CERT-PASS

CompTIA Security+ SY0-701

Free Practice Questions Preview

Here are 35 sample questions to help you get started. Unlock the full exam to access all 1100+ questions with detailed explanations.

Question 1 : Threats, Vulnerabilities, and Mitigations

While reviewing the clinical application at a media company, several public servers must remain reachable from the internet, but they should not have unrestricted access to internal databases. Which choice BEST explains the situation?

A. Disable logging on the public servers

B. Put all servers and databases on one flat VLAN

C. Use the same administrator credentials on all hosts

D. Place the public servers in a segmented DMZ with narrowly allowed flows

Answer: D
The scenario points to Place the public servers in a segmented DMZ with narrowly allowed flows. The best wrong answer misses the requirement because a flat VLAN increases lateral-movement risk; segmentation limits the blast radius.

Question 2 : Security Operations

A security analyst working with a cloud consulting firm learns that the team restores a service after repeated compromise but has not identified how attackers regain access. Which answer best matches the scenario?

A. Close the case because uptime returned

B. Disable logging to reduce noise

C. Rotate only one unrelated user password

D. Perform root cause analysis and remediate the persistence mechanism

Answer: D
Perform root cause analysis and remediate the persistence mechanism addresses the specific issue described. The best wrong answer misses the requirement because restoring availability without addressing persistence leaves the organization vulnerable to recurrence.

Question 3 : Threats, Vulnerabilities, and Mitigations

During an assessment of an online retailer, a consultant observes that a malicious document is suspected, and analysts need to observe behavior without risking production systems. What should the team implement?

A. Open the document in an isolated sandbox

B. Email it to more users for comparison

C. Disable endpoint protection before testing

D. Open it on an administrator workstation

Answer: A
Open the document in an isolated sandbox is correct because it directly matches the requirement. The closest alternative is weaker because opening a suspicious file on an administrator workstation risks compromise; a sandbox isolates execution.

Question 4 : Threats, Vulnerabilities, and Mitigations

A security analyst supporting a managed service provider learns that a staff member deploys an unsanctioned file-sharing application to finish work faster, bypassing company review. An analyst is asked to recommend the most defensible next step. What is the best recommendation?

A. Watering-hole attack

B. Nation-state activity

C. Cryptographic downgrade

D. Shadow IT

Answer: D
Shadow IT addresses the specific issue described. The competing option is less appropriate because shadow IT is the use of technology without organizational approval; it is not an external cryptographic attack.

Question 5 : General Security Concepts

At a construction contractor, a team needs to protect confidentiality while exchanging a symmetric session key with a remote party that has a trusted certificate. Which response is most appropriate?

A. Encrypt the session key with the recipient public key

B. Store the session key in a DNS TXT record

C. Publish the session key hash as the key

D. Encrypt the session key with the sender public key

Answer: A
Encrypt the session key with the recipient public key is the best fit for the stated need. The best wrong answer misses the requirement because using the sender public key would not restrict decryption to the intended recipient.

Question 6 : Security Architecture

A security analyst working with a research laboratory learns that monitoring systems need authenticated and encrypted management polling for network devices. The organization wants the option that most directly addresses the stated requirement.

Which choice BEST explains the situation?

A. Use Telnet

B. Use SNMPv3

C. Use SNMPv1 with a default community string

D. Use unauthenticated syslog only

Answer: B
The scenario points to Use SNMPv3. A tempting wrong answer fails because sNMPv1 community strings do not provide the authentication and encryption available in SNMPv3.

Question 7 : Threats, Vulnerabilities, and Mitigations

During an assessment of a construction contractor, a consultant observes that an attacker compromises a website frequently visited by a targeted group and adds malicious code to infect visitors. Which response is most appropriate?

A. Credential stuffing

B. Smishing

C. Pass-the-hash

D. Watering-hole attack

Answer: D
Watering-hole attack is correct because it directly matches the requirement. The best wrong answer misses the requirement because smishing uses SMS lures; a watering-hole attack compromises a site the target group already visits.

Question 8 : Threats, Vulnerabilities, and Mitigations

At a managed service provider, researchers find two different inputs that produce the same hash output and exploit that weakness. The organization wants the option that most directly addresses the stated requirement. Which option most directly solves the problem?

A. Session fixation

B. Collision attack

C. Downgrade attack

D. Password spraying

Answer: B
The scenario points to Collision attack. A tempting wrong answer fails because password spraying targets authentication; a collision attack targets hash uniqueness.

Question 9 : Security Program Management and Oversight

The administrator for the payment service reports that employees need step-by-step instructions for securely onboarding a new vendor account. An analyst is asked to recommend the most defensible next step. Which option best addresses the requirement?

A. Use a network diagram with no instructions

B. Create only a general policy

C. Rely on memory

D. Create a documented procedure

Answer: D
The most direct answer is Create a documented procedure. The competing option is less appropriate because a policy states intent; a procedure supplies repeatable step-by-step actions.

Question 10 : Threats, Vulnerabilities, and Mitigations

An administrator responsible for the public website reports that a trusted software update server distributes a malicious package after the vendor build environment is compromised. Which answer best matches the scenario?

A. Physical tailgating

B. On-path attack

C. Supply-chain attack

D. SQL injection

Answer: C
Supply-chain attack is the best fit for the stated need. The main distractor is not sufficient because an on-path attack intercepts communications; the compromise here enters through a trusted supplier process.

Question 11 : Security Program Management and Oversight

The administrator for the data analytics platform reports that an assessor asks which document should contain mandatory password length and lockout requirements. Which choice is the most appropriate?

A. Marketing brochure

B. Security standard

C. High-level security policy only

D. Optional guideline only

Answer: B
Security standard addresses the specific issue described. The best wrong answer misses the requirement because a high-level policy states intent, while a standard contains mandatory detailed requirements.

Question 12 : Security Operations

While updating the payment service, the security team at a cloud consulting firm notes that the team wants to block malicious network traffic automatically when signatures or behavior match high-confidence rules. The organization wants the option that most directly addresses the stated requirement. Which choice BEST explains the situation?

A. Remove firewall rules

B. Place an IPS inline and tune blocking policies

C. Deploy an IDS only and expect it to block inline

D. Use a passive packet capture appliance only

Answer: B
Place an IPS inline and tune blocking policies is correct because it directly matches the requirement. The closest alternative is weaker because an IDS generally alerts rather than blocks traffic inline.

Question 13 : Security Program Management and Oversight

During a privileged-access review for a payment processor, a new vendor will host sensitive records and the company needs enforceable expectations plus ongoing assurance. Which TWO actions should be included? Select the option containing the BEST two answers.

A. Rely only on the vendor logo and share administrator credentials

B. Use a verbal promise and disable audit rights

C. Include contractual security requirements and monitor vendor performance and evidence

D. Grant access before review and skip monitoring

Answer: C
Include contractual security requirements and monitor vendor performance and evidence is the best fit for the stated need. A tempting wrong answer fails because a verbal promise without monitoring or enforceable requirements is inadequate for sensitive-data third-party risk.

Question 14 : Security Architecture

A security analyst working with an energy utility learns that a company wants to retain responsibility for its applications and data while using provider-managed compute, storage, and networking. An analyst is asked to recommend the most defensible next step. Which control should the team select?

A. Use a public DNS zone as the application platform

B. Use an IaaS model and secure the guest operating systems, applications, and data

C. Use on-premises hosting and assume no security responsibility

D. Use SaaS and manage the provider hypervisor

Answer: B
Use an IaaS model and secure the guest operating systems, applications, and data is correct because it directly matches the requirement. A tempting wrong answer fails because in SaaS, the provider manages much more of the application stack; it is not the fit for customer-managed applications on provider infrastructure.

Question 15 : Security Operations

During an assessment of a cloud consulting firm, a consultant observes that the SOC wants to proactively look for attacker behavior not yet detected by alerts. Which choice BEST explains the situation?

A. Form a hypothesis and query relevant telemetry for supporting or disproving evidence

B. Wait only for users to report problems

C. Delete older telemetry

D. Turn off alerting during the hunt

Answer: A
The scenario points to Form a hypothesis and query relevant telemetry for supporting or disproving evidence. The closest alternative is weaker because threat hunting is proactive and hypothesis-driven, not limited to waiting for existing alerts.

Question 16 : General Security Concepts

At a research laboratory, a new requirement applies to the mobile workforce. a camera records activity at a loading dock so investigators can review events later. Which answer best matches the scenario?

A. Detective physical control

B. Preventive managerial control

C. Corrective technical control

D. Directive operational control

Answer: A
The most direct answer is Detective physical control. The best wrong answer misses the requirement because a camera primarily records or detects activity; it does not physically prevent entry.

Question 17 : Security Architecture

The security team at a municipal agency is updating the payment service and notes that a hospital needs to isolate medical devices from office workstations while allowing only required application traffic. What is the best recommendation?

A. Use a single VLAN for easier management

B. Share local administrator credentials across devices

C. Create dedicated network segments with narrowly scoped firewall rules

D. Disable NAC checks for medical devices and permit all traffic

Answer: C
Create dedicated network segments with narrowly scoped firewall rules addresses the specific issue described. A tempting wrong answer fails because a single VLAN allows unnecessary east-west connectivity and increases the blast radius.

Question 18 : Security Program Management and Oversight

At a legal services firm, a new requirement applies to the clinical application. a penetration-test contract needs to define permitted targets, timing, methods, contacts, and stop conditions. Which option most directly solves the problem?

A. Document rules of engagement

B. Leave scope implicit

C. Skip escalation contacts

D. Allow any target worldwide

Answer: A
Document rules of engagement addresses the specific issue described. The strongest distractor fails because implicit scope can result in unauthorized testing and avoidable disruption.

Question 19 : Security Operations

As part of an internal audit, analysts want correlated detections across endpoints, identities, email, and cloud workloads. Which response is most appropriate?

A. Disable cloud telemetry

B. Store alerts in separate unreviewed inboxes

C. Use a standalone unmanaged antivirus scanner only

D. Use an XDR-capable platform or integration strategy

Answer: D
The scenario points to Use an XDR-capable platform or integration strategy. The closest alternative is weaker because standalone antivirus lacks the cross-domain correlation requested.

Question 20 : Security Program Management and Oversight

After a recent change to the manufacturing floor, records should be kept only as long as required for business and legal purposes. Which control should the team select?

A. Let each employee decide independently

B. Keep every record forever by default

C. Delete records immediately regardless of obligations

D. Apply a documented retention and secure-disposal schedule

Answer: D
Apply a documented retention and secure-disposal schedule is correct because it directly matches the requirement. A tempting wrong answer fails because keeping data forever increases exposure and may conflict with privacy principles and policy.

Question 21 : Security Operations

At a legal services firm, a new requirement applies to the branch office. a scanner reports a vulnerable library, but the application owner believes the finding is incorrect. Which choice BEST explains the situation?

A. Patch unrelated systems only

B. Delete the scan history

C. Validate the finding with asset context and additional evidence before disposition

D. Mark every finding as a false positive

Answer: C
The scenario points to Validate the finding with asset context and additional evidence before disposition. A tempting wrong answer fails because a belief without validation is insufficient to classify a finding as a false positive.

Question 22 : Security Program Management and Oversight

An administrator responsible for the identity platform reports that leaders want reasonable safeguards and ongoing verification that those safeguards remain appropriate. Which option best addresses the requirement?

A. Disable audits to reduce cost

B. Delegate all accountability to a vendor

C. Buy one tool and stop reviewing risk

D. Apply due care by implementing controls and due diligence by reviewing and monitoring them

Answer: D
Apply due care by implementing controls and due diligence by reviewing and monitoring them is correct because it directly matches the requirement. The strongest distractor fails because a one-time tool purchase without ongoing review does not demonstrate due diligence.

Question 23 : Threats, Vulnerabilities, and Mitigations

During a review of the file-sharing service at a payment processor, a finance employee receives an apparently legitimate message from the CEO requesting an urgent wire transfer, but the sender account was spoofed. The organization wants the option that most directly addresses the stated requirement. Which answer best matches the scenario?

A. Password spraying

B. DNSSEC validation

C. Business email compromise

D. Cross-site scripting

Answer: C
The scenario points to Business email compromise. The closest alternative is weaker because business email compromise commonly impersonates executives to induce fraudulent payments.

Question 24 : Security Operations

The security team at a university is updating the production API and notes that company phones store business data and may be lost or stolen. What is the best recommendation?

A. Allow unrestricted sideloading

B. Disable device PINs for convenience

C. Store data only in personal apps

D. Enforce screen locks, encryption, remote wipe, and managed application policies

Answer: D
The scenario points to Enforce screen locks, encryption, remote wipe, and managed application policies. A tempting wrong answer fails because removing screen locks increases the risk of unauthorized access after loss.

Question 25 : Threats, Vulnerabilities, and Mitigations

A new requirement affects the file-sharing service at a biotech startup. several public servers must remain reachable from the internet, but they should not have unrestricted access to internal databases. Which control should the team select?

A. Place the public servers in a segmented DMZ with narrowly allowed flows

B. Disable logging on the public servers

C. Put all servers and databases on one flat VLAN

D. Use the same administrator credentials on all hosts

Answer: A
Place the public servers in a segmented DMZ with narrowly allowed flows is correct because it directly matches the requirement. The competing option is less appropriate because a flat VLAN increases lateral-movement risk; segmentation limits the blast radius.

Question 26 : Threats, Vulnerabilities, and Mitigations

At a media company, a new requirement applies to the public website. a malicious attachment arrives through a trusted vendor mailbox that was itself compromised. Which option most directly solves the problem?

A. Air-gap bypass only

B. Tailgating

C. Secure boot validation

D. Message-based threat vector using a trusted relationship

Answer: D
The scenario points to Message-based threat vector using a trusted relationship. A tempting wrong answer fails because the attack arrives through messaging and abuses trust in the vendor account.

Question 27 : Security Operations

At a software-as-a-service provider, company phones store business data and may be lost or stolen. Which choice BEST explains the situation?

A. Enforce screen locks, encryption, remote wipe, and managed application policies

B. Disable device PINs for convenience

C. Allow unrestricted sideloading

D. Store data only in personal apps

Answer: A
Enforce screen locks, encryption, remote wipe, and managed application policies is the best fit for the stated need. The main distractor is not sufficient because removing screen locks increases the risk of unauthorized access after loss.

Question 28 : Security Architecture

After a recent change to the data analytics platform, a hospital needs to isolate medical devices from office workstations while allowing only required application traffic. Which answer best matches the scenario?

A. Use a single VLAN for easier management

B. Disable NAC checks for medical devices and permit all traffic

C. Create dedicated network segments with narrowly scoped firewall rules

D. Share local administrator credentials across devices

Answer: C
The most direct answer is Create dedicated network segments with narrowly scoped firewall rules. The closest alternative is weaker because a single VLAN allows unnecessary east-west connectivity and increases the blast radius.

Question 29 : Security Operations

While updating the production API, the security team at a cloud consulting firm notes that a new employee needs role-appropriate access on the start date and removed access promptly upon departure. Which option best addresses the requirement?

A. Use joiner-mover-leaver provisioning workflows tied to authoritative HR events

B. Create permanent shared accounts

C. Wait for annual reviews to remove access

D. Allow managers to share credentials

Answer: A
Use joiner-mover-leaver provisioning workflows tied to authoritative HR events addresses the specific issue described. The competing option is less appropriate because annual removal is too slow for departures and shared accounts weaken accountability.

Question 30 : Security Program Management and Oversight

Following a recent change to the mobile workforce, management wants one maintained record of identified risks, owners, treatments, and status. An analyst is asked to recommend the most defensible next step. Which response is most appropriate?

A. Use a risk register

B. Use an employee directory only

C. Use a packet capture only

D. Use a password vault only

Answer: A
The most direct answer is Use a risk register. The main distractor is not sufficient because a password vault stores credentials, not risk ownership and treatment status.

Question 31 : Security Operations

At a cloud consulting firm, an incident is contained and eradicated, and the organization wants to improve future defenses. Which response is most appropriate?

A. Stop collecting evidence immediately after containment

B. Delete the incident ticket

C. Conduct lessons learned and root cause analysis and update controls

D. Remove monitoring rules that generated alerts

Answer: C
Conduct lessons learned and root cause analysis and update controls addresses the specific issue described. The main distractor is not sufficient because deleting the incident record prevents learning and weakens future response.

Question 32 : Threats, Vulnerabilities, and Mitigations

During a review of the payment service at a construction contractor, a file-download parameter can be changed to ../../etc/passwd and returns operating-system files. What should the team implement?

A. Race condition

B. XML injection

C. Directory traversal

D. Credential stuffing

Answer: C
Directory traversal is the best fit for the stated need. The closest alternative is weaker because directory traversal abuses path handling to access files outside the intended directory.

Question 33 : Security Architecture

During an assessment of a regional hospital, a consultant observes that clients need assurance that DNS responses are authentic and have not been tampered with. What is the best recommendation?

A. Use Base64 encoding for hostnames

B. Use FTP for zone transfers without controls

C. Disable certificate validation

D. Use DNSSEC validation

Answer: D
The scenario points to Use DNSSEC validation. The competing option is less appropriate because dNSSEC provides signed DNS data validation; encoding hostnames does not provide authenticity.

Question 34 : Security Architecture

A security analyst working with a construction contractor learns that a containerized workload should run with fewer privileges and reduced risk if compromised. Which option best addresses the requirement?

A. Expose the container runtime socket to the application

B. Embed long-lived secrets in the image

C. Run every container as privileged

D. Use a minimal image, drop unnecessary capabilities, and run as a non-root user

Answer: D
The scenario points to Use a minimal image, drop unnecessary capabilities, and run as a non-root user. The strongest distractor fails because privileged containers increase the potential impact of compromise.

Question 35 : Threats, Vulnerabilities, and Mitigations

During a review of the developer environment at a managed service provider, a caller claims to be an executive, creates urgency, and pressures help-desk staff to reset an MFA method. Which response is most appropriate?

A. Vishing

B. Credential stuffing

C. Smishing

D. Typosquatting

Answer: A
The scenario points to Vishing. The main distractor is not sufficient because smishing uses text messages; this attempt uses a voice call.