



**CertsMania**



**CertsMania**

## **Free Questions for SY0-701**

**Shared by Marisol on Apr 26, 2026**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**



**CertsMania**

## Questions # 1:

Which of the following is used to validate a certificate when it is presented to a user?

### Options:

A.

OCSP

B.

CSR

C.

CA

D.

CRC



CertsMania

### Answer

A

### Explanation

OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA). References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 337 1

## Questions # 2:

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

**Options:**

A.

Compromise

B.

Retention

C.

Analysis

D.

Transfer

E.

Inventory



CertsMania

**Answer**

B

**Explanation**

A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.

References

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211

CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832



CertsMania

Questions # 3:

Which of the following describes the difference between encryption and hashing?

**Options:**

A.

Encryption protects data in transit, while hashing protects data at rest.

B.

Encryption replaces cleartext with ciphertext, while hashing calculates a checksum.

C.

Encryption ensures data integrity, while hashing ensures data confidentiality.

D.

Encryption uses a public-key exchange, while hashing uses a private key.

**Answer**

B

**Explanation**

Encryption is a reversible process that transforms cleartext data into ciphertext to protect confidentiality. It uses cryptographic keys to both encrypt and decrypt data, ensuring that only authorized parties can access the original data.

Hashing, on the other hand, is a one-way function that converts data into a fixed-length hash value or checksum. Hashing is primarily used to verify data integrity by detecting changes, since any modification in the input will produce a different hash output. Unlike encryption, hashing cannot be reversed to obtain the original data.

While encryption can protect data both at rest and in transit, hashing does not protect data confidentiality but supports integrity verification. Public-key exchange is a cryptographic mechanism within asymmetric encryption but is unrelated to hashing key usage.

This distinction is thoroughly explained in the Cryptography chapter of the SY0-701 syllabus [6:Chapter 7†CompTIA Security+ Study Guide].

**Questions # 4:**

Which of the following provides the details about the terms of a test with a third-party penetration tester?

**Options:**

A.

Rules of engagement

B.

Supply chain analysis

C.

Right to audit clause

D.

Due diligence



CertsMania

**Answer**

A

**Explanation**

Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:

The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.

The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.

The testing team credentials and the authorized tools and techniques that they can use.

The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.

The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.

The timeline and duration of the test, and the hours of operation and testing windows.

The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.

Supply chain analysis, right to audit clause, and due diligence are not related to the terms

of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.

References =

<https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of-engagement/>

<https://bing.com/search?q=rules+of+engagement+penetration+testing>

#### Questions # 5:

An employee used a company ' s billing system to issue fraudulent checks. The administrator is looking for evidence of other occurrences of this activity. Which of the following should the administrator examine?

#### Options:

A.

Application logs

B.

Vulnerability scanner logs

C.

IDS/IPS logs

D.

Firewall logs

#### Answer

A

#### Questions # 6:

Which of the following can be used to identify potential attacker activities without affecting production servers?

**Options:**

A.

Honey pot

B.

Video surveillance

C.

Zero Trust

D.

Geofencing



CertsMania

**Answer**

A

**Explanation**

A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker's methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker's attention from the real targets and waste their time and resources<sup>12</sup>.

The other options are not effective ways to identify potential attacker activities without affecting production servers:

Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker's activities on the network or the servers<sup>3</sup>.

Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker's activities on the network or the servers<sup>4</sup>.

Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data

sovereignty and compliance of an organization, but it does not directly identify the attacker's activities on the network or the servers<sup>5</sup>.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honeypots and Deception - SY0-601 CompTIA Security+ : 2.1, video by Professor Messer<sup>3</sup>: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985: CompTIA Security+ SY0-701 Certification Study Guide, page 99.

## Questions # 7:

Cadets speaking a foreign language are using company phone numbers to make unsolicited phone calls to a partner organization. A security analyst validates through phone system logs that the calls are occurring and the numbers are not being spoofed. Which of the following is the most likely explanation?

### Options:

A.

The executive team is traveling internationally and trying to avoid roaming charges

B.

The company's SIP server security settings are weak.

C.

Disgruntled employees are making calls to the partner organization.

D.

The service provider has assigned multiple companies the same numbers

### Answer

B

### Explanation

If cadets are using company phone numbers to make unsolicited calls, and the logs confirm the numbers are not being spoofed, it suggests that the SIP (Session Initiation Protocol) server's security settings might be weak. This could allow unauthorized access or exploitation of the company's telephony services, potentially leading to misuse by unauthorized individuals.

References = CompTIA Security+ SY0-701 study materials, especially on SIP security and common vulnerabilities.

### Questions # 8:

Which of the following is most likely to be used as a just-in-time reference document within a security operations center?

#### Options:

A.

Change management policy

B.

Risk profile

C.

Playbook

D.

SIEM profile

#### Answer

C

#### Explanation

Comprehensive and Detailed Explanation From Exact Extract:

A playbook is a step-by-step, just-in-time reference used by Security Operations Center (SOC) analysts when responding to security alerts, incidents, and suspicious activities. Playbooks provide documented procedures for common scenarios such as malware detection, phishing investigations, ransomware response, and account compromise.

According to the CompTIA Security+ SY0-701 exam framework, playbooks support incident response by reducing analyst guesswork and ensuring consistency. They include details such as triage steps, required tools, escalation paths, log sources, and containment actions. This makes playbooks the most suitable document for immediate reference during live investigations.

Change management policies (A) govern system or configuration changes, not SOC

operations. Risk profiles (B) provide organizational risk overviews, not incident-response steps. SIEM profiles (D) define correlation rules or dashboards but are not procedural guides.

Therefore, the correct answer is playbooks, which enable efficient, standardized, and repeatable responses to operational security events.

#### Questions # 9:

Which of the following will harden access to a new database system? (Select two)

#### Options:

A.

Jump server

B.

NIDS

C.

Monitoring

D.

Proxy server

E.

Host-based firewall

F.

WAF

#### Answer

A, E

#### Explanation

Hardening access to a new database system requires implementing controls that restrict and secure how administrators and applications connect to the database. A jump server (A) is a hardened intermediary system used to manage access to sensitive systems such

as databases. By forcing administrators to authenticate through a controlled, monitored jump host instead of connecting directly, organizations reduce attack surfaces and prevent unauthorized lateral movement. Security+ SY0-701 identifies jump servers as critical in securing high-value systems.

A host-based firewall (E) provides system-level traffic filtering directly on the database server. It allows only trusted IPs, ports, and services to communicate with the database, significantly reducing exposure. This is an essential hardening measure because databases should only accept connections from specific application servers or administrative hosts.

NIDS (B) monitors traffic but does not harden access. Monitoring (C) provides visibility but does not restrict access. A proxy server (D) is not typically used for database access. A WAF (F) protects web applications, not internal database systems.

Thus, A (Jump server) and E (Host-based firewall) are the correct hardening controls.

#### Questions # 10:

While investigating a recent security breach an analyst finds that an attacker gained access by SQL injection through a company website. Which of the following should the analyst recommend to the website developers to prevent this from reoccurring?

#### Options:

- A.  
Secure cookies
- B.  
Input sanitization
- C.  
Code signing
- D.  
Blocklist

#### Answer

B

## Explanation

Input sanitization is a critical security measure to prevent SQL injection attacks, which occur when an attacker exploits vulnerabilities in a website 's input fields to execute malicious SQL code. By properly sanitizing and validating all user inputs, developers can prevent malicious code from being executed, thereby securing the website against such attacks.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common vulnerability mitigation strategies.

## Questions # 11:

A service provider wants a cost-effective way to rapidly expand from providing internet links to managing them. Which of the following methods will allow the service provider to best scale its services while maintaining performance consistency?

### Options:

A.

Escalation support

B.

Increased workforce

C.

Baseline enforcement

D.

Technical debt

## Answer

C

## Explanation

Baseline enforcement involves establishing standard configurations and operational baselines that allow a service provider to scale services efficiently while ensuring consistent performance and security. By enforcing baselines, automation can be applied, reducing manual intervention and variability, which supports rapid, cost-effective

expansion.

Increasing workforce (B) adds operational cost and may introduce inconsistency. Escalation support (A) is reactive and does not inherently support scaling. Technical debt (D) refers to accumulated suboptimal design or quick fixes that hamper future scalability and is a negative factor.

Baseline enforcement is recognized as a best practice in the Security Program Management domain for scaling services reliably [6:Chapter 16†CompTIA Security+ Study Guide].



CertsMania

### Questions # 12:

Which of the following must be considered when designing a high-availability network? (Choose two).

#### Options:

A.

Ease of recovery

B.

Ability to patch

C.

Physical isolation

D.

Responsiveness

E.

Attack surface

F.

Extensible authentication



CertsMania

#### Answer

A, E

## Explanation

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors<sup>12</sup>:

**Ease of recovery:** This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.

**Attack surface:** This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.

The other options are not directly related to high-availability network design:

**Ability to patch:** This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.

**Physical isolation:** This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.

**Responsiveness:** This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.

**Extensible authentication:** This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer.

### Questions # 13:

An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as \$, |, ;, &

, ` , and ? from variables set by forms in a web application.

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

**Options:**

A.

Identify embedded keys

B.

Code debugging

C.

Input validation

D.

Static code analysis



CertsMania

**Answer**

C

**Explanation**

Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as \$, |, ;, &, ` , and ?, can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.

Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a

process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security - SY0-601 CompTIA Security+ : 3.2, 0:00 - 2:00.

#### Questions # 14:

A growing company would like to enhance the ability of its security operations center to detect threats but reduce the amount of manual work required for the security analysts. Which of the following would best enable the reduction in manual work?

#### Options:

A.

SOAR

B.

SIEM

C.

MDM

D.

DLP

#### Answer

A

#### Explanation

Security Orchestration, Automation, and Response (SOAR) systems help organizations automate repetitive security tasks, reduce manual intervention, and improve the efficiency of security operations. By integrating with various security tools, SOAR can automatically respond to incidents, helping to enhance threat detection while reducing the manual workload on security analysts.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of

security operations and automation technologies.

### Questions # 15:

Which of the following agreements defines response time, escalation points, and performance metrics?



CertsMania

#### Options:

- A.  
BPA
- B.  
MOA
- C.  
NDA
- D.  
SLA

#### Answer

D

#### Explanation

A Service Level Agreement (SLA) defines the expectations between service providers and customers, including response times, escalation procedures, and performance metrics. It ensures accountability and measurable service quality.

BPA (Blanket Purchase Agreement) relates to purchasing terms, MOA (Memorandum of Agreement) outlines responsibilities but is less specific on performance, NDA (Non-Disclosure Agreement) covers confidentiality.

SLAs are key in Security Program Management for managing vendor and internal service expectations [6:Chapter 16†CompTIA Security+ Study Guide].

### Questions # 16:

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following best describes the user's activity?

**Options:**

- A.  
Penetration testing
- B.  
Phishing campaign
- C.  
External audit
- D.  
Insider threat



CertsMania

**Answer**

D

**Explanation**

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data. References = Insider Threats - CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

Questions # 17:

A software developer wishes to implement an application security technique that will provide

assurance of the application ' s integrity. Which of the following techniques will achieve this?

**Options:**

- A.  
Secure cookies
- B.  
Input validation
- C.  
Static analysis
- D.  
Code signing



CertsMania

**Answer**

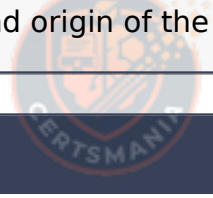
D

**Explanation**

Code signing (D) uses cryptographic digital signatures to confirm the integrity and authenticity of software code. It ensures that the code has not been altered after being signed, providing assurance that the application is trustworthy.

This aligns with CompTIA Security+ SY0-701 Domain 2.3: Application security techniques, which includes code signing as a method to validate code integrity.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.3 - "Code signing: Validates integrity and origin of the software." , , , , , , , , , ]



CertsMania

Questions # 18:

During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

**Options:**

- A.  
Analysis

B.

Lessons learned

C.

Detection

D.

Containment



CertsMania

## Answer

A

## Explanation

Analysis is the incident response activity that describes the process of understanding the source of an incident. Analysis involves collecting and examining evidence, identifying the root cause, determining the scope and impact, and assessing the threat actor's motives and capabilities. Analysis helps the incident response team to formulate an appropriate response strategy, as well as to prevent or mitigate future incidents. Analysis is usually performed after detection and before containment, eradication, recovery, and lessons learned. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 223. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.2, page 13.

## Questions # 19:

Which of the following is a reason why a forensic specialist would create a plan to preserve data after an incident and prioritize the sequence for performing forensic analysis?

### Options:

A.

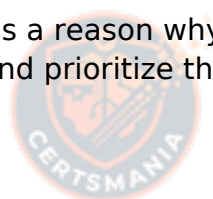
Order of volatility

B.

Preservation of event logs

C.

Chain of custody



CertsMania

D.

Compliance with legal hold

## Answer

A

## Explanation



CertsMania

When conducting a forensic analysis after an incident, it ' s essential to prioritize the data collection process based on the " order of volatility. " This principle dictates that more volatile data (e.g., data in memory, network connections) should be captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.

References =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Digital Forensics.

## Questions # 20:

A company evaluates several options that would allow employees to have remote access to the network. The security team wants to ensure the solution includes AAA to comply with internal security policies. Which of the following should the security team recommend?

## Options:

A.

IPSec with RADIUS



CertsMania

B.

RDP connection with LDAPS

C.

Web proxy for all remote traffic

D.

Jump server with 802.1X

## Answer

A

### Questions # 21:

An attacker submits a request containing unexpected characters in an attempt to gain unauthorized access to information within the underlying systems. Which of the following best describes this attack?

#### Options:

A.

Side loading

B.

Target of evaluation

C.

Resource reuse

D.

SQL injection

## Answer

D

### Questions # 22:

Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?

#### Options:

A.

Reporting structure for the data privacy officer

B.

Request process for data subject access

C.

Role as controller or processor

D.

Physical location of the company



CertsMania

## Answer

C

## Explanation

The most important consideration when establishing a data privacy program is defining the organization ' s role as a controller or processor. These roles, as outlined in privacy regulations such as the General Data Protection Regulation (GDPR), determine the responsibilities regarding the handling of personal data. A controller is responsible for determining the purpose and means of data processing, while a processor acts on behalf of the controller. This distinction is crucial for compliance with data privacy laws.

Reporting structure for the data privacy officer is important, but it is a secondary consideration compared to legal roles.

Request process for data subject access is essential for compliance but still depends on the organization ' s role as controller or processor.

Physical location of the company can affect jurisdiction, but the role as controller or processor has a broader and more immediate impact.

Questions # 23:



CertsMania

Which of the following is the most likely to be included as an element of communication in a security awareness program?

## Options:

A.

Reporting phishing attempts or other suspicious activities

B.

Detecting insider threats using anomalous behavior recognition

C.

Verifying information when modifying wire transfer data

D.

Performing social engineering as part of third-party penetration testing

## Answer

A

## Explanation

A security awareness program is a set of activities and initiatives that aim to educate and inform the users and employees of an organization about the security policies, procedures, and best practices. A security awareness program can help to reduce the human factor in security risks, such as social engineering, phishing, malware, data breaches, and insider threats. A security awareness program should include various elements of communication, such as newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms, to deliver the security messages and reinforce the security culture. One of the most likely elements of communication to be included in a security awareness program is reporting phishing attempts or other suspicious activities, as this can help to raise the awareness of the users and employees about the common types of cyberattacks and how to respond to them. Reporting phishing attempts or other suspicious activities can also help to alert the security team and enable them to take appropriate actions to prevent or mitigate the impact of the attacks. Therefore, this is the best answer among the given options.

The other options are not as likely to be included as elements of communication in a security awareness program, because they are either technical or operational tasks that are not directly related to the security awareness of the users and employees. Detecting insider threats using anomalous behavior recognition is a technical task that involves using security tools or systems to monitor and analyze the activities and behaviors of the users and employees and identify any deviations or anomalies that may indicate malicious or unauthorized actions. This task is usually performed by the security team or the security operations center, and it does not require the communication or participation of the users and employees. Verifying information when modifying wire transfer data is an operational task that involves using verification methods, such as phone calls, emails, or digital signatures, to confirm the authenticity and accuracy of the information related to wire transfers, such as the account number, the amount, or the recipient. This task is usually performed by the financial or accounting department, and it does not involve the security awareness of the users and employees. Performing social engineering as part of third-party penetration testing is a technical task that involves using deception or manipulation techniques, such as phishing, vishing, or impersonation, to test the security posture and the vulnerability of the users and employees to social engineering attacks. This task is usually performed by external security professionals or consultants, and it does

not require the communication or consent of the users and employees. Therefore, these options are not the best answer for this question. References = Security Awareness and Training - CompTIA Security+ SY0-701: 5.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 263.

#### Questions # 24:

Which of the following aspects of the data management life cycle is most directly impacted by local and international regulations?

#### Options:

A.

Destruction

B.

Certification

C.

Retention

D.

Sanitization

#### Answer

C

#### Explanation

Detailed Explanation:

Retention policies dictate how long data must be stored to comply with local and international regulations. Non-compliance can result in legal and financial penalties. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: " Data Retention and Legal Requirements " .

#### Questions # 25:

A penetration tester visits a client's website and downloads the site's content. Which of the following actions is the penetration tester performing?

**Options:**

A.

Unknown environment testing

B.

Vulnerability scan

C.

Due diligence

D.

Passive reconnaissance



CertsMania

**Answer**

D

**Explanation**

Comprehensive and Detailed Explanation From Exact Extract:

The described activity—visiting a website and downloading publicly accessible content—is a classic example of passive reconnaissance. Passive reconnaissance involves gathering information about a target without interacting with its internal systems or generating traffic that could be detected by security monitoring tools.

According to SY0-701, passive recon uses open-source intelligence (OSINT), such as:

Public websites

DNS records

News articles

Metadata

Public document repositories

The key distinction is that passive reconnaissance does not probe the system for vulnerabilities, nor does it send active scanning traffic.

Vulnerability scanning (B) requires active probing. Unknown environment testing (A) applies to black-box testing but still may involve active scanning. Due diligence (C) refers to risk assessment or compliance reviews, not technical reconnaissance.

Therefore, downloading the website's content is a non-intrusive information-gathering technique, perfectly matching passive reconnaissance as defined in the exam materials under Threats, Vulnerabilities, Attack Vectors, and Pen Testing Phases.

#### Questions # 26:

Which of the following architectures is most suitable to provide redundancy for critical business processes?

#### Options:

- A.  
Network-enabled
- B.  
Server-side
- C.  
Cloud-native
- D.  
Multitenant

#### Answer

C

#### Questions # 27:

An organization is implementing a COPE mobile device management policy. Which of the following should the organization include in the COPE policy? (Select two).

**Options:**

A.

Remote wiping of the device

B.

Data encryption

C.

Requiring passwords with eight characters

D.

Data usage caps

E.

Employee data ownership

F.

Personal application store access

**Answer**

A, B

Questions # 28:

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?

**Options:**

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

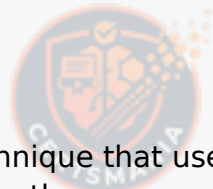
D.

Ensuring secure cookies are use

## Answer

B

## Explanation



# CertsMania

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

## Questions # 29:

During a SQL update of a database, a temporary field used as part of the update sequence was modified by an attacker before the update completed in order to allow access to the system. Which of the following best describes this type of vulnerability?

### Options:

A.

Race condition

B.

Memory injection

C.

Malicious update

D.

Side loading



# CertsMania

## Answer

A

## Explanation

A race condition occurs when two or more processes attempt to access and modify a shared resource simultaneously, leading to unintended behavior. In this scenario, the attacker was able to modify a temporary field before the SQL update completed, indicating a time-of-check to time-of-use (TOCTOU) vulnerability, which is a type of race condition.

Memory injection (B) refers to inserting malicious code into a running process's memory, but that is not what is happening here.

Malicious update (C) is too broad and does not specifically describe this scenario.

Side loading (D) is a technique where malicious software is loaded via a trusted application, unrelated to this case.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain., , , , , , , , , ]

## Questions # 30:

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

### Options:

A.

Concurrent session usage

B.

Secure DNS cryptographic downgrade

C.

On-path resource consumption

D.

Reflected denial of service

## Answer

D

## Explanation

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

## Questions # 31:

Which of the following describes the procedures a penetration tester must follow while conducting a test?

### Options:

A.

Rules of engagement

B.

Rules of acceptance

C.

Rules of understanding

D.

Rules of execution



CertsMania

## Answer

A

## Explanation

Detailed Explanation: Rules of engagement specify the agreed-upon boundaries, scope, and procedures for a penetration test to ensure compliance and avoid disruption to the environment. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: " Penetration Testing Procedures " .

## Questions # 32:

Which of the following security controls would best guard a payroll system against insider manipulation threats?

### Options:

A.

Compensating

B.

Deterrent

C.

Detective

D.

Corrective

## Answer

C

### Explanation

Detective controls (such as audit logs, monitoring, and alerts) are specifically designed to identify and reveal unauthorized or malicious activity, including insider manipulation, in systems like payroll. These controls help ensure that any attempts to manipulate data are discovered and investigated.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 3.3: "Detective controls monitor and identify violations or malicious activity after they have occurred.", Exam Objectives 3.3: "Summarize various security control types and methods.", , , , , , , , , , ]

### Questions # 33:

Which of the following is a type of vulnerability that involves inserting scripts into web-based applications in order to take control of the client ' s web browser?

#### Options:

- A.  
SQL injection
- B.  
Cross-site scripting
- C.  
Zero-day exploit
- D.  
On-path attack



CertsMania

#### Answer

B

#### Explanation

Cross-site scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into a website, which are then executed in the user's web browser, potentially leading to data theft or session hijacking. References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

### Questions # 34:

The internal audit team determines a software application is no longer in scope for external reporting requirements. Which of the following will confirm management's perspective that the application is no longer applicable?

**Options:**

A.

Data inventory and retention

B.

Right to be forgotten

C.

Due care and due diligence

D.

Acknowledgement and attestation



CertsMania

**Answer**

D

**Explanation**

Acknowledgement and attestation involve formal confirmation that an application is no longer in scope for compliance, auditing, or reporting requirements. This typically includes documentation signed by relevant stakeholders confirming that the software no longer processes, stores, or transmits relevant data.

Data inventory and retention (A) is related to managing data assets, not software scope confirmation.

Right to be forgotten (B) pertains to privacy laws (e.g., GDPR), allowing individuals to request data deletion.

Due care and due diligence (C) focus on security best practices rather than software applicability.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain., , , , , , , , , ]

**Questions # 35:**

Which of the following is a type of vulnerability that may result from outdated algorithms or keys?

**Options:**

A.

Hash collision

B.

Cryptographic

C.

Buffer overflow

D.

Input validation



CertsMania

**Answer**

B

**Explanation**

A cryptographic vulnerability refers to weaknesses caused by the use of outdated or insecure cryptographic algorithms, protocols, or keys. These vulnerabilities make it easier for attackers to compromise encrypted data or communications. Use of deprecated ciphers or insufficient key lengths are typical examples.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Cryptographic vulnerabilities arise from the use of weak or outdated cryptographic algorithms or keys.", Exam Objectives 2.3: "Analyze potential indicators associated with network attacks.", , , , , , , , ]

Questions # 36:

A company implemented an MDM policy to mitigate risks after repeated instances of employees losing company-provided mobile phones. In several cases, the lost phones were used maliciously to perform social engineering attacks against other employees. Which of the following MDM features should be configured to best address this issue? (Select two).

**Options:**

A.

Screen locks

B.

Remote wipe

C.

Full device encryption

D.

Push notifications

E.

Application management

F.

Geolocation



CertsMania

## Answer

A, B

## Explanation

Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.

References =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

## Questions # 37:

A security analyst sees an increase of vulnerabilities on workstations after a deployment of a company group policy. Which of the following vulnerability types will the analyst most likely find on the workstations?

**Options:**

- A.  
Misconfiguration
- B.  
Zero-day
- C.  
Malicious update
- D.  
Supply chain



CertsMania

**Answer**

A

**Explanation**

Group policies can inadvertently introduce misconfigurations, such as enabling insecure settings or failing to disable legacy protocols, increasing vulnerabilities.

Zero-day (B) are previously unknown vulnerabilities, malicious updates (C) are attacker-controlled, and supply chain (D) risks come from third-party components.

Misconfiguration vulnerabilities are commonly introduced during changes and are emphasized in Security Operations [6:Chapter 14†CompTIA Security+ Study Guide].

Questions # 38:

Which of the following 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



CertsMania

**Answer**

A

Questions # 39:

Which of the following is the most important element when defining effective security governance?

**Options:**

A.

Discovering and documenting external considerations

B.

Developing procedures for employee onboarding and offboarding

C.

Assigning roles and responsibilities for owners, controllers, and custodians

D.

Defining and monitoring change management procedures



CertsMania

**Answer**

C

**Explanation**

Effective security governance requires clear assignment of roles and responsibilities, such as owners, controllers, and custodians, to ensure accountability for security-related tasks and data management within the organization. This establishes clear lines of responsibility

and authority, which is fundamental to governance frameworks.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: "Assigning roles and responsibilities is fundamental to effective security governance.", Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks." , , , , , , , , ]

#### Questions # 40:

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

#### Options:

A.

NGFW

B.

WAF

C.

TLS

D.

SD-WAN

#### Answer

B

#### Explanation

A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A

WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data. References = Buffer Overflows - CompTIA Security+ SY0-701 - 2.3, Web Application Firewalls - CompTIA Security+ SY0-701 - 2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

#### Questions # 41:

A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

The systems administrator checks the OS logs and notices that no patches were applied in the last two months. Which of the following most likely occurred?

#### Options:

A.

The end user changed the file permissions.

B.

A cryptographic collision was detected.

C.

A snapshot of the file system was taken.

D.

A rootkit was deployed.

#### Answer

D

#### Explanation

A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data,

installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

#### Questions # 42:

Which of the following is die most important security concern when using legacy systems to provide production service?

#### Options:

- A.  
Instability
- B.  
Lack of vendor support
- C.  
Loss of availability
- D.  
Use of insecure protocols

#### Answer

B

#### Explanation

The most important security concern when using legacy systems is the lack of vendor support. Without support from the vendor, systems may not receive critical security patches and updates, leaving them vulnerable to exploitation. This lack of support can result in increased risk of security breaches, as vulnerabilities discovered in the software may never be addressed.

References = CompTIA Security+ SY0-701 study materials, particularly in the context of risk management and the challenges posed by legacy systems.

## Questions # 43:

An organization experiences a compromise in a cloud-hosted solution that contains customer information. Which of the following strategies will help determine the sensitivity level of the breach?

### Options:

- A.  
Permission restrictions
- B.  
Tabletop exercise
- C.  
Data classification
- D.  
Asset inventory



CertsMania

### Answer

C

### Explanation

The correct answer is Data classification because it is the primary mechanism used to determine the sensitivity and criticality of information involved in a security incident. According to the Security+ SY0-701 governance and risk management concepts, data classification assigns labels—such as public, internal, confidential, or restricted—to information based on its sensitivity, value to the organization, and potential impact if disclosed, altered, or destroyed. When a breach occurs, these classifications allow security teams and management to quickly assess how severe the incident is and what regulatory, legal, or business consequences may apply.

In this scenario, the compromised cloud-hosted solution contains customer information. By referencing the organization's data classification scheme, incident responders can determine whether the exposed data includes personally identifiable information (PII), financial data, health records, or other regulated data types. This directly influences breach notification requirements, incident escalation, response prioritization, and communication with stakeholders. The SY0-701 study guide emphasizes that effective security governance depends on having clearly defined classification standards before an incident occurs, so decisions during response are consistent and defensible.

The other options do not meet the goal of determining sensitivity. Permission restrictions are access control mechanisms used to prevent unauthorized access, not to evaluate the importance of data after a compromise. Tabletop exercises are preparedness and training activities designed to test incident response plans, not to classify real data. Asset inventory identifies systems, hardware, software, and data locations, but it does not define how sensitive the data is; it only helps locate what may be affected.

Therefore, data classification is the most appropriate strategy for determining the sensitivity level of the breach, aligning directly with Security+ SY0-701 objectives related to risk management, privacy, and incident impact assessment.

#### Questions # 44:

The security operations center is researching an event concerning a suspicious IP address A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced failed log-in attempts when authenticating from the same IP address:

```
184.168.131.241 - userA - failed authentication
184.168.131.241 - userA - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userC - failed authentication
184.168.131.241 - userC - failed authentication
```

Which of the following most likely describes attack that took place?

#### Options:

A.

Spraying

B.

Brute-force

C.

Dictionary

D.

Rainbow table

#### Answer

A

## Explanation

Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for many user accounts from the same IP address are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

## Questions # 45:

An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website. Which of the following should the administrator do?

### Options:

A.

Deploy multifactor authentication.

B.

Decrease the level of the web filter settings

C.

Implement security awareness training.

D.

Update the acceptable use policy

## Answer

C

### Explanation

In this scenario, employees are attempting to navigate to spoofed websites, which is being blocked by the web filter. To address this issue, the administrator should implement security awareness training. Training helps employees recognize phishing and other social engineering attacks, reducing the likelihood that they will attempt to access malicious

websites in the future.

Deploying multifactor authentication (MFA) would strengthen authentication but does not directly address user behavior related to phishing websites.

Decreasing the level of the web filter would expose the organization to more threats.

Updating the acceptable use policy may clarify guidelines but is not as effective as hands-on training for improving user behavior.

#### Questions # 46:

Which of the following activities should a systems administrator perform to quarantine a potentially infected system?

#### Options:

- A.  
Move the device into an air-gapped environment.
- B.  
Disable remote log-in through Group Policy.
- C.  
Convert the device into a sandbox.
- D.  
Remote wipe the device using the MDM platform.

#### Answer

A

#### Explanation

Detailed Explanation: Quarantining a potentially infected system by placing it into an air-gapped environment physically disconnects it from the network. This prevents the spread of malware while maintaining the integrity of forensic evidence. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: " Incident Response and Containment " .

## Questions # 47:

Which of the following phases of an incident response involves generating reports?

### Options:

- A.  
Recovery
- B.  
Preparation
- C.  
Lessons learned
- D.  
Containment



CertsMania

### Answer

C

### Explanation

The lessons learned phase of an incident response process involves reviewing the incident and generating reports. This phase helps identify what went well, what needs improvement, and what changes should be made to prevent future incidents. Documentation and reporting are essential parts of this phase to ensure that the findings are recorded and used for future planning.

Recovery focuses on restoring services and normal operations.

Preparation involves creating plans and policies for potential incidents, not reporting.

Containment deals with isolating and mitigating the effects of the incident, not generating reports.

## Questions # 48:

An employee clicked a malicious link in an email and downloaded malware onto the company '

s computer network. The malicious program exfiltrated thousands of customer records. Which of the following should the company implement to prevent this in the future?

**Options:**

A.

User awareness training

B.

Network monitoring

C.

Endpoint protection

D.

Data loss prevention



CertsMania

**Answer**

A

**Explanation**

User awareness training is essential in preventing security incidents caused by human error, such as clicking on malicious links. Employees need to be educated on recognizing phishing attempts, verifying email senders, and avoiding suspicious downloads.

Network monitoring detects and alerts on malicious activity but does not prevent employees from clicking on harmful links.

Endpoint protection can mitigate malware infections but is not foolproof, especially if users continue to fall for phishing attacks.

Data loss prevention (DLP) can prevent data exfiltration but does not stop malware from being introduced into the system.

By training employees to recognize and avoid phishing scams, organizations can reduce the risk of malware infections and data breaches.

**To Get Premium Files for SY0-701 Visit**

**<https://www.certsmania.com/comptia/sy0-701-practice>**

**For More Free Questions Visit**

**<https://www.certsmania.com/comptia/pdf/sy0-701>**



**CertsMania**