CAS-005$^{Q\&As}$

CompTIA SecurityX Exam

QUESTION 1

An organization has deployed a cloud-based application that provides virtual event services globally to clients. During a typical event, thousands of users access various entry pages within a short period of time. The entry pages include sponsor-related content that is relatively static and is pulled from a database. When the first major event occurs, users report poor response time on the entry pages. Which of the following features is the most appropriate for the company to implement?

A. Horizontal scalability

B. Vertical scalability

C. Containerization

D. Static code analysis

E. Caching

Correct Answer: E

Caching is the most appropriate feature for the company to implement in this scenario. Caching involves storing frequently accessed data closer to the user, reducing the need to retrieve data from the original source repeatedly. In the context of the virtual event services application, caching sponsor-related content on the entry pages can significantly improve response times for users. This approach leverages the static nature of the content and reduces the load on the database during peak usage times.

QUESTION 2

A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise.

Which of the following is the most secure way to achieve this goal?

A. Executing a script that deletes and overwrites all data on the SSD three times

B. Wiping the SSD through degaussing

C. Securely deleting the encryption keys used by the SSD

D. Writing non-zero, random data to all cells of the SSD

Correct Answer: C

The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively

unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

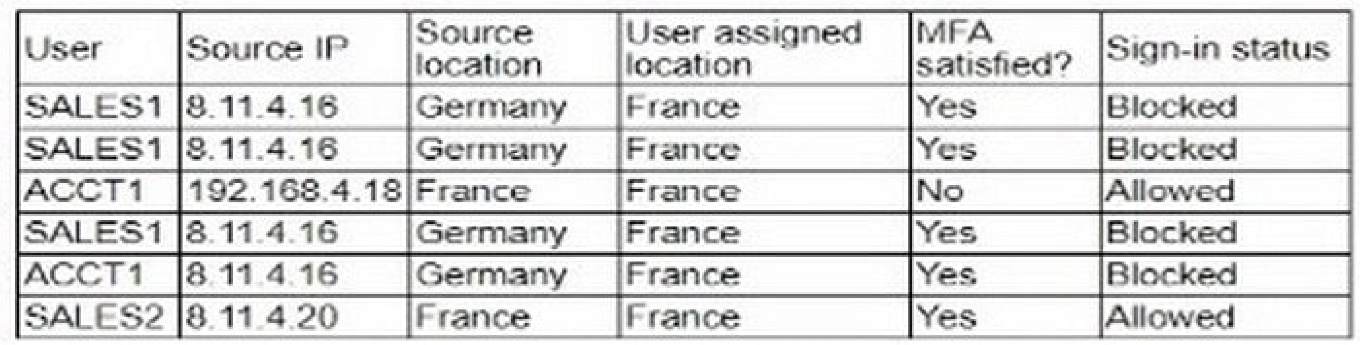
References:

CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data. NIST Special Publication 800-88, "Guidelines for Media Sanitization":

Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

QUESTION 3

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



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

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

A. The local network access has been configured to bypass MFA requirements.

B. A network geolocation is being misidentified by the authentication server

C. Administrator access from an alternate location is blocked by company policy

D. Several users have not configured their mobile devices to receive OTP codes

Correct Answer: B

The table shows that the user "SALES1" is consistently blocked despite having met the MFA requirements. The common factor in these blocked attempts is the source IP address (8.11.4.16) being identified as from Germany while the user is

assigned to France. This discrepancy suggests that the network geolocation is being misidentified by the authentication server, causing legitimate access attempts to be blocked.

Why Network Geolocation Misidentification?

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

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

"SALES1" from the IP address 8.11.4.16 is always blocked, indicating a consistent issue with geolocation. Other options do not align with the pattern observed:

A. Bypass MFA requirements: MFA is satisfied, so bypassing MFA is not the issue. C. Administrator access policy: This is about user access, not specific administrator access.

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

References:

CompTIA SecurityX Study Guide

"Geolocation and Authentication," NIST Special Publication 800-63B "IP Geolocation Accuracy," Cisco Documentation

QUESTION 4

A security architect is reviewing the following organizational specifications for a new application:

1.

Be sessionless and API-based

2.

Accept uploaded documents with PII, so all storage must be ephemeral

3.

Be able to scale on-demand across multiple nodes

4.

Restrict all network access except for the TLS port

Which of the following ways should the architect recommend the application be deployed in order to meet security and organizational infrastructure requirements?

A. Utilizing the cloud container service

B. On server instances with autoscaling groups

C. Using scripted delivery

D. With a content delivery network

Correct Answer: A

Deploying the application using a cloud container service aligns well with the specified security and organizational infrastructure requirements. It ensures sessionless, API-based operation, supports ephemeral storage for uploaded documents with PII, enables on-demand scalability across multiple nodes, and facilitates strict restriction of network access except for the TLS port.

QUESTION 5

Audit findings indicate several user endpoints are not utilizing full disk encryption During me remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption

Which of the following is the most likely reason me device must be replaced\\'

A. The HSM is outdated and no longer supported by the manufacturer

B. The vTPM was not properly initialized and is corrupt.

C. The HSM is vulnerable to common exploits and a firmware upgrade is needed

D. The motherboard was not configured with a TPM from the OEM supplier.

E. The HSM does not support sealing storage

Correct Answer: D

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

Why TPM is Necessary for Full Disk Encryption:

Hardware-Based Security: TPM provides a hardware-based mechanism to store encryption keys securely, which is essential for full disk encryption. Compatibility: Full disk encryption solutions, such as BitLocker, require TPM to ensure that

the encryption keys are securely stored and managed. Integrity Checks: TPM enables system integrity checks during boot, ensuring that the device has not been tampered with.

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

A. The HSM is outdated: While HSM (Hardware Security Module) is important for security, it is not typically used for full disk encryption. B. The vTPM was not properly initialized: vTPM (virtual TPM) is less common and not typically a reason for requiring hardware replacement. C. The HSM is vulnerable to common exploits: This would require a firmware upgrade, not replacement of the device. E. The HSM does not support sealing storage: Sealing storage is relevant but not the primary reason for requiring TPM for full disk encryption. References: CompTIA SecurityX Study Guide "Trusted Platform Module (TPM) Overview," Microsoft Documentation "BitLocker Deployment Guide," Microsoft Documentation