# SY0-701 Q&As

CompTIA Security+ 2024

**QUESTION 1**

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

A. Testing input validation on the user input fields

B. Performing code signing on company-developed software

C. Performing static code analysis on the software

D. Ensuring secure cookies are use

Correct Answer: B

Code signing is a technique that uses cryptography to verify the authenticity and integrity of the code created by the company. Code signing involves applying a digital signature to the code using a private key that only the company possesses. The digital signature can be verified by anyone who has the corresponding public key, which can be distributed through a trusted certificate authority. Code signing can prevent unauthorized modifications, tampering, or malware injection into the code, and it can also assure the users that the code is from a legitimate source.

References: CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 74. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security SY0-601 CompTIA Security+ : 3.2

**QUESTION 2**

A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.

Which of the following is the most important consideration during development?

A. Scalability

B. Availability

C. Cost

D. Ease of deployment

Correct Answer: B

Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of- service attacks, and have backup and recovery plans in case of failures2.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

**QUESTION 3**

A company wants to improve end users experiences when they tog in to a trusted partner website The company does not want the users to be issued separate credentials for the partner website

Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner\\'s website?

A. Directory service

B. AAA server

C. Federation

D. Multifactor authentication

Correct Answer: C

Federation means the company trusts accounts created and managed by a different network. It connects the identity management services of multiple systems

**QUESTION 4**

Which of the following is the best reason to complete an audit in a banking environment?

A. Regulatory requirement

B. Organizational change

C. Self-assessment requirement

D. Service-level requirement

Correct Answer: A

A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws,

standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization.

References:

Official CompTIA Security+ Study Guide (SY0-701), page 507 Security+ (Plus) Certification | CompTIA IT Certifications 2

**QUESTION 5**

Which of the following would be the best way to handle a critical business application that is running on a legacy server?

A. Segmentation

B. Isolation

C. Hardening

D. Decommissioning

Correct Answer: C

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats. One of the best ways to handle a legacy server running a critical business application is to harden it. Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as: Applying patches and updates to the operating system and the application, if available Removing or disabling unnecessary services, features, or accounts Configuring firewall rules and network access control lists to restrict inbound and outbound traffic Enabling encryption and authentication for data transmission and storage Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible.

References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems 2

Latest SY0-701 Dumps    SY0-701 PDF Dumps    SY0-701 Study Guide