SY0-701$^{\text{Q\&As}}$

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in, so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?

A. Enable SAML

B. Create OAuth tokens.

C. Use password vaulting.

D. Select an IdP

Correct Answer: D

The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On

(SSO), enabling users to access multiple applications with a single set of credentials. Enabling SAML would be part of the technical implementation but comes after selecting an IdP.

OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.

Password vaulting stores multiple passwords securely but doesn\\'t reduce the need for separate logins.

QUESTION 2

A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider. Which of the following is a risk in the new system?

A. Default credentials

B. Non-segmented network

C. Supply chain vendor

D. Vulnerable software

Correct Answer: D

QUESTION 3

Which of the following best describes configuring devices to log to an off-site location for possible future reference?

A. Log aggregation

B. DLP

C. Archiving

D. SCAP

Correct Answer: A

Configuring devices to log to an off-site location for possible future reference is best described as log aggregation. Log aggregation involves collecting logs from multiple sources and storing them in a centralized location, often off-site, to

ensure they are preserved and can be analyzed in the future.

Log aggregation: Centralizes log data from multiple devices, making it easier to analyze and ensuring logs are available for future reference. DLP (Data Loss Prevention): Focuses on preventing unauthorized data transfer and ensuring data

security.

Archiving: Involves storing data for long-term retention, which could be part of log aggregation but is broader in scope.

SCAP (Security Content Automation Protocol): A standard for automating vulnerability management and policy compliance.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.4 - Explain security alerting and monitoring concepts and tools (Log aggregation).

QUESTION 4

Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

A. Risk tolerance

B. Risk transfer

C. Risk register

D. Risk analysis

Correct Answer: C

A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks.

References: CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question4.

QUESTION 5

Which of the following is an algorithm performed to verify that data has not been modified?

A. Hash

B. Code check

C. Encryption

D. Checksum

Correct Answer: A

A hash is an algorithm used to verify data integrity by generating a fixed-size string of characters from input data. If even a single bit of the input data changes, the hash value will change, allowing users to detect any modification to the data.

Hashing algorithms like SHA-256 and MD5 are commonly used to ensure data has not been altered.

References:

CompTIA Security+ SY0-701 Course Content: Domain 6: Cryptography and PKI, which discusses the role of hashing in verifying data integrity.