Free Questions for SY0-701

Shared by Aurora on Apr 30, 2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Questions # 1:

Which of the following should an organization implement to avoid unnecessary liability after the end of a legal contract obligation with a third party?

Options:

○ A.

Data encryption

○ B.

Data classification

○ C.

Data retention

○ D.

Data inventory

Answer

C

Explanation

The best answer is C. Data retention.

To avoid unnecessary liability after the end of a legal contract obligation with a third party, an organization should follow a proper data retention policy. Data retention policies define how long data must be kept and when it should be deleted or securely destroyed once it is no longer needed for legal, contractual, regulatory, or business purposes.

Keeping third-party data longer than necessary can increase:

legal exposure

privacy risk

breach impact

storage and governance burden

Why the other options are incorrect:

A. Data encryptionEncryption protects data confidentiality, but it does not address whether the data should still be retained at all.

B. Data classificationClassification helps determine sensitivity and handling requirements, but it does not define when data should be disposed of.

D. Data inventoryAn inventory helps identify what data exists, but it does not by itself reduce liability after contractual obligations end.

From the SY0-701 perspective, reducing liability after contractual or legal obligations end requires proper retention schedules and secure disposal, so C is the correct answer.

Questions # 2:

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

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 # 3:

The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company ' s security policies compare to the requirements imposed by external regulators. Which of the following should the CISO use?

Options:

○ A.

Penetration test

○ B.

Internal audit

○ C.

Attestation

○ D.

External examination

Answer

D

Explanation

An external examination (also known as an external audit or external review) is the best method for the Chief Information Security Officer (CISO) to gain an understanding of how the company’s security policies compare to external regulatory requirements. External examinations are conducted by third-party entities that assess an organization’s compliance with laws, regulations, and industry standards.

Penetration tests focus on identifying vulnerabilities, not compliance.

Internal audits assess internal controls but are not impartial or focused on regulatory requirements.

Attestation is a formal declaration but does not involve the actual evaluation of compliance.

Questions # 4:

Which of the following can automate vulnerability management?

Options:

○ A.

CVE

○ B.

SCAP

○ C.

OSINT

○ D.

CVSS

Answer

B

Explanation

SCAP (Security Content Automation Protocol) is designed to automate vulnerability management, configuration assessment, and compliance checking. According to CompTIA Security+ SY0-701, SCAP standardizes how vulnerability information is expressed, measured, and shared, allowing security tools to automatically scan systems, identify weaknesses, and assess compliance against predefined baselines.

SCAP integrates multiple standards such as CVE, CVSS, CPE, and XCCDF, enabling automated vulnerability scanning, scoring, and reporting across large environments. This makes it a core technology for continuous vulnerability management and compliance automation.

CVE (A) is a catalog of known vulnerabilities, not an automation framework. OSINT (C) provides publicly available intelligence but does not automate remediation or assessment. CVSS (D) provides severity scoring but does not automate vulnerability management.

Because SCAP enables automated identification, assessment, and reporting of vulnerabilities, the correct answer is B: SCAP.

Questions # 5:

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

Options:

○ A.

Place posters around the office to raise awareness of common phishing activities.

○ B.

Implement email security filters to prevent phishing emails from being delivered

○ C.

Update the EDR policies to block automatic execution of downloaded programs.

○ D.

Create additional training for users to recognize the signs of phishing attempts.

Answer

C

Explanation

An endpoint detection and response (EDR) system is a security tool that monitors and analyzes the activities and behaviors of endpoints, such as computers, laptops, mobile devices, and servers. An EDR system can detect, prevent, and respond to various types of threats, such as malware, ransomware, phishing, and advanced persistent threats (APTs). One of the features of an EDR system is to block the automatic execution of downloaded programs, which can prevent malicious code from running on the endpoint when a user clicks on a link in a phishing message. This can reduce the impact of a phishing attack and protect the endpoint from compromise. Updating the EDR policies to block automatic execution of downloaded programs is a technical control that can mitigate the risk of phishing, regardless of the user's awareness or behavior. Therefore, this is the best answer among the given options.

The other options are not as effective as updating the EDR policies, because they rely on administrative or physical controls that may not be sufficient to prevent or stop a phishing attack. Placing posters around the office to raise awareness of common phishing activities is a physical control that can increase the user's knowledge of phishing, but it may not

change their behavior or prevent them from clicking on a link in a phishing message. Implementing email security filters to prevent phishing emails from being delivered is an administrative control that can reduce the exposure to phishing, but it may not be able to block all phishing emails, especially if they are crafted to bypass the filters. Creating additional training for users to recognize the signs of phishing attempts is an administrative control that can improve the user's skills of phishing detection, but it may not guarantee that they will always be vigilant or cautious when receiving an email. Therefore, these options are not the best answer for this question. References = Endpoint Detection and Response – CompTIA Security+ SY0-701 – 2.2, video at 5:30; CompTIA Security+ SY0-701 Certification Study Guide, page 163.

CertsMania

Questions # 6:

A government official receives a blank envelope containing photos and a note instructing the official to wire a large sum of money by midnight to prevent the photos from being leaked on the Internet. Which of the following best describes the threat actor ' s intent?

Options:

○ A.

Organized crime

○ B.

Philosophical beliefs

○ C.

Espionage

○ D.

Blackmail

CertsMania

Answer

D

Explanation

The threat actor's intent is clearly blackmail, a form of extortion where sensitive information is used to coerce an individual into taking an action, usually involving financial gain. In this scenario, the attacker threatens to leak incriminating or compromising photos unless the government official wires a large sum of money. CompTIA Security+ SY0-701

defines blackmail as the use of sensitive or embarrassing information to manipulate or force actions from victims.

This differs from organized crime (A), which focuses on profit-driven cyber operations but typically uses technical attacks such as ransomware, data theft, or fraud rather than anonymous mailed threats. Philosophical beliefs (B) refers to hacktivism, where attackers pursue ideological motives—not present here. Espionage (C) involves intelligence gathering for political or competitive advantage, typically performed by nation-states or advanced persistent threats (APTs).

This scenario aligns directly with extortion-based social engineering, where attackers manipulate victims through fear and emotional pressure. According to Security+ guidance, blackmail often occurs through email, physical mail, or compromised personal data leaks, all fitting this situation. Therefore, the threat actor's intent is blackmail.

Questions # 7:

A company wants to ensure that only authorized devices can enter an environment. Which of the following will the company most likely use to implement the control?

Options:

○ A.

Access lists

○ B.

Remote connection

○ C.

Screened subnets

○ D.

Centralized proxy

Answer

A

Explanation

The best answer is A. Access lists.

To ensure that only authorized devices can enter or connect to an environment, the organization needs a control that explicitly allows approved devices and denies unapproved ones. Access lists are used to define which devices, systems, or addresses are permitted access.

This can include allowlists based on:

device identifiers

MAC addresses

IP addresses

approved system entries

predefined access control rules

Why the other options are incorrect:

B. Remote connectionThis is a method of connecting, not a control that determines which devices are authorized.

C. Screened subnetsA screened subnet helps separate public-facing systems from internal systems, but it does not directly ensure only authorized devices can enter.

D. Centralized proxyA proxy mediates traffic requests, but it is not the primary control for allowing only authorized devices into an environment.

From a Security+ perspective, restricting access to only approved devices is best aligned with allow/deny rules through access lists, so A is the strongest answer.

Questions # 8:

A company is implementing a vendor ' s security tool in the cloud. The security director does not want to manage users and passwords specific to this tool but would rather utilize the company ' s standard user directory. Which of the following should the company implement?

Options:

○ A.

802.1X

○ B.

SAML

○ C.

RADIUS

○ D.

CHAP

Answer

B

Explanation

The company should implement Security Assertion Markup Language (SAML) to integrate the vendor ' s security tool with their existing user directory. SAML is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP), enabling Single Sign-On (SSO). This allows the company to use its existing directory services for authentication, avoiding the need to manage a separate set of user credentials for the new tool.

[References:, CompTIA Security+ SY0-701 Course Content: Domain 4: Identity and Access Management, which includes SAML as a key identity federation standard for SSO., CompTIA Security+ Study Guide (SY0-601): Chapter 8, "Identity and Access Management," details the role of SAML in enabling SSO by utilizing an existing identity provider., , , , , , , , , ,]

Questions # 9:

A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from. Which of the following is the best way for the company to confirm this information?

Options:

○ A.

Validate the code signature.

○ B.

Execute the code in a sandbox.

○ C.

Search the executable for ASCII strings.

○ D.

Generate a hash of the files.

Answer

A

Explanation

Validating the code signature is the best way to verify software authenticity, as it ensures that the software has not been tampered with and that it comes from a verified source. Code signatures are digital signatures applied by the software vendor, and validating them confirms the software ' s integrity and origin.References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

Questions # 10:

Which of the following objectives is best achieved by a tabletop exercise?

Options:

○ A.

Familiarizing participants with the incident response process

○ B.

Deciding red and blue team rules of engagement

○ C.

Quickly determining the impact of an actual security breach

○ D.

Conducting multiple security investigations in parallel

Answer

A

Explanation

A tabletop exercise is a discussion-based simulation where incident response (IR) team members walk through hypothetical security scenarios to understand roles,

responsibilities, escalation paths, and communication processes. According to Security+ SY0-701, tabletop exercises are ideal for familiarizing participants with the incident response process and improving organizational readiness without the pressure or resource demands of full-scale simulations.

These exercises highlight:

IR workflow clarity

Decision-making processes

Coordination between technical and non-technical teams

Communication procedures

Identification of gaps in policies or documentation

Option B (rules of engagement) is part of penetration testing planning, not tabletop exercises. Option C refers to real breach analysis, not simulations. Option D refers to forensic operations, not tabletop objectives.

Thus, A is correct.

CertsMania

Questions # 11:

A systems administrator needs to ensure the secure communication of sensitive data within the organization ' s private cloud. Which of the following is the best choice for the administrator to implement?

Options:

○ A.

IPSec

○ B.

SHA-1

○ C.

RSA

○ D.

TGT

CertsMania

Answer

A

Questions # 12:

An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization. Which of the following best describes the tool the administrator is using?

Options:

○ A.

DLP

○ B.

SNMP traps

○ C.

SCAP

○ D.

IPS

Answer

A

Explanation

The administrator is using a Data Loss Prevention (DLP) tool, which is designed to identify, monitor, and protect sensitive data. By fingerprinting specific files, DLP ensures that these files cannot be emailed or sent outside the organization without triggering an alert or blocking the action. This is a key feature of DLP systems, which prevent data exfiltration and ensure data security compliance.

SNMP traps are used for network management and monitoring, not data protection.

SCAP (Security Content Automation Protocol) is a set of standards for automating vulnerability management and policy compliance, unrelated to file monitoring.

IPS (Intrusion Prevention System) blocks network-based attacks but does not handle file

fingerprinting.

Questions # 13:

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.

Questions # 14:

During a penetration test, a vendor attempts to enter an unauthorized area using an access badge Which of the following types of tests does this represent?

Options:

○ A.

Defensive

○ B.

Passive

○ C.

Offensive

○ D.

Physical

Answer

D

Explanation

Attempting to enter an unauthorized area using an access badge during a penetration test is an example of a physical test. This type of test evaluates the effectiveness of physical security controls, such as access badges, security guards, and locks, in preventing unauthorized access to restricted areas.

Defensive and offensive testing typically refer to digital or network-based penetration testing strategies.

Passive testing involves observing or monitoring but not interacting with the environment.

Questions # 15:

Which of the following best describes the practice of preserving and documenting the handling of forensic evidence?

Options:

○ A.

Acquisition of evidence

○ B.

E-discovery

○ C.

Chain of custody

○ D.

Forensic tabletop exercises

CertsMania

Answer

C

Explanation

The best answer is C. Chain of custody.

Chain of custody is the documented process used to track forensic evidence from the moment it is collected until it is presented, stored, transferred, or disposed of. It records:

who handled the evidence

when it was handled

where it was stored

how it was transferred

how its integrity was preserved

This is critical to ensure the evidence remains credible and admissible.

Why the other options are incorrect:

A. Acquisition of evidenceAcquisition refers to collecting or imaging evidence, but it does not specifically cover the full documentation of handling over time.

CertsMania

B. E-discoveryE-discovery relates to identifying and producing electronically stored information for legal matters, not specifically preserving forensic handling records.

D. Forensic tabletop exercisesThese are discussion-based practice activities, not evidence handling procedures.

From a Security+ perspective, preserving and documenting forensic evidence handling is the definition of chain of custody.

Questions # 16:

A company is aware of a given security risk related to a specific market segment. The business chooses not to accept responsibility and target their services to a different market segment. Which of the following describes this risk management strategy?

Options:

○ A.

Exemption

○ B.

Exception

○ C.

Avoid

○ D.

Transfer

Answer

C

Explanation

Detailed Explanation:Avoidance involves choosing not to engage in activities or markets where certain risks are present. This is a proactive approach to risk management. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: " Risk Management Strategies " .

Questions # 17:

The analyst wants to move data from production to the UAT server for testing the latest release. Which of the following strategies to protect data should the analyst use?

Options:

○ A.

Data masking

○ B.

Data tokenization

○ C.

Data obfuscation

○ D.

Data encryption

Answer

A

Explanation

Data masking replaces sensitive data with realistic but fictional data, preserving format and usability while protecting confidential information during testing in environments like UAT (User Acceptance Testing).

Tokenization (B) replaces data with tokens but is more common for payment data in production. Obfuscation (C) scrambles data but is less structured than masking. Encryption (D) protects data confidentiality but may not be practical for testing.

Data masking is a best practice for protecting sensitive data in non-production environments covered in the General Security Concepts domain□6:Chapter 7†CompTIA Security+ Study Guide□.

Questions # 18:

A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the

increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO ' s report?

Options:

○ A.

Insider threat

○ B.

Hacktivist

○ C.

Nation-state

○ D.

Organized crime

Answer

D

Explanation

Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17 1

CertsMania

Questions # 19:

Which of the following can assist in recovering data if the decryption key is lost?

Options:

○ A.

CSR

○ B.

Salting

○ C.

Root of trust

○ D.

Escrow

CertsMania

Answer

D

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

Key escrow is the process of storing encryption keys (or copies of them) with a trusted third party so data can be recovered if the primary decryption key is lost. In Security+ SY0-701, escrow is emphasized as a required safeguard for organizations that rely heavily on encryption, especially for regulated data or systems requiring guaranteed recoverability.

A CSR (A) is a Certificate Signing Request and does not store keys. Salting (B) is used with hashing to prevent password attacks and does not assist in data recovery. A root of trust (C) ensures secure hardware initialization but does not store backup decryption keys.

Key escrow directly addresses scenarios where encryption keys are misplaced, corrupted, deleted, or lost due to employee departure or system failure. Without escrow, encrypted data could become permanently inaccessible.

Thus, the correct answer is Escrow, the only mechanism specifically designed to allow recovery when decryption keys are unavailable.

CertsMania

Questions # 20:

A systems administrator receives an alert that a company ' s internal file server is very slow and is only working intermittently. The systems administrator reviews the server management software and finds the following information about the server:

>

Which of the following indicators most likely triggered this alert?

Options:

○ A.

Concurrent session usage

○ B.

Network saturation

○ C.

Account lockout

○ D.

Resource consumption

Answer

D

Questions # 21:

A network security analyst monitors the network's IDS, which has flagged unusual activity. The IDS has detected multiple login attempts to a database server within a short period. These attempts come from various IP addresses that are not normally recognized by the network's usual traffic patterns. Each attempt uses the same username and password. Based on the following log output (corrected formatting for readability):

2025-04-10 14:22:01.4532 — Source IP: 192.168.15.101 — Status: Failed — User: JDoe — Action: Login Attempt

2025-04-10 14:22:02.1122 — Source IP: 192.168.15.102 — Status: Failed — User: JDoe — Action: Login Attempt

2025-04-10 14:22:02.7835 — Source IP: 192.168.15.103 — Status: Failed — User: JDoe — Action: Login Attempt

2025-04-10 14:22:03.5637 — Source IP: 192.168.15.104 — Status: Failed — User: JDoe — Action: Login Attempt

2025-04-10 14:22:04.9474 — Source IP: 192.168.15.105 — Status: Failed — User: JDoe — Action: Login Attempt

2025-04-10 14:22:05.5673 — Source IP: 192.168.15.106 — Status: Failed — User: JDoe — Action: Login Attempt

2025-04-10 14:22:06.1573 — Source IP: 192.168.15.107 — Status: Failed — User: JDoe — Action: Login Attempt

2025-04-10 14:22:07.7462 — Source IP: 192.168.15.108 — Status: Failed — User: JDoe — Action: Login Attempt

Which of the following types of network attacks is most likely occurring?

Options:

○ A.

Cross-site scripting

○ B.

Credential replay

○ C.

Distributed denial of service

○ D.

SQL injection

Answer

B

Explanation

The pattern shows rapid, repeated authentication attempts against a database server using the same username (JDoe) and the same password, originating from multiple different IP addresses in a short window. Among the choices, this most closely aligns with a credential replay style attack (often discussed as replaying captured authentication material or repeatedly reusing stolen credentials) rather than an application-layer injection (SQLi/XSS) or a volumetric availability attack (DDoS). The Study Guide describes credential replay as follows: “Credential replay attacks are a form of network attack that requires the attacker to be able to capture valid network data and to re-send it or delay it so that the attacker’s own use of the data is successful.”

In practice, defenders may see replay-like behavior when an attacker (or botnet) repeatedly tries the same captured credential pair (or captured authentication artifact) from different sources. The multiple IPs can indicate automation or distributed infrastructure used to evade rate limits and lockout controls. The other options don’t fit the evidence: XSS requires script injection into web content; SQL injection would show suspicious SQL payloads, not repeated logins; DDoS focuses on overwhelming availability and typically shows traffic floods rather than repeated authentication attempts using a

single account credential set. Therefore, the best answer is credential replay.

[References: Credential replay definition and explanation ., , , , , , ,]

Questions # 22:

A company processes a large volume of business-to-business transactions and prioritizes data confidentiality over transaction availability. The company ' s firewall administrator must configure a new hardware-based firewall to replace the current one. Which of the following should the administrator do to best align with the company requirements in case a security event occurs?

Options:

○ A.

Ensure the firewall data plane moves to fail-closed mode.

○ B.

Implement a deny-all rule as the last firewall ACL rule.

○ C.

Prioritize business-critical application traffic through the firewall.

○ D.

Configure rate limiting between the firewall interfaces.

Answer

A

Explanation

The best answer is A. Ensure the firewall data plane moves to fail-closed mode.

The key requirement is that the company prioritizes confidentiality over availability. In a failure or security event, a fail-closed firewall blocks traffic rather than allowing traffic to continue through an untrusted or degraded state.

This choice protects sensitive business data, even if it temporarily interrupts transactions.

Why the other options are incorrect:

B. Implement a deny-all rule as the last firewall ACL rule.This is a standard best practice,

but it does not specifically address behavior during a security event.

C. Prioritize business-critical application traffic through the firewall.This emphasizes availability and performance, not confidentiality.

D. Configure rate limiting between the firewall interfaces.Rate limiting can help with traffic control, but it is not the best match for the stated priority.

From a Security+ standpoint, when confidentiality is more important than uptime, fail closed is the correct choice.

CertsMania

Questions # 23:

A website user is locked out of an account after clicking an email link and visiting a different website Web server logs show the user ' s password was changed, even though the user did not change the password. Which of the following is the most likely cause?

Options:

○ A.

Cross-sue request forgery

○ B.

Directory traversal

○ C.

ARP poisoning

○ D.

SQL injection

CertsMania

Answer

A

Explanation

The scenario describes a situation where a user unknowingly triggers an unwanted action, such as changing their password, by clicking a malicious link. This is indicative of a Cross-Site Request Forgery (CSRF) attack, where an attacker tricks the user into executing actions they did not intend to perform on a web application in which they are authenticated.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common attack vectors like CSRF.

Questions # 24:

A malicious update was distributed to a common software platform and disabled services at many organizations. Which of the following best describes this type of vulnerability?

Options:

○ A.

DDoS attack

○ B.

Rogue employee

○ C.

Insider threat

○ D.

Supply chain

Answer

D

Questions # 25:

A security analyst investigates an incident in which a PowerShell script was identified as a potential IoC. Which of the following will best help the analyst identify an attempt to compromise the system?

Options:

○ A.

SNMP logs

○ B.

Firewall logs

○ C.

EDR logs

○ D.

IPS logs

CertsMania

Answer

C

Explanation

The best answer is C. EDR logs.

EDR (Endpoint Detection and Response) tools are designed to monitor endpoint activity in detail, including process execution, command-line usage, script activity, file changes, persistence attempts, and suspicious behavior. Since the incident involves a PowerShell script, EDR logs are the most useful source for identifying whether the script attempted to compromise the system.

PowerShell is commonly abused by attackers for fileless malware, persistence, lateral movement, downloading payloads, and privilege escalation. EDR can capture this kind of endpoint-level behavior much more effectively than general network logs.

Why the other options are incorrect:

A. SNMP logsSNMP is mainly used for network device monitoring and management, not detailed endpoint script execution analysis.

B. Firewall logsFirewall logs can show allowed or blocked traffic, but they usually do not provide deep visibility into local PowerShell execution or endpoint compromise attempts.

D. IPS logsAn IPS may detect known malicious traffic patterns, but it is focused on network-based activity. It is not the best source for detailed analysis of a PowerShell script running on a host.

From a Security+ standpoint, when analyzing suspicious scripts or endpoint behavior, EDR provides the strongest visibility into actual compromise attempts.

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