CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

NEW QUESTION 1
An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

A. SASE
B. CMDB
C. SBoM
D. SLM

Answer: B

Explanation:
A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets. References:
? CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.
? ITIL (Information Technology Infrastructure Library) Framework: Recommends the
use of CMDBs for effective configuration and asset management.
? "Configuration Management Best Practices" by Bob Aiello and Leslie Sachs: Covers the importance of CMDBs in managing IT assets and addressing vulnerabilities.

NEW QUESTION 2
The identity and access management team is sending logs to the SIEM for continuous monitoring. The deployed log collector is forwarding logs to the SIEM. However, only false positive alerts are being generated. Which of the following is the most likely reason for the inaccurate alerts?

A. The compute resources are insufficient to support the SIEM
B. The SIEM indexes are 100 large
C. The data is not being properly parsed
D. The retention policy is not property configured

Answer: C

Explanation:
Proper parsing of data is crucial for the SIEM to accurately interpret and analyze the logs being forwarded by the log collector. If the data is not parsed correctly, the SIEM may misinterpret the logs, leading to false positives and inaccurate alerts. Ensuring that the log data is correctly parsed allows the SIEM to correlate and analyze the logs effectively, which is essential for accurate alerting and monitoring.

NEW QUESTION 3
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

Answer: A

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

NEW QUESTION 4
Within a SCADA a business needs access to the historian server in order together metric about the functionality of the environment. Which of the following actions should be taken to address this requirement?

A. Isolating the historian server for connections only from The SCADA environment
B. Publishing the C$ share from SCADA to the enterprise
C. Deploying a screened subnet between 11 and SCADA
D. Adding the business workstations to the SCADA domain

Answer: A

Explanation:
The best action to address the requirement of accessing the historian server within a SCADA system is to isolate the historian server for connections only from the

SCADA environment. Here??s why:
? Security and Isolation: Isolating the historian server ensures that only authorized
devices within the SCADA environment can connect to it. This minimizes the attack surface and protects sensitive data from unauthorized access.
? Access Control: By restricting access to the historian server to only SCADA
devices, the organization can better control and monitor interactions, ensuring that only legitimate queries and data retrievals occur.
? Best Practices for Critical Infrastructure: Following the principle of least privilege,
isolating critical components like the historian server is a standard practice in securing SCADA systems, reducing the risk of cyberattacks.
? References:

NEW QUESTION 5
A global manufacturing company has an internal application mat is critical to making products This application cannot be updated and must Be available in the production area A security architect is implementing security for the application. Which of the following best describes the action the architect should take-?

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

Answer: D

Explanation:
Creating a separate network for users who need access to the application is the best action to secure an internal application that is critical to the production area and cannot be updated.
Why Separate Network?
? Network Segmentation: Isolates the critical application from the rest of the network, reducing the risk of compromise and limiting the potential impact of any security incidents.
? Controlled Access: Ensures that only authorized users have access to the application, enhancing security and reducing the attack surface.
? Minimized Risk: Segmentation helps in protecting the application from vulnerabilities that could be exploited from other parts of the network.
Other options, while beneficial, do not provide the same level of security for a critical application:
? A. Disallow wireless access: Useful but does not provide comprehensive protection.
? B. Deploy intrusion detection capabilities using a network tap: Enhances monitoring but does not provide the same level of isolation and control.
? C. Create an acceptable use policy: Important for governance but does not provide technical security controls.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-125, "Guide to Security for Full Virtualization Technologies"
? "Network Segmentation Best Practices," Cisco Documentation

NEW QUESTION 6
A security officer received several complaints from users about excessive MPA push notifications at night The security team investigates and suspects malicious activities regarding user account authentication Which of the following is the best way for the security officer to restrict MI~A notifications"

A. Provisioning FID02 devices
B. Deploying a text message based on MFA
C. Enabling OTP via email
D. Configuring prompt-driven MFA

Answer: D

Explanation:
Excessive MFA push notifications can be a sign of an attempted push notification attack, where attackers repeatedly send MFA prompts hoping the user will eventually approve one by mistake. To mitigate this:
? A. Provisioning FIDO2 devices: While FIDO2 devices offer strong authentication,
they may not be practical for all users and do not directly address the issue of excessive push notifications.
? B. Deploying a text message-based MFA: SMS-based MFA can still be vulnerable
to similar spamming attacks and phishing.
? C. Enabling OTP via email: Email-based OTPs add another layer of security but do not directly solve the issue of excessive notifications.
? D. Configuring prompt-driven MFA: This option allows users to respond to prompts in a secure manner, often including features like time-limited approval windows, additional verification steps, or requiring specific actions to approve. This can help prevent users from accidentally approving malicious attempts.
Configuring prompt-driven MFA is the best solution to restrict unnecessary MFA notifications and improve security.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-63B, "Digital Identity Guidelines"
? "Multi-Factor Authentication: Best Practices" by Microsoft

NEW QUESTION 7
A security engineer is developing a solution to meet the following requirements?
• All endpoints should be able to establish telemetry with a SIEM.
• All endpoints should be able to be integrated into the XDR platform.
• SOC services should be able to monitor the XDR platform
Which of the following should the security engineer implement to meet the requirements?

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

Answer: D

Explanation:
To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR

platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host- based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.
References:
? CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.
? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.
? "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

NEW QUESTION 8
A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems. Which of the following should the security engineer modify?

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

Answer: D

Explanation:
The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.
By editing the /etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the
SSH server does not use insecure encryption methods.
References:
? CompTIA Security+ Study Guide
? OpenSSH manual pages (man sshd_config)
? CIS Benchmarks for Linux

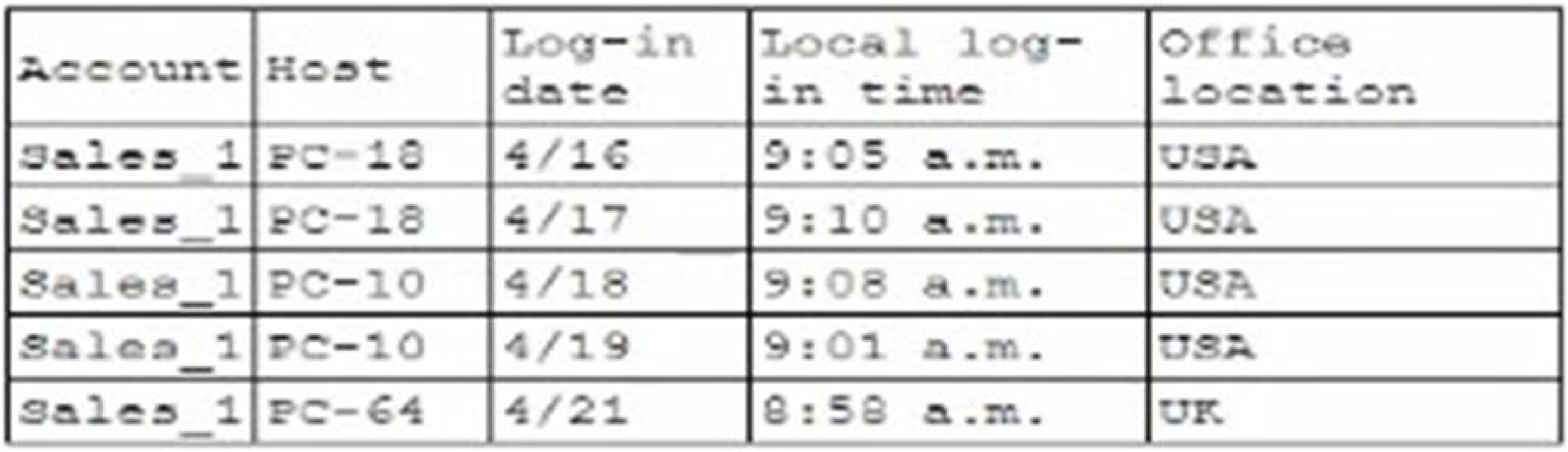
NEW QUESTION 9
An audit finding reveals that a legacy platform has not retained loos for more than 30 days The platform has been segmented due to its interoperability with newer technology. As a temporary solution, the IT department changed the log retention to 120 days. Which of the following should 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.

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
Which of the following is the security engineer most likely doing?



Account	Host	Log-in date	Local log-in time	Office location
Sales_1	PC-18	4/16	9:05 a.m.	USA
Sales_1	PC-18	4/17	9:10 a.m.	USA
Sales_1	PC-10	4/18	9:08 a.m.	USA
Sales_1	PC-10	4/19	9:01 a.m.	USA
Sales_1	PC-64	4/21	8:58 a.m.	UK

A. Assessing log in activities using geolocation to tune impossible Travel rate alerts
B. Reporting on remote log-in activities to track team metrics
C. Threat hunting for suspicious activity from an insider threat
D. Baselining user behavior to support advanced analytics

Answer: A

Explanation:
In the given scenario, the security engineer is likely examining login activities and their associated geolocations. This type of analysis is aimed at identifying unusual login patterns that might indicate an impossible travel scenario. An impossible travel scenario is when a single user account logs in from geographically distant locations in a short time, which is physically impossible. By assessing login activities using geolocation, the engineer can tune alerts to identify and respond to potential security breaches more effectively.

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 11
Which of the following AI concerns is most adequately addressed by input sanitation?

A. Model inversion
B. Prompt Injection
C. Data poisoning
D. Non-explainable model

Answer: B

Explanation:
Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:
? A. Model inversion involves an attacker inferring sensitive data from model
outputs, typically requiring sophisticated methods beyond just manipulating input data.
? B. Prompt Injection is a form of attack where an adversary provides malicious input
to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.
? C. Data poisoning involves injecting malicious data into the training set to
compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.
? D. Non-explainable model refers to the lack of transparency in how AI models
make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.
Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.
References:
? CompTIA Security+ Study Guide
? "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov
? OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks
Top of Form Bottom of Form

NEW QUESTION 14
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

Answer: C

Explanation:
Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?
? Continuous Security Assessment: Regular DAST scans help in identifying
vulnerabilities in real-time, ensuring they are addressed promptly.
? Compliance: Routine scans ensure that the development process complies with security standards and regulations.
? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.

? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.
Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:
? A. If developers are unable to promote to production: This is more of an
operational issue than a security assessment.
? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.
? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.
References:
? CompTIA SecurityX Study Guide
? OWASP Testing Guide
? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

NEW QUESTION 19
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

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 22
An organization wants to create a threat model to identity vulnerabilities in its infrastructure. Which of the following, should be prioritized first?

A. External-facing Infrastructure with known exploited vulnerabilities
B. Internal infrastructure with high-seventy and Known exploited vulnerabilities
C. External facing Infrastructure with a low risk score and no known exploited vulnerabilities
D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource

Answer: A

Explanation:
When creating a threat model to identify vulnerabilities in an organization's infrastructure, prioritizing external-facing infrastructure with known exploited vulnerabilities is critical. Here??s why:
? Exposure to Attack: External-facing infrastructure is directly exposed to the
internet, making it a primary target for attackers. Any vulnerabilities in this layer pose an immediate risk to the organization's security.
? Known Exploited Vulnerabilities: Vulnerabilities that are already known and
exploited in the wild are of higher concern because they are actively being used by attackers. Addressing these vulnerabilities reduces the risk of exploitation significantly.
? Risk Mitigation: By prioritizing external-facing infrastructure with known exploited
vulnerabilities, the organization can mitigate the most immediate and impactful threats, thereby improving overall security posture.
? References:

NEW QUESTION 26
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 last 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 29
Audit findings indicate several user endpoints are not utilizing full disk encryption During me remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption Which of the following is the most likely reason me device must be replaced'

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

Answer: D

Explanation:
The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.
Why TPM is Necessary for Full Disk Encryption:
? Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.
? Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.
? Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.
Other options do not directly address the requirement for TPM in supporting full disk encryption:
? A. The HSM is outdated: While HSM (Hardware Security Module) is important for
security, it is not typically used for full disk encryption.
? B. The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.
? C. The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.
? E. The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.
References:
? CompTIA SecurityX Study Guide
? "Trusted Platform Module (TPM) Overview," Microsoft Documentation
? "BitLocker Deployment Guide," Microsoft Documentation

NEW QUESTION 32
A company wants to install a three-tier approach to separate the web. database, and application servers A security administrator must harden the environment which of the following is the best solution?

A. Deploying a VPN to prevent remote locations from accessing server VLANs
B. Configuring a SASb solution to restrict users to server communication
C. Implementing microsegmentation on the server VLANs
D. installing a firewall and making it the network core

Answer: C

Explanation:
The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here??s why:
? Enhanced Security: Microsegmentation creates granular security zones within the
data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.
? Isolation of Tiers: By segmenting the web, database, and application servers, the
organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.
? Compliance and Best Practices: Microsegmentation aligns with best practices for
network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.
? References:

NEW QUESTION 34
A financial services organization is using Al lo 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"

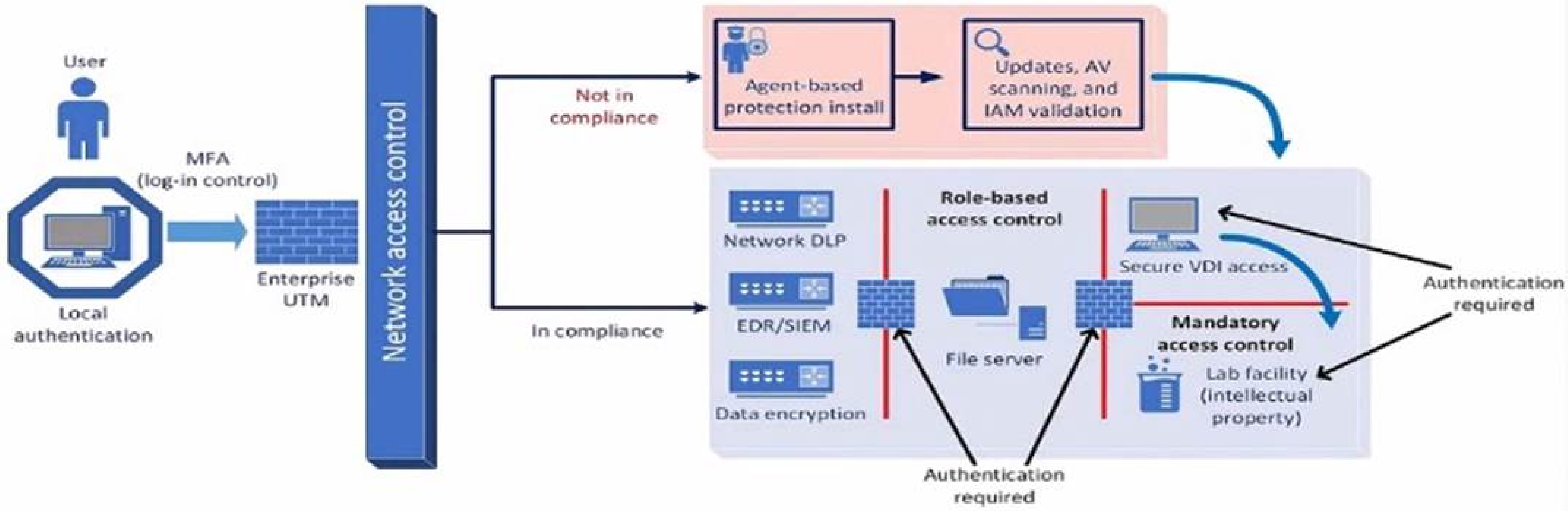
NEW QUESTION 37
A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

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

Answer: C

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

NEW QUESTION 41
A company plans to implement a research facility with Intellectual property data that should be protected The following is the security diagram proposed by the security architect



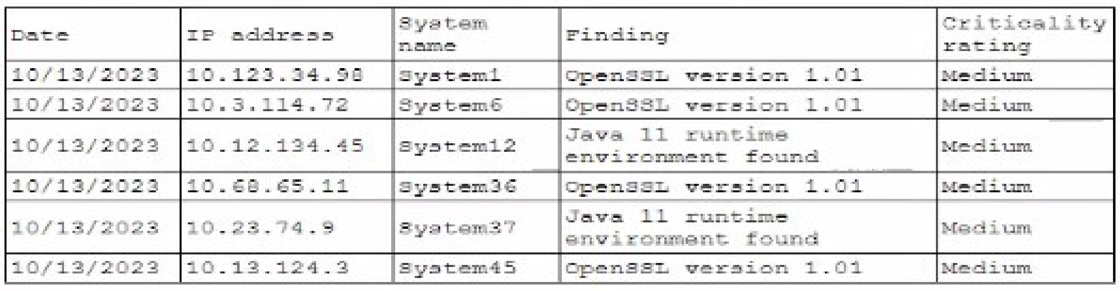
Which of the following security architect models is illustrated by the diagram?

A. Identity and access management model
B. Agent based security model
C. Perimeter protection security model
D. Zero Trust security model

Answer: D

Explanation:
The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.
Key Characteristics of Zero Trust in the Diagram:
? Role-based Access Control: Ensures that users have access only to the resources necessary for their role.
? Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.
? Network Access Control: Ensures that devices meet security standards before accessing the network.
? Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.
This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-207, "Zero Trust Architecture"
? "Implementing a Zero Trust Architecture," Forrester Research

NEW QUESTION 44
A security professional is investigating a trend in vulnerability findings for newly deployed cloud systems Given the following output:



Date	IP address	System name	Finding	Criticality rating
10/13/2023	10.123.34.98	System1	OpenSSL version 1.01	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.01	Medium
10/13/2023	10.12.134.45	System12	Java 11 runtime environment found	Medium
10/13/2023	10.68.65.11	System36	OpenSSL version 1.01	Medium
10/13/2023	10.23.74.9	System37	Java 11 runtime environment found	Medium
10/13/2023	10.13.124.3	System45	OpenSSL version 1.01	Medium

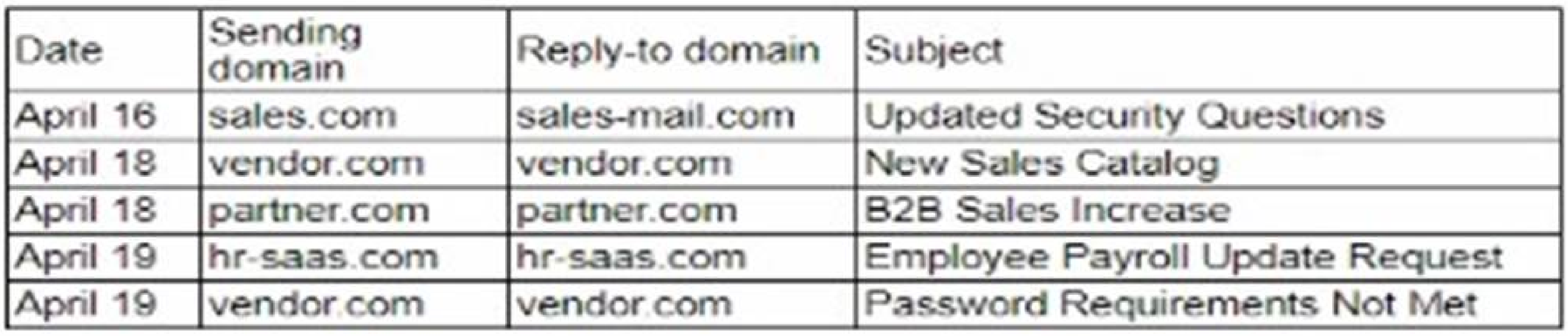
Which of the following actions would address the root cause of this issue?

A. Automating the patching system to update base Images
B. Recompiling the affected programs with the most current patches
C. Disabling unused/unneeded ports on all servers
D. Deploying a WAF with virtual patching upstream of the affected systems

Answer: A

Explanation:
The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.
? A. Automating the patching system to update base images: Automating the
patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.
? B. Recompiling the affected programs with the most current patches: While this
can fix the immediate vulnerabilities, it does not address the root cause of the problem, which is the lack of regular updates.
? C. Disabling unused/unneeded ports on all servers: This improves security but does not address the specific issue of outdated software.
? D. Deploying a WAF with virtual patching upstream of the affected systems: This can provide a temporary shield but does not resolve the underlying issue of outdated software.
Automating the patching system to update base images ensures that all deployed systems are using the latest, most secure versions of software, addressing the root cause of the vulnerability trend.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-40 Rev. 3, "Guide to Enterprise Patch Management Technologies"
? CIS Controls, "Control 7: Continuous Vulnerability Management"

NEW QUESTION 48
A security analyst needs to ensure email domains that send phishing attempts without previous communications are not delivered to mailboxes The following email headers are being reviewed



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

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

A. Block messages from hr-saas.com because it is not a recognized domain.
B. Reroute all messages with unusual security warning notices to the IT administrator
C. Quarantine all messages with sales-mail.com in the email header
D. Block vendor com for repeated attempts to send suspicious messages

Answer: D

Explanation:
In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here??s the analysis of the options provided:
* A. Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.
* B. Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.
* C. Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.
* D. Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.
References:
? CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.
? NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.
? "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.

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

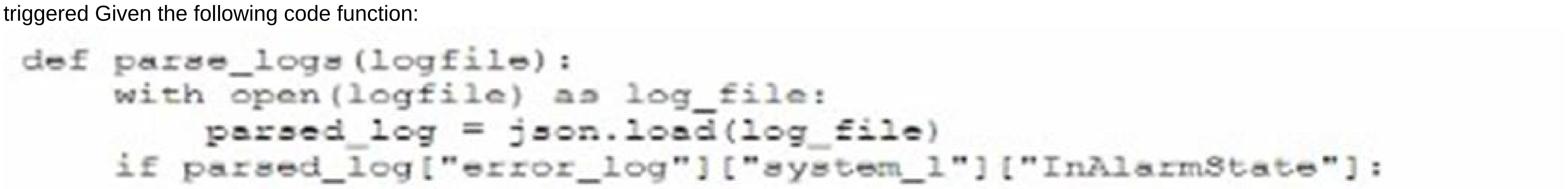
NEW QUESTION 49
After an incident occurred, a team reported during the lessons-learned review that the team.
* Lost important Information for further analysis.
* Did not utilize the chain of communication
* Did not follow the right steps for a proper response
Which of the following solutions is the best way to address these findinds?

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

Answer: B

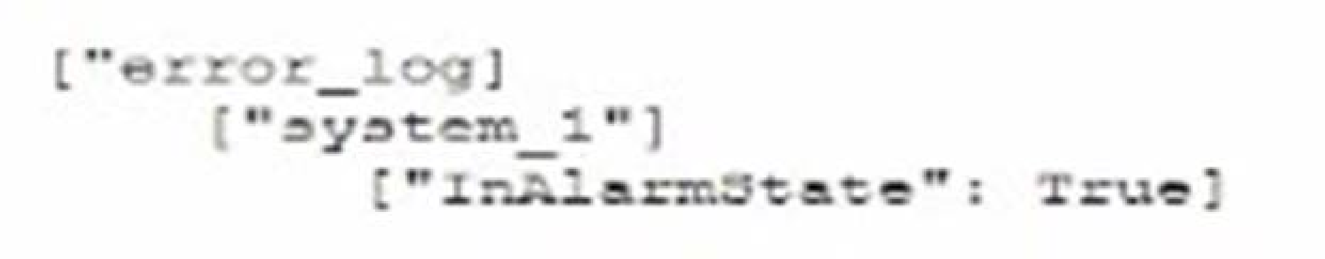
Explanation:
Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:
? Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.
? Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.
? Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.
Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
? SANS Institute, "Incident Handler's Handbook"

NEW QUESTION 53
A security administrator needs to automate alerting. The server generates structured log files that need to be parsed to determine whether an alarm has been triggered Given the following code function:



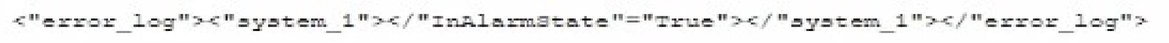
```
def parse_logs(logfile):
    with open(logfile) as log_file:
        parsed_log = json.load(log_file)
    if parsed_log["error_log"]["system_1"]["InAlarmState"]:
```

Which of the following is most likely the log input that the code will parse?
A)



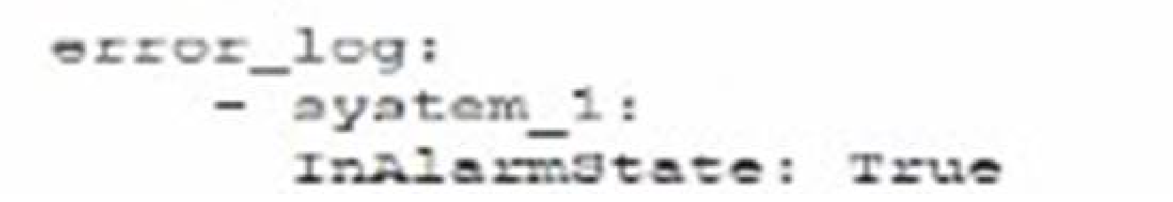
```
["error_log]
    ["system_1"]
        ["InAlarmState": True]
```

B)



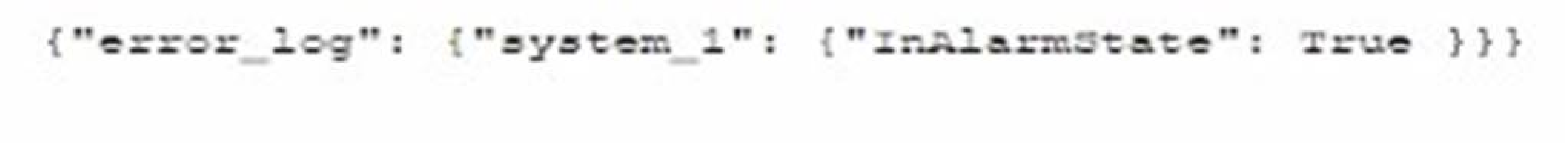
```
<"error_log"><"system_1"></"InAlarmState"="True"></"system_1"></"error_log">
```

C)



```
error_log:
    - system_1:
      InAlarmState: True
```

D)



```
{"error_log": {"system_1": {"InAlarmState": True }}}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:
The code function provided in the question seems to be designed to parse JSON formatted logs to check for an alarm state. Option A is a JSON format that

matches the structure likely expected by the code. The presence of the "error_log" and "InAlarmState" keys suggests that this is the correct input format.
Reference: CompTIA SecurityX Study Guide, Chapter on Log Management and Automation, Section on Parsing Structured Logs.

NEW QUESTION 57
After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.
• Exfiltration of intellectual property
• Unencrypted files
• Weak user passwords
Which of the following is the best way to mitigate these vulnerabilities? (Select two).

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

Answer: AE

Explanation:
To mitigate the identified vulnerabilities, the following solutions are most appropriate:
? A. Implementing data loss prevention (DLP): DLP solutions help prevent the
unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.
? E. Enabling modern authentication that supports Multi-Factor Authentication
(MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.
Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:
? B. Deploying file integrity monitoring helps detect changes to files but does not
prevent data exfiltration or address weak passwords.
? C. Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.
? D. Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.
? F. Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.
? G. Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"
? CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

NEW QUESTION 60
A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions. The architect discovers that the acquired companies use different vendors for detection and monitoring The architect's goal is to:
• Create a collection of use cases to help detect known threats
• Include those use cases in a centralized library for use across all of the companies Which of the following is the best way to achieve this goal?

A. Sigma rules
B. Ariel Query Language
C. UBA rules and use cases
D. TAXII/STIX library

Answer: A

Explanation:
To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option. Here??s why:
? Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing
SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.
? Centralized Rule Management: By using Sigma rules, the cybersecurity architect
can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.
? Ease of Use and Flexibility: Sigma provides a structured and straightforward
format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

NEW QUESTION 65
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 67
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 69
A software engineer is creating a CI/CD pipeline to support the development of a web application The DevSecOps team is required to identify syntax errors Which of the following is the most relevant to the DevSecOps team's task'

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

Answer: A

Explanation:
Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.
? A. Static application security testing (SAST): SAST tools analyze the source code
to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.
? B. Software composition analysis: This focuses on identifying vulnerabilities in
open-source components and libraries used in the application but does not address syntax errors directly.
? C. Runtime application self-protection (RASP): RASP involves monitoring and
protecting applications during runtime, which does not help in identifying syntax errors during the development phase.
? D. Web application vulnerability scanning: This involves scanning the running
application for vulnerabilities but does not address syntax errors in the code.
References:
? CompTIA Security+ Study Guide
? OWASP (Open Web Application Security Project) guidelines on SAST
? NIST SP 800-95, "Guide to Secure Web Services" Top of Form
Bottom of Form

NEW QUESTION 74
During a gap assessment, an organization notes that OYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following
solutions should the organization implement to b»« reduce the risk of OYOD devices? (Select two).

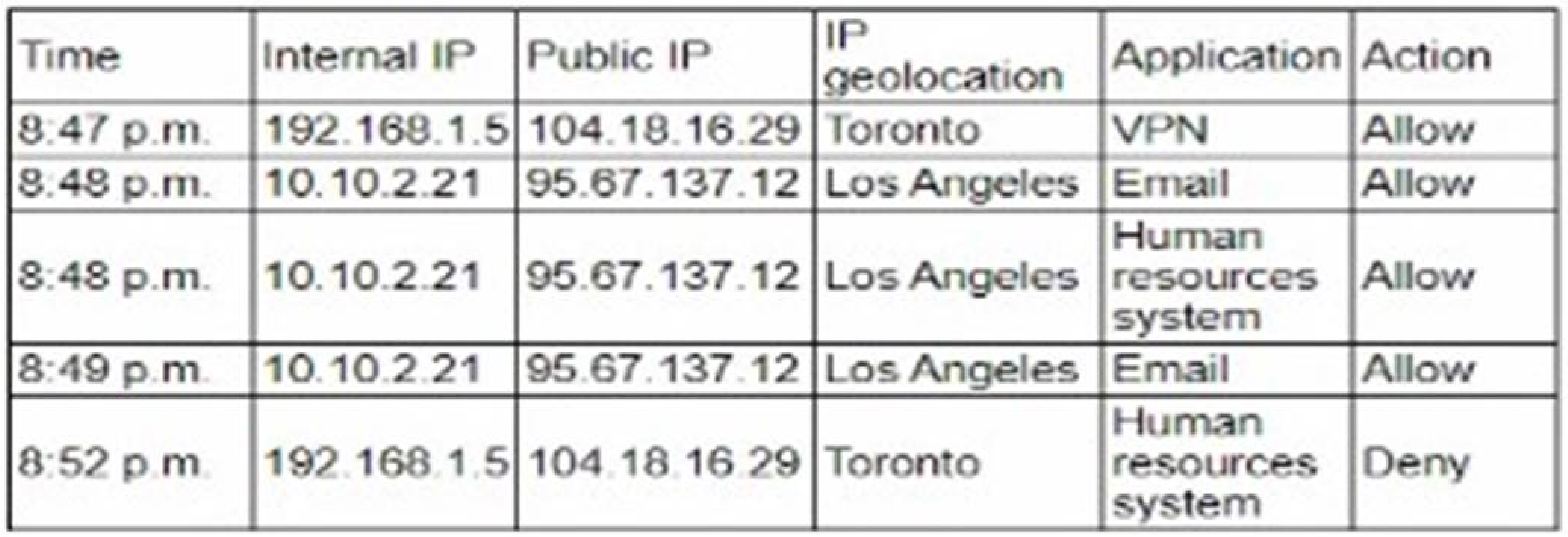
A. Cloud 1AM to enforce the use of token based MFA
B. Conditional access, to enforce user-to-device binding
C. NAC, to enforce device configuration requirements
D. PA
E. to enforce local password policies
F. SD-WA
G. to enforce web content filtering through external proxies
H. DLP, to enforce data protection capabilities

Answer: BC

Explanation:
To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC). Why Conditional Access and NAC?
? Conditional Access:
? Network Access Control (NAC):
Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:
? A. Cloud IAM to enforce token-based MFA: Enhances authentication security but

does not control device compliance.
? D. PAM to enforce local password policies: Focuses on privileged account management, not BYOD control.
? E. SD-WAN to enforce web content filtering: Enhances network performance and security but does not enforce BYOD device compliance.
? F. DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.
References:
? CompTIA SecurityX Study Guide
? "Conditional Access Policies," Microsoft Documentation
? "Network Access Control (NAC)," Cisco Documentation

NEW QUESTION 75
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 lop, m
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 76
A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved lo the repository The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).

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

Answer: BD

Explanation:
? B. Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.
? D. Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.
Other options:
? A. Software composition analysis: This helps identify vulnerabilities in third-party components but does not directly address code quality or deployment failures.
? C. Repository branch protection: While this can help manage the code submission process, it does not directly prevent deployment failures caused by code issues or security check failures.
? E. Code submit authorization workflow: This manages who can submit code but does not address the quality of the code being submitted.

? F. Pipeline compliance scanning: This checks for compliance with security policies but does not address syntax or regression issues.
References:
? CompTIA Security+ Study Guide
? "Continuous Integration and Continuous Delivery" by Jez Humble and David Farley
? OWASP (Open Web Application Security Project) guidelines on secure coding practices

NEW QUESTION 81
A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise. Which of the following is the most secure way to achieve this goal?

A. Executing a script that deletes and overwrites all data on the SSD three times
B. Wiping the SSD through degaussing
C. Securely deleting the encryption keys used by the SSD
D. Writing non-zero, random data to all cells of the SSD

Answer: C

Explanation:
The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.
References:
? CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data.
? NIST Special Publication 800-88, "Guidelines for Media Sanitization": Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

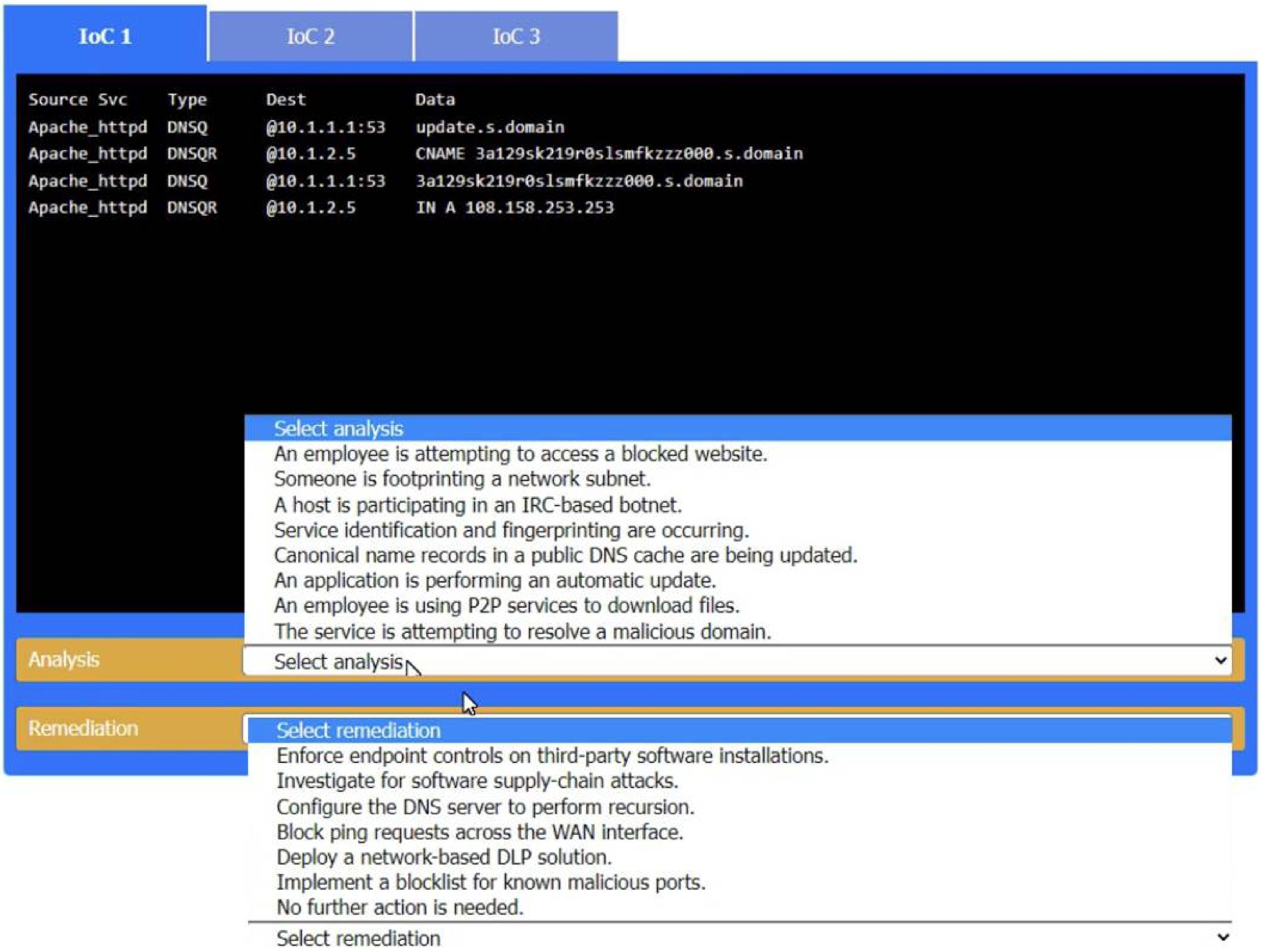
NEW QUESTION 84
While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?

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

Answer: A

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

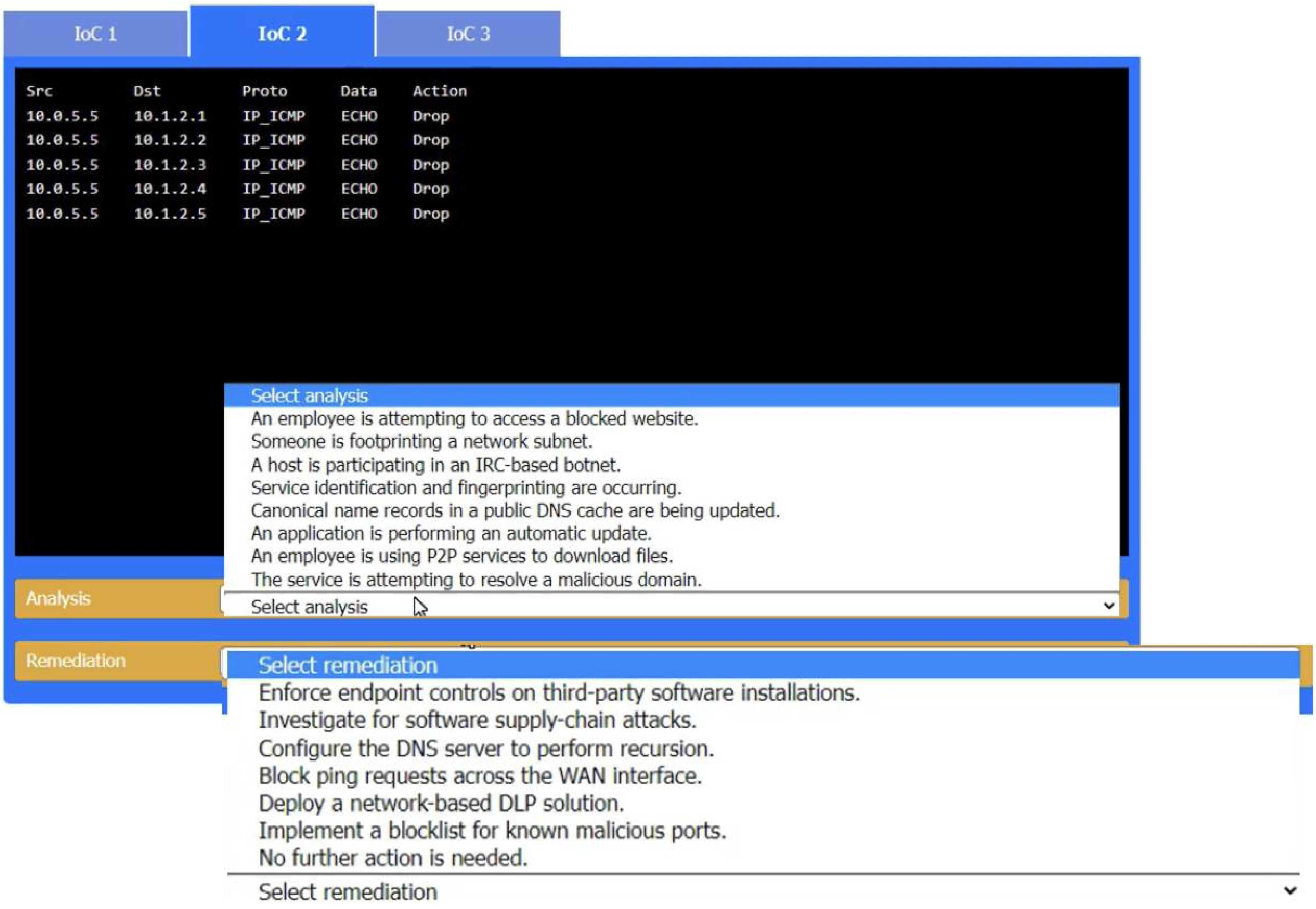
NEW QUESTION 87
SIMULATION
During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.
INSTRUCTIONS
Review each of the events and select the appropriate analysis and remediation options for each IoC.



```
Source Svc    Type     Dest          Data
Apache_httpd  DNSQ     @10.1.1.1:53  update.s.domain
Apache_httpd  DNSQR    @10.1.2.5     CNAME 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd  DNSQ     @10.1.1.1:53  3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd  DNSQR    @10.1.2.5     IN A 108.158.253.253
```

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

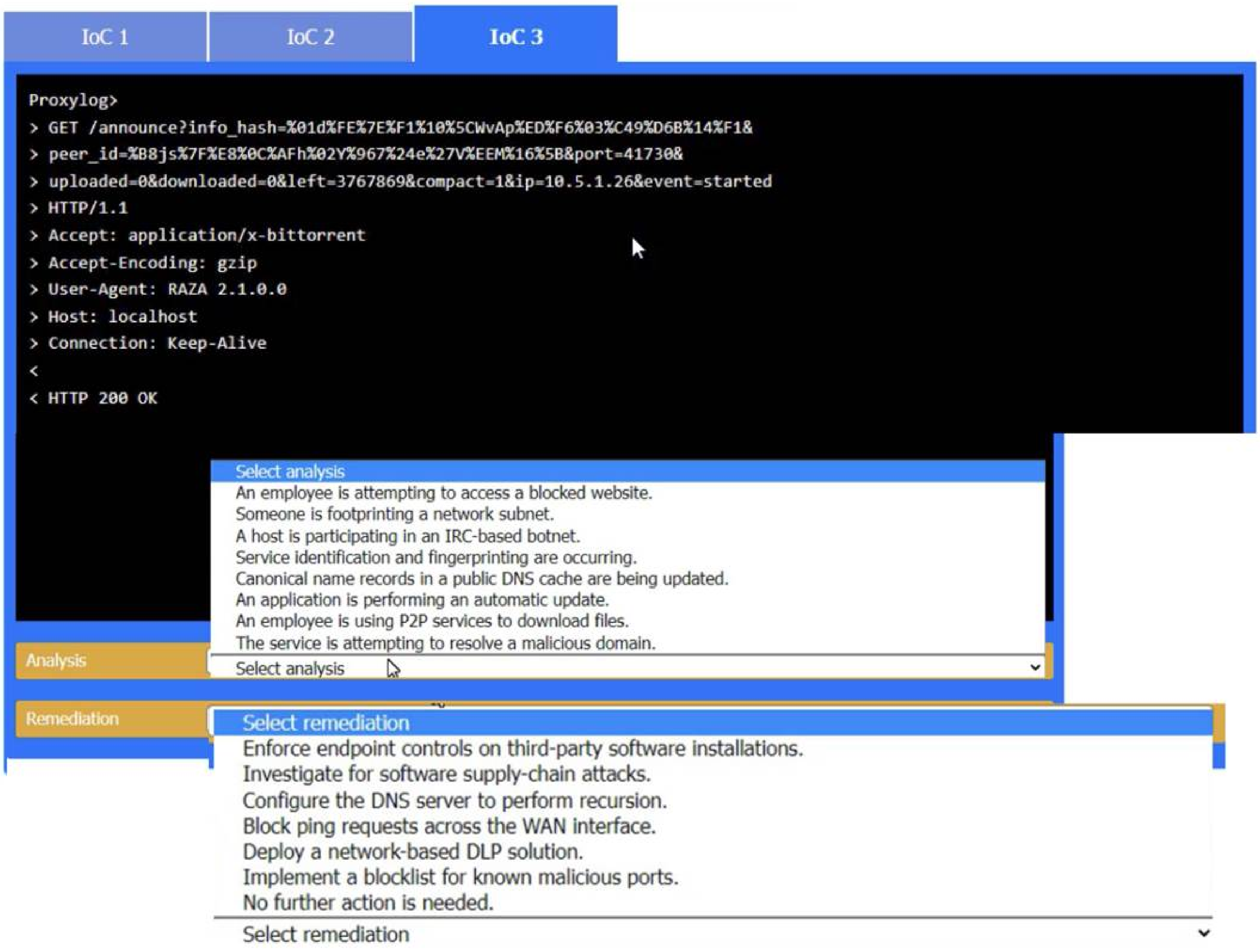
Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious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



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

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

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



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

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

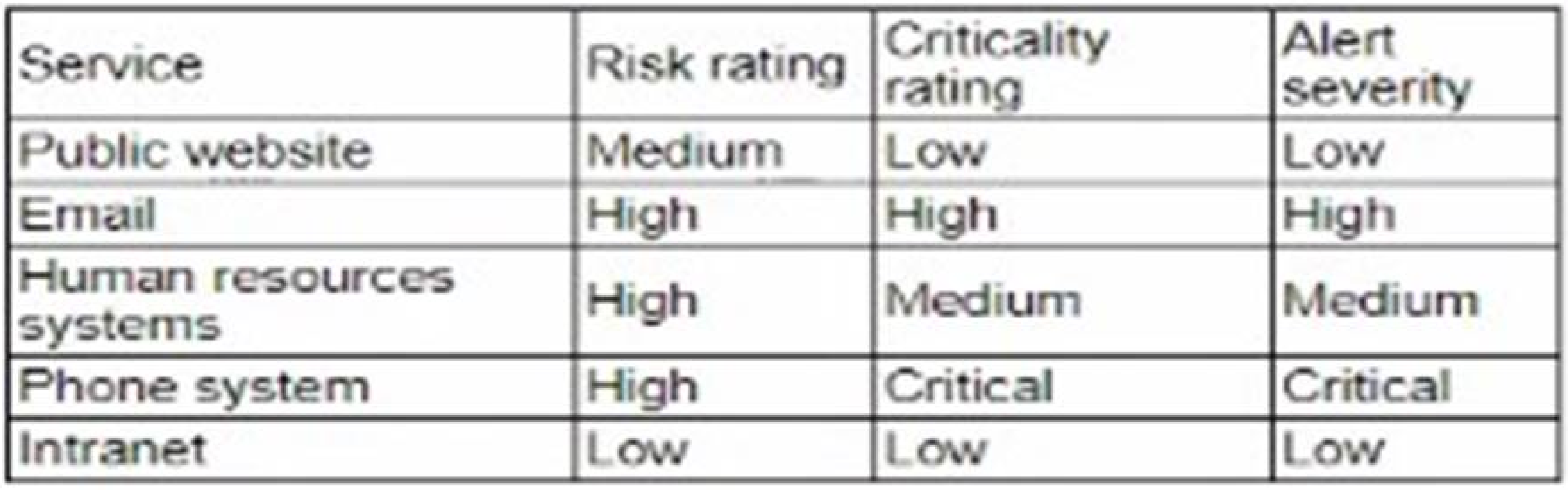
Select remediation
Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Analysis and Remediation Options for Each IoC: IoC 1:
? Evidence:
? Analysis:
? Remediation:
IoC 2:
? Evidence:
? Analysis:
? Remediation:
IoC 3:
? Evidence:
? Analysis:
? Remediation:
References:
? CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.
? CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.
? Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration
changes.
By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

NEW QUESTION 91
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

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 93
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 96
......