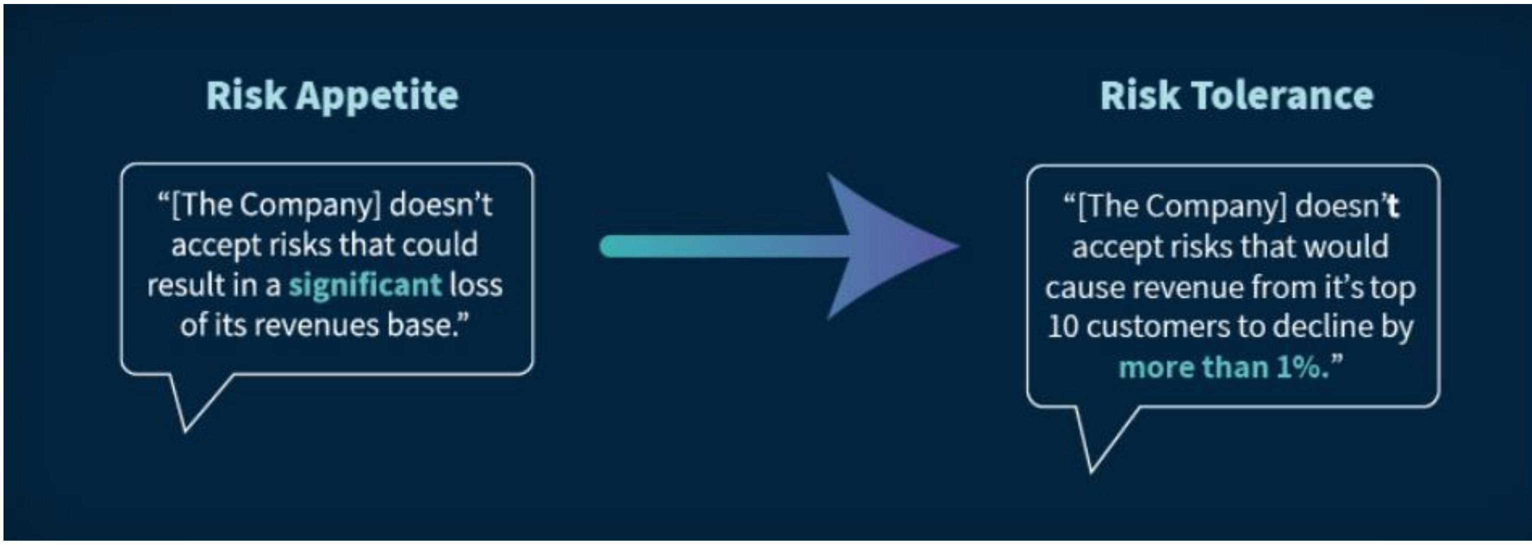
Bezhan Safah Today at 2:28 PM

Risk appetite is about “taking risk” and risk tolerance is about “controlling risk.”

Mohammadreza Mostafaei Today at 2:28 PM

RISK APPETITE V/S RISK CAPACITY V/S RISK TOLERANCE

Risk Appetite	Risk Capacity	Risk Tolerance
Willingness to take risks	Ability to take risks	Defines limits or boundaries of the risks
Asset class and Investment Product reflect it	Will depend on personal factors like age, income levels, etc	e.g. Downside risk tolerance of 15%



Risk Appetite

“[The Company] doesn’t accept risks that could result in a **significant** loss of its revenues base.”

Risk Tolerance

“[The Company] doesn’t accept risks that would cause revenue from it’s top 10 customers to decline by **more than 1%.**”

Question #:104 - (Exam Topic 1)

Developers are writing code and merging it into shared repositories several times a day, where it is tested automatically. Which of the following concepts does this BEST represent?

A. Functional testing

B. Stored procedures

C. Elasticity

D. Continuous integration

Answer: D

Explanation

Continuous integration (CI) is a software development practice where developers frequently integrate their code changes into a shared repository, which is tested automatically. The goal of CI is to detect and resolve integration issues early in the development process, thereby reducing the time and effort required to fix them later. By integrating code changes frequently and automatically testing them, developers can identify issues and resolve them quickly, ensuring that the software remains stable and reliable. This approach helps to reduce the risk of bugs and makes it easier to maintain and improve the codebase over time.

A: is a type of testing that verifies that the software application behaves as expected from a functional perspective, meaning that it meets the requirements specified by the stakeholders.

B: are a type of database object that encapsulates a series of SQL statements and can be called by other database objects or applications.

C: refers to the ability of a system to scale up or down automatically in response to changes in workload or demand. While elasticity is an important concept in cloud computing and distributed systems, it is not directly related to the scenario described in the question.

Question #:105 - (Exam Topic 1)

As part of annual audit requirements, the security team performed a review of exceptions to the company policy that allows specific users the ability to use USB storage devices on their laptops. The review yielded the following results.

- The exception process and policy have been correctly followed by the majority of users
- A small number of users did not create tickets for the requests but were granted access
- All access had been approved by supervisors.
- Valid requests for the access sporadically occurred across multiple departments.
- Access, in most cases, had not been removed when it was no longer needed

Which of the following should the company do to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame?

A. Create an automated, monthly attestation process that removes access if an employee's supervisor denies the approval

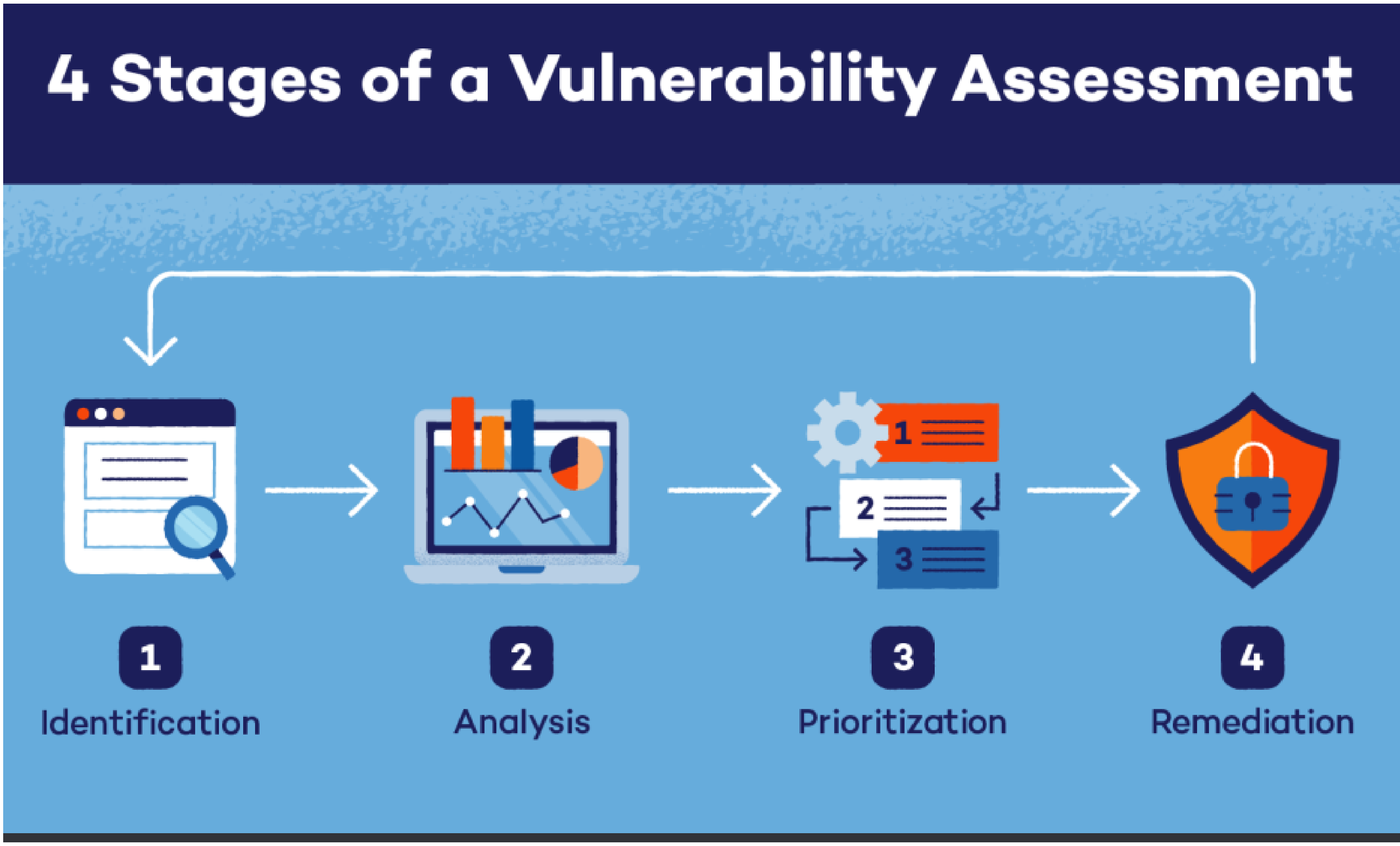
B. Remove access for all employees and only allow new access to be granted if the employee's supervisor approves the request

C. Perform a quarterly audit of all user accounts that have been granted access and verify the exceptions with the management team

D. Implement a ticketing system that tracks each request and generates reports listing which employees actively use USB storage devices

Answer: D

Implementing a ticketing system that tracks each request and generates reports is an effective way to ensure that appropriate access is not disrupted but unneeded access is removed in a reasonable time frame. This would enable the organization to keep track of all requests for USB access and ensure that access is only granted for approved requests. Reports generated by the ticketing system would also allow the organization to identify any instances of unauthorized access and take appropriate action.



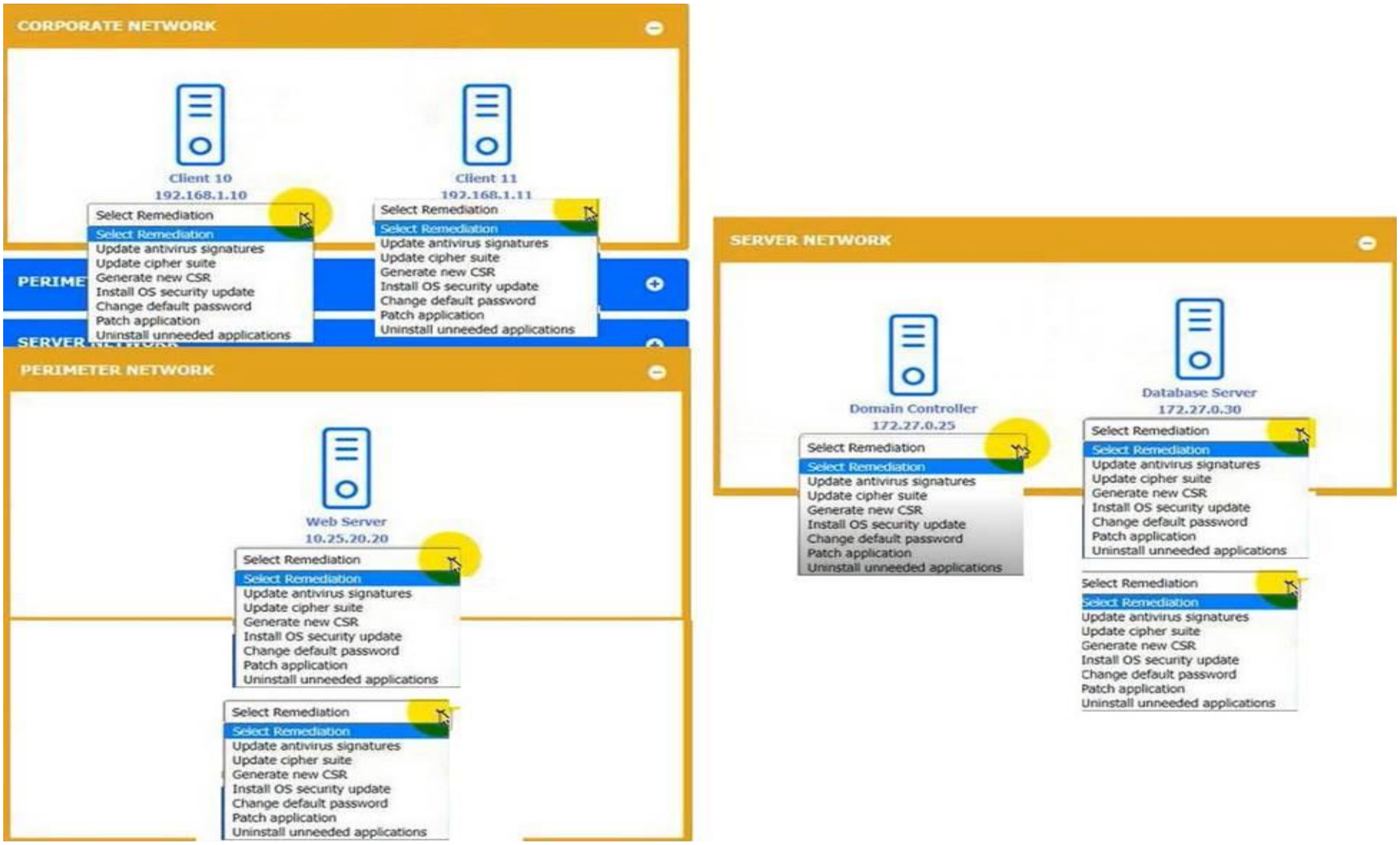
Question #:106 - (Exam Topic 1)

You received the output of a recent vulnerability assessment.

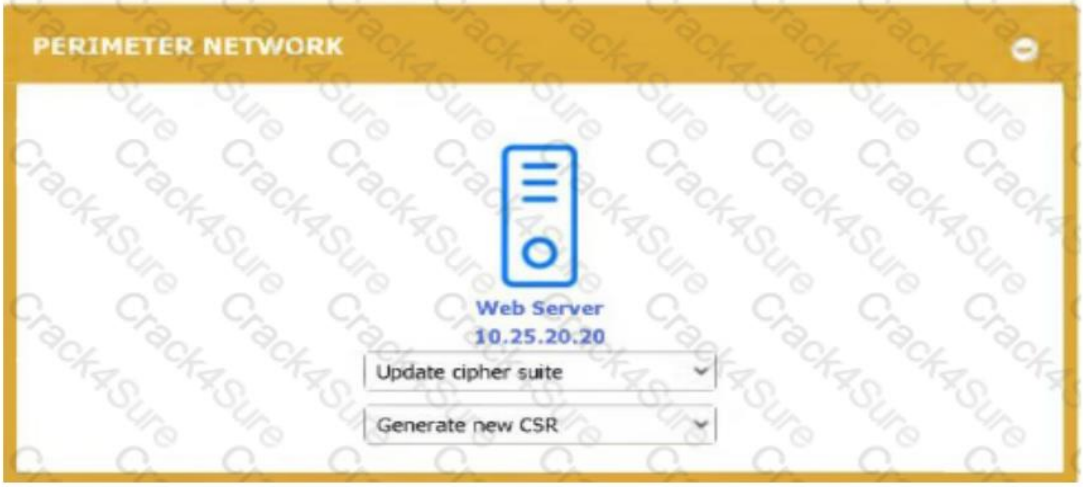
Review the assessment and scan output and determine the appropriate remediation(s) for each device.

Remediation options may be selected multiple times, and some devices may require more than one remediation.

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


CORPORATE NETWORK
Client 10
192.168.1.10
Select Remediation
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
Client 11
192.168.1.11
Select Remediation
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
PERIME
SERVER
PERIMETER NETWORK
Web Server
10.25.20.20
Select Remediation
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
Select Remediation
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
SERVER NETWORK
Domain Controller
172.27.0.25
Select Remediation
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
Database Server
172.27.0.30
Select Remediation
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
Select Remediation
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications

Answer:

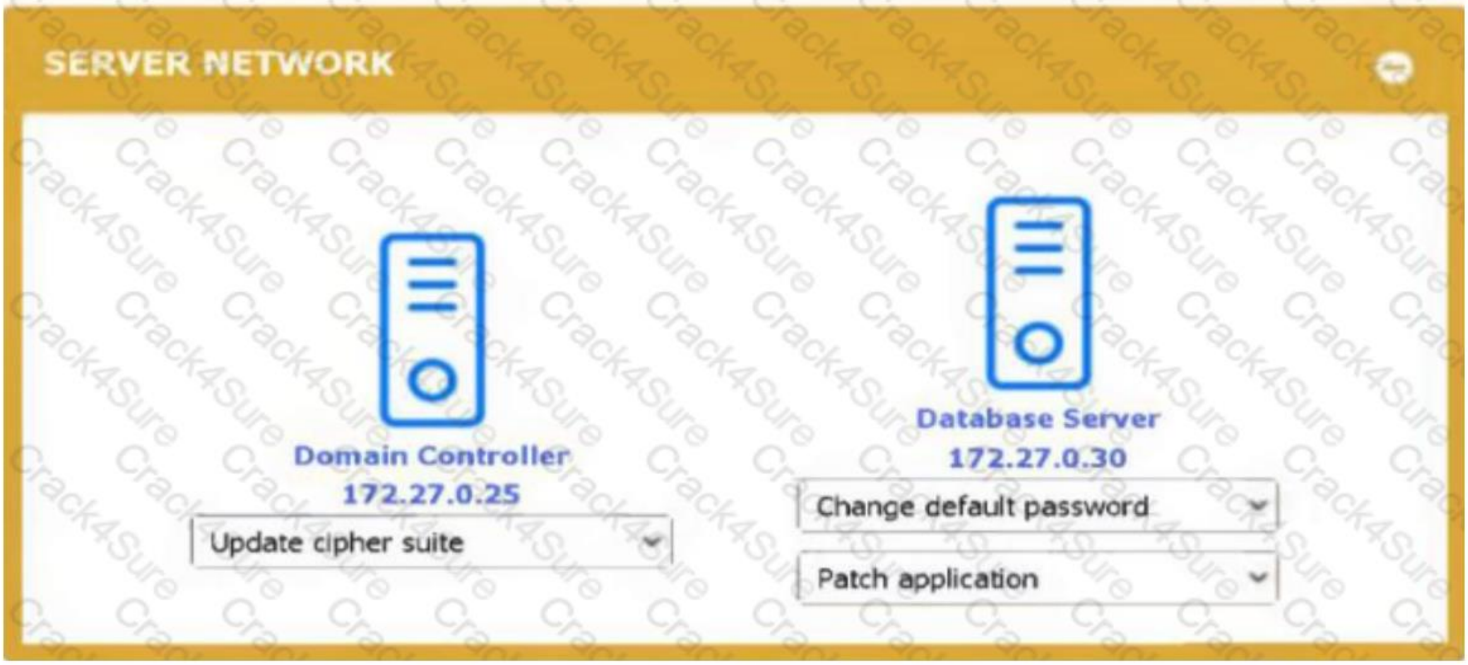


PERIMETER NETWORK

Web Server
10.25.20.20

Update cipher suite

Generate new CSR



SERVER NETWORK

Domain Controller
172.27.0.25

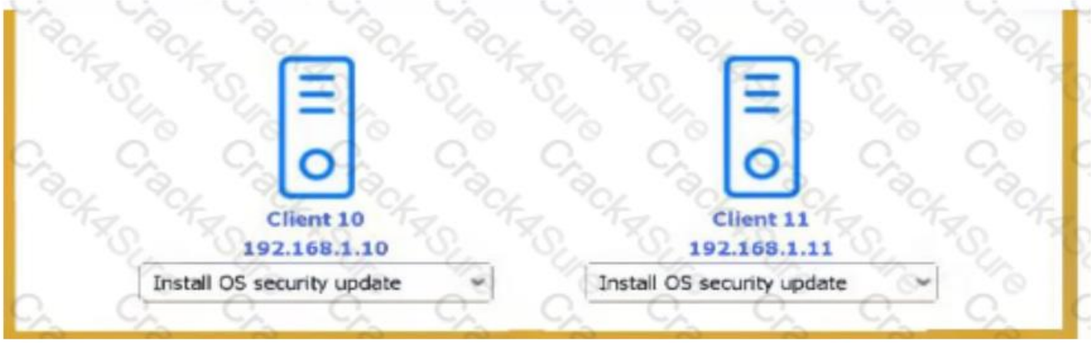
Update cipher suite

Database Server
172.27.0.30

Change default password

Patch application

Graphical user interface, application, website, Teams Description automatically generated



Client 10
192.168.1.10

Install OS security update

Client 11
192.168.1.11

Install OS security update

Graphical user interface, text, application Description automatically generated

Question #:107 - (Exam Topic 1)

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

A. Block cipher

B. Hashing

C. Private key

D. Perfect forward secrecy

E. Salting

F. Symmetric keys

Answer: B C

Explanation

Non-repudiation is the ability to ensure that a party cannot deny a previous action or event. Cryptographic concepts that can be used to implement non-repudiation include hashing and digital signatures, which use a private key to sign a message and ensure that the signature is unique to the signer.

Hashing: Hashing is used to create a unique fixed-length representation (hash) of data. In the context of non-repudiation, it is often used to create a hash of a message or document. If a user signs the hash with their private key, it becomes difficult for them to deny sending or authoring the message later, as the hash can be used as evidence.

Private key: Non-repudiation often involves digital signatures, where a sender signs a message using their private key. This private key is used to verify the authenticity of the sender and ensure that the message has not been tampered with.

Non-repudiation is a cryptographic concept that ensures that a sender cannot deny sending a message and that a receiver cannot deny receiving a message. To implement non-repudiation, a security engineer would typically use digital signatures and/or digital certificates.

Of the given options, the following two are cryptographic concepts that a security engineer would utilize while implementing non-repudiation:

B. Hashing: A cryptographic hash function is used to create a unique digital fingerprint of a message or data. The sender can create a hash of the message and then sign the hash using their private key. The receiver can then verify the signature using the sender's public key and compare the hash of the message to the signed hash to ensure that the message has not been tampered with.

C. Private key: A private key is used to sign a message or data, and the corresponding public key is used to verify the signature. This ensures that the sender cannot deny sending the message, as only they possess the private key necessary to sign the message.

The other options (Block cipher, Perfect forward secrecy, Salting, Symmetric keys) are not typically associated with non-repudiation but may have other cryptographic purposes in security.

Question #:108 - (Exam Topic 1)

A security analyst notices several attacks are being blocked by the NIPS but does not see anything on the boundary firewall logs. The attack seems to have been thwarted. Which of the following resiliency techniques was applied to the network to prevent this attack?

A. NIC Teaming

B. Port mirroring

C. Defense in depth

D. High availability

E. Geographic dispersal

Answer: C

Explanation

Defense in depth is a resiliency technique that involves implementing multiple layers of security controls to protect against different types of threats. In this scenario, the NIPS likely provided protection at a different layer than the boundary firewall, demonstrating the effectiveness of defense in depth.

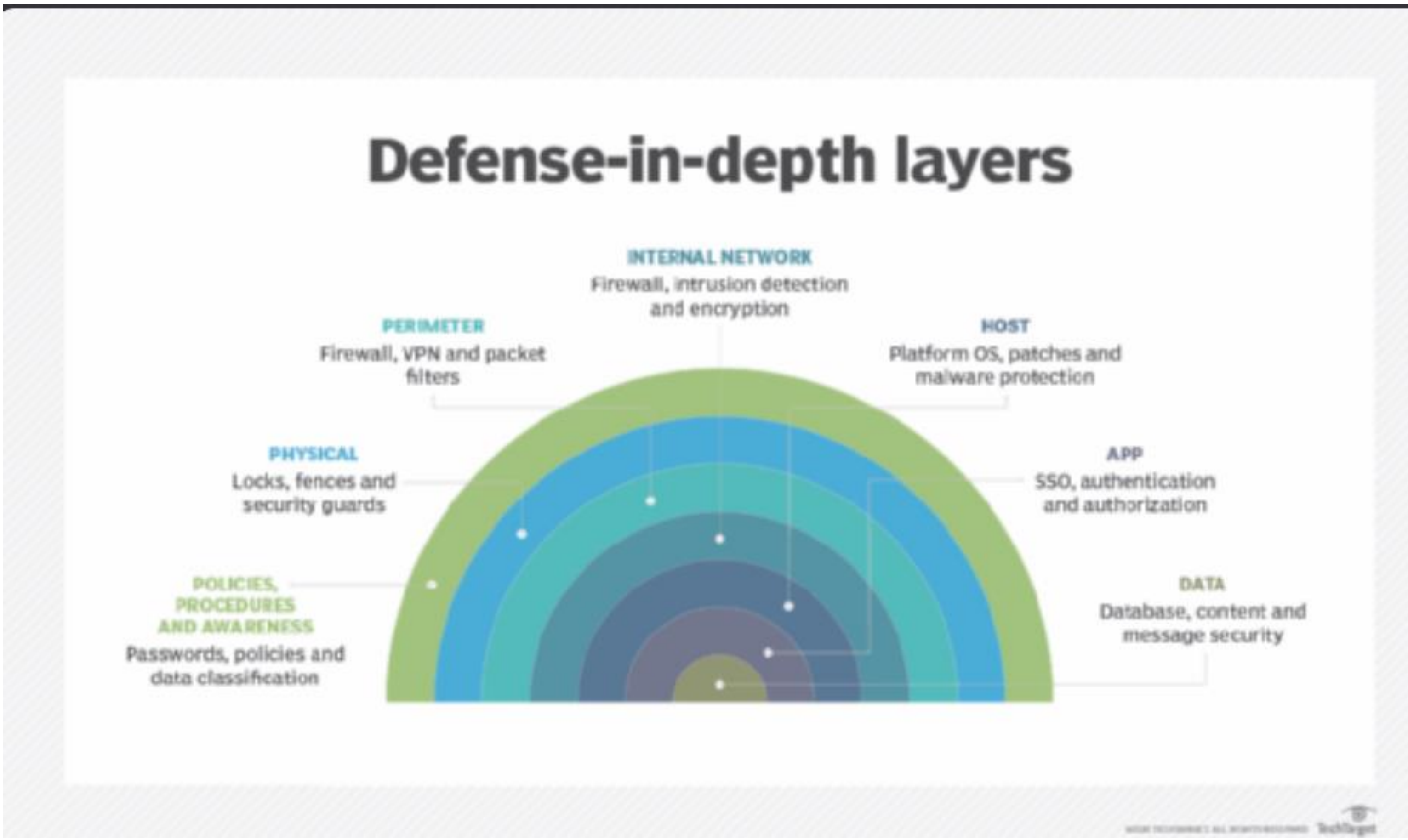
If an attack is blocked by a Network Intrusion Prevention System (NIPS) but doesn't appear in the boundary firewall logs, it suggests that multiple layers of security controls have been deployed to provide comprehensive protection, even if the attack reaches a certain point in the network.

A: NIC Teaming: NIC teaming involves grouping multiple network interface cards (NICs) together to provide redundancy and load balancing. While it can enhance network availability, it may not directly address the prevention of attacks.

B: Port mirroring: Port mirroring is a network monitoring feature that copies traffic from one network port to another for analysis or monitoring purposes. It helps with network visibility but does not necessarily prevent attacks.

D: High availability: High availability configurations are designed to ensure continuous service availability by minimizing downtime through redundancy and failover mechanisms. While important for service continuity, high availability alone may not prevent specific attacks.

E: Geographic dispersal: Geographic dispersal involves spreading IT resources across multiple geographic locations to enhance resilience and disaster recovery capabilities. It may help with business continuity but may not be related to the specific prevention of attacks.


Defense-in-depth layers
INTERNAL NETWORK
Firewall, intrusion detection and encryption
PERIMETER
Firewall, VPN and packet filters
HOST
Platform OS, patches and malware protection
PHYSICAL
Locks, fences and security guards
APP
SSO, authentication and authorization
POLICIES, PROCEDURES AND AWARENESS
Passwords, policies and data classification
DATA
Database, content and message security
TechTarget

Question #:109 - (Exam Topic 1)

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned if servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

A. 135

B. 139

C. 143

D. 161

E. 443

F. 445

Answer: B F

Explanation

To protect the servers in the DMZ from potential **external attacks** related to the SMB vulnerability when patches are not available, you should block the following TCP ports for all **external inbound connections**:

Port 139: This is the NetBIOS Session Service port. It is commonly used for SMB over NetBIOS and is a potential vector for attacks. Blocking this port helps mitigate the risk.

Port 445: This is the standard port for SMB over TCP. Blocking this port is essential because it directly relates to SMB, and blocking it prevents external attackers from attempting to exploit the vulnerability over SMB connections.

Blocking ports 135, 143, 161, and 443 is not directly related to mitigating SMB vulnerabilities and may disrupt legitimate services or applications that rely on those ports. Therefore, it's best to focus on ports 139 and 445 as the primary measures to **protect the servers in the DMZ**.

Question #:110 - (Exam Topic 1)

After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?

A. The unexpected traffic correlated against multiple rules, generating multiple alerts.

B. Multiple alerts were generated due to an attack occurring at the same time.

C. An error in the correlation rules triggered multiple alerts.

D. The SIEM was unable to correlate the rules, triggering the alerts.

Answer: A

Explanation

A hardware incident can cause changes in network traffic patterns, leading to an increase in the volume of traffic. This increase in traffic can cause the traffic to be flagged by multiple rules in the SIEM, leading to multiple alerts being generated. This is because the SIEM is designed to monitor network traffic and detect any potential security threats, and the increased traffic may be seen as suspicious. The systems administrator needs to review the alerts and determine if any further action is needed to secure the network.