



# CompTIA

## Exam Questions CAS-005

CompTIA SecurityX Exam

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

- A. Improve firewall rules to avoid access to those platforms.
- B. Implement a cloud-access security broker
- C. Create SIEM rules to raise alerts for access to those platforms
- D. Deploy an internet proxy that filters certain domains

**Answer: B**

#### Explanation:

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:

? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.

? B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.

? C. Create SIEM rules to raise alerts for access to those platforms: This helps in monitoring but does not prevent data leaks.

? D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB. Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services. References:

? CompTIA Security+ Study Guide

? Gartner, "Magic Quadrant for Cloud Access Security Brokers"

? NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

### NEW QUESTION 2

A company detects suspicious activity associated with external connections Security detection tools are unable to categorize this activity. Which of the following is the best solution to help the company overcome this challenge?

- A. Implement an Interactive honeypot
- B. Map network traffic to known IoCs.
- C. Monitor the dark web
- D. implement UEBA

**Answer: D**

#### Explanation:

User and Entity Behavior Analytics (UEBA) is the best solution to help the company overcome challenges associated with suspicious activity that cannot be categorized by traditional detection tools. UEBA uses advanced analytics to establish baselines of normal behavior for users and entities within the network. It then identifies deviations from these baselines, which may indicate malicious activity. This approach is particularly effective for detecting unknown threats and sophisticated attacks that do not match known indicators of compromise (IoCs).

Reference: CompTIA SecurityX Study Guide, Chapter on Advanced Threat Detection and Mitigation, Section on User and Entity Behavior Analytics (UEBA).

### NEW QUESTION 3

A security analyst discovered requests associated with IP addresses known for born legitimate 3rd bot-related traffic. Which of the following should the analyst use to determine whether the requests are malicious?

- A. User-agent string
- B. Byte length of the request
- C. Web application headers
- D. HTML encoding field

**Answer: A**

#### Explanation:

The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.

Why Use User-Agent String?

? Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.

? Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.

? Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.

Other options provide useful information but may not be as effective for initial determination of the nature of the request:

? B. Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.

? C. Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.

? D. HTML encoding field: This is not typically used for identifying the nature of the request.

References:

? CompTIA SecurityX Study Guide

? "User-Agent Analysis for Security," OWASP

? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)"

### NEW QUESTION 4

Users are willing passwords on paper because of the number of passwords needed in an environment. Which of the following solutions is the best way to manage this situation and decrease risks?

- A. Increasing password complexity to require 31 least 16 characters
- B. implementing an SSO solution and integrating with applications
- C. Requiring users to use an open-source password manager
- D. Implementing an MFA solution to avoid reliance only on passwords

**Answer: B**

**Explanation:**

Implementing a Single Sign-On (SSO) solution and integrating it with applications is the best way to manage the situation and decrease risks. Here??s why:  
? Reduced Password Fatigue: SSO allows users to log in once and gain access to multiple applications and systems without needing to remember and manage multiple passwords. This reduces the likelihood of users writing down passwords.  
? Improved Security: By reducing the number of passwords users need to manage, SSO decreases the attack surface and potential for password-related security breaches. It also allows for the implementation of stronger authentication methods.  
? User Convenience: SSO improves the user experience by simplifying the login process, which can lead to higher productivity and satisfaction.  
? References:

**NEW QUESTION 5**

A global manufacturing company has an internal application mat is critical to making products This application cannot be updated and must Be available in the production area A security architect is implementing security for the application. Which of the following best describes the action the architect should take-?

- A. Disallow wireless access to the application.
- B. Deploy Intrusion detection capabilities using a network tap
- C. Create an acceptable use policy for the use of the application
- D. Create a separate network for users who need access to the application

**Answer: D**

**Explanation:**

Creating a separate network for users who need access to the application is the best action to secure an internal application that is critical to the production area and cannot be updated.

Why Separate Network?

? Network Segmentation: Isolates the critical application from the rest of the network, reducing the risk of compromise and limiting the potential impact of any security incidents.

? Controlled Access: Ensures that only authorized users have access to the application, enhancing security and reducing the attack surface.

? Minimized Risk: Segmentation helps in protecting the application from vulnerabilities that could be exploited from other parts of the network.

Other options, while beneficial, do not provide the same level of security for a critical application:

? A. Disallow wireless access: Useful but does not provide comprehensive protection.

? B. Deploy intrusion detection capabilities using a network tap: Enhances monitoring but does not provide the same level of isolation and control.

? C. Create an acceptable use policy: Important for governance but does not provide technical security controls.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-125, "Guide to Security for Full Virtualization Technologies"

? "Network Segmentation Best Practices," Cisco Documentation

**NEW QUESTION 6**

A user submits a help desk ticket stating then account does not authenticate sometimes. An analyst reviews the following logs for the user: Which of the following best explains the reason the user's access is being denied?

- A. incorrectly typed password
- B. Time-based access restrictions
- C. Account compromise
- D. Invalid user-to-device bindings

**Answer: B**

**Explanation:**

The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.

References:

? CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.

? "Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

**NEW QUESTION 7**

During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:

Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)



After five days, the EDR console reports an infection on the host 0WIN23 by a remote access Trojan Which of the following is the most probable cause of the infection?

- A. 0W1N23 uses a legacy version of Windows that is not supported by the EDR
- B. LN002 was not supported by the EDR solution and propagates the RAT
- C. The EDR has an unknown vulnerability that was exploited by the attacker.
- D. 0W1N29 spreads the malware through other hosts in the network

Answer: A

Explanation:

OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).

? A. OWIN23 uses a legacy version of Windows that is not supported by the EDR:

This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.

? B. LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.

? C. The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.

? D. OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.

References:

? CompTIA Security+ Study Guide

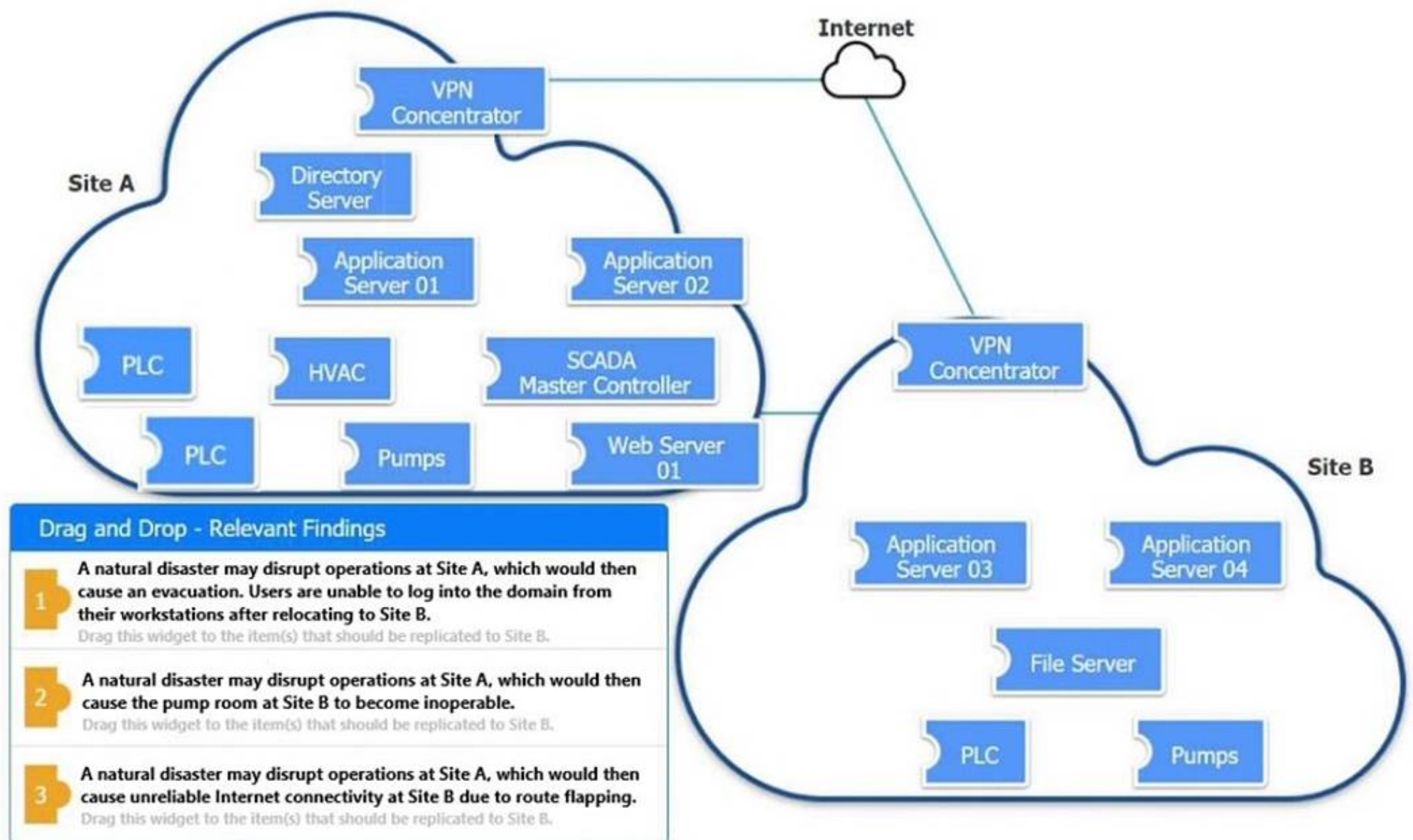
? NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations"

? Microsoft's Windows 7 End of Support documentation

NEW QUESTION 8

DRAG DROP

An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS

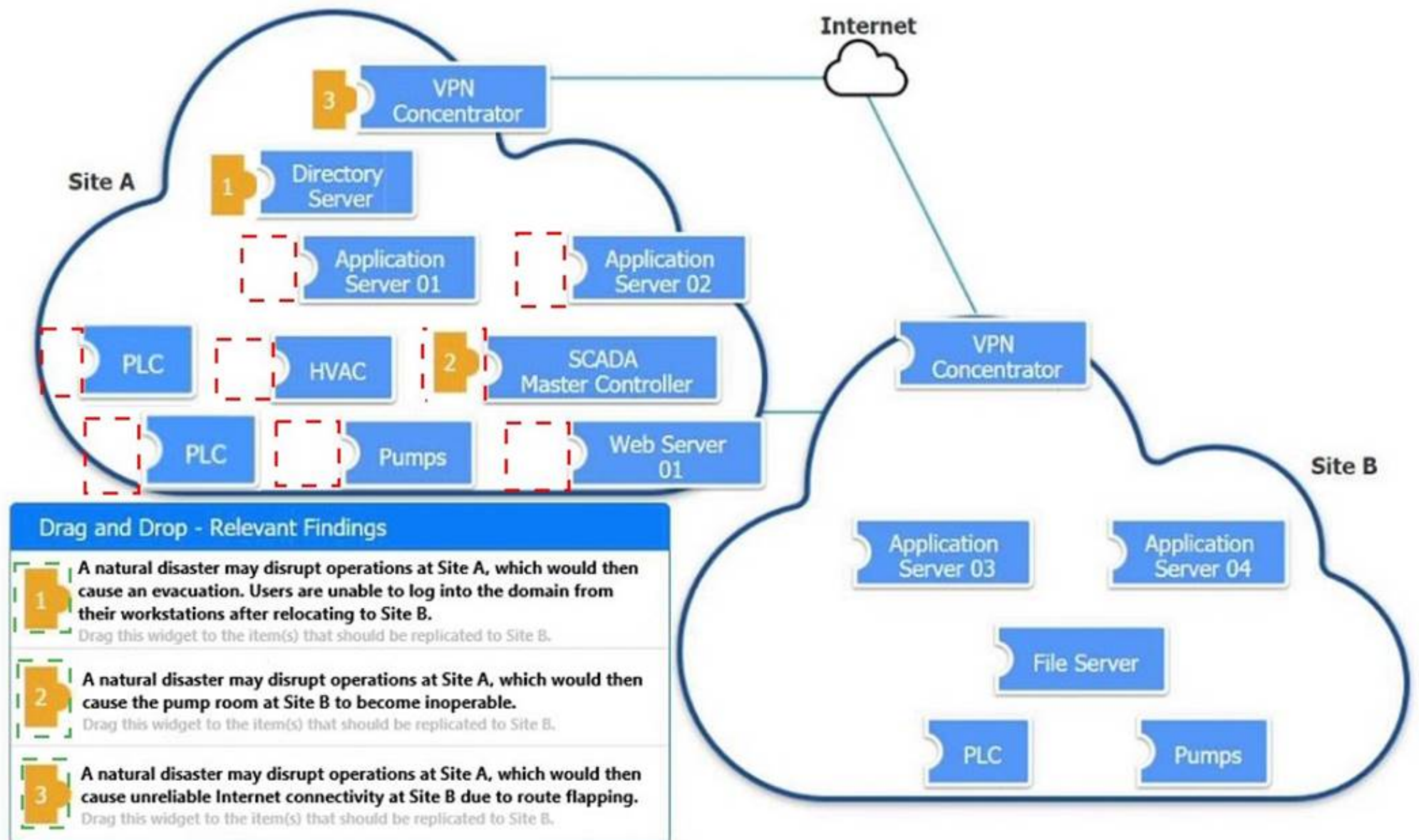


Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

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



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

✕

A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Corrective Action

Modify the BGP configuration
▼

#### NEW QUESTION 9

A security engineer is developing a solution to meet the following requirements?

- All endpoints should be able to establish telemetry with a SIEM.
- All endpoints should be able to be integrated into the XDR platform.
- SOC services should be able to monitor the XDR platform

Which of the following should the security engineer implement to meet the requirements?

- A. CDR and central logging
- B. HIDS and vTPM
- C. WAF and syslog
- D. HIPS and host-based firewall

**Answer:** D

**Explanation:**

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the



SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

References:

- ? CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.
- ? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.
- ? "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

#### NEW QUESTION 10

A security engineer is building a solution to disable weak CBC configuration for remote access connections to Linux systems. Which of the following should the security engineer modify?

- A. The /etc/openssl.conf file, updating the virtual site parameter
- B. The /etc/nsswith.conf file, updating the name server
- C. The /etc/hosts file, updating the IP parameter
- D. The /etc/ssh/sshd\_config file, updating the ciphers

**Answer: D**

#### Explanation:

The sshd\_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd\_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.

By editing the /etc/ssh/sshd\_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the SSH server does not use insecure encryption methods.

References:

- ? CompTIA Security+ Study Guide
- ? OpenSSH manual pages (man sshd\_config)
- ? CIS Benchmarks for Linux

#### NEW QUESTION 10

A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

Which of the following should the company implement to best resolve the issue?

- A. IDS
- B. CDN
- C. WAF
- D. NAC

**Answer: B**

#### Explanation:

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website's performance.

- ? A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.
  - ? B. CDN (Content Delivery Network): A CDN stores copies of the website's content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.
  - ? C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.
  - ? D. NAC (Network Access Control): NAC solutions control access to network resources but are not designed to address web performance issues.
- Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

References:

- ? CompTIA Security+ Study Guide
- ? "CDN: Content Delivery Networks Explained" by Akamai Technologies
- ? NIST SP 800-44, "Guidelines on Securing Public Web Servers"

#### NEW QUESTION 12

Company A and Company D are merging. Company A's compliance reports indicate branch protections are not in place. A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should the analyst

consider when completing this basic?

- A. If developers are unable to promote to production
- B. If DAST code is being stored to a single code repository
- C. If DAST scans are routinely scheduled
- D. If role-based training is deployed

**Answer: C**

**Explanation:**

Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?

? Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.

? Compliance: Routine scans ensure that the development process complies with security standards and regulations.

? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.

? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.

Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:

? A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.

? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.

? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

References:

? CompTIA SecurityX Study Guide

? OWASP Testing Guide

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

**NEW QUESTION 16**

Audit findings indicate several user endpoints are not utilizing full disk encryption During the remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption Which of the following is the most likely reason the device must be replaced'

- A. The HSM is outdated and no longer supported by the manufacturer
- B. The vTPM was not properly initialized and is corrupt.
- C. The HSM is vulnerable to common exploits and a firmware upgrade is needed
- D. The motherboard was not configured with a TPM from the OEM supplier.
- E. The HSM does not support sealing storage

**Answer: D**

**Explanation:**

The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.

Why TPM is Necessary for Full Disk Encryption:

? Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.

? Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.

? Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.

Other options do not directly address the requirement for TPM in supporting full disk encryption:

? A. The HSM is outdated: While HSM (Hardware Security Module) is important for security, it is not typically used for full disk encryption.

? B. The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.

? C. The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.

? E. The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.

References:

? CompTIA SecurityX Study Guide

? "Trusted Platform Module (TPM) Overview," Microsoft Documentation

? "BitLocker Deployment Guide," Microsoft Documentation

**NEW QUESTION 18**

A systems administrator wants to use existing resources to automate reporting from disparate security appliances that do not currently communicate. Which of the following is the best way to meet this objective?

- A. Configuring an API Integration to aggregate the different data sets
- B. Combining back-end application storage into a single, relational database
- C. Purchasing and deploying commercial off the shelf aggregation software
- D. Migrating application usage logs to on-premises storage

**Answer: A**

**Explanation:**

The best way to automate reporting from disparate security appliances that do not currently communicate is to configure an API Integration to aggregate the different data sets. Here's why:

? Interoperability: APIs allow different systems to communicate and share data, even

if they were not originally designed to work together. This enables the integration of various security appliances into a unified reporting system.

? Automation: API integrations can automate the process of data collection, aggregation, and reporting, reducing manual effort and increasing efficiency.

? Scalability: APIs provide a scalable solution that can easily be extended to include additional security appliances or data sources as needed.

? References:



#### NEW QUESTION 19

Third parties notified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

- A. Using IaC to include the newest dependencies
- B. Creating a bug bounty program
- C. Implementing a continuous security assessment program
- D. Integrating a SAST tool as part of the pipeline

**Answer: D**

#### Explanation:

The best solution to address reported vulnerabilities in third-party libraries is integrating a Static Application Security Testing (SAST) tool as part of the development pipeline. Here's why:

- ? Early Detection: SAST tools analyze source code for vulnerabilities before the code is compiled. This allows developers to identify and fix security issues early in the development process.
- ? Continuous Security: By integrating SAST tools into the CI/CD pipeline, the organization ensures continuous security assessment of the codebase, including third-party libraries, with each code commit and build.
- ? Comprehensive Analysis: SAST tools provide a detailed analysis of the code, identifying potential vulnerabilities in both proprietary code and third-party dependencies, ensuring that known issues in libraries are addressed promptly.
- ? References:

#### NEW QUESTION 24

A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suites:
The server accepted the following 4 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA          56
TLS_RSA_WITH_AES_128_CBC_SHA      128
TLS_RSA_WITH_3DES_EDE_CBC_SHA     168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 168 DH (1024 bits)
```

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).

- A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
- B. Removing support for CBC-based key exchange and signing algorithms
- C. Adding TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA256
- D. Implementing HIPS rules to identify and block BEAST attack attempts
- E. Restricting cipher suites to only allow TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- F. Increasing the key length to 256 for TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

**Answer: BC**

#### Explanation:

On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:

- ? B. Removing support for CBC-based key exchange and signing algorithms: CBC mode is vulnerable to certain attacks like BEAST. By removing support for CBC- based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.
- ? C. Adding TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA256: This cipher suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"
- ? OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

#### NEW QUESTION 29

A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes The following email headers are being reviewed

Date	Sending domain	Reply-to domain	Subject
April 16	sales.com	sales-mail.com	Updated Security Questions
April 18	vendor.com	vendor.com	New Sales Catalog
April 18	partner.com	partner.com	B2B Sales Increase
April 19	hr-saas.com	hr-saas.com	Employee Payroll Update Request
April 19	vendor.com	vendor.com	Password Requirements Not Met

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

- A. Block messages from hr-saas.com because it is not a recognized domain.
- B. Reroute all messages with unusual security warning notices to the IT administrator

- C. Quarantine all messages with sales-mail.com in the email header
- D. Block vendor.com for repeated attempts to send suspicious messages

**Answer:** D

**Explanation:**

In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here's the analysis of the options provided:

- \* A. Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.
- \* B. Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.
- \* C. Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.
- \* D. Block vendor.com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.

References:

? CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.

? NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.

? "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.

By blocking the domain that has consistently attempted to send suspicious messages, the security analyst can effectively reduce the risk of phishing attacks.

**NEW QUESTION 33**

A security analyst Detected unusual network traffic related to program updating processes The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing, valid binaries but. with different hashes which of the following solutions would most likely prevent this situation from reoccurring?

- A. Improving patching processes
- B. Implementing digital signature
- C. Performing manual updates via USB ports
- D. Allowing only files from internal sources

**Answer:** B

**Explanation:**

Implementing digital signatures ensures the integrity and authenticity of software binaries. When a binary is digitally signed, any tampering with the file (e.g., replacing it with a malicious version) would invalidate the signature. This allows systems to verify the origin and integrity of binaries before execution, preventing the execution of unauthorized or compromised binaries.

? A. Improving patching processes: While important, this does not directly address the issue of verifying the integrity of binaries.

? B. Implementing digital signatures: This ensures that only valid, untampered binaries are executed, preventing attackers from substituting legitimate binaries with malicious ones.

? C. Performing manual updates via USB ports: This is not practical and does not scale well, especially in large environments.

? D. Allowing only files from internal sources: This reduces the risk but does not provide a mechanism to verify the integrity of binaries.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-57, "Recommendation for Key Management"

? OWASP (Open Web Application Security Project) guidelines on code signing

**NEW QUESTION 38**

An incident response team is analyzing malware and observes the following:

- Does not execute in a sandbox
- No network IoCs
- No publicly known hash match
- No process injection method detected

Which of the following should the team do next to proceed with further analysis?

- A. Use an online vims analysis tool to analyze the sample
- B. Check for an anti-virtualization code in the sample
- C. Utilize a new deployed machine to run the sample.
- D. Search oilier internal sources for a new sample.

**Answer:** B

**Explanation:**

Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:

? It helps determine if the malware is designed to evade analysis tools.

? Identifying such code can provide insights into the malware's behavior and intent.

? This step can also inform further analysis methods, such as running the malware on physical hardware.

References:

? CompTIA Security+ Study Guide

? SANS Institute, "Malware Analysis Techniques"

? "Practical Malware Analysis" by Michael Sikorski and Andrew Honig

**NEW QUESTION 39**

After an incident occurred, a team reported during the lessons-learned review that the team.

- \* Lost important Information for further analysis.
- \* Did not utilize the chain of communication
- \* Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findings?

- A. Requesting budget for better forensic tools to Improve technical capabilities for Incident response operations
- B. Building playbooks for different scenarios and performing regular table-top exercises
- C. Requiring professional incident response certifications for each new team member
- D. Publishing the incident response policy and enforcing it as part of the security awareness program

**Answer: B**

**Explanation:**

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:

? Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.

? Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.

? Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"

? SANS Institute, "Incident Handler's Handbook"

**NEW QUESTION 43**

A security engineer wants to reduce the attack surface of a public-facing containerized application Which of the following will best reduce the application's privilege escalation attack surface?

- A. Implementing the following commands in the Dockerfile:RUN echo user:x:1000:1000iuser:/home/user:/dew/null > /etc/passwd
- B. Installing an EDR on the container's host with reporting configured to log to a centralized SIEM and Implementing the following alerting rules TF PBOCESS\_USEB=rooC ALERT\_TYPE=critical
- C. Designing a multicontainer solution, with one set of containers that runs the main application, and another set of containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts
- D. Running the container in an isolated network and placing a load balancer in a public-facing network
- E. Adding the following ACL to the load balancer:PZRKZI HTTP from 0-0.0.0.0/0 port 443

**Answer: A**

**Explanation:**

Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of

privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.

? A. Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.

? B. Installing an EDR on the container's host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application.

? C. Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation.

? D. Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.

References:

? CompTIA Security+ Study Guide

? Docker documentation on security best practices

? NIST SP 800-190, "Application Container Security Guide"

**NEW QUESTION 48**

A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows to meet hospital policy

- Full disk encryption is enabled
- "Always On" corporate VPN is enabled
- ef-use-backed keystore is enabled ready.
- Wi-Fi 6 is configured with SAE.
- Location services is disabled.
- Application allow list is configured

- A. Revoking the user certificates used for VPN and Wi-Fi access
- B. Performing cryptographic obfuscation
- C. Using geolocation to find the device
- D. Configuring the application allow list to only permit emergency calls
- E. Returning the device's solid-state media to zero

**Answer: E**



**Explanation:**

To mitigate the risk of data loss on a lost or stolen tablet quickly, the most effective strategy is to return the device's solid-state media to zero, which effectively erases all data on the device. Here's why:

? Immediate Data Erasure: Returning the solid-state media to zero ensures that all data is wiped instantly, mitigating the risk of data loss if the device is lost or stolen.

? Full Disk Encryption: Even though the tablets are already encrypted, physically erasing the data ensures that no residual data can be accessed if someone attempts to bypass encryption.

? Compliance and Security: This method adheres to best practices for data security and compliance, ensuring that sensitive patient data cannot be accessed by unauthorized parties.

**NEW QUESTION 52**

A senior security engineer flags me following log file snippet as having likely facilitated an attacker's lateral movement in a recent breach:

```
[log.txt]
...
qry_source: 19.27.214.22 TCP/53
qry_dest: 199.105.22.13 TCP/53
qry_type: AXFR
| in comptia.org
-----| directoryserver1 A 10.80.8.10
-----| directoryserver2 A 10.80.8.11
-----| directoryserver3 A 10.80.8.12
-----| internal-dns A 10.80.9.1
-----| www-int A 10.80.9.2
-----| fshare A 10.80.9.4
-----| sip A 10.80.9.5
-----| man-crit-apps A 10.81.22.33
...
```

Which of the following solutions, if implemented, would mitigate the risk of this issue reoccurring?

- A. Disabling DNS zone transfers
- B. Restricting DNS traffic to UDP/W
- C. Implementing DNS masking on internal servers
- D. Permitting only clients from internal networks to query DNS

**Answer:** A

**Explanation:**

The log snippet indicates a DNS AXFR (zone transfer) request, which can be exploited by attackers to gather detailed information about an internal network's infrastructure. Disabling DNS zone transfers is the best solution to mitigate this risk. Zone transfers should generally be restricted to authorized secondary DNS servers and not be publicly accessible, as they can reveal sensitive network information that facilitates lateral movement during an attack.

References:

? CompTIA SecurityX Study Guide: Discusses the importance of securing DNS configurations, including restricting zone transfers.

? NIST Special Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide": Recommends restricting or disabling DNS zone transfers to prevent information leakage.

**NEW QUESTION 54**

A network engineer must ensure that always-on VPN access is enabled and restricted to company assets. Which of the following best describes what the engineer needs to do?

- A. Generate device certificates using the specific template settings needed
- B. Modify signing certificates in order to support IKE version 2
- C. Create a wildcard certificate for connections from public networks
- D. Add the VPN hostname as a SAN entry on the root certificate

**Answer:** A

**Explanation:**

To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.

Why Device Certificates are Necessary:

? Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.

? Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.

? Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.

Other options do not provide the same level of control and security for always-on VPN access:

? B. Modify signing certificates for IKE version 2: While important for VPN protocols, it does not address device-specific authentication.

? C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.

? D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.

References:

? CompTIA SecurityX Study Guide

? "Device Certificates for VPN Access," Cisco Documentation

? NIST Special Publication 800-77, "Guide to IPsec VPNs"

#### NEW QUESTION 55

A security engineer needs to secure the OT environment based on the following requirements

- Isolate the OT network segment
- Restrict Internet access.
- Apply security updates to workstations
- Provide remote access to third-party vendors

Which of the following design strategies should the engineer implement to best meet these requirements?

- A. Deploy a jump box on the third party network to access the OT environment and provide updates using a physical delivery method on the workstations
- B. Implement a bastion host in the OT network with security tools in place to monitor access and use a dedicated update server for the workstations.
- C. Enable outbound internet access on the OT firewall to any destination IP address and use the centralized update server for the workstations
- D. Create a staging environment on the OT network for the third-party vendor to access and enable automatic updates on the workstations.

**Answer: B**

#### Explanation:

To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network.

The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect

while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.

References:

? CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.

? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.

? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

#### NEW QUESTION 59

A software engineer is creating a CI/CD pipeline to support the development of a web application. The DevSecOps team is required to identify syntax errors. Which of the following is the most relevant to the DevSecOps team's task?

- A. Static application security testing
- B. Software composition analysis
- C. Runtime application self-protection
- D. Web application vulnerability scanning

**Answer: A**

#### Explanation:

Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.

? A. Static application security testing (SAST): SAST tools analyze the source code

to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.

? B. Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.

? C. Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.

? D. Web application vulnerability scanning: This involves scanning the running application for vulnerabilities but does not address syntax errors in the code.

References:

? CompTIA Security+ Study Guide

? OWASP (Open Web Application Security Project) guidelines on SAST

? NIST SP 800-95, "Guide to Secure Web Services" Top of Form

Bottom of Form

#### NEW QUESTION 63

A company hired an email service provider called my-email.com to deliver company emails. The company stalled having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmARC include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Select two).

- A. The email CNAME record must be changed to a type A record pointing to 192.168.111
- B. The TXT record must be Changed to "v=dmARC ip4:192.168.1.10 include:my-email.com - all"
- C. The srv01 A record must be changed to a type CNAME record pointing to the email server
- D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10
- E. The TXT record must be changed to "v=dkim ip4:192.168.1.11 include my-email.com - ell"
- F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"
- G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

**Answer:** BD

#### Explanation:

The security engineer should modify the following to fix the email migration issues:

? Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.

? TXT Record for DMARC: The TXT record must be changed to "v=dmARC ip4:192.168.1.10 include com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.

? uk.co.certification.simulator.questionpool.PList@488ba0cc

? References:

#### NEW QUESTION 66

A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved to the repository. The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment. Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

- A. Software composition analysis
- B. Pre-commit code linting
- C. Repository branch protection
- D. Automated regression testing
- E. Code submit authorization workflow
- F. Pipeline compliance scanning

**Answer:** BD

#### Explanation:

? B. Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.

? D. Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.

Other options:

? A. Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures.

? C. Repository branch protection: While this can help manage the code submission process, it does not directly prevent deployment failures caused by code issues or security check failures.

? E. Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted.

? F. Pipeline compliance scanning: This checks for compliance with security policies but does not address syntax or regression issues.

References:

? CompTIA Security+ Study Guide

? "Continuous Integration and Continuous Delivery" by Jez Humble and David Farley

? OWASP (Open Web Application Security Project) guidelines on secure coding practices

#### NEW QUESTION 71

A security architect is establishing requirements to design resilience in an enterprise system that will be extended to other physical locations. The system must

- Be survivable to one environmental catastrophe
- Be recoverable within 24 hours of critical loss of availability
- Be resilient to active exploitation of one site-to-site VPN solution

- A. Load-balance connection attempts and data Ingress at internet gateways
- B. Allocate fully redundant and geographically distributed standby sites.
- C. Employ layering of routers from diverse vendors
- D. Lease space to establish cold sites throughout other countries
- E. Use orchestration to procure, provision, and transfer application workloads to cloudservices



F. Implement full weekly backups to be stored off-site for each of the company's sites

**Answer:** B

**Explanation:**

To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant and geographically distributed standby sites. Here??s why:

? Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.

? Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.

? Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.

? References:

**NEW QUESTION 72**

**SIMULATION**

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

**INSTRUCTIONS**

Review each of the events and select the appropriate analysis and remediation options for each IoC.

IoC 1	IoC 2	IoC 3																									
<table border="1"><thead><tr><th>Source</th><th>Svc</th><th>Type</th><th>Dest</th><th>Data</th></tr></thead><tbody><tr><td>Apache_httpd</td><td></td><td>DNSQ</td><td>@10.1.1.1:53</td><td>update.s.domain</td></tr><tr><td>Apache_httpd</td><td></td><td>DNSQR</td><td>@10.1.2.5</td><td>CNAME 3a129sk219r0slsmfkzzz000.s.domain</td></tr><tr><td>Apache_httpd</td><td></td><td>DNSQ</td><td>@10.1.1.1:53</td><td>3a129sk219r0slsmfkzzz000.s.domain</td></tr><tr><td>Apache_httpd</td><td></td><td>DNSQR</td><td>@10.1.2.5</td><td>IN A 108.158.253.253</td></tr></tbody></table>			Source	Svc	Type	Dest	Data	Apache_httpd		DNSQ	@10.1.1.1:53	update.s.domain	Apache_httpd		DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzzz000.s.domain	Apache_httpd		DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzzz000.s.domain	Apache_httpd		DNSQR	@10.1.2.5	IN A 108.158.253.253
Source	Svc	Type	Dest	Data																							
Apache_httpd		DNSQ	@10.1.1.1:53	update.s.domain																							
Apache_httpd		DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzzz000.s.domain																							
Apache_httpd		DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzzz000.s.domain																							
Apache_httpd		DNSQR	@10.1.2.5	IN A 108.158.253.253																							
<div>Select analysis</div> <div>An employee is attempting to access a blocked website. Someone is footprinting a network subnet. A host is participating in an IRC-based botnet. Service identification and fingerprinting are occurring. Canonical name records in a public DNS cache are being updated. An application is performing an automatic update. An employee is using P2P services to download files. The service is attempting to resolve a malicious domain.</div>																											
<div>Analysis</div> <div>Select analysis</div>																											
<div>Remediation</div> <div>Select remediation</div> <div>Enforce endpoint controls on third-party software installations. Investigate for software supply-chain attacks. Configure the DNS server to perform recursion. Block ping requests across the WAN interface. Deploy a network-based DLP solution. Implement a blocklist for known malicious ports. No further action is needed.</div> <div>Select remediation</div>																											

IoC 1		IoC 2		IoC 3	
Src	Dst	Proto	Data	Action	
10.0.5.5	10.1.2.1	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.2	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.3	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.4	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.5	IP_ICMP	ECHO	Drop	

Select analysis

An employee is attempting to access a blocked website.  
 Someone is footprinting a network subnet.  
 A host is participating in an IRC-based botnet.  
 Service identification and fingerprinting are occurring.  
 Canonical name records in a public DNS cache are being updated.  
 An application is performing an automatic update.  
 An employee is using P2P services to download files.  
 The service is attempting to resolve a malicious domain.

Select analysis

Select remediation

Enforce endpoint controls on third-party software installations.  
 Investigate for software supply-chain attacks.  
 Configure the DNS server to perform recursion.  
 Block ping requests across the WAN interface.  
 Deploy a network-based DLP solution.  
 Implement a blocklist for known malicious ports.  
 No further action is needed.

Select remediation

IoC 1		IoC 2		IoC 3	
<pre> Proxylog&gt; &gt; GET /announce?info_hash=%01d%FE%7E%F1%10%5CwvAp%ED%F6%03%C49%D6B%14%F1&amp; &gt; peer_id=%B8js%7F%E8%0C%AFh%02Y%967%24e%27V%EEM%16%5B&amp;port=41730&amp; &gt; uploaded=0&amp;downloaded=0&amp;left=3767869&amp;compact=1&amp;ip=10.5.1.26&amp;event=started &gt; HTTP/1.1 &gt; Accept: application/x-bittorrent &gt; Accept-Encoding: gzip &gt; User-Agent: RAZA 2.1.0.0 &gt; Host: localhost &gt; Connection: Keep-Alive &lt; &lt; HTTP 200 OK           </pre>					

Select analysis

An employee is attempting to access a blocked website.  
 Someone is footprinting a network subnet.  
 A host is participating in an IRC-based botnet.  
 Service identification and fingerprinting are occurring.  
 Canonical name records in a public DNS cache are being updated.  
 An application is performing an automatic update.  
 An employee is using P2P services to download files.  
 The service is attempting to resolve a malicious domain.

Select analysis

Select remediation

Enforce endpoint controls on third-party software installations.  
 Investigate for software supply-chain attacks.  
 Configure the DNS server to perform recursion.  
 Block ping requests across the WAN interface.  
 Deploy a network-based DLP solution.  
 Implement a blocklist for known malicious ports.  
 No further action is needed.

Select remediation

A. Mastered  
 B. Not Mastered

Answer: A

**Explanation:**

Analysis and Remediation Options for Each IoC: IoC 1:

? Evidence:

? Analysis:

? Remediation:

IoC 2:

? Evidence:

? Analysis:

? Remediation:

IoC 3:

? Evidence:

? Analysis:

? Remediation:

References:

? CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.

? CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.

? Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.

By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

**NEW QUESTION 77**

.....



## Relate Links

**100% Pass Your CAS-005 Exam with ExamBible Prep Materials**

<https://www.exambible.com/CAS-005-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>