

## Exam Questions CAS-005

CompTIA SecurityX Exam

<https://www.2passeasy.com/dumps/CAS-005/>



### 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 lake 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 lime 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 11 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 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 4

A company's SIEM 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 5

A company wants to use IoT devices to manage and monitor thermostats at all facilities. The thermostats must receive vendor security updates and limit access to other devices within the organization. Which of the following best addresses the company's requirements?

- A. Only allowing Internet access to a set of specific domains
- B. Operating IoT devices on a separate network with no access to other devices internally
- C. Only allowing operation for IoT devices during a specified time window
- D. Configuring IoT devices to always allow automatic updates

**Answer:** B

#### Explanation:

The best approach for managing and monitoring IoT devices, such as thermostats, is to operate them on a separate network with no access to other internal devices. This segmentation ensures that the IoT devices are isolated from the main network, reducing the risk of potential security breaches affecting other critical systems. Additionally, this setup allows for secure vendor updates without exposing the broader network to potential vulnerabilities inherent in IoT devices.

References:

? CompTIA SecurityX Study Guide: Recommends network segmentation for IoT devices to minimize security risks.

? NIST Special Publication 800-183, "Network of Things": Advises on the isolation of IoT devices to enhance security.

? "Practical IoT Security" by Brian Russell and Drew Van Duren: Discusses best practices for securing IoT devices, including network segmentation.

#### NEW QUESTION 6

Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

- A. Encryption systems based on large prime numbers will be vulnerable to exploitation
- B. Zero Trust security architectures will require homomorphic encryption.
- C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques
- D. Quantum computers will enable malicious actors to capture IP traffic in real time

**Answer:** A

#### Explanation:

Advancements in quantum computing pose a significant threat to current encryption systems, especially those based on the difficulty of factoring large prime numbers, such as RSA. Quantum computers have the potential to solve these problems exponentially faster than classical computers, making current cryptographic systems vulnerable.

Why Large Prime Numbers are Vulnerable:

? Shor's Algorithm: Quantum computers can use Shor's algorithm to factorize large integers efficiently, which undermines the security of RSA encryption.

? Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that encrypted data, which relies on the hardness of this mathematical problem, can be decrypted.

Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:

? B. Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms.

? C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption algorithms.

? D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.



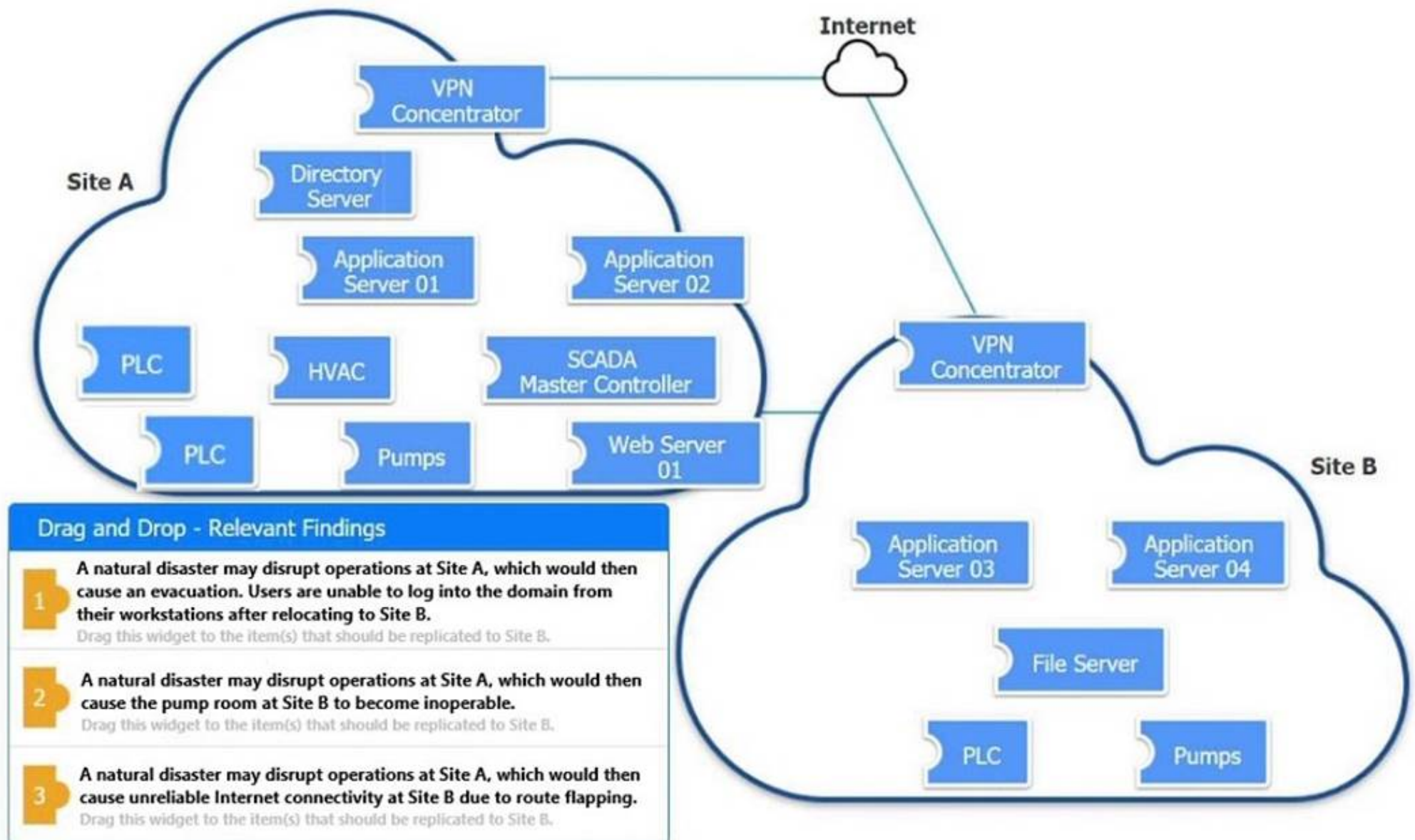
References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"
- ? "Quantum Computing and Cryptography," MIT Technology Review

NEW QUESTION 7

DRAG DROP

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

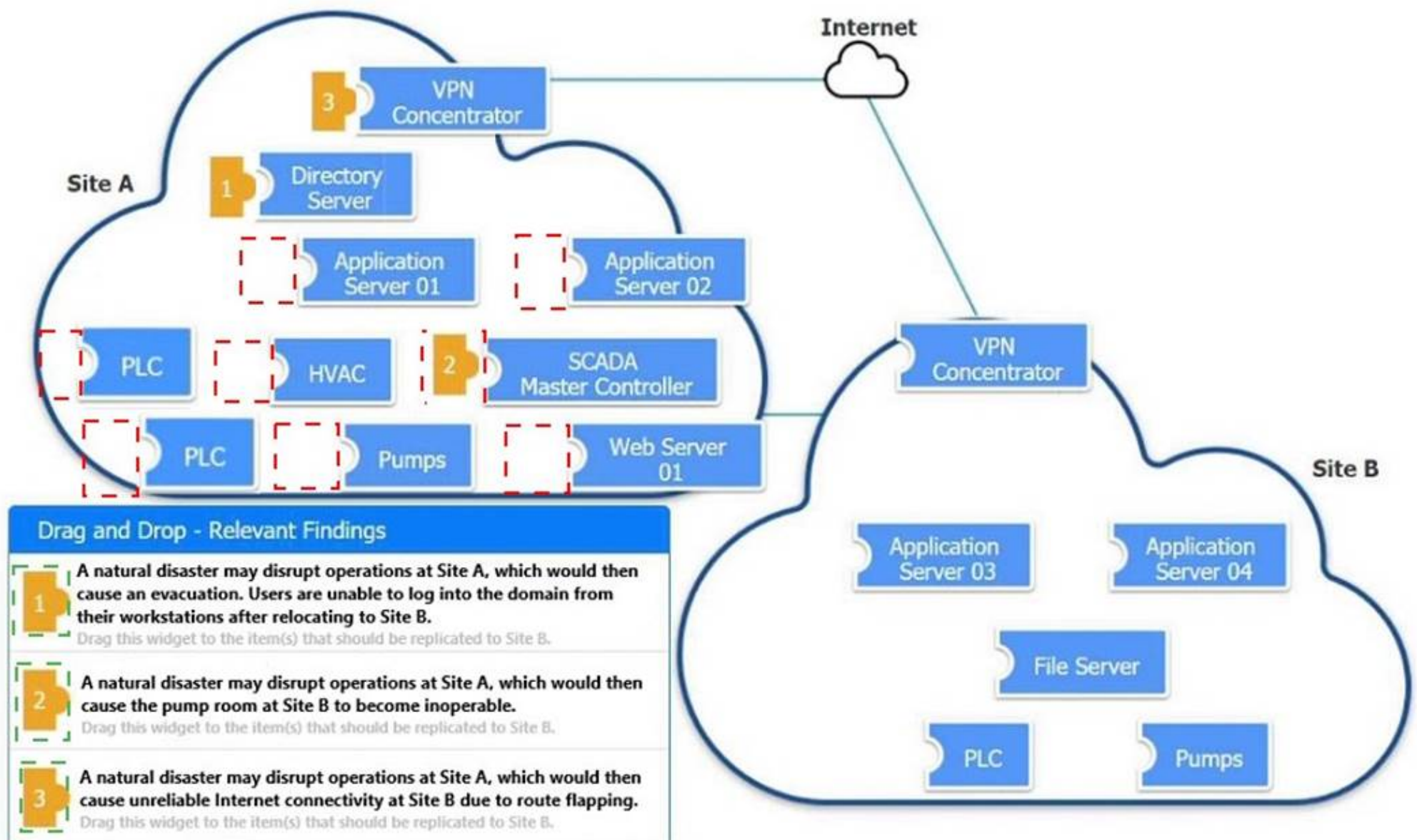


Review the following scenarios and instructions. Match each relevant finding to the affected host.

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 8

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 9

An audit finding reveals that a legacy platform has not retained logs for more than 30 days. The platform has been segmented due to its interoperability with newer technology. As a temporary solution, the IT department changed the log retention to 120 days. Which of the following should the security engineer do to ensure the logs are being properly retained?

- A. Configure a scheduled task nightly to save the logs
- B. Configure event-based triggers to export the logs at a threshold.
- C. Configure the SIEM to aggregate the logs
- D. Configure a Python script to move the logs into a SQL database.

**Answer:** C

**Explanation:**

To ensure that logs from a legacy platform are properly retained beyond the default retention period, configuring the SIEM to aggregate the logs is the best approach. SIEM solutions are designed to collect, aggregate, and store logs from various sources, providing centralized log management and retention. This setup ensures that logs are retained according to policy and can be easily accessed for analysis and compliance purposes. References:

? CompTIA SecurityX Study Guide: Discusses the role of SIEM in log management and retention.

? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Recommends the use of centralized log management solutions, such as SIEM, for effective log retention and analysis.

? "Security Information and Event Management (SIEM) Implementation" by David Miller: Covers best practices for configuring SIEM systems to aggregate and retain logs from various sources.

#### NEW QUESTION 10

An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry. Which of the following should the security analyst use to perform threat modeling?

- A. ATT&CK
- B. OWASP
- C. CAPEC
- D. STRIDE



**Answer:** A

**Explanation:**

The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry. Here's why:

? Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.

? Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.

? Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.

? References:

**NEW QUESTION 10**

An engineering team determines the cost to mitigate certain risks is higher than the asset values The team must ensure the risks are prioritized appropriately. Which of the following is the best way to address the issue?

- A. Data labeling
- B. Branch protection
- C. Vulnerability assessments
- D. Purchasing insurance

**Answer:** D

**Explanation:**

When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. This method allows the company to transfer the risk to an insurance provider, ensuring that financial losses are covered in the event of an incident. This approach is cost-effective and ensures that risks are prioritized appropriately without overspending on mitigation efforts.

References:

? CompTIA SecurityX Study Guide: Discusses risk management strategies, including risk transfer through insurance.

? NIST Risk Management Framework (RMF): Highlights the use of insurance as a risk mitigation strategy.

? "Information Security Risk Assessment Toolkit" by Mark Talabis and Jason Martin: Covers risk management practices, including the benefits of purchasing insurance.

**NEW QUESTION 14**

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 17**

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

- A. Risk appetite directly impacts acceptance of high-impact low-likelihood events.
- B. Organizational risk appetite varies from organization to organization
- C. Budgetary pressure drives risk mitigation planning in all companies
- D. Risk appetite directly influences which breaches are disclosed publicly

**Answer:** A

**Explanation:**

Risk appetite is the amount of risk an organization is willing to accept to achieve its objectives. When operating with a constrained budget, understanding the organization's risk appetite is crucial because:

? It helps prioritize security investments based on the level of risk the organization is

willing to tolerate.

? High-impact, low-likelihood events may be deemed acceptable if they fall within the organization's risk appetite, allowing for budget allocation to other critical areas.

? Properly understanding and defining risk appetite ensures that limited resources are used effectively to manage risks that align with the organization's strategic goals.

References:

? CompTIA Security+ Study Guide

? NIST Risk Management Framework (RMF) guidelines

? ISO 31000, "Risk Management – Guidelines"

#### NEW QUESTION 19

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 22

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 26

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 31

A financial services organization is using AI to fully automate the process of deciding client loan rates. Which of the following should the organization be most concerned about from a privacy perspective?

- A. Model explainability
- B. Credential Theft
- C. Possible prompt injections
- D. Exposure to social engineering

**Answer:** A

#### Explanation:

When using AI to fully automate the process of deciding client loan rates, the primary concern from a privacy perspective is model explainability.

Why Model Explainability is Critical:

? Transparency: It ensures that the decision-making process of the AI model can be understood and explained to stakeholders, including clients.

? Accountability: Helps in identifying biases and errors in the model, ensuring that the AI is making fair and unbiased decisions.

? Regulatory Compliance: Various regulations require that decisions, especially those affecting individuals' financial status, can be explained and justified.

? Trust: Builds trust among users and stakeholders by demonstrating that the AI decisions are transparent and justifiable.

Other options, such as credential theft, prompt injections, and social engineering, are significant concerns but do not directly address the privacy and fairness implications of automated decision-making.

References:

? CompTIA SecurityX Study Guide

? "The Importance of Explainability in AI," IEEE Xplore

? GDPR Article 22, "Automated Individual Decision-Making, Including Profiling"

#### NEW QUESTION 34

Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Select two).

Implementing DLP controls preventing sensitive data from leaving Company B's network

- A. Documenting third-party connections used by Company B
- B. Reviewing the privacy policies currently adopted by Company B
- C. Requiring data sensitivity labeling for all files shared with Company B
- D. Forcing a password reset requiring more stringent passwords for users on Company B's network
- E. Performing an architectural review of Company B's network

**Answer:** AB

#### Explanation:

To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:

\* A. Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.

\* E. Performing an architectural review of Company B's network: This review will identify

vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface.

These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions.

? NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections.

? "Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis: Discusses the importance of security assessments during acquisitions.

#### NEW QUESTION 38

An organization is implementing Zero Trust architecture. A systems administrator must increase the effectiveness of the organization's context-aware access system. Which of the following is the best way to improve the effectiveness of the system?

- A. Secure zone architecture
- B. Always-on VPN
- C. Accurate asset inventory
- D. Microsegmentation

**Answer:** D

#### Explanation:

Microsegmentation is a critical strategy within Zero Trust architecture that enhances context-aware access systems by dividing the network into smaller, isolated segments. This reduces the attack surface and limits lateral movement of attackers within the network. It ensures that even if one segment is compromised, the attacker cannot easily access other segments. This granular approach to network security is essential for enforcing strict access controls and monitoring within Zero Trust environments.

Reference: CompTIA SecurityX Study Guide, Chapter on Zero Trust Security, Section on Microsegmentation and Network Segmentation.

#### NEW QUESTION 39

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 44**

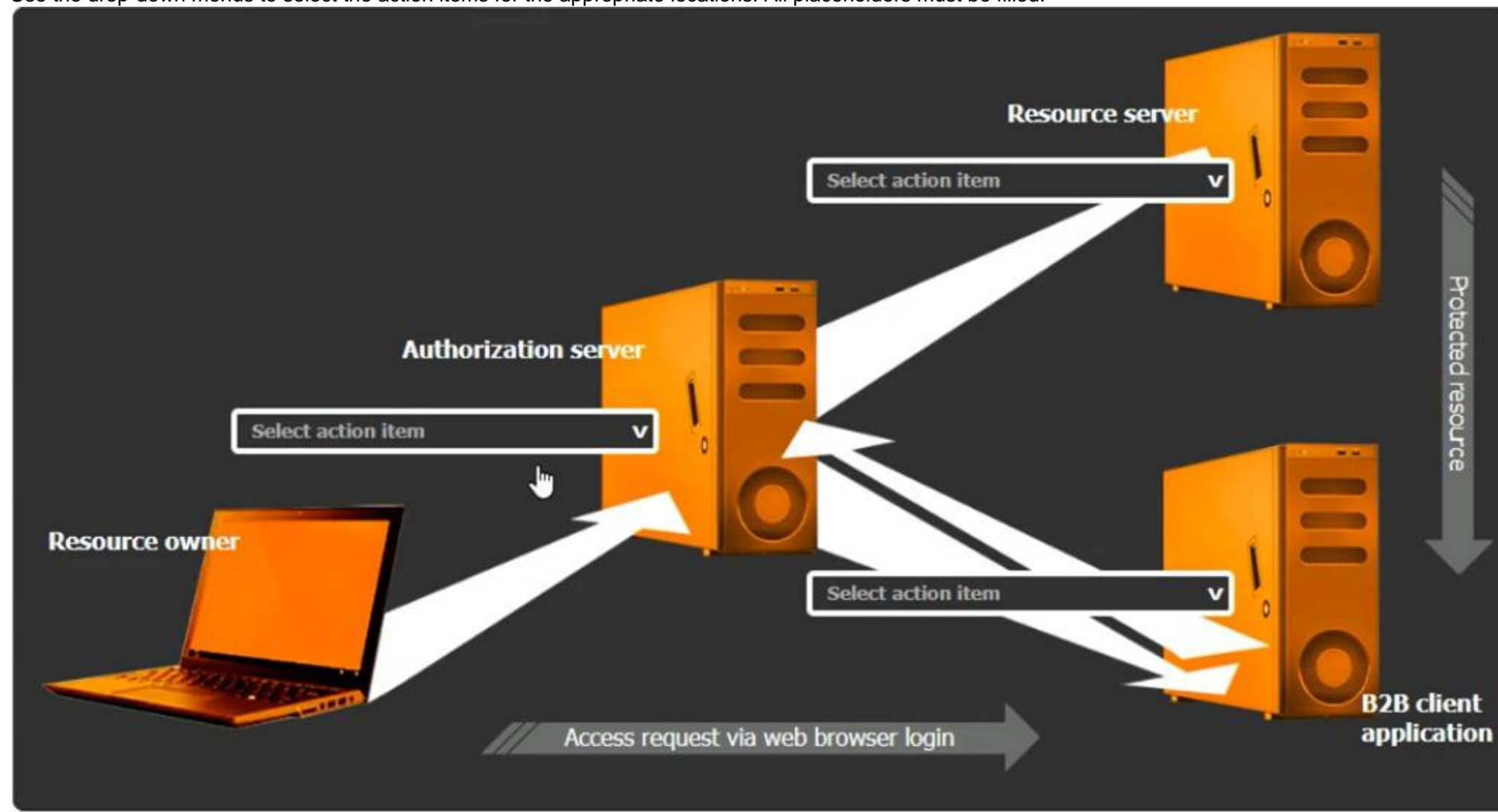
**SIMULATION**

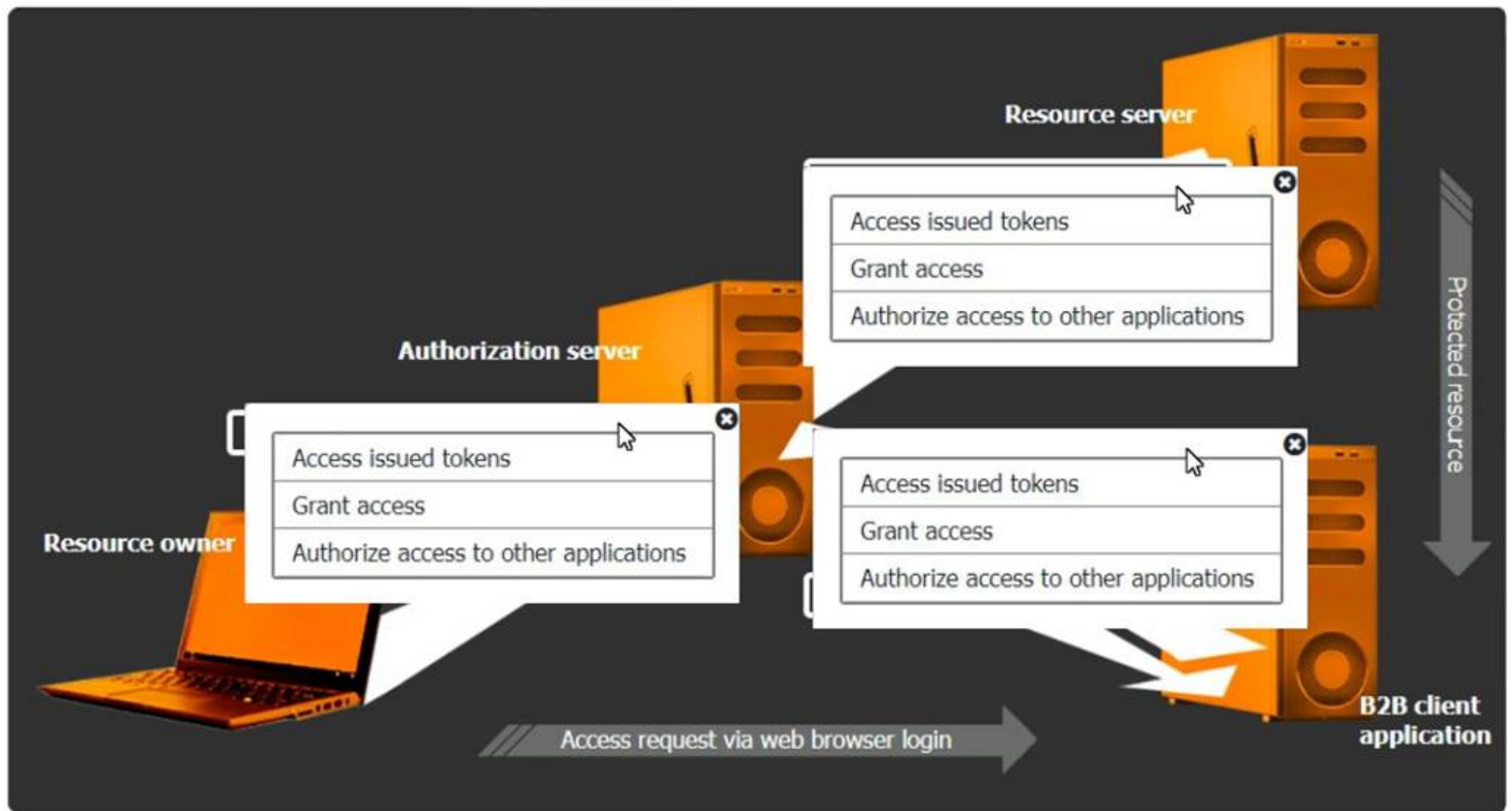
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- . The application does not need to know the users' credentials.
- . An approval interaction between the users and the HTTP service must be orchestrated.
- . The application must have limited access to users' data.

INSTRUCTIONS

Use the drop-down menus to select the action items for the appropriate locations. All placeholders must be filled.





- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Select the Action Items for the Appropriate Locations:

? Authorization Server:

? Resource Server:

? B2B Client Application:

Detailed Explanation

OAuth 2.0 is designed to provide specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. The integration involves multiple steps and components, including:

? Resource Owner (User):

? Client Application (B2B Client Application):

? Authorization Server:

? Resource Server:

OAuth Workflow:

? The resource owner accesses the client application.

? The client application redirects the resource owner to the authorization server for authentication.

? The authorization server authenticates the resource owner and asks for consent to grant access to the client application.

? Upon consent, the authorization server issues an authorization code or token to the client application.

? The client application uses the authorization code or token to request access to the resources from the resource server.

? The resource server verifies the token with the authorization server and, if valid, grants access to the requested resources.

References:

? CompTIA Security+ Study Guide: Provides comprehensive information on various authentication and authorization protocols, including OAuth.

? OAuth 2.0 Authorization Framework (RFC 6749): The official documentation detailing the OAuth 2.0 framework, its flows, and components.

? OAuth 2.0 Simplified: A book by Aaron Parecki that provides a detailed yet easy- to-understand explanation of the OAuth 2.0 protocol.

By ensuring that each component in the OAuth workflow performs its designated role, the B2B client application can securely access the necessary resources without compromising user credentials, adhering to the principle of least privilege.

**NEW QUESTION 46**

**SIMULATION**

An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:

\* 1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from-their workstations after relocating to Site B.

\* 2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.

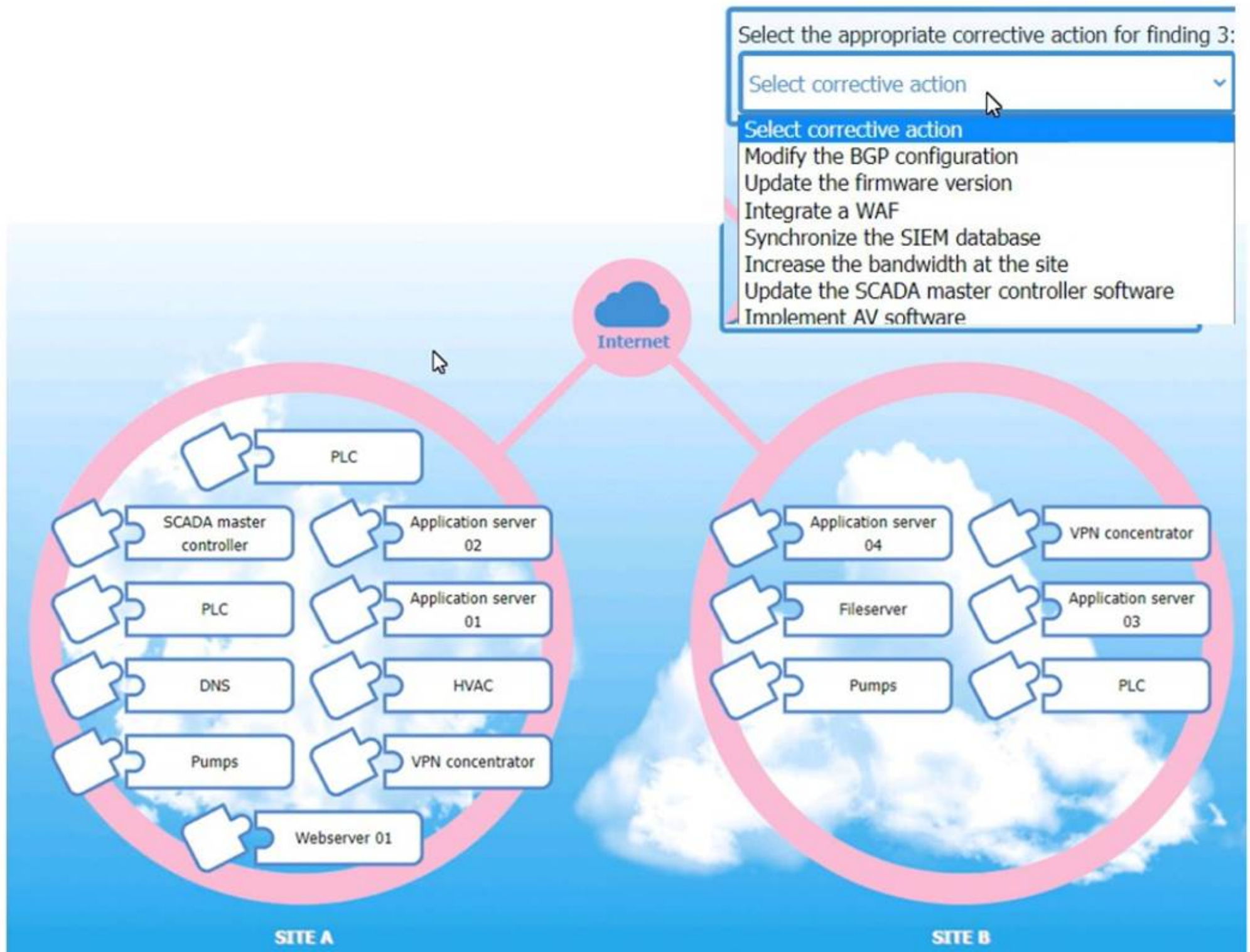
\* 3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.

**INSTRUCTIONS**

Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.

For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.





## Relevant findings



A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.

Select this for the item that should be replicated to Site B.



A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.

Select this for the item that should be replicated to Site B.



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

Select this for the item requiring configuration changes.

A. Mastered  
 B. Not Mastered

Answer: A

Explanation:



Matching Relevant Findings to the Affected Hosts:

? Finding 1:

? Finding 2:

? Finding 3:

Corrective Actions for Finding 3:

? Finding 3 Corrective Action:

? Replication to Site B for Finding 1:

? Replication to Site B for Finding 2:

? Configuration Changes for Finding 3:

References:

? CompTIA Security+ Study Guide: This guide provides detailed information on disaster recovery and continuity of operations, emphasizing the importance of replicating critical services and making necessary configuration changes to ensure seamless operation during disruptions.

? CompTIA Security+ Exam Objectives: These objectives highlight key areas in disaster recovery planning, including the replication of critical services and network configuration adjustments.

? Disaster Recovery and Business Continuity Planning (DRBCP): This resource outlines best practices for ensuring that operations can continue at an alternate site during a disaster, including the replication of essential services and network stability measures.

By ensuring that critical services like DNS and control systems for pumps are replicated at the alternate site, and by addressing network routing issues through proper BGP configuration, the organization can maintain operational continuity and minimize the impact of natural disasters on their operations.

#### NEW QUESTION 49

The material finding from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue? (Select two).

Setting different access controls defined by business area

A. Implementing a role-based access policy

B. Designing a least-needed privilege policy

C. Establishing a mandatory vacation policy

D. Performing periodic access reviews

E. Requiring periodic job rotation

**Answer:** AD

#### Explanation:

To mitigate the issue of excessive permissions and privilege creep, the best solutions are:

? Implementing a Role-Based Access Policy:

? Performing Periodic Access Reviews:

#### NEW QUESTION 54

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 57

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 61

### SIMULATION

A product development team has submitted code snippets for review prior to release. INSTRUCTIONS

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

Code Snippet 1

#### Code Snippet 1

#### Code Snippet 2

Web browser:

URL: <https://comptia.org/profiles/userdetails?userid=103>

Web server code:

```
--
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
--
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103

API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5', 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
    userId = request.getParam(userid)

    ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                  -h loginserver.comptia.org
                  -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
    accountLookup = subprocess.Popen(ldapLookup)

    if (userExists(accountLookup))
        accountFound = true
    else
        accountFound = false
    ...
```

Vulnerability 1:

- ? SQL injection
- ? Cross-site request forgery
- ? Server-side request forgery
- ? Indirect object reference
- ? Cross-site scripting

Fix 1:

- ? Perform input sanitization of the userid field.
- ? Perform output encoding of queryResponse,
- ? Ensure usex:ia belongs to logged-in user.
- ? Inspect URLs and disallow arbitrary requests.
- ? Implement anti-forgery tokens.

Vulnerability 2

- 1) Denial of service
- 2) Command injection
- 3) SQL injection

- 4) Authorization bypass  
5) Credentials passed via GET  
Fix 2  
A) Implement prepared statements and bind variables.  
B) Remove the serve\_forever instruction.  
C) Prevent the "authenticated" value from being overridden by a GET parameter.  
D) HTTP POST should be used for sensitive parameters.  
E) Perform input sanitization of the userid field.

- A. Mastered  
B. Not Mastered

**Answer: A**

**Explanation:**

Code Snippet 1

Vulnerability 1: SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

**NEW QUESTION 64**

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 69**

A software company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application Which of the following is the most likely cause of the alerts?

- A. Misconfigured code commit  
B. Unsecure bundled libraries  
C. Invalid code signing certificate  
D. Data leakage

**Answer: B**

**Explanation:**

The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.

Why Unsecure Bundled Libraries?

? Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.

? Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.

? Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.



Other options, while relevant, are less likely to cause widespread anti-malware alerts:

- ? A. Misconfigured code commit: Could lead to issues but less likely to trigger anti- malware alerts.
- ? C. Invalid code signing certificate: Would lead to trust issues but not typically anti- malware alerts.
- ? D. Data leakage: Relevant for privacy concerns but not directly related to anti- malware alerts.

References:

- ? CompTIA SecurityX Study Guide
- ? "Securing Open Source Libraries," OWASP
- ? "Managing Third-Party Software Security Risks," Gartner Research

### NEW QUESTION 73

A user reports application access issues to the help desk. The help desk reviews the logs for the user

| Time      | Internal IP | Public IP    | IP geolocation | Application            | Action |
|-----------|-------------|--------------|----------------|------------------------|--------|
| 8:47 p.m. | 192.168.1.5 | 104.18.16.29 | Toronto        | VPN                    | Allow  |
| 8:48 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Email                  | Allow  |
| 8:48 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Human resources system | Allow  |
| 8:49 p.m. | 10.10.2.21  | 95.67.137.12 | Los Angeles    | Email                  | Allow  |
| 8:52 p.m. | 192.168.1.5 | 104.18.16.29 | Toronto        | Human resources system | Deny   |

Which of the following is most likely The reason for the issue?

- A. The user inadvertently tripped the impossible travel security rule in the SSO system.
- B. A threat actor has compromised the user's account and attempted to log in.
- C. The user is not allowed to access the human resources system outside of business hours
- D. The user did not attempt to connect from an approved subnet

**Answer:** A

#### Explanation:

Based on the provided logs, the user has accessed various applications from different geographic locations within a very short timeframe. This pattern is indicative of the "impossible travel" security rule, a common feature in Single Sign-On (SSO) systems designed to detect and prevent fraudulent access attempts.

Analysis of Logs:

- ? At 8:47 p.m., the user accessed a VPN from Toronto.
- ? At 8:48 p.m., the user accessed email from Los Angeles.
- ? At 8:48 p.m., the user accessed the human resources system from Los Angeles.
- ? At 8:49 p.m., the user accessed email again from Los Angeles.
- ? At 8:52 p.m., the user attempted to access the human resources system from Toronto, which was denied.

These rapid changes in location are physically impossible and typically trigger security measures to prevent unauthorized access. The SSO system detected these inconsistencies and likely flagged the activity as suspicious, resulting in access denial. References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-63B, "Digital Identity Guidelines"
- ? "Impossible Travel Detection," Microsoft Documentation

### NEW QUESTION 74

After an incident response exercise, a security administrator reviews the following table:

| Service                 | Risk rating | Criticality rating | Alert severity |
|-------------------------|-------------|--------------------|----------------|
| Public website          | Medium      | Low                | Low            |
| Email                   | High        | High               | High           |
| Human resources systems | High        | Medium             | Medium         |
| Phone system            | High        | Critical           | Critical       |
| Intranet                | Low         | Low                | Low            |

Which of the following should the administrator do to best support rapid incident response in the future?

- A. Automate alerting to IT support for phone system outages.
- B. Enable dashboards for service status monitoring
- C. Send emails for failed log-in attempts on the public website

D. Configure automated Isolation of human resources systems

**Answer:** B

**Explanation:**

Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response, real-time visibility into the status of these services is crucial.

Why Dashboards for Service Status Monitoring?

? Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues.

? Centralized Monitoring: A single platform to monitor the status of multiple services helps streamline incident response efforts.

? Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise.

? Improved Decision Making: Real-time data helps incident response teams make informed decisions quickly, reducing downtime and mitigating impact.

Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:

? A. Automate alerting to IT support for phone system outages: This addresses one service but does not provide a holistic view.

? C. Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services.

? D. Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

? "Best Practices for Implementing Dashboards," Gartner Research

**NEW QUESTION 75**

A security review revealed that not all of the client proxy traffic is being captured. Which of the following architectural changes best enables the capture of traffic for analysis?

- A. Adding an additional proxy server to each segmented VLAN
- B. Setting up a reverse proxy for client logging at the gateway
- C. Configuring a span port on the perimeter firewall to ingest logs
- D. Enabling client device logging and system event auditing

**Answer:** C

**Explanation:**

Configuring a span port on the perimeter firewall to ingest logs is the best architectural change to ensure that all client proxy traffic is captured for analysis.

Here's why:

? Comprehensive Traffic Capture: A span port (or mirror port) on the perimeter firewall can capture all inbound and outbound traffic, including traffic that might bypass the proxy. This ensures that all network traffic is available for analysis.

? Centralized Logging: By capturing logs at the perimeter firewall, the organization can centralize logging and analysis, making it easier to detect and investigate anomalies.

? Minimal Disruption: Implementing a span port is a non-intrusive method that does not require significant changes to the network architecture, thus minimizing disruption to existing services.

? References:

**NEW QUESTION 80**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-005 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-005 Product From:

<https://www.2passeasy.com/dumps/CAS-005/>

## Money Back Guarantee

### 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