CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

NEW QUESTION 1
A company's help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:

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

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

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

Answer: C

Explanation:
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.
In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.
? Recursive DNS resolution failure (A) would generally lead to inability to resolve
DNS at all, not to a specific HTTP error.
? DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.
? Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.
By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.
References:
? CompTIA SecurityX study materials on DNS security mechanisms.
? Standard HTTP status codes and their implications.

NEW QUESTION 2
Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

A. Securing data transfer between hospitals
B. Providing for non-repudiation data
C. Reducing liability from identity theft
D. Protecting privacy while supporting portability.

Answer: D

Explanation:
Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised. Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.
? HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.
? "Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

NEW QUESTION 3
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 4
A developer needs to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module. Which of the following is the most appropriate technique?

A. Key splitting
B. Key escrow
C. Key rotation
D. Key encryption
E. Key stretching

Answer: E

Explanation:
The most appropriate technique to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto- module is key stretching. Here's why:
? Enhanced Security: Key stretching algorithms, such as PBKDF2, bcrypt, and scrypt, increase the computational effort required to derive the encryption key from the password, making brute-force attacks more difficult and time-consuming.
? Compatibility: Key stretching can be implemented alongside existing cryptographic modules, enhancing their security without the need for a complete overhaul.
? Industry Best Practices: Key stretching is a widely recommended practice for securely storing passwords, as it significantly improves resistance to password-cracking attacks.
? References:

NEW QUESTION 5
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 6
Users must accept the terms presented in a captive petal when connecting to a guest network. Recently, users have reported that they are unable to access the Internet after joining the network A network engineer observes the following:
• Users should be redirected to the captive portal.
• The Motive portal runs Tl. S 1 2
• Newer browser versions encounter security errors that cannot be bypassed
• Certain websites cause unexpected re directs
Which of the following mow likely explains this behavior?

A. The TLS ciphers supported by the captive portal ate deprecated
B. Employment of the HSTS setting is proliferating rapidly.
C. Allowed traffic rules are causing the NIPS to drop legitimate traffic
D. An attacker is redirecting supplicants to an evil twin WLAN.

Answer: A

Explanation:
The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here??s why:
? TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.
? HSTS and Browser Security: Browsers with HTTP Strict Transport Security
(HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.
? References:
By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

NEW QUESTION 7
A security officer received several complaints from users about excessive MPA push notifications at night The security team investigates and suspects malicious

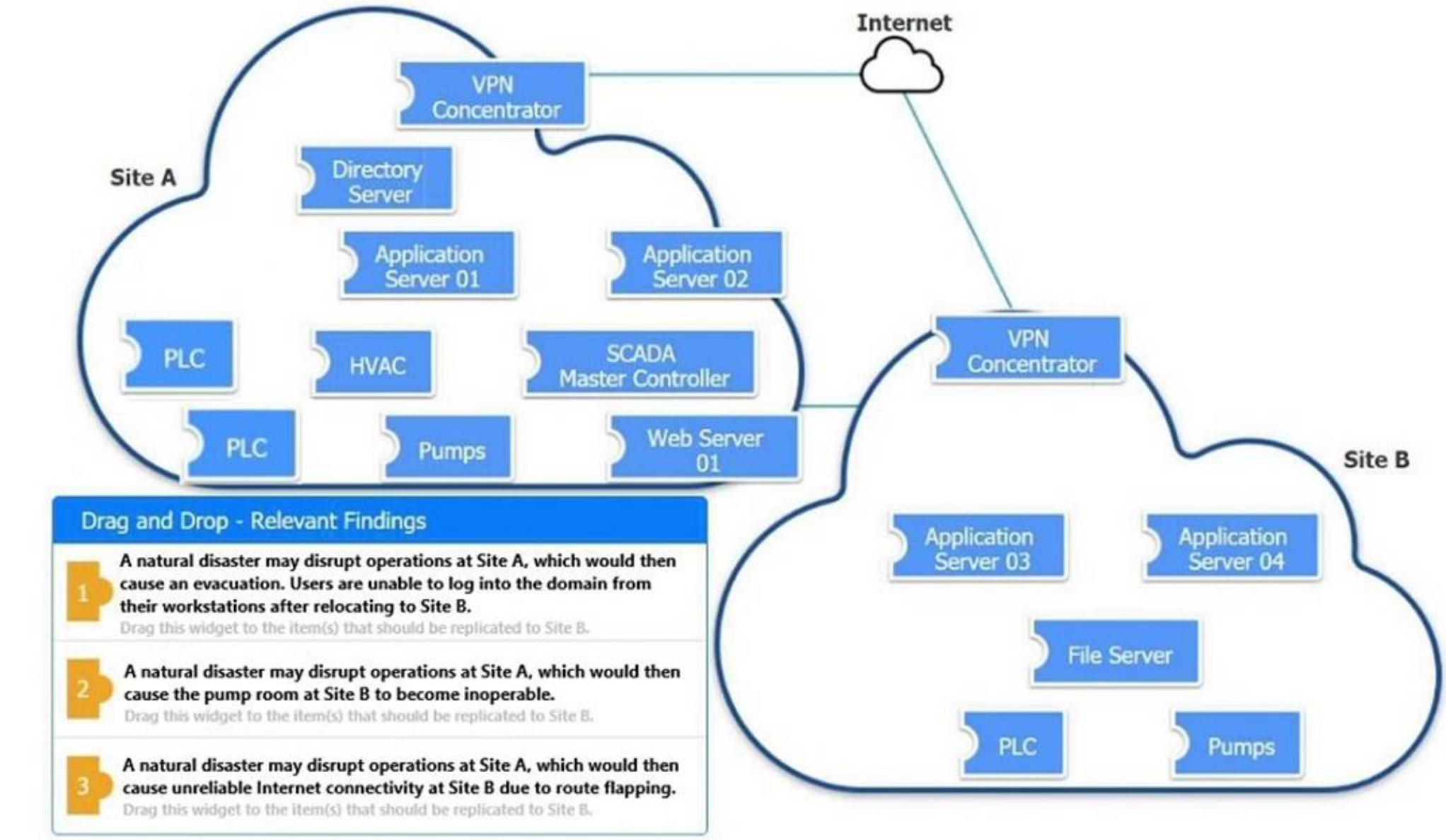
activities regarding user account authentication Which of the following is the best way for the security officer to restrict MI~A notifications"

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

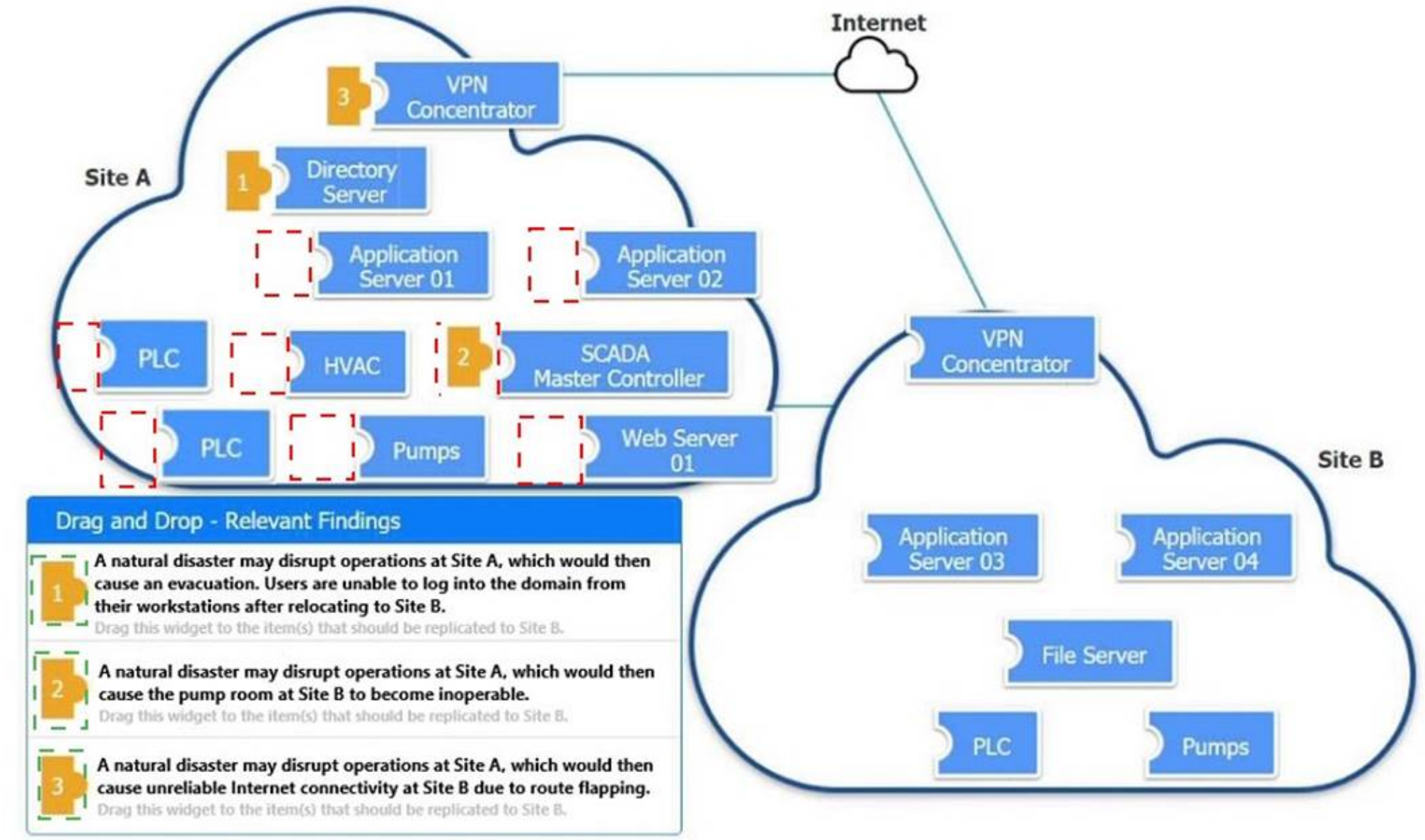
Answer: D

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 8
DRAG DROP
An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS



Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.
Each finding may be used more than once.
If at any time you would like to bring back the initial state of the simul-ation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 9
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
A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

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

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

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

Answer: B

Explanation:
The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website's performance.
? A. IDS (Intrusion Detection System): While an IDS is useful for detecting malicious
activities, it does not address performance issues related to latency and geographical distribution of content.
? B. CDN (Content Delivery Network): A CDN stores copies of the website's content
in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.
? C. WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.
? D. NAC (Network Access Control): NAC solutions control access to network
resources but are not designed to address web performance issues.
Implementing a CDN is the best solution to resolve the performance issues observed in the log output.
References:
? CompTIA Security+ Study Guide
? "CDN: Content Delivery Networks Explained" by Akamai Technologies
? NIST SP 800-44, "Guidelines on Securing Public Web Servers"

NEW QUESTION 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 12
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 17
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

Answer: C

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.
References:
? CompTIA Security+ Study Guide
? GDPR and other global data protection regulations
? "Data Sovereignty: The Future of Data Protection?" by Mark Burdon

NEW QUESTION 20
A company hosts a platform-as-a-service solution with a web-based front end, through which customer interact with data sets. A security administrator needs to

deploy controls to prevent application-focused attacks. Which of the following most directly supports the administrator's objective'

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

Answer: D

Explanation:
The best way to prevent application-focused attacks for a platform-as-a- service solution with a web-based front end is to create Web Application Firewall (WAF) policies for relevant programming languages. Here's why:
? Application-Focused Attack Prevention: WAFs are designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. They help prevent attacks such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.
? Customizable Rules: WAF policies can be tailored to the specific programming languages and frameworks used by the web application, providing targeted protection based on known vulnerabilities and attack patterns.
? Real-Time Protection: WAFs provide real-time protection, blocking malicious requests before they reach the application, thereby enhancing the security posture of the platform.
? References:

NEW QUESTION 21
A company receives reports about misconfigurations and vulnerabilities in a third-party hardware device that is part of its released products. Which of the following solutions is the best way for the company to identify possible issues at an earlier stage?

A. Performing vulnerability tests on each device delivered by the providers
B. Performing regular red-team exercises on the vendor production line
C. Implementing a monitoring process for the integration between the application and the vendor appliance
D. Implementing a proper supply chain risk management program

Answer: D

Explanation:
Addressing misconfigurations and vulnerabilities in third-party hardware requires a comprehensive approach to manage risks throughout the supply chain. Implementing a proper supply chain risk management (SCRM) program is the most effective solution as it encompasses the following:
? Holistic Approach: SCRM considers the entire lifecycle of the product, from initial design through to delivery and deployment. This ensures that risks are identified and managed at every stage.
? Vendor Management: It includes thorough vetting of suppliers and ongoing assessments of their security practices, which can identify and mitigate vulnerabilities early.
? Regular Audits and Assessments: A robust SCRM program involves regular audits and assessments, both internally and with suppliers, to ensure compliance with security standards and best practices.
? Collaboration and Communication: Ensures that there is effective communication and collaboration between the company and its suppliers, leading to faster identification and resolution of issues.
Other options, while beneficial, do not provide the same comprehensive risk management:
? A. Performing vulnerability tests on each device delivered by the providers: While useful, this is reactive and only addresses issues after they have been delivered.
? B. Performing regular red-team exercises on the vendor production line: This can identify vulnerabilities but is not as comprehensive as a full SCRM program.
? C. Implementing a monitoring process for the integration between the application and the vendor appliance: This is important but only covers the integration phase, not the entire supply chain.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
? ISO/IEC 27036-1:2014, "Information technology — Security techniques — Information security for supplier relationships"

NEW QUESTION 25
A systems administrator wants to introduce a newly released feature for an internal application. The administrate docs not want to test the feature in the production environment. Which of the following locations is the best place to test the new feature?

A. Staging environment
B. Testing environment
C. CI/CO pipeline
D. Development environment

Answer: A

Explanation:
The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment. Here??s a detailed Explanation
? Staging Environment: This environment closely mirrors the production environment in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging environment ensures that the new feature will behave as expected in the actual production setup.
? Isolation from Production: The staging environment is isolated from production, which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change management and risk mitigation.
? Realistic Testing: Since the staging environment replicates the production environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which often have different configurations and workloads.
? References:

NEW QUESTION 27

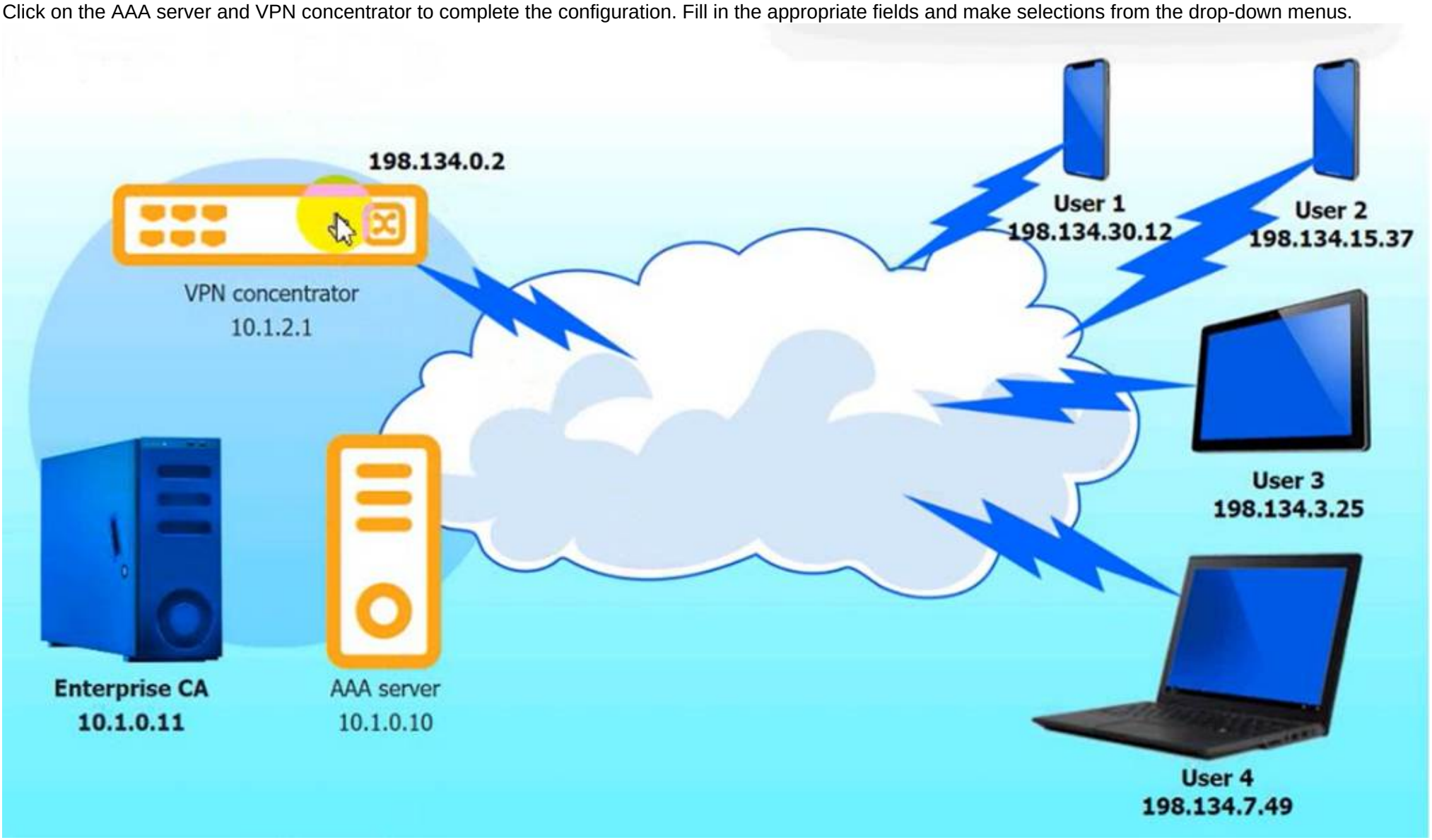
A company wants to install a three-tier approach to separate the web. database, and application servers A security administrator must harden the environment which of the following is the best solution?

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

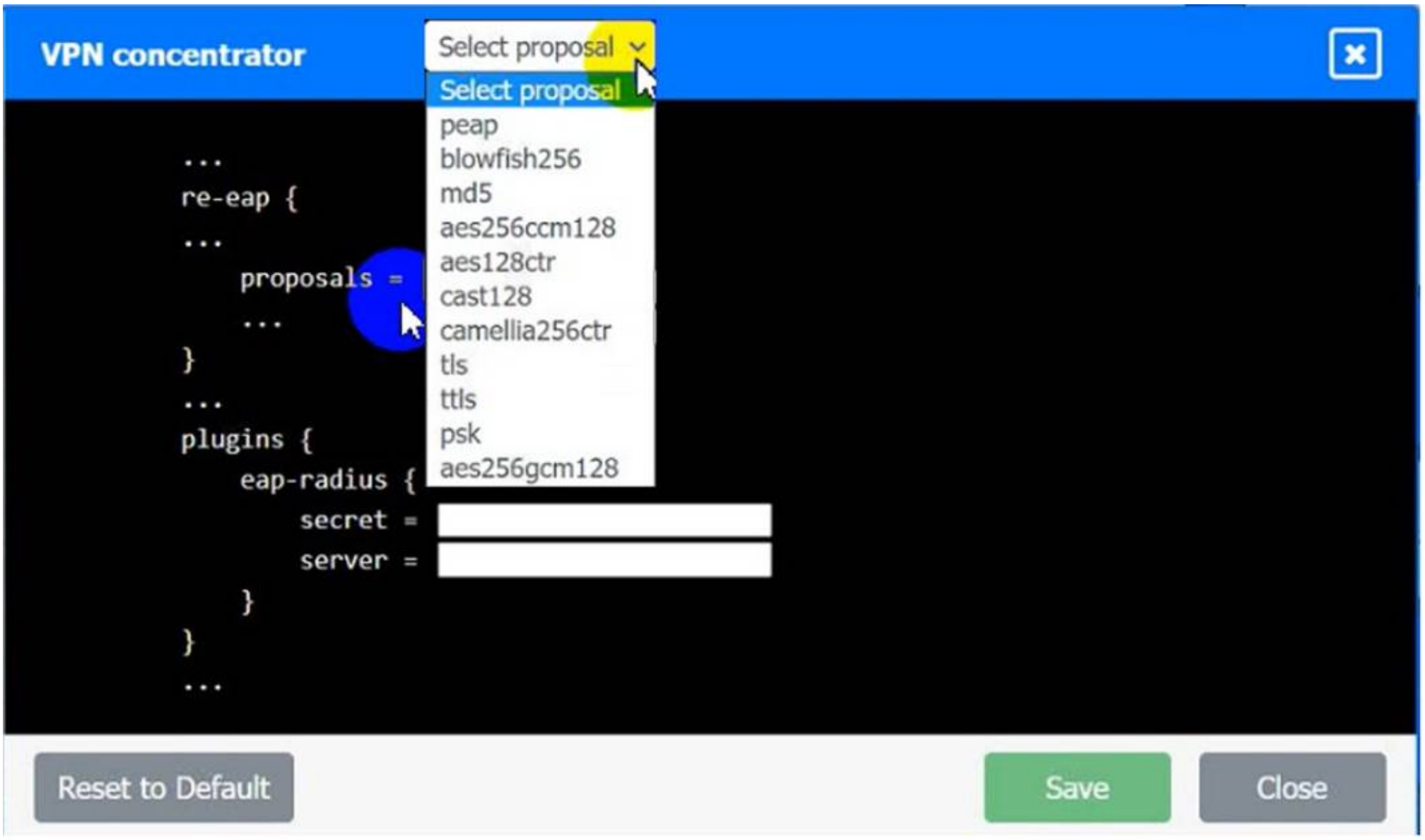
Answer: C

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:

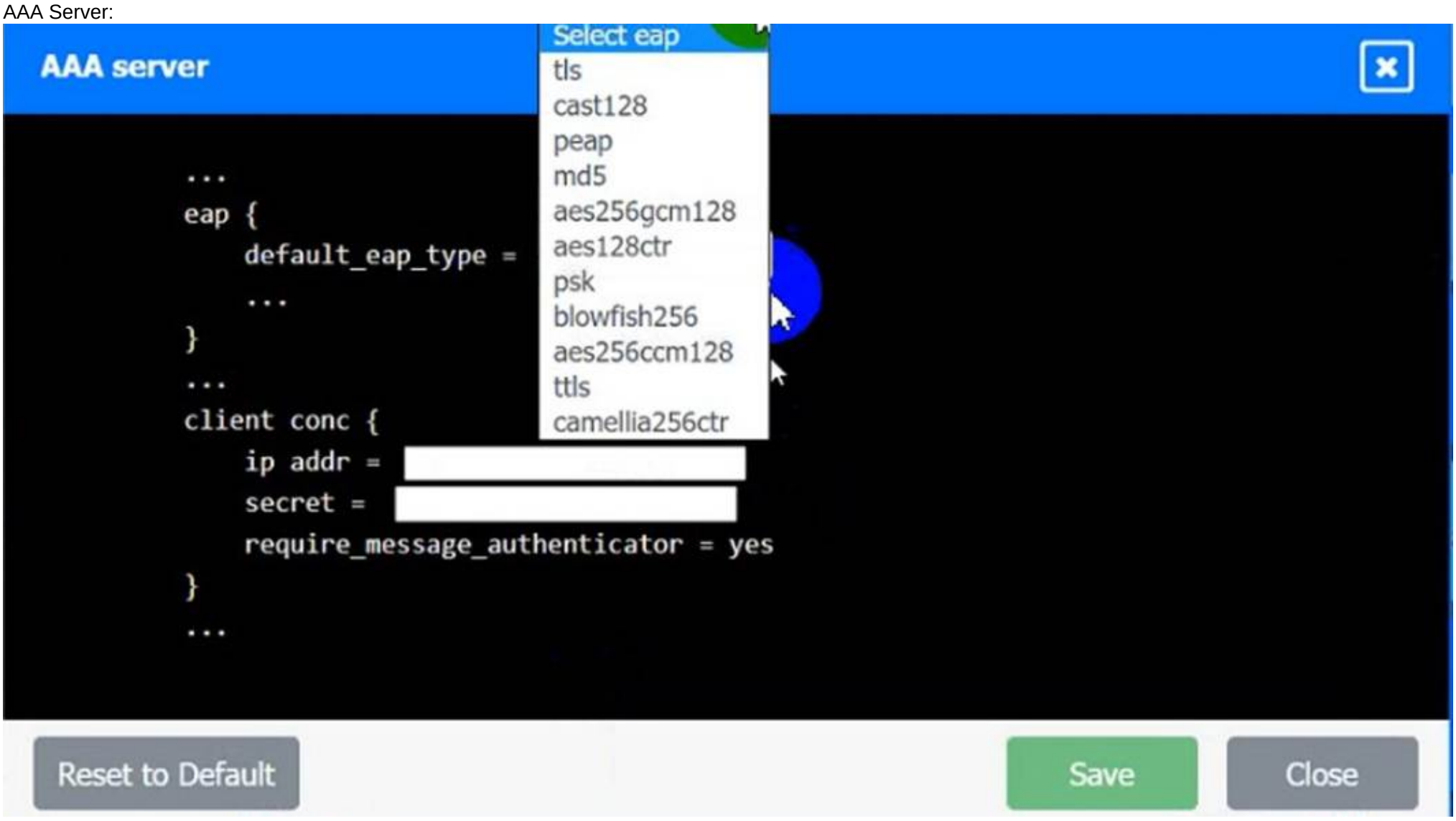
NEW QUESTION 31
SIMULATION
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
• The EAP method must use mutual certificate-based authentication (With issued client certificates).
• The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
• The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,
INSTRUCTIONS
Click on the AAA server and VPN concentrator to complete the configuration. Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



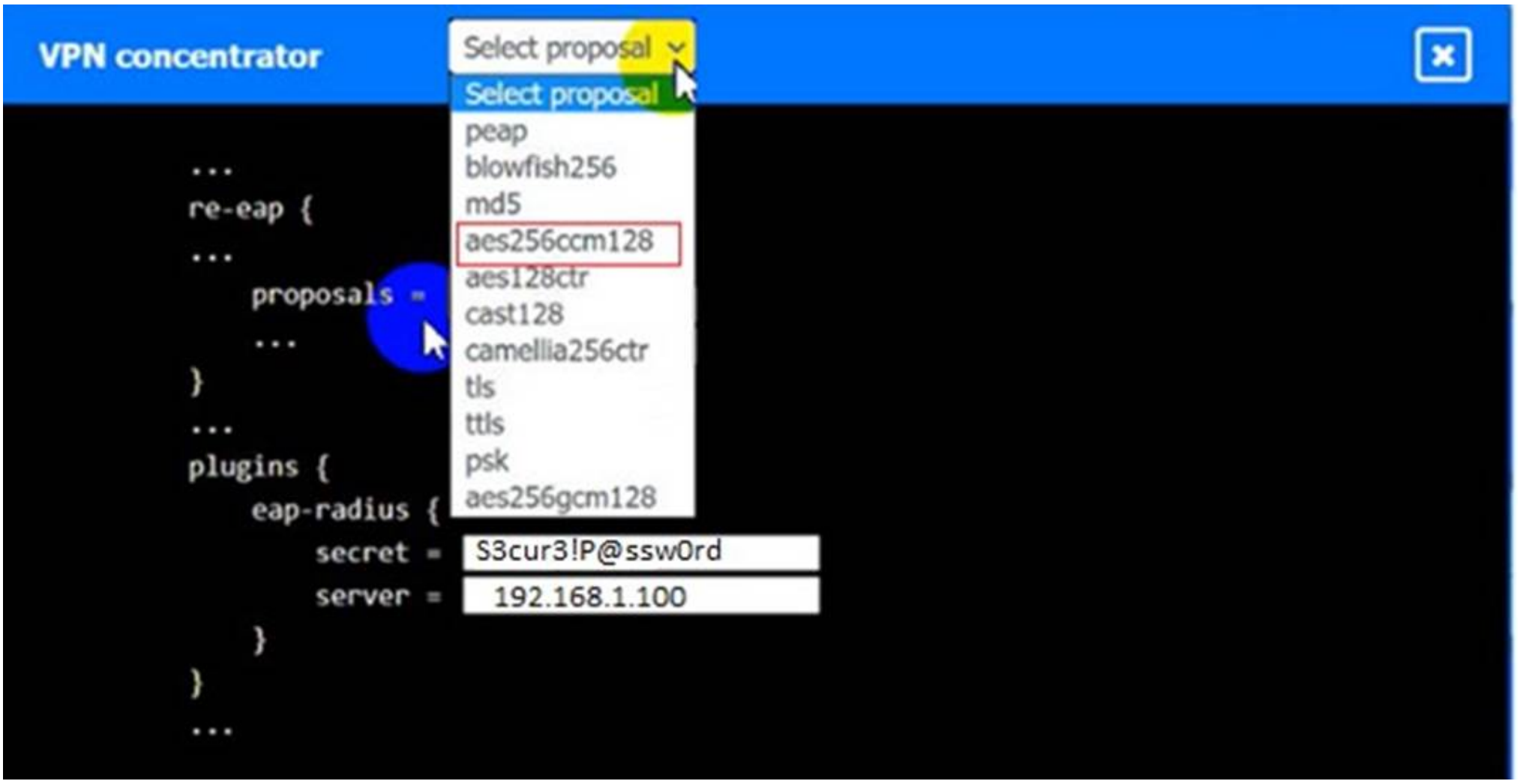
AAA Server:



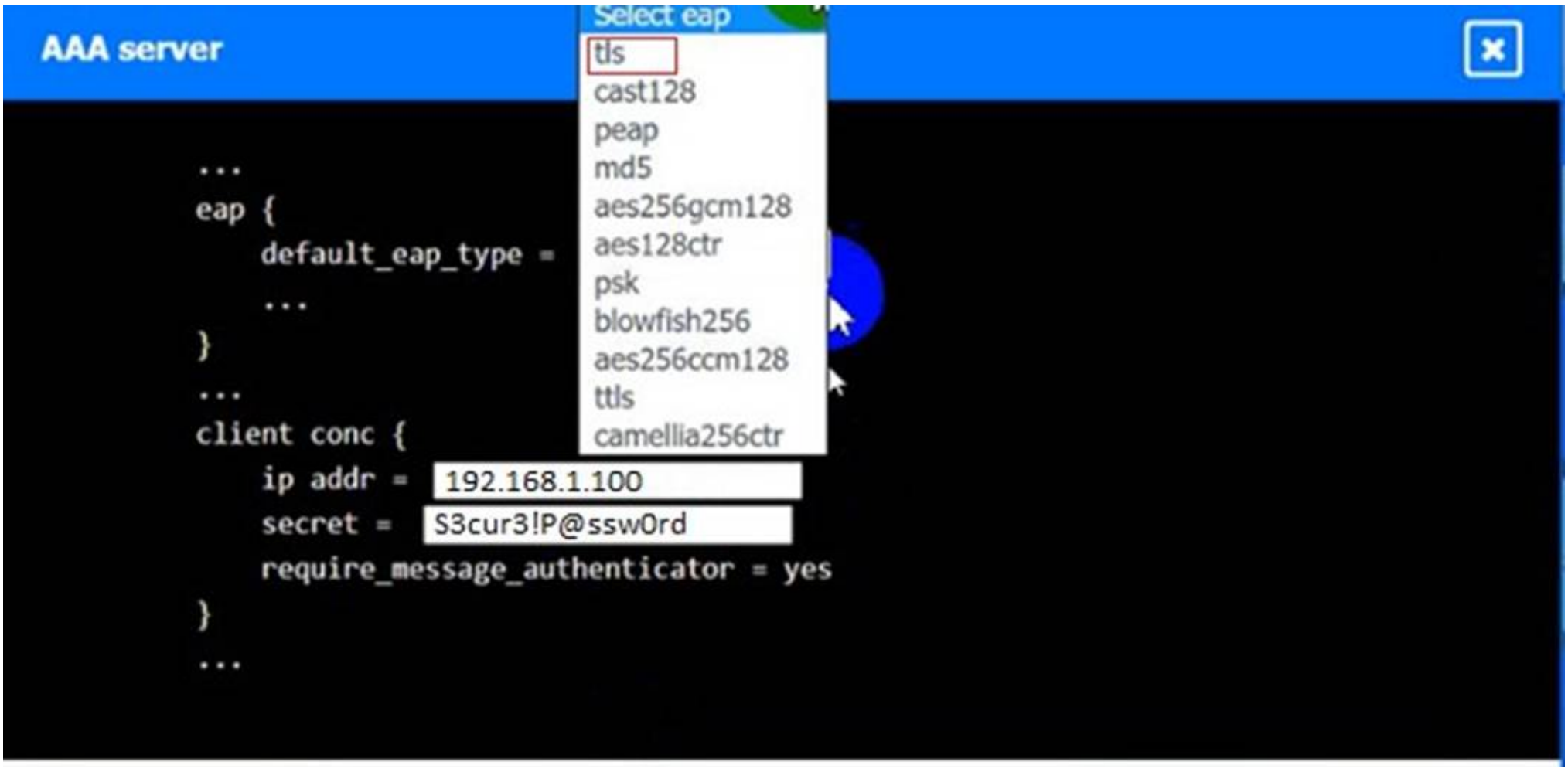
A. Mastered
B. Not Mastered

Answer: A

Explanation:
VPN Concentrator:



AAA Server:



NEW QUESTION 33
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

Answer: D

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

NEW QUESTION 35
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 39
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 44
A vulnerability can on a web server identified the following:

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

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

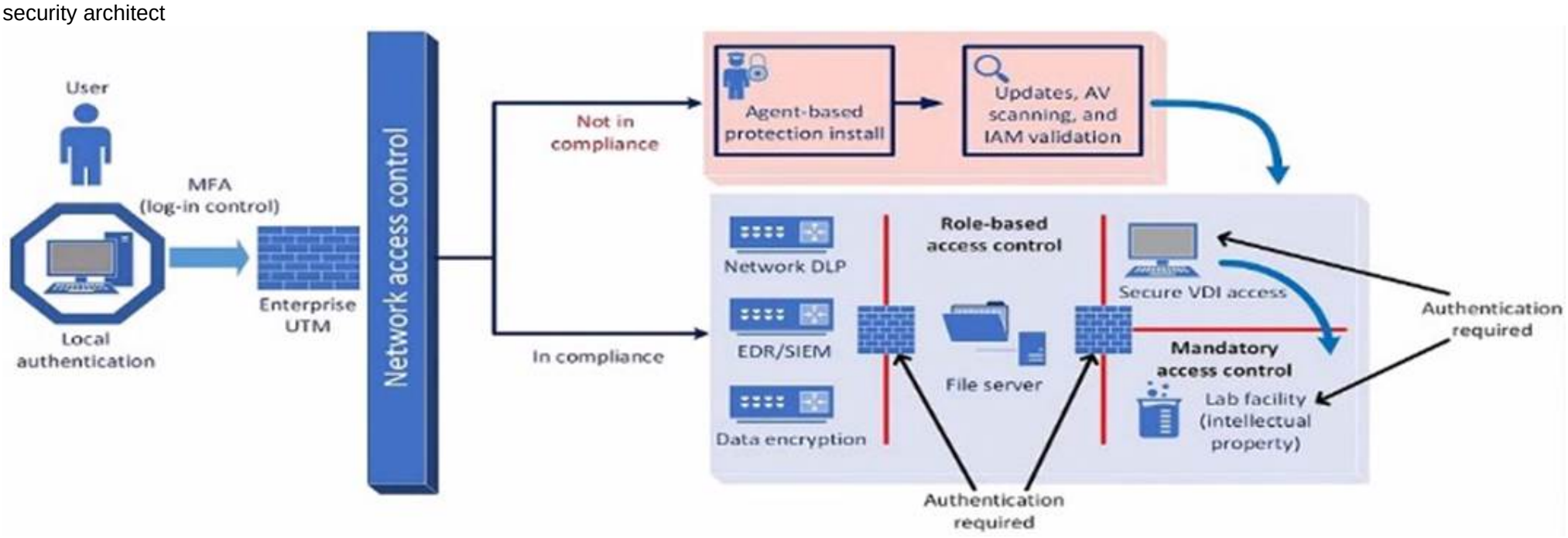
A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
B. Removing support for CBC-based key exchange and signing algorithms
C. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256
D. Implementing HIPS rules to identify and block BEAST attack attempts
E. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA
F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA

Answer: BC

Explanation:
On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:
? B. Removing support for CBC-based key exchange and signing algorithms: CBC
mode is vulnerable to certain attacks like BEAST. By removing support for CBC- based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.
? C. Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher

suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"
? OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

NEW QUESTION 46
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 47
A systems administrator works with engineers to process and address vulnerabilities as a result of continuous scanning activities. The primary challenge faced by the administrator is differentiating between valid and invalid findings. Which of the following would the systems administrator most likely verify is properly configured?

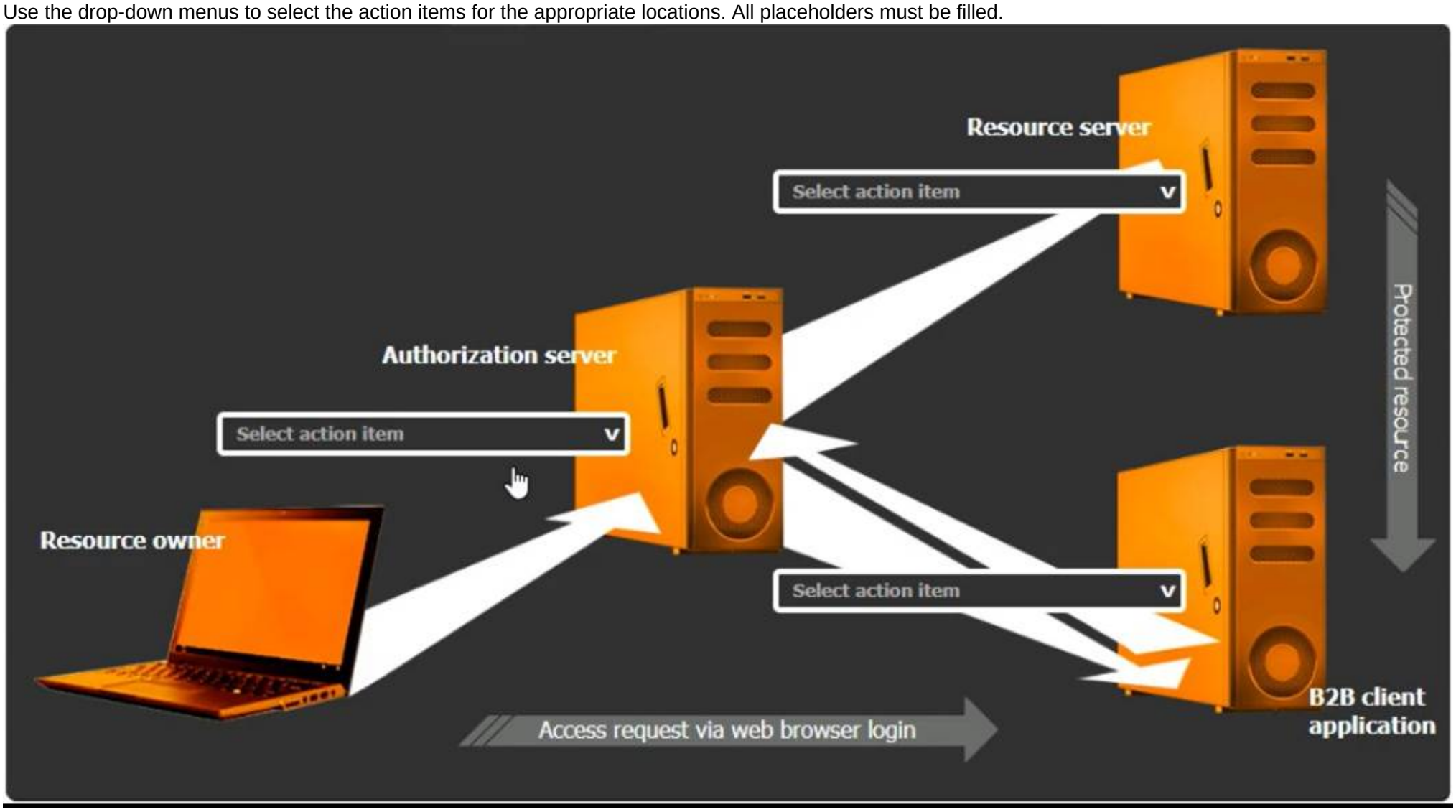
A. Report retention time
B. Scanning credentials
C. Exploit definitions
D. Testing cadence

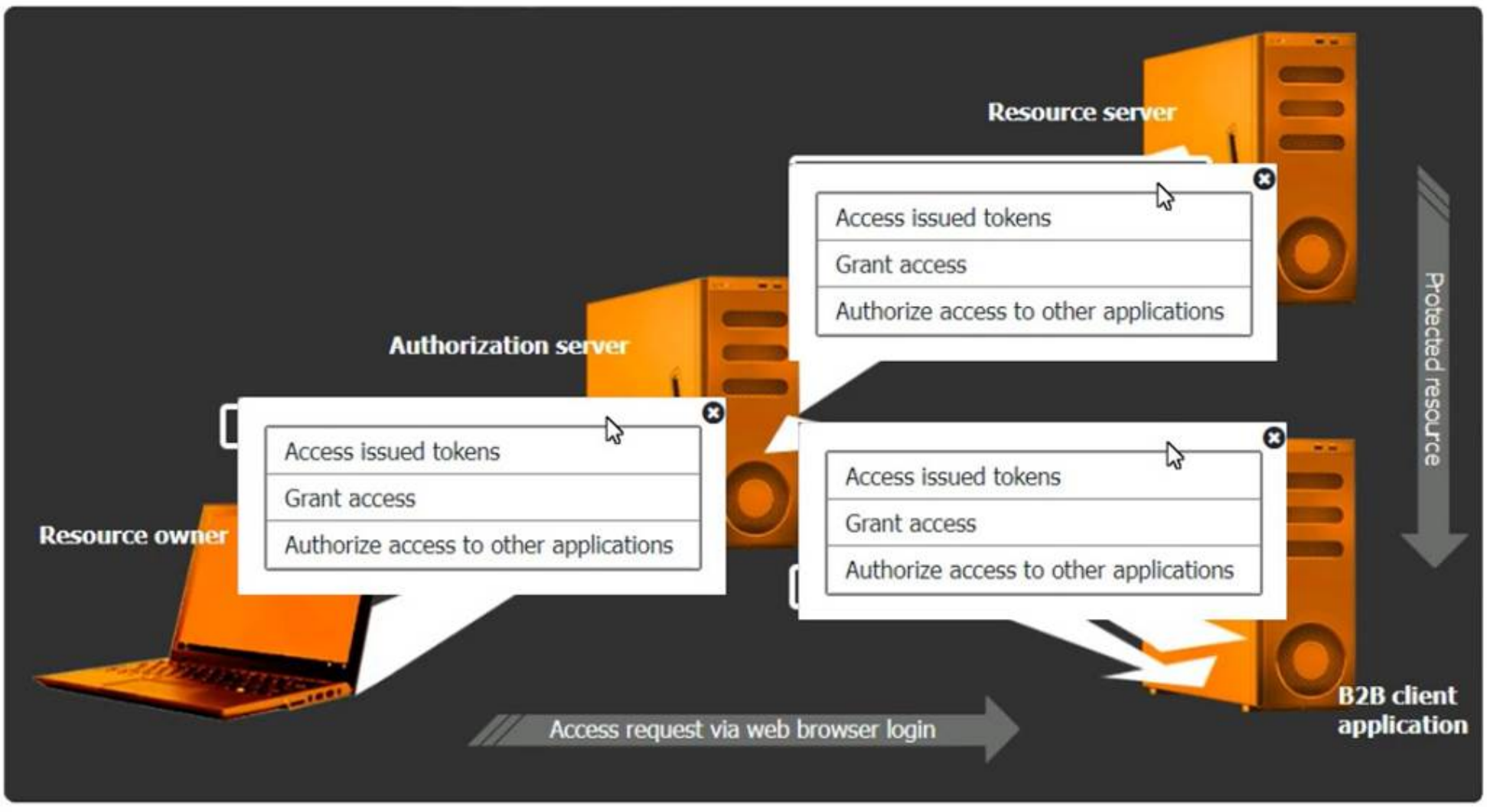
Answer: B

Explanation:
When differentiating between valid and invalid findings from vulnerability scans, the systems administrator should verify that the scanning credentials are properly configured. Valid credentials ensure that the scanner can authenticate and access the systems being evaluated, providing accurate and comprehensive results. Without proper credentials, scans may miss vulnerabilities or generate false positives, making it difficult to prioritize and address the findings effectively.
References:
? CompTIA SecurityX Study Guide: Highlights the importance of using valid credentials for accurate vulnerability scanning.
? "Vulnerability Management" by Park Foreman: Discusses the role of scanning credentials in obtaining accurate scan results and minimizing false positives.
? "The Art of Network Security Monitoring" by Richard Bejtlich: Covers best practices for configuring and using vulnerability scanning tools, including the need for valid credentials.

NEW QUESTION 50
SIMULATION
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:
. The application does not need to know the users' credentials.
. An approval interaction between the users and the HTTP service must be orchestrated.
. The application must have limited access to users' data. INSTRUCTIONS

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





A. Mastered
B. Not Mastered

Answer: A

Explanation:
Select the Action Items for the Appropriate Locations:
? Authorization Server:
? Resource Server:
? B2B Client Application:
Detailed Explanation
OAuth 2.0 is designed to provide specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. The integration involves multiple steps and components, including:
? Resource Owner (User):
? Client Application (B2B Client Application):

? Authorization Server:
? Resource Server:
OAuth Workflow:
? The resource owner accesses the client application.
? The client application redirects the resource owner to the authorization server for authentication.
? The authorization server authenticates the resource owner and asks for consent to grant access to the client application.
? Upon consent, the authorization server issues an authorization code or token to the client application.
? The client application uses the authorization code or token to request access to the resources from the resource server.
? The resource server verifies the token with the authorization server and, if valid, grants access to the requested resources.
References:
? CompTIA Security+ Study Guide: Provides comprehensive information on various authentication and authorization protocols, including OAuth.
? OAuth 2.0 Authorization Framework (RFC 6749): The official documentation detailing the OAuth 2.0 framework, its flows, and components.
? OAuth 2.0 Simplified: A book by Aaron Parecki that provides a detailed yet easy- to-understand explanation of the OAuth 2.0 protocol.
By ensuring that each component in the OAuth workflow performs its designated role, the B2B client application can securely access the necessary resources without compromising user credentials, adhering to the principle of least privilege.

NEW QUESTION 52
A cloud engineer needs to identify appropriate solutions to:
• Provide secure access to internal and external cloud resources.
• Eliminate split-tunnel traffic flows.
• Enable identity and access management capabilities.
Which of the following solutions arc the most appropriate? (Select two).

A. Federation
B. Microsegmentation
C. CASB
D. PAM
E. SD-WAN
F. SASE

Answer: CF

Explanation:
To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).
Why CASB and SASE?
? CASB (Cloud Access Security Broker):
? SASE (Secure Access Service Edge):
Other options, while useful, do not comprehensively address all the requirements:
? A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.
? B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.
? D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.
? E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.
References:
? CompTIA SecurityX Study Guide
? "CASB: Cloud Access Security Broker," Gartner Research

NEW QUESTION 54
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 59
An organization wants to manage specialized endpoints and needs a solution that provides the ability to
* Centrally manage configurations
* Push policies.
• Remotely wipe devices
• Maintain asset inventory
Which of the following should the organization do to best meet these requirements?

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

Answer: B

Explanation:
To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.
MDM Capabilities:
? Central Management: MDM allows administrators to manage the configurations of all devices from a central console.
? Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.
? Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.
? Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.
Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.
References:
? CompTIA SecurityX Study Guide
? NIST Special Publication 800-124 Revision 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"
? "Mobile Device Management Overview," Gartner Research

NEW QUESTION 64
Emails that the marketing department is sending to customers are pomp to the customers' spam folders. The security team is investigating the issue and discovers that the certificates used by the email server were reissued, but DNS records had not been updated. Which of the following should the security team update in order to fix this issue? (Select three.)

A. DMARC
B. SPF
C. DKIM
D. DNSSEC
E. SASC
F. SAN
G. SOA
H. MX

Answer: ABC

Explanation:
To prevent emails from being marked as spam, several DNS records related to email authentication need to be properly configured and updated when there are changes to the email server's certificates:
? A. DMARC (Domain-based Message Authentication, Reporting & Conformance):
DMARC records help email servers determine how to handle messages that fail SPF or DKIM checks, improving email deliverability and reducing the likelihood of emails being marked as spam.
? B. SPF (Sender Policy Framework): SPF records specify which mail servers are authorized to send email on behalf of your domain. Updating the SPF record ensures that the new email server is recognized as an authorized sender.
? C. DKIM (DomainKeys Identified Mail): DKIM adds a digital signature to email
headers, allowing the receiving server to verify that the email has not been tampered with and is from an authorized sender. Updating DKIM records ensures that emails are properly signed and authenticated.
? D. DNSSEC (Domain Name System Security Extensions): DNSSEC adds security
to DNS by enabling DNS responses to be verified. While important for DNS security, it does not directly address the issue of emails being marked as spam.
? E. SASC: This is not a relevant standard for this scenario.
? F. SAN (Subject Alternative Name): SAN is used in SSL/TLS certificates for securing multiple domain names, not for email delivery issues.
? G. SOA (Start of Authority): SOA records are used for DNS zone administration and do not directly impact email deliverability.
? H. MX (Mail Exchange): MX records specify the mail servers responsible for receiving email on behalf of a domain. While important, the primary issue here is the authentication of outgoing emails, which is handled by SPF, DKIM, and DMARC.
References:
? CompTIA Security+ Study Guide
? RFC 7208 (SPF), RFC 6376 (DKIM), and RFC 7489 (DMARC)
? NIST SP 800-45, "Guidelines on Electronic Mail Security"

NEW QUESTION 67
A security analyst is troubleshooting the reason a specific user is having difficulty accessing company resources The analyst reviews the following information:

User	Source IP	Source location	User assigned location	MFA satisfied?	Sign-in status
SALES1	8.11.4.16	Germany	France	Yes	Blocked
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	192.168.4.18	France	France	No	Allowed
SALES1	8.11.4.16	Germany	France	Yes	Blocked
ACCT1	8.11.4.16	Germany	France	Yes	Blocked
SALES2	8.11.4.20	France	France	Yes	Allowed

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

A. The local network access has been configured to bypass MFA requirements.
B. A network geolocation is being misidentified by the authentication server
C. Administrator access from an alternate location is blocked by company policy
D. Several users have not configured their mobile devices to receive OTP codes

Answer: B

Explanation:
The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements. The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.
Why Network Geolocation Misidentification?
? Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.
? Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.
? Consistent Pattern: The user "SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.
Other options do not align with the pattern observed:
? A. Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.
? C. Administrator access policy: This is about user access, not specific administrator access.
? D. OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.
References:
? CompTIA SecurityX Study Guide
? "Geolocation and Authentication," NIST Special Publication 800-63B
? "IP Geolocation Accuracy," Cisco Documentation

NEW QUESTION 68
A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

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

Answer: C

Explanation:
To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments.
? ITIL (Information Technology Infrastructure Library) Framework: Provides best practices for change management in IT services.
? "The Phoenix Project" by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

NEW QUESTION 73
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 74
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

Answer: C

Explanation:
In the context of improving incident response and reducing dwell time, the security analyst needs to focus on proactive measures that can quickly detect and alert on potential security breaches. Here??s a detailed analysis of the options provided:
* A. Adjusting the SIEM to alert on attempts to visit phishing sites: While this is a useful measure to prevent phishing attacks, it primarily addresses external threats and doesn??t directly impact dwell time reduction, which focuses on the time a threat remains undetected within a network.
* B. Allowing TRACE method traffic to enable better log correlation: The TRACE method in HTTP is used for debugging purposes, but enabling it can introduce security vulnerabilities. It??s not typically recommended for enhancing security monitoring or incident response.
* C. Enabling alerting on all suspicious administrator behavior: This option directly targets the potential misuse of administrator accounts, which are often high-value targets for attackers. By monitoring and alerting on suspicious activities from admin accounts, the organization can quickly identify and respond to potential breaches, thereby reducing dwell
time significantly. Suspicious behavior could include unusual login times, access to sensitive data not usually accessed by the admin, or any deviation from normal behavior patterns. This proactive monitoring is crucial for quick detection and response, aligning well with best practices in incident response.
* D. Utilizing allow lists on the WAF for all users using GET methods: This measure is aimed at restricting access based on allowed lists, which can be effective in preventing unauthorized access but doesn??t specifically address the need for quick detection and response to internal threats.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of monitoring and alerting on admin activities as part of a robust incident response plan.
? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide": Highlights best practices for incident response, including the importance of detecting and responding to suspicious activities quickly.
? "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia: Discusses techniques for reducing dwell time through effective monitoring and alerting mechanisms, particularly focusing on privileged account activities.
By focusing on enabling alerting for suspicious administrator behavior, the security analyst addresses a critical area that can help reduce the time a threat goes undetected, thereby improving the overall security posture of the organization.
Top of Form Bottom of Form

NEW QUESTION 76
A network engineer must ensure that always-on VPN access is enabled Curt restricted to company assets Which of the following best describes what the engineer needs to do"

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

Answer: A

Explanation:
To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.
Why Device Certificates are Necessary:
? Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.
? Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.
? Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.
Other options do not provide the same level of control and security for always-on VPN access:
? B. Modify signing certificates for IKE version 2: While important for VPN protocols,
it does not address device-specific authentication.

? C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.
? D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.
References:
? CompTIA SecurityX Study Guide
? "Device Certificates for VPN Access," Cisco Documentation
? NIST Special Publication 800-77, "Guide to IPsec VPNs"

NEW QUESTION 81
An organization is developing on Al-enabled digital worker to help employees complete common tasks such as template development, editing, research, and scheduling. As part of the Al workload the organization wants to Implement guardrails within the platform. Which of the following should the company do to secure the Al environment?

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

Answer: A

Explanation:
Limiting the platform's abilities to only non-sensitive functions helps to mitigate risks associated with AI operations. By ensuring that the AI-enabled digital worker is only allowed to perform tasks that do not involve sensitive or critical data, the organization reduces the potential impact of any security breaches or misuse. Enhancing the training model's effectiveness (Option B) is important but does not directly address security guardrails. Granting the system the ability to self-govern (Option C) could increase risk as it may act beyond the organization's control. Requiring end-user acknowledgement of organizational policies (Option D) is a good practice but does not implement technical guardrails to secure the AI environment.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"
? ISO/IEC 27001, "Information Security Management"

NEW QUESTION 86
A security engineer needs 10 secure the OT environment based on me following requirements
• Isolate the OT network segment
• Restrict Internet access.
• Apply security updates two workstations
• Provide remote access to third-party vendors
Which of the following design strategies should the engineer implement to best meet these requirements?

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

Answer: B

Explanation:
To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect
while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.
References:
? CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.
? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.
? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

NEW QUESTION 87
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 89
A security architect is establishing requirements to design resilience in un enterprise system trial will be extended to other physical locations. The system must
• Be survivable to one environmental catastrophe
• Re recoverable within 24 hours of critical loss of availability
• Be resilient to active exploitation of one site-to-site VPN solution

A. Load-balance connection attempts and data Ingress at internet gateways
B. Allocate fully redundant and geographically distributed standby sites.
C. Employ layering of routers from diverse vendors
D. Lease space to establish cold sites throughout other countries
E. Use orchestration to procure, provision, and transfer application workloads lo cloudservices
F. Implement full weekly backups to be stored off-site for each of the company's sites

Answer: B

Explanation:
To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant and geographically distributed standby sites. Here??s why:
? Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.
? Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.
? Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.
? References:

NEW QUESTION 90
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.

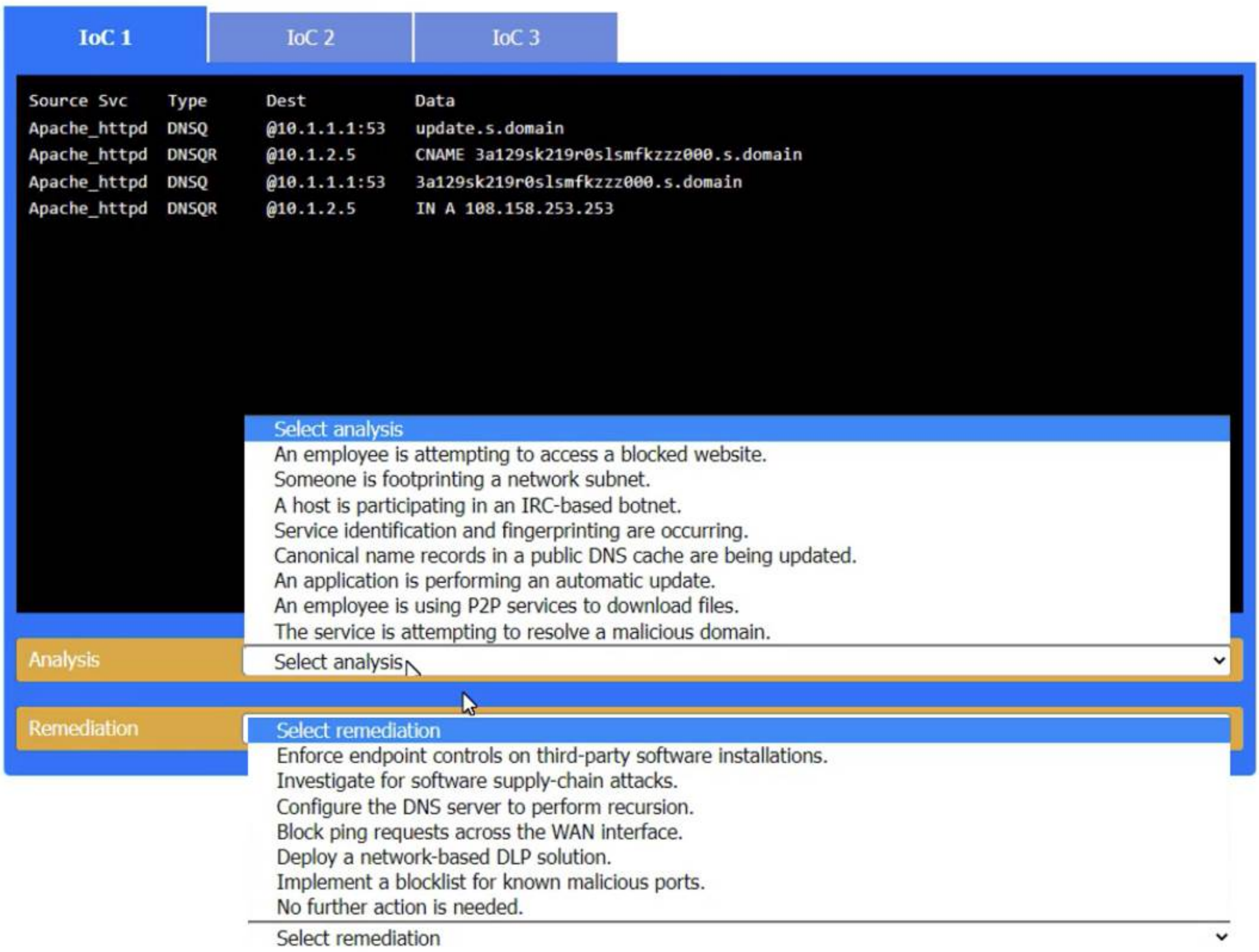
NEW QUESTION 92
While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?

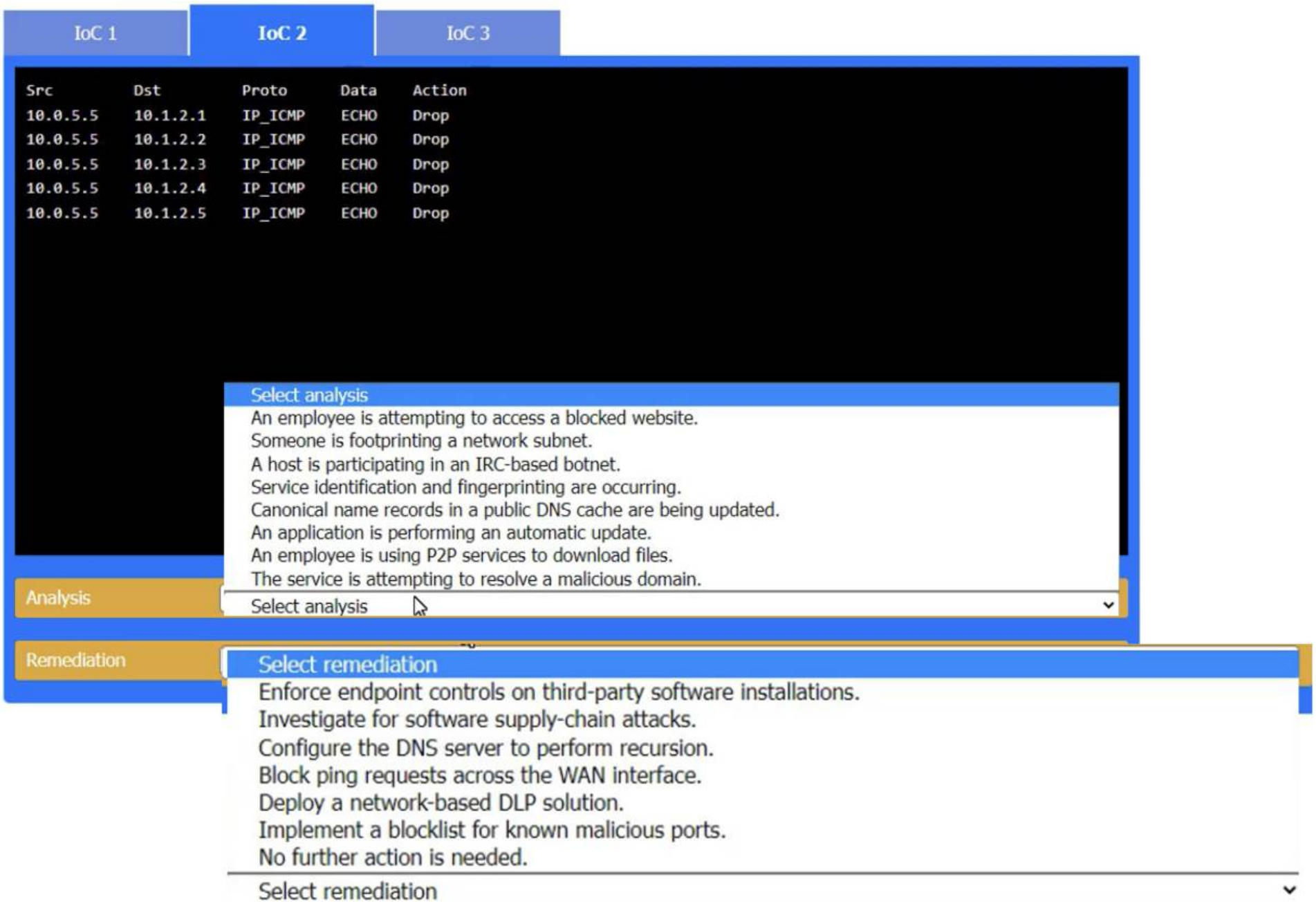
A. Spear-phishing campaign
B. Threat modeling
C. Red team assessment
D. Attack pattern analysis

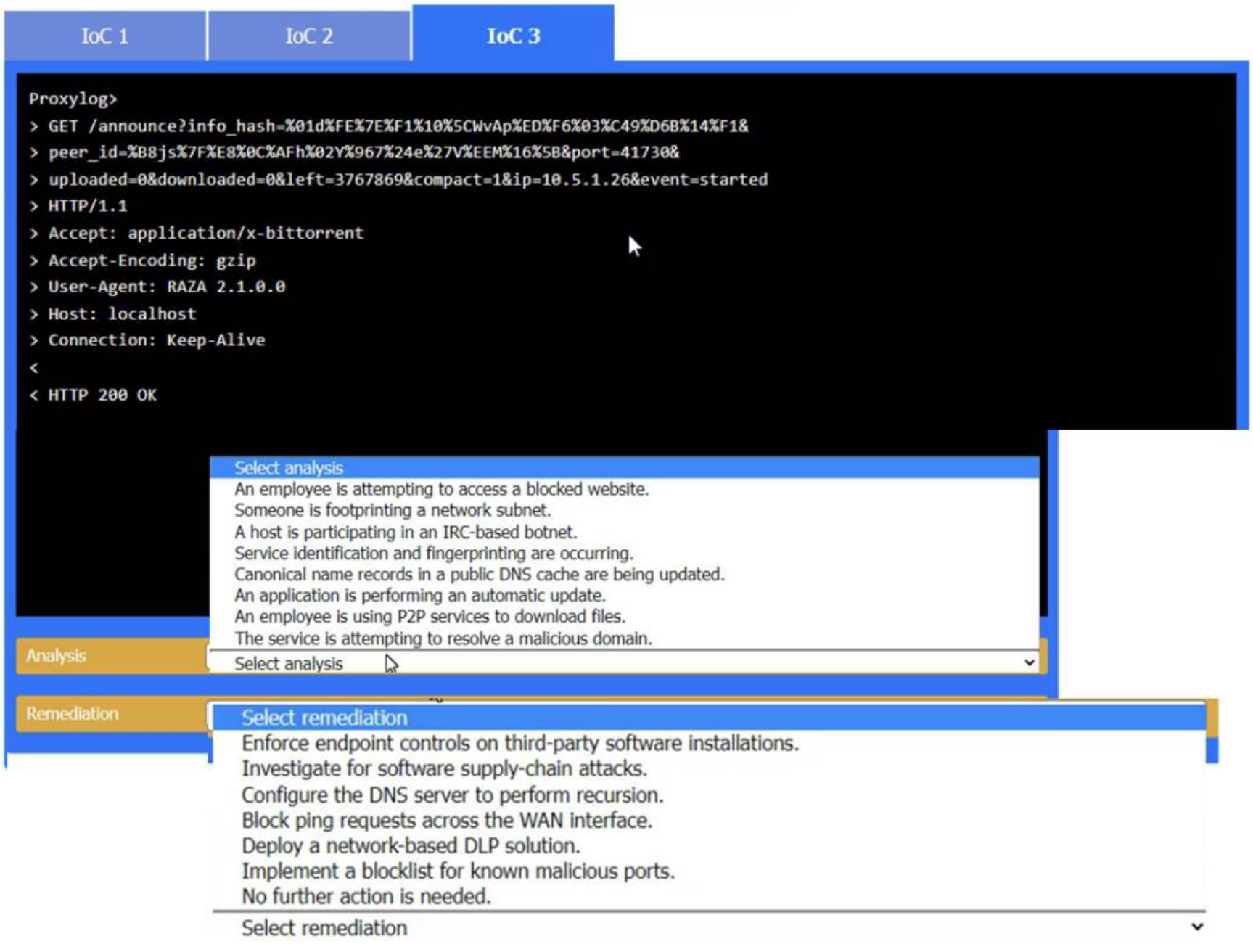
Answer: A

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 95
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.







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 98
A security architect wants to develop a baseline of security configurations These configurations automatically will be utilized machine is created Which of the following technologies should the security architect deploy to accomplish this goal?

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

Answer: C

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

NEW QUESTION 101
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CAS-005 Practice Exam Features:

* CAS-005 Questions and Answers Updated Frequently

* CAS-005 Practice Questions Verified by Expert Senior Certified Staff

* CAS-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year