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

A. Request a weekly report with all new assets deployed and decommissioned
B. Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.
C. Implement a shadow IT detection process to avoid rogue devices on the network
D. Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool

Answer: D

Explanation:
To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Here??s why:
? Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date
inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.
? Consistency in Reporting: By continuously discovering and scanning new and
existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.
? Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.
? References:

NEW QUESTION 3
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
After some employees were caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation. Which of the following would the company most likely do to decrease this type of risk?

A. Improve firewall rules to avoid access to those platforms.
B. Implement a cloud-access security broker
C. Create SIEM rules to raise alerts for access to those platforms
D. Deploy an internet proxy that filters certain domains

Answer: B

Explanation:
A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed. Implementing a CASB provides several benefits:
? A. Improve firewall rules to avoid access to those platforms: This can help but is not as effective or comprehensive as a CASB.
? B. Implement a cloud-access security broker: A CASB can provide visibility into cloud application usage, enforce data security policies, and protect against data leaks by monitoring and controlling access to cloud services. It also provides advanced features like data encryption, data loss prevention (DLP), and compliance monitoring.
? C. Create SIEM rules to raise alerts for access to those platforms: This helps in

monitoring but does not prevent data leaks.
? D. Deploy an internet proxy that filters certain domains: This can block access to specific sites but lacks the granular control and visibility provided by a CASB.
Implementing a CASB is the most comprehensive solution to decrease the risk of data leaks by providing visibility, control, and enforcement of security policies for cloud services. References:
? CompTIA Security+ Study Guide
? Gartner, "Magic Quadrant for Cloud Access Security Brokers"
? NIST SP 800-144, "Guidelines on Security and Privacy in Public Cloud Computing"

NEW QUESTION 5
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 6
A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

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

Answer: A

Explanation:
The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.
References:
? CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.
? GDPR official documentation: Details the rights of individuals, including data erasure and the right to be forgotten.
? "GDPR: A Practical Guide to the General Data Protection Regulation" by IT Governance Privacy Team: Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

NEW QUESTION 7
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 8
A company's SICM Is continuously reporting false positives and false negatives The security operations team has Implemented configuration changes to troubleshoot possible reporting errors Which of the following sources of information best supports the required analysts process? (Select two).

A. Third-party reports and logs
B. Trends

C. Dashboards
D. Alert failures
E. Network traffic summaries
F. Manual review processes

Answer: AB

Explanation:
When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:
* A. Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader
perspective on potential threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives.
* B. Trends: Analyzing trends over time can help in understanding patterns and anomalies in the data. By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning the SIEM configurations to better detect true positives and reduce false alerts.
Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM configurations.
References:
? CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection.
? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection.
? "Security Information and Event Management (SIEM) Implementation" by David Miller: Discusses the use of external intelligence and trends to enhance SIEM accuracy.

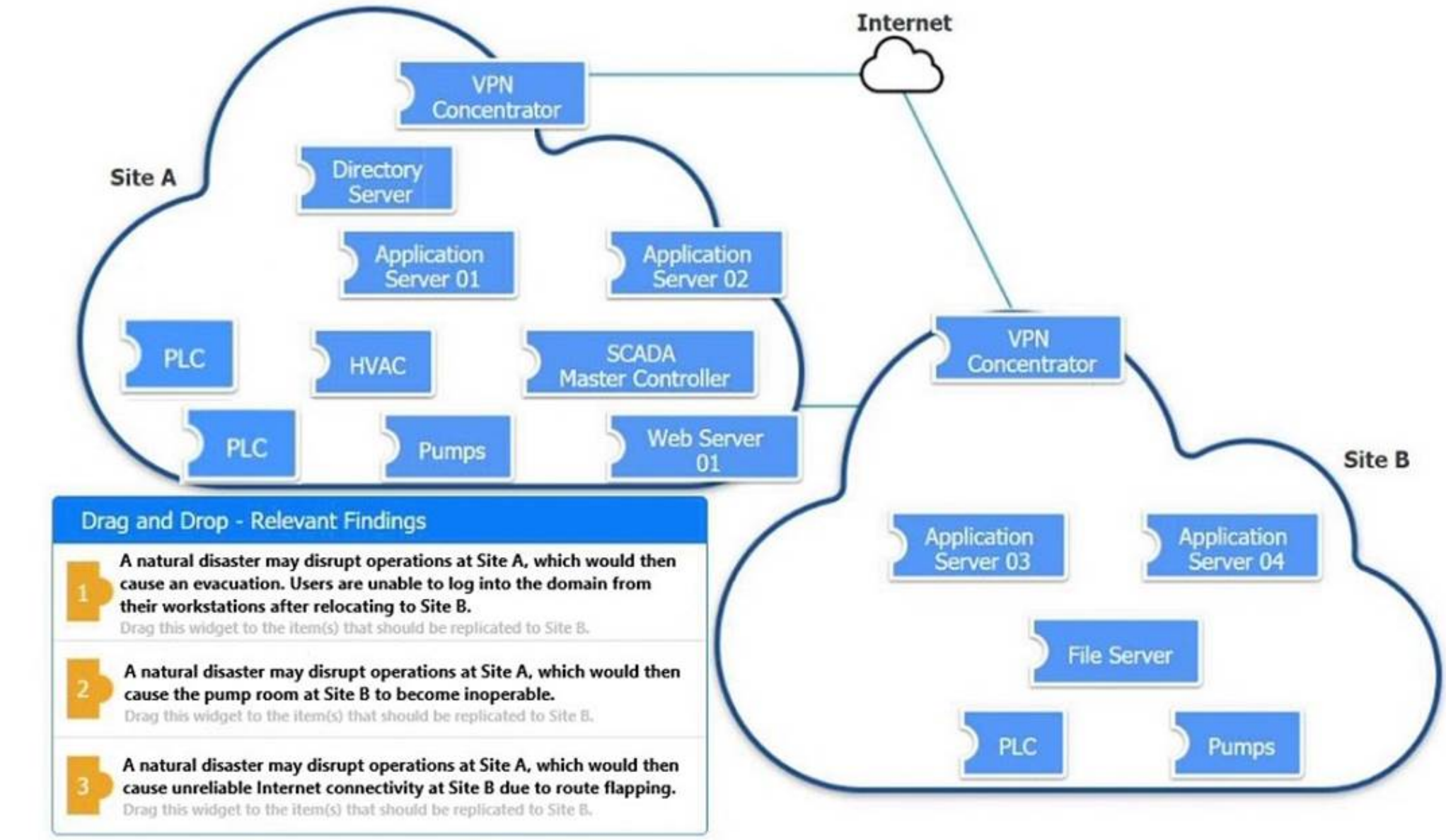
NEW QUESTION 9
A global manufacturing company has an internal application mat is critical to making products This application cannot be updated and must Be available in the production area A security architect is implementing security for the application. Which of the following best describes the action 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

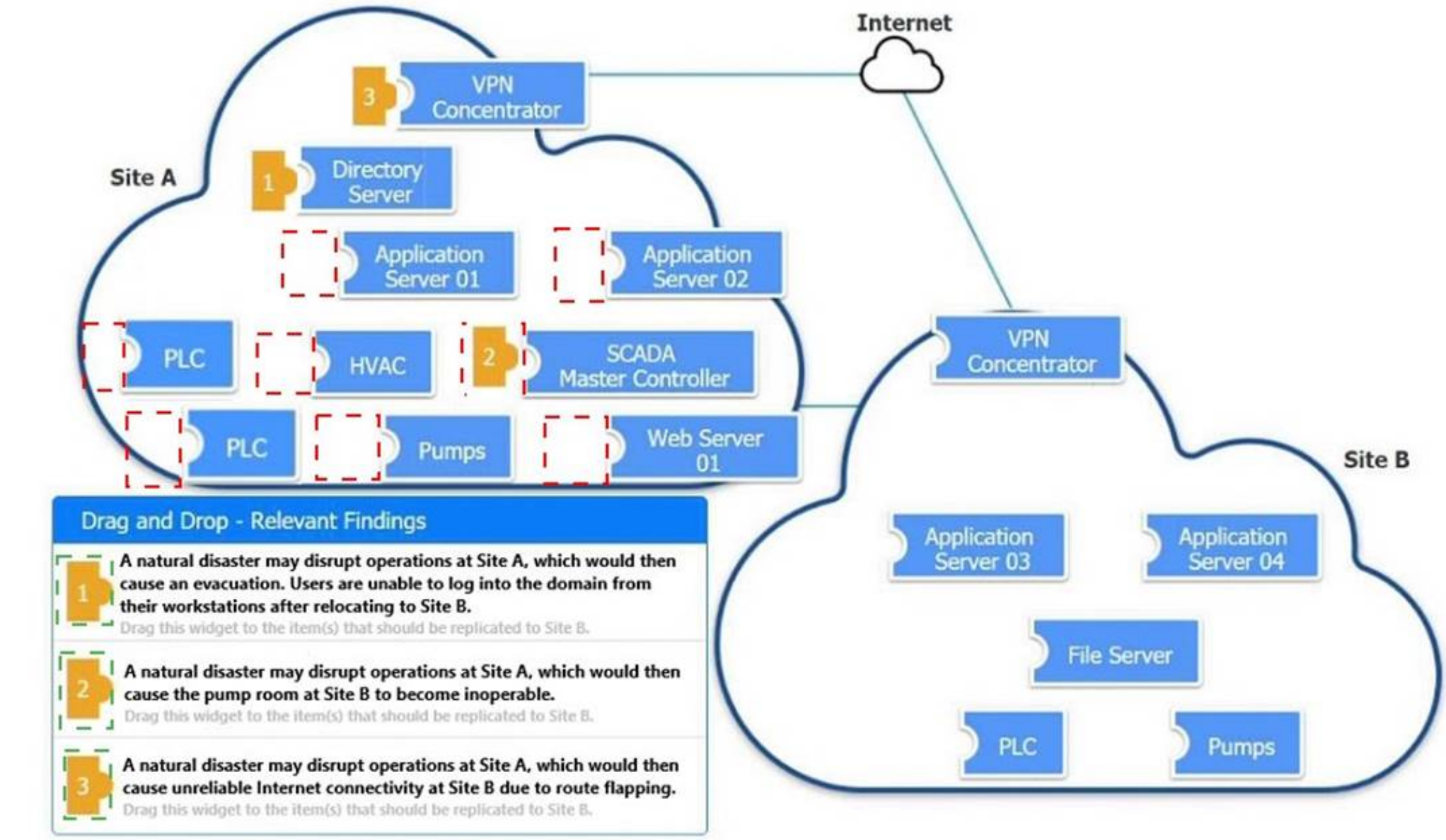
Answer: D

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 10
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 10
Recent repents indicate that a software tool is being exploited Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output:

```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS Mode
dBl0ad3r!
Load Database jmp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dBl0ad3r!
```

Which of the following would the analyst most likely recommend?

A. Installing appropriate EDR tools to block pass-the-hash attempts
B. Adding additional time to software development to perform fuzz testing
C. Removing hard coded credentials from the source code
D. Not allowing users to change their local passwords

Answer: C

Explanation:
The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The most likely recommendation is to remove hard-coded credentials from the source code. Here??s why:
? Security Best Practices: Hard-coded credentials are a significant security risk
because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.
? Credential Management: Credentials should be managed securely using
environment variables, secure vaults, or configuration management tools that provide encryption and access controls.
? Mitigation of Exploits: By eliminating hard-coded credentials, the organization can
prevent attackers from easily bypassing authentication mechanisms and gaining
unauthorized access to sensitive systems.
? References:

NEW QUESTION 14
A security engineer performed a code scan that resulted in many false positives. The security engineer must find a solution that improves the quality of scanning results before application deployment. Which of the following is the best solution?

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

Answer: A

Explanation:
To improve the quality of code scanning results and reduce false positives, the best solution is to limit the tool to a specific coding language and fine-tune the rule set. By configuring the code scanning tool to focus on the specific language used in the application, the tool can more accurately identify relevant issues and reduce the number of false positives. Additionally, tuning the rule set ensures that the tool's checks are
appropriate for the application's context, further improving the accuracy of the scan results.
References:
? CompTIA SecurityX Study Guide: Discusses best practices for configuring code scanning tools, including language-specific tuning and rule set adjustments.
? "Secure Coding: Principles and Practices" by Mark G. Graff and Kenneth R. van Wyk: Highlights the importance of customizing code analysis tools to reduce false positives.
? OWASP (Open Web Application Security Project): Provides guidelines for configuring and tuning code scanning tools to improve accuracy.

NEW QUESTION 16
A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent llS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:

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

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

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

Answer: A

Explanation:
Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here??s why:
? Public Availability: Host 1 is externally available, making it accessible from the
internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.
? Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.
? Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.
? References:

NEW QUESTION 21
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 26
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 30
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 34
Users are experiencing a variety of issues when trying to access corporate resources examples include
• Connectivity issues between local computers and file servers within branch offices
• Inability to download corporate applications on mobile endpoints wtiilc working remotely
• Certificate errors when accessing internal web applications
Which of the following actions are the most relevant when troubleshooting the reported issues? (Select two).

A. Review VPN throughput
B. Check IPS rules
C. Restore static content on lite CDN.
D. Enable secure authentication using NAC
E. Implement advanced WAF rules.
F. Validate MDM asset compliance

Answer: AF

Explanation:
The reported issues suggest problems related to network connectivity, remote access, and certificate management:
? A. Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.
? F. Validate MDM asset compliance: Mobile Device Management (MDM) systems ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.
? B. Check IPS rules: While important for security, IPS rules are less likely to directly address the connectivity and certificate issues described.
? C. Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.
? D. Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.
? E. Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.
References:
? CompTIA Security+ Study Guide
? NIST SP 800-77, "Guide to IPsec VPNs"

? CIS Controls, "Control 11: Secure Configuration for Network Devices"

NEW QUESTION 37
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 42
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 43
A systems administrator wants to use existing resources to automate reporting from disparate security appliances that do not currently communicate. Which of the following is the best way to meet this objective?

A. Configuring an API Integration to aggregate the different data sets
B. Combining back-end application storage into a single, relational database
C. Purchasing and deploying commercial off the shelf aggregation software
D. Migrating application usage logs to on-premises storage

Answer: A

Explanation:
The best way to automate reporting from disparate security appliances that do not currently communicate is to configure an API Integration to aggregate the different data sets. Here's why:

? Interoperability: APIs allow different systems to communicate and share data, even
if they were not originally designed to work together. This enables the integration of various security appliances into a unified reporting system.
? Automation: API integrations can automate the process of data collection,
aggregation, and reporting, reducing manual effort and increasing efficiency.
? Scalability: APIs provide a scalable solution that can easily be extended to include
additional security appliances or data sources as needed.
? References:

NEW QUESTION 45
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 48
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 50
A security analyst is reviewing the following event timeline from an COR solution:

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

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

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

Answer: C

Explanation:
The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of- Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.
References:
? CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
? NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
? "The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

NEW QUESTION 52
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 57
An incident response team is analyzing malware and observes the following:
• Does not execute in a sandbox
• No network loCs
• No publicly known hash match
• No process injection method detected
Which of the following should the team do next to proceed with further analysis?

A. Use an online vims analysis tool to analyze the sample
B. Check for an anti-virtualization code in the sample
C. Utilize a new deployed machine to run the sample.
D. Search oilier internal sources for a new sample.

Answer: B

Explanation:
Malware that does not execute in a sandbox environment often contains anti-analysis
techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection.
Checking for anti-virtualization code is a logical next step because:
? It helps determine if the malware is designed to evade analysis tools.
? Identifying such code can provide insights into the malware's behavior and intent.
? This step can also inform further analysis methods, such as running the malware on physical hardware.
References:
? CompTIA Security+ Study Guide
? SANS Institute, "Malware Analysis Techniques"
? "Practical Malware Analysis" by Michael Sikorski and Andrew Honig

NEW QUESTION 60
A security analyst is reviewing suspicious log-in activity and sees the following data in the SICM:

Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

Which of the following is the most appropriate action for the analyst to take?

A. Update the log configuration settings on the directory server that Is not being captured properly.
B. Have the admin account owner change their password to avoid credential stuffing.
C. Block employees from logging in to applications that are not part of their business area.
D. implement automation to disable accounts that nave been associated with high-risk activity.

Answer: D

Explanation:
The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.
? Updating log configuration settings (A) may help in better logging future activities
but does not address the immediate threat.
? Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.
? Blocking employees (C) from logging into non-business applications might help in
reducing attack surfaces but doesn't directly address the compromised account issue.
Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.
References:
? CompTIA SecurityX guide on incident response and account management.
? Best practices for handling compromised accounts.
? Automation tools and techniques for security operations centers (SOCs).

NEW QUESTION 62
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 64
A security architect for a global organization with a distributed workforce recently received funding lo deploy a CASB solution Which of the following most likely explains the choice to use a proxy-based CASB?

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

Answer: A

Explanation:
A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here??s why:
? Application and Service Control: Proxy-based CASBs can monitor and control the
use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.
? Visibility and Monitoring: By routing traffic through the proxy, the CASB can
provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.
? Real-Time Protection: Proxy-based CASBs can provide real-time protection
against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.
? References:

NEW QUESTION 68
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 73
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 74
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 79
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 83
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 84
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 86
A software company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application Which of the following is the most likely cause of the alerts?

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

Answer: B

Explanation:
The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.
Why Unsecure Bundled Libraries?
? Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.
? Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.
? Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.
Other options, while relevant, are less likely to cause widespread anti-malware alerts:
? A. Misconfigured code commit: Could lead to issues but less likely to trigger anti- malware alerts.
? C. Invalid code signing certificate: Would lead to trust issues but not typically anti- malware alerts.

? D. Data leakage: Relevant for privacy concerns but not directly related to anti- malware alerts.
References:
? CompTIA SecurityX Study Guide
? "Securing Open Source Libraries," OWASP
? "Managing Third-Party Software Security Risks," Gartner Research

NEW QUESTION 87
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 88
A company lined an email service provider called my-email.com to deliver company emails. The company stalled having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmarc include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Select two).

A. The email CNAME record must be changed to a type A record pointing to 192.168.111
B. The TXT record must be Changed to "v=dmarc ip4:192.168.1.10 include:my-email.com - all"
C. The srvo1 A record must be changed to a type CNAME record pointing to the email server
D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10
E. The TXT record must be changed to "v=dkim ip4:l92.168.1.11 include my-email.com - ell"
F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"
G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

Answer: BD

Explanation:
The security engineer should modify the following to fix the email migration issues:
? Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.
? TXT Record for DMARC: The TXT record must be changed to "v=dmarc ip4:192.168.1.10 include
com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.
? uk.co.certification.simulator.questionpool.PList@488ba0cc
? References:

NEW QUESTION 91
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 94
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 99
SIMULATION
During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.
INSTRUCTIONS
Review each of the events and select the appropriate analysis and remediation options for each IoC.

IoC 1 | IoC 2 | IoC 3

```
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
```

Analysis: Select analysis

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

Remediation: Select remediation

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

IoC 1 | IoC 2 | IoC 3

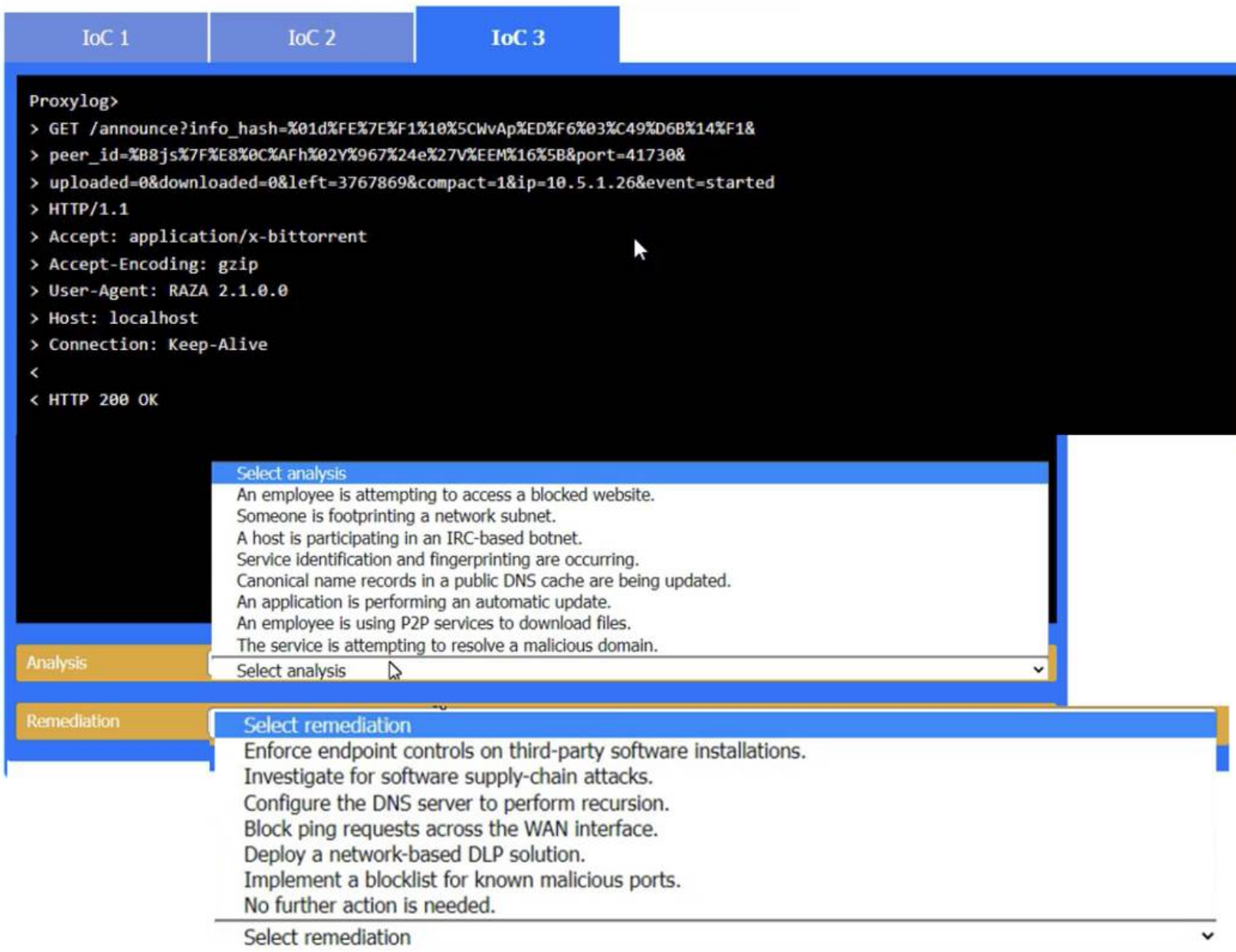
```
Src        Dst        Proto     Data   Action
10.0.5.5   10.1.2.1   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.2   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.3   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.4   IP_ICMP   ECHO   Drop
10.0.5.5   10.1.2.5   IP_ICMP   ECHO   Drop
```

Analysis: Select analysis

- 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.

Remediation: Select remediation

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



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 101
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 106
.....

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