Free Questions for CAS-005

Shared by Wells on 12-11-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

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

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

Options:

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

Answer:

B

Explanation:

The table indicates varying load times for users accessing the website from different geographic locations. Customers from Australia and India are experiencing significantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website's performance.

A . IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.

B . CDN (Content Delivery Network): A CDN stores copies of the website's content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.

C . WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.

D . NAC (Network Access Control): NAC solutions control access to network resources but are not designed to address web performance issues.

Implementing a CDN is the best solution to resolve the performance issues observed in the log output.

CompTIA Security+ Study Guide

'CDN: Content Delivery Networks Explained' by Akamai Technologies

NIST SP 800-44, 'Guidelines on Securing Public Web Servers'

Question 2

Question Type: MultipleChoice

A software company deployed a new application based on its internal code repository Several customers are reporting anti-malware alerts on workstations used to test the application Which of the following is the most likely cause of the alerts?

Options:

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

Answer:

B

Explanation:

The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.

Why Unsecure Bundled Libraries?

Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.

Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.

Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.

Other options, while relevant, are less likely to cause widespread anti-malware alerts:

A . Misconfigured code commit: Could lead to issues but less likely to trigger anti-malware alerts.

C . Invalid code signing certificate: Would lead to trust issues but not typically anti-malware alerts.

D . Data leakage: Relevant for privacy concerns but not directly related to anti-malware alerts.

CompTIA SecurityX Study Guide

'Securing Open Source Libraries,' OWASP

'Managing Third-Party Software Security Risks,' Gartner Research

Question 3

Question Type: MultipleChoice

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

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

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

Options:

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

Answer:

B

Explanation:

The table shows that the user 'SALES1' is consistently blocked despite having met the MFA requirements. The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

Geolocation Accuracy: Authentication systems often use IP geolocation to verify the location of access attempts. Incorrect geolocation data can lead to legitimate requests being denied if they appear to come from unexpected locations.

Security Policies: Company security policies might block access attempts from certain locations to prevent unauthorized access. If the geolocation is wrong, legitimate users can be inadvertently blocked.

Consistent Pattern: The user 'SALES1' from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation.

Other options do not align with the pattern observed:

A . Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue.

C . Administrator access policy: This is about user access, not specific administrator access.

D . OTP codes: The user has satisfied MFA, so OTP code configuration is not the issue.

CompTIA SecurityX Study Guide

'Geolocation and Authentication,' NIST Special Publication 800-63B

'IP Geolocation Accuracy,' Cisco Documentation

Question 4

Question Type: MultipleChoice

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

Options:

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

Answer:

C

Explanation:

To develop a baseline of security configurations that will be automatically utilized when a machine is created, the security architect should deploy Ansible. Here's why:

Automation: Ansible is an automation tool that allows for the configuration, management, and deployment of applications and systems. It ensures that security configurations are consistently applied across all new machines.

Scalability: Ansible can scale to manage thousands of machines, making it suitable for large enterprises that need to maintain consistent security configurations across their infrastructure.

Compliance: By using Ansible, organizations can enforce compliance with security policies and standards, ensuring that all systems are configured according to best practices.

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

Ansible Documentation: Best Practices

NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies

Question 5

Question Type: MultipleChoice

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

Options:

A- The HSM is outdated and no longer supported by the manufacturer
B- The vTPM was not properly initialized and is corrupt.

C- The HSM is vulnerable to common exploits and a firmware upgrade is needed
D- The motherboard was not configured with a TPM from the OEM supplier.
E- The HSM does not support sealing storage

Answer:

D

Explanation:

The most likely reason the device must be replaced is that the motherboard was not configured with a TPM (Trusted Platform Module) from the OEM (Original Equipment Manufacturer) supplier.

Why TPM is Necessary for Full Disk Encryption:

Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption.

Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that the encryption keys are securely stored and managed.

Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.

Other options do not directly address the requirement for TPM in supporting full disk encryption:

A . The HSM is outdated: While HSM (Hardware Security Module) is important for security, it is not typically used for full disk encryption.

B . The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement.

C . The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device.

E . The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption.

CompTIA SecurityX Study Guide

'Trusted Platform Module (TPM) Overview,' Microsoft Documentation

'BitLocker Deployment Guide,' Microsoft Documentation

Question 6

Question Type: MultipleChoice

SIMULATION

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

* The EAP method must use mutual certificate-based authentication (With issued client certificates).

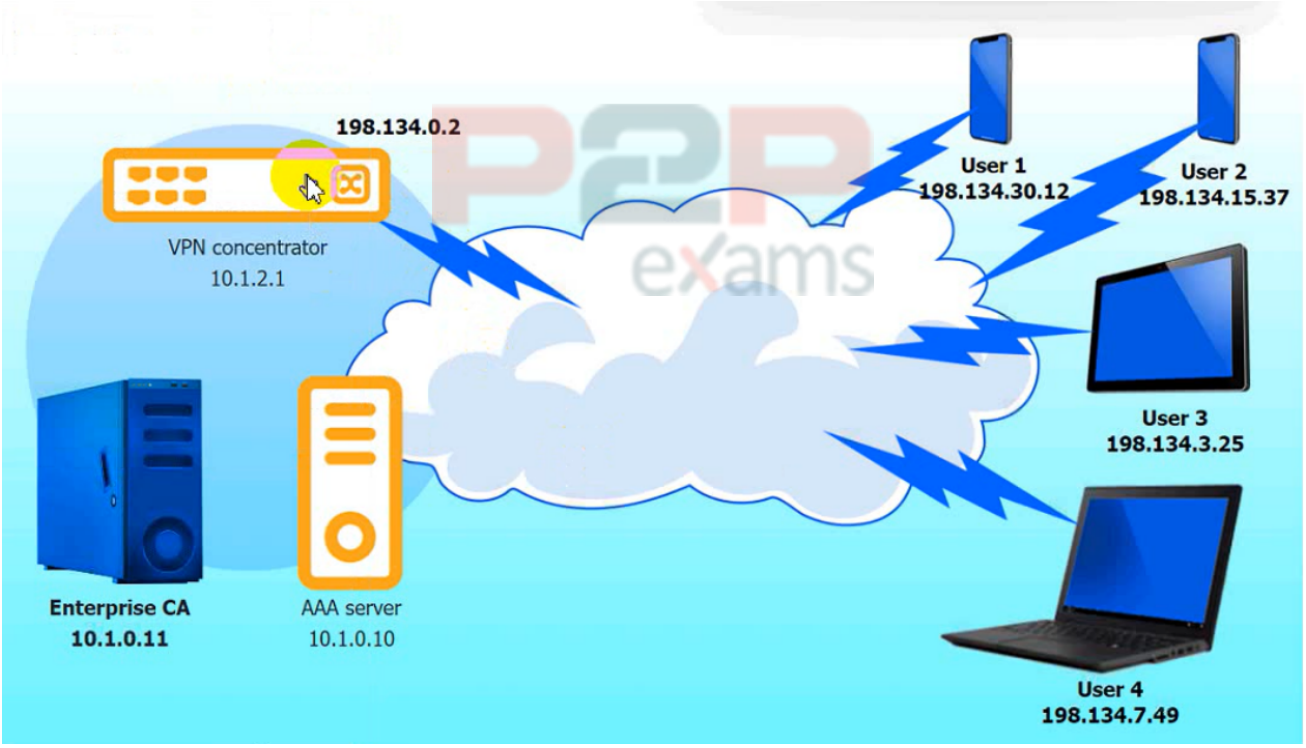
* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,

* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

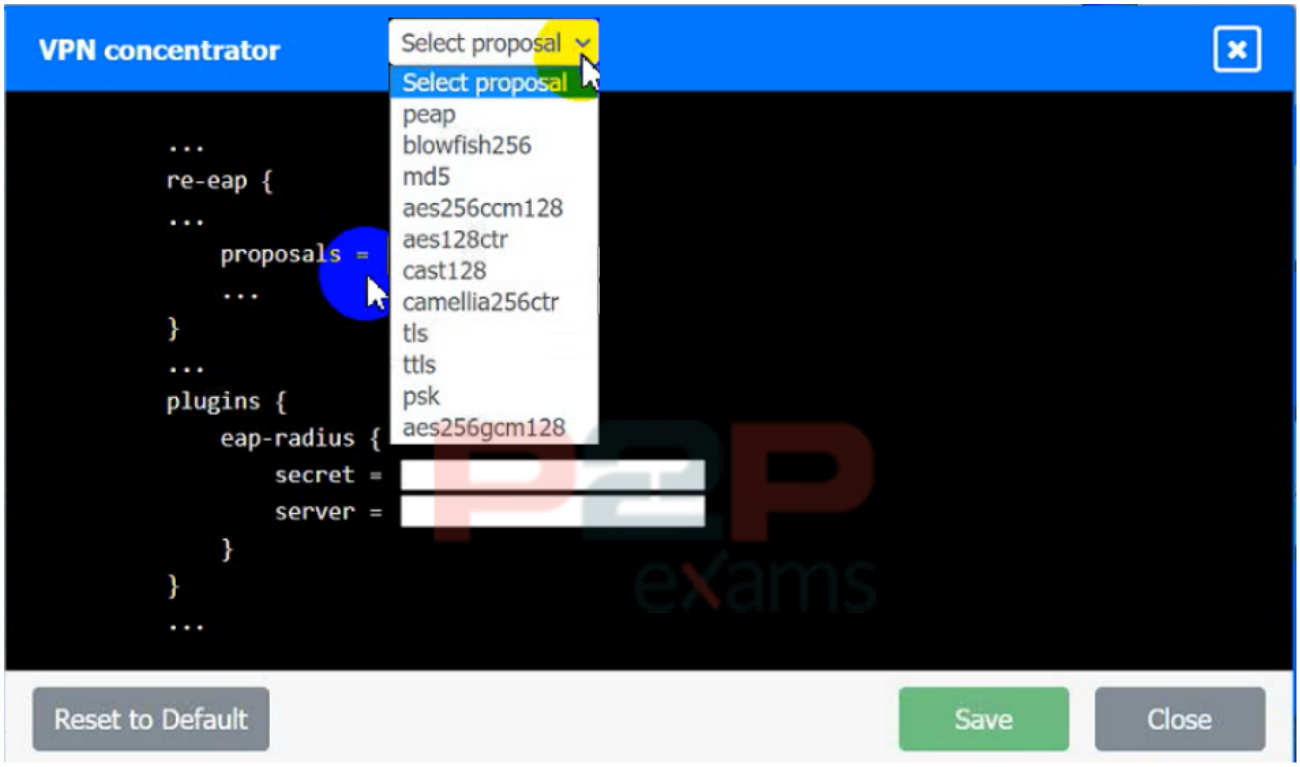
INSTRUCTIONS

Click on the AAA server and VPN concentrator to complete the configuration.

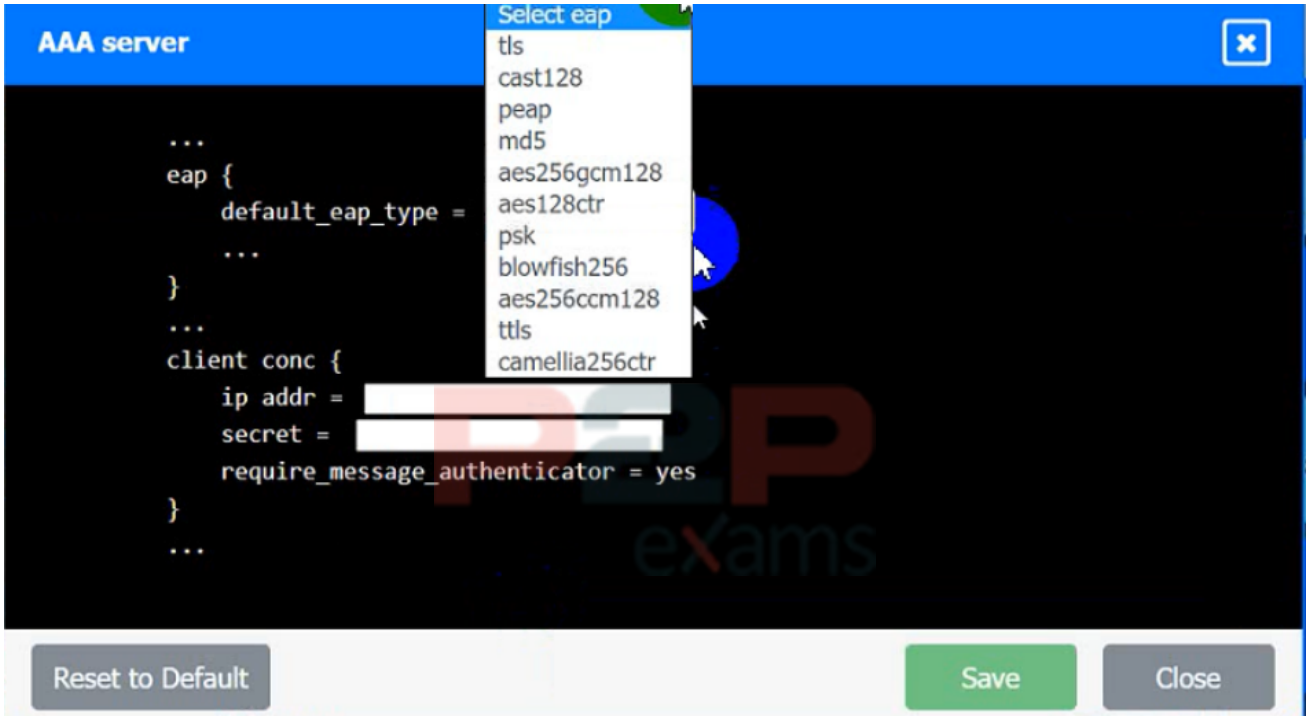
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:



Options:

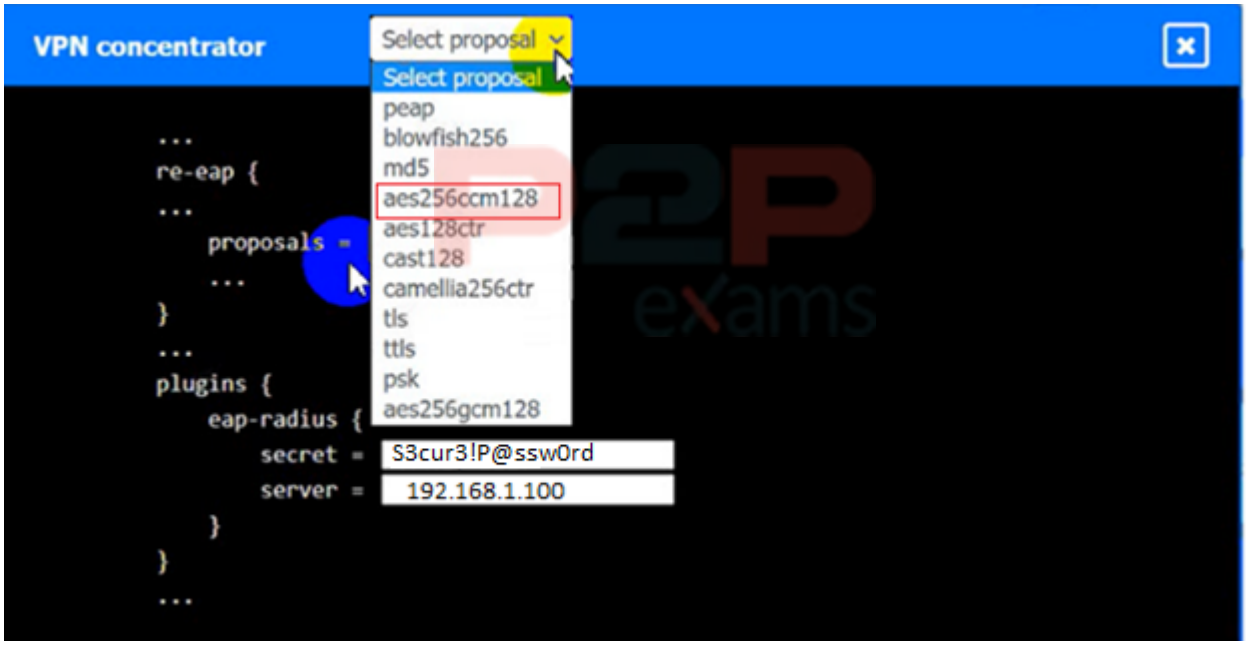
A- See the answer below in Explanation

Answer:

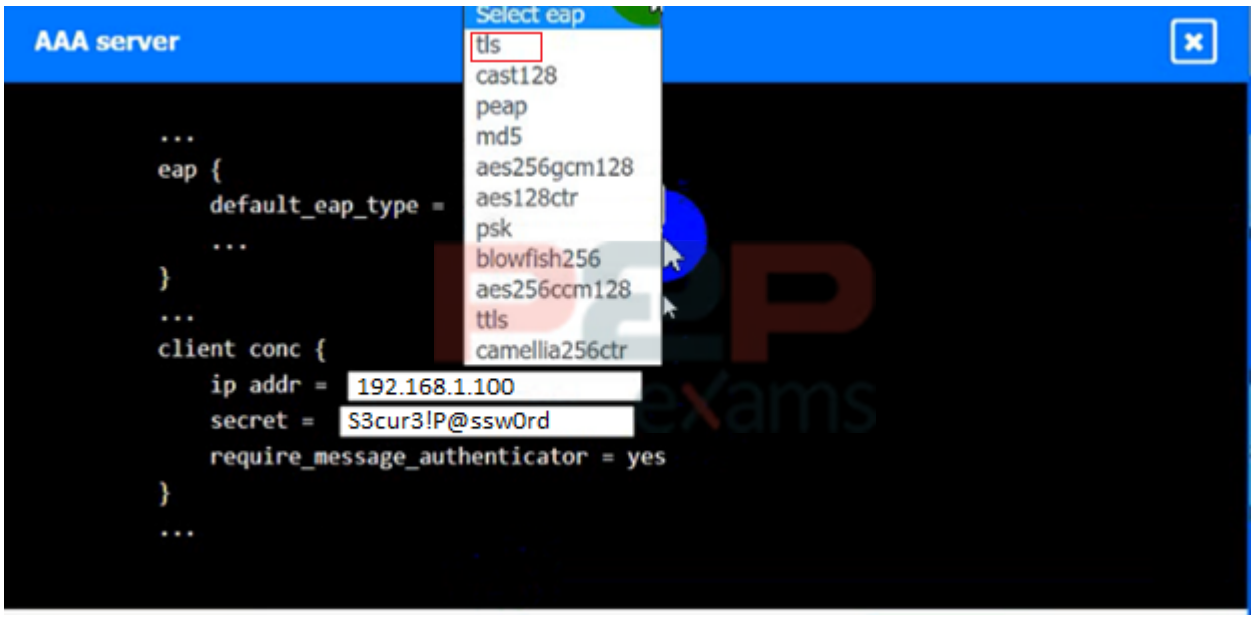
A

Explanation:

VPN Concentrator:



AAA Server:



Question 7

Question Type: MultipleChoice

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

Options:

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

Answer:

C

Explanation:

The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data.

NIST Special Publication 800-88, 'Guidelines for Media Sanitization': Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

Question 8

Question Type: MultipleChoice

The identity and access management team is sending logs to the SIEM for continuous monitoring. The deployed log collector is forwarding logs to

the SIEM. However, only false positive alerts are being generated. Which of the following is the most likely reason for the inaccurate alerts?

Options:

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

Answer:

C

Explanation:

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

Question 9

Question Type: MultipleChoice

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

Options:

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.

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies

Gartner CASB Market Guide

Question 10

Question Type: MultipleChoice

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

Options:

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

Answer:

A

Explanation:

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

crucial because:

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

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

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

CompTIA Security+ Study Guide

NIST Risk Management Framework (RMF) guidelines

ISO 31000, 'Risk Management -- Guidelines'

To Get Premium Files for CAS-005 Visit
https://www.p2pexams.com/products/cas-005

For More Free Questions Visit
https://www.p2pexams.com/comptia/pdf/cas-005