CompTIA Security+ SY0-701 Practice Questions

Shared by Mccullough on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following receives logs from various devices and services, and then presents alerts?

Options:

A- SIEM
B- SCADA
C- SNMP
D- SCAP

Answer:

A

Explanation:

A SIEM (Security Information and Event Management) system aggregates logs from diverse sources, analyzes them, and generates alerts on suspicious activities. It provides centralized monitoring and incident detection.

SCADA (B) is industrial control, SNMP (C) is a protocol for network management, and SCAP (D) is a standard for security content automation.

SIEMs are foundational in Security Operations monitoring6:Chapter 14CompTIA Security+ Study Guide.

Question 2

Question Type: MultipleChoice

Which of the following metrics impacts the backup schedule as part of the BIA?

Options:

A- RTO
B- RPO

C- MTTR
D- MTBF

Answer:

B

Explanation:

Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. It directly impacts how frequently backups should occur to ensure data can be restored to a point no older than the RPO after a disruption.

Recovery Time Objective (RTO) (A) defines how quickly systems must be restored but does not dictate backup frequency. Mean Time To Repair (MTTR) (C) and Mean Time Between Failures (MTBF) (D) relate to system repair and reliability metrics, not backup schedules.

Understanding and defining RPO is a key part of the Business Impact Analysis (BIA) process covered in the Risk Management domain6:Chapter 17CompTIA Security+ Study Guide.

Question 3

Question Type: MultipleChoice

Which option best types of vulnerabilities is primarily caused by improper use and management of cryptographic certificates?

Options:

A- Misconfiguration
B- Resource reuse
C- Insecure key storage
D- Weak cipher suites

Answer:

C

Explanation:

Detailed Insecure key storage refers to vulnerabilities caused by improper handling of

cryptographic keys and certificates, such as storing them in plaintext or lacking access controls. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: 'Cryptographic Vulnerabilities and Mitigation'.

Question 4

Question Type: MultipleChoice

Which of the following data types best describes an AI tool developed by a company to automate the ticketing system under a specific contract?

Options:

A- Classified
B- Regulated information
C- Open source
D- Intellectual property

Answer:

D

Explanation:

An AI tool developed internally for automating a ticketing system represents intellectual property (IP). Security+ SY0-701 defines IP as proprietary creations developed by an organization, such as software, machine learning models, algorithms, and trade secrets. This type of data must be protected because it provides competitive advantage and is often contractually bound.

The scenario notes the tool is developed under a specific contract, meaning it is bound by ownership, licensing, and confidentiality agreements. Protecting IP is critical to prevent theft, unauthorized reuse, or compromise that could affect legal obligations or business value.

Classified (A) refers to government-protected national security information. Regulated information (B) includes data covered by laws such as HIPAA or PCI-DSS. Open source (C) refers to publicly shared code, which this AI tool is not.

Thus, the correct category for this data is D: Intellectual property.

Question 5

Question Type: MultipleChoice

Which of the following types of identification methods can be performed on a deployed application during runtime?

Options:

A- Dynamic analysis
B- Code review
C- Package monitoring
D- Bug bounty

Answer:

A

Explanation:

Dynamic analysis is performed on software during execution to identify vulnerabilities based on how the software behaves in real-world scenarios. It is useful in detecting security issues that only appear when the application is running.Reference: CompTIA SY0-701 Course Content.

Question 6

Question Type: MultipleChoice

Which of the following would be the most appropriate way to protect data in transit?

Options:

A- SHA-256
B- SSL 3.0
C- TLS 1.3
D- AES-256

Answer:

C

Question 7

Question Type: MultipleChoice

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

Options:

A- Fines
B- Audit findings
C- Sanctions
D- Reputation damage

Answer:

A

Explanation:

PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.

If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. An internal PCI DSS compliance assessment is a self-assessment that the bank performs to evaluate its own compliance with the PCI DSS requirements. The bank must submit the results of the internal assessment to the payment card brands or their designated agents, such as acquirers or qualified security assessors (QSAs). If the internal assessment reveals that the bank is not compliant with the PCI DSS requirements, the payment card brands may impose fines on the bank as a penalty for violating the PCI DSS contract. The amount and frequency of the fines may vary depending on the severity and duration of the non-compliance, the number and type of cardholder data compromised, and the level of cooperation and remediation from the bank. The fines can range from thousands to millions of dollars per month, and can increase over time if the non-compliance is not resolved.

The other options are not correct because they are not the most likely outcomes if a large bank fails an internal PCI DSS compliance assessment. B. Audit findings. Audit findings are the

results of an external PCI DSS compliance assessment that is performed by a QSA or an approved scanning vendor (ASV). An external assessment is required for certain entities that handle a large volume of cardholder data or have a history of non-compliance. An external assessment may also be triggered by a security incident or a request from the payment card brands. Audit findings may reveal the gaps and weaknesses in the bank's security controls andrecommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself. C. Sanctions. Sanctions are the measures that the payment card brands may take against the bank if the bank fails to pay the fines or comply with the PCI DSS requirements. Sanctions may include increasing the fines, suspending or terminating the bank's ability to accept or process payment cards, or revoking the bank's PCI DSS certification. Sanctions are not the immediate outcome of an internal assessment, but rather the possible consequence of prolonged or repeated non-compliance. D. Reputation damage. Reputation damage is the loss of trust and credibility that the bank may suffer from its customers, partners, regulators, and the public if the bank fails an internal PCI DSS compliance assessment. Reputation damage may affect the bank's brand image, customer loyalty, market share, and profitability. Reputation damage is not a direct outcome of an internal assessment, but rather a potential risk that the bank may face if the non-compliance is exposed or exploited by malicious actors.Reference: =CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 388.Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: PCI DSS (5:12).PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4.PCI Security Standards Council, PCI DSS FAQs, question 8.PCI Security Standards Council, PCI DSS FAQs, question 9. [PCI Security Standards Council], PCI DSS FAQs, question 10. [PCI Security Standards Council], PCI DSS FAQs, question 11. [PCI Security Standards Council], PCI DSS FAQs, question 12. [PCI Security Standards Council], PCI DSS FAQs, question 13. [PCI Security Standards Council], PCI DSS FAQs, question 14. [PCI Security Standards Council], PCI DSS FAQs, question 15. [PCI Security Standards Council], PCI DSS FAQs, question 16. [PCI Security Standards Council], PCI DSS FAQs, question 17. [PCI Security Standards Council], PCI DSS FAQs, question 18. [PCI Security Standards Council], PCI DSS FAQs, question 19. [PCI Security Standards Council], PCI DSS FAQs, question 20. [PCI Security Standards Council], PCI DSS FAQs, question 21. [PCI Security Standards Council], PCI DSS FAQs, question 22. [PCI Security Standards Council], PCI DSS FAQs, question 23. [PCI Security Standards Council], PCI DSS FAQs, question 24. [PCI Security Standards Council], PCI DSS FAQs, question 25. [PCI Security Standards Council], PCI DSS FAQs, question 26. [PCI Security Standards Council], PCI DSS FAQs, question 27. [PCI Security Standards Council], PCI DSS FAQs, question 28. [PCI Security Standards Council], PCI DSS FAQs, question 29. [PCI Security Standards Council], PCI DSS FAQs, question 30. [PCI Security Standards Council]

Question 8

Question Type: MultipleChoice

Which option best organizational documents is most often used to establish and communicate expectations associated with integrity and ethical behavior within an organization?

Options:

A- AUP
B- SLA
C- EULA
D- MOA

Answer:

A

Question 9

Question Type: MultipleChoice

An unexpected and out-of-character email message from a Chief Executive Officer's corporate account asked an employee to provide financial information and to change the recipient's contact number. Which of the following attack vectors is most likely being used?

Options:

A- Business email compromise
B- Phishing
C- Brand impersonation
D- Pretexting

Answer:

A

Explanation:

Business Email Compromise (BEC)is atargeted phishing attackin whichattackers impersonate executives or high-ranking officials(such as a CEO) to manipulate employees intotransferring money or providing sensitive data. Since the request is coming from the CEO's corporate email (possibly spoofed or compromised), this is aclassic example of BEC.

Phishing (B)is a broader term but typically involvesmassfraudulent emails rather than targeted executive impersonation.

Brand impersonation (C)involves faking a company's identity (e.g., fake PayPal emails).

Pretexting (D)involves social engineering tactics but does not necessarily involve email compromise.

Question 10

Question Type: MultipleChoice

Which of the following is most likely associated with introducing vulnerabilities on a corporate network by the deployment of unapproved software?

Options:

A- Hacktivists
B- Script kiddies
C- Competitors
D- Shadow IT

Answer:

D

Explanation:

Shadow IT refers to the use of information technology systems, devices, software, applications, and services without explicit IT department approval. This is the most likely cause of introducing vulnerabilities on a corporate network by deploying unapproved software, as such software may not have been vetted for security compliance, increasing the risk of vulnerabilities.

CompTIA Security+ SY0-701 Course Content: The concept of Shadow IT is discussed as a significant risk due to the introduction of unapproved and potentially vulnerable software into the corporate network.