# 100% Pass Quiz 2026 Professional SY0-701: CompTIA Security+ Certification Exam Valid Test Preparation


ExamCompass
CompTIA Practice Exams

CompTIA Security+ Certification Exam SY0-701 Practice Test 1

Which of the following answers can be used to describe technical security controls? (Select 3 answers)

- Focused on protecting material assets (Your answer)
- Sometimes called logical security controls (Missed)
- Executed by computer systems (instead of people) (Your answer)
- Also known as administrative controls
- Implemented with technology (Missed)
- Primarily implemented and executed by people (as opposed to computer systems) (Your answer)

Your answer to this question is incorrect or incomplete.

Which of the answers listed below refer to examples of technical security controls? (Select 3 answers)

- Security audits
- Encryption (Missed)
- Organizational security policy
- IDSs (Missed)
- Configuration management
- Firewalls (Missed)

Your answer to this question is incorrect or incomplete.

Which of the following answers refer to the characteristic features of managerial security controls? (Select 3 answers)

DOWNLOAD the newest NewPassLeader SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1DHET8ex_Bxi3urCobpWcwj11GNLAZ9dj

The CompTIA Security+ Certification Exam (SY0-701) PDF dumps format can be accessed from any smart device such as laptops, tablets, and smartphones. NewPassLeader regularly updates the SY0-701 PDF Questions to reflect the latest CompTIA SY0-701 exam content. All test questions in the SY0-701 exam PDF format are real and latest.

In order to cater to the different requirements of people from different countries in the international market, we have prepared three kinds of versions of our SY0-701 preparation questions in this website, namely, PDF version, online engine and software version, and you can choose any one of them as you like. The three versions have their own unique characteristics. The PDF version of SY0-701 Training Materials is convenient for you to print, the software version can provide practice test for you and the online version is for you to read anywhere at any time. If you are hesitating about which version should you choose, you can download our SY0-701 free demo first to get a firsthand experience before you make any decision.

**>> SY0-701 Valid Test Preparation <<**

## CompTIA SY0-701 Practice Exams Questions

We offer you free demo for SY0-701 pdf dumps. You can check out the questions quality and usability of our training material before you buy. CompTIA SY0-701 questions are written to the highest standards of technical accuracy with accurate answers. If you prepare for your exams using NewPassLeader SY0-701 practice torrent, it is easy to succeed for your certification in the first

attempt. Besides, we offer the money refund policy, in case of failure, you can ask for full refund.

## CompTIA SY0-701 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Security Operations: This topic delves into applying common security techniques to computing resources, addressing security implications of proper hardware, software, and data asset management, managing vulnerabilities effectively, and explaining security alerting and monitoring concepts. It also discusses enhancing enterprise capabilities for security, implementing identity and access management, and utilizing automation and orchestration for secure operations. |
| Topic 2 | • General Security Concepts: This topic covers various types of security controls, fundamental security concepts, the importance of change management processes in security, and the significance of using suitable cryptographic solutions. |
| Topic 3 | • Security Architecture: Here, you'll learn about security implications across different architecture models, applying security principles to secure enterprise infrastructure in scenarios, and comparing data protection concepts and strategies. The topic also delves into the importance of resilience and recovery in security architecture. |
| Topic 4 | • Threats, Vulnerabilities, and Mitigations: In this topic, you'll find discussions comparing threat actors and motivations, explaining common threat vectors and attack surfaces, and outlining different types of vulnerabilities. Moreover, the topic focuses on analyzing indicators of malicious activity in scenarios and exploring mitigation techniques used to secure enterprises against threats. |
| Topic 5 | • Security Program Management and Oversight: Finally, this topic discusses elements of effective security governance, the risk management process, third-party risk assessment, and management processes. Additionally, the topic focuses on security compliance requirements, types and purposes of audits and assessments, and implementing security awareness practices in various scenarios. |

## CompTIA Security+ Certification Exam Sample Questions (Q545-Q550):

**NEW QUESTION # 545**
A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

- A. Defensive
- B. Offensive
- C. Passive
- D. Active

**Answer: D**

Explanation:
Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information. References = CompTIA Security+Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

**NEW QUESTION # 546**
An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted?
(Choose two.)

- A. Misinformation
- B. Impersonation
- C. Vishing
- D. Typosquatting
- E. Phishing
- F. Smishing

**Answer: E,F**

Explanation:
Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware. Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action12. In this scenario, the text message that claims to be from the payroll department is an example of smishing.
Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target. Impersonation can be done through various channels, such as phone calls, emails, text messages, or in- person visits, and can be used to obtain information, access, or money from the victim34. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.
A). Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions. Typosquatting aims to exploit the common mistakes that users make when typingweb addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads56. Typosquatting is not related to text messages or credential verification.
B). Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action78. Phishing is not related to text messages or credential verification.
C). Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply9 . Vishing is not related to text messages or credential verification.
D). Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda . Misinformation is not related to text messages or credential verification.
References = 1: What is Smishing? | Definition and Examples | Kaspersky 2: Smishing - Wikipedia 3: Impersonation Attacks: What Are They and How Do You Protect Against Them? 4: Impersonation - Wikipedia 5: What is Typosquatting? | Definition and Examples | Kaspersky 6: Typosquatting - Wikipedia 7: What is Phishing? | Definition and Examples | Kaspersky 8: Phishing - Wikipedia 9: What is Vishing? | Definition and Examples | Kaspersky : Vishing - Wikipedia : What is Misinformation? | Definition and Examples | Britannica : Misinformation - Wikipedia

**NEW QUESTION # 547**
A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks. SIEM alerts have not yet been configured. Which of the followingbestdescribes what the security analyst should do to identify this behavior?

- A. Incident response
- B. [Digital forensics
- C. E-discovery
- D. Threat hunting

**Answer: D**

Explanation:
Threat hunting is the process of proactively searching for signs of malicious activity or compromise in a network, rather than waiting for alerts or indicators of compromise (IOCs) to appear. Threat hunting can help identify new tactics, techniques, and procedures (TTPs) used by malicious actors, as well as uncover hidden or stealthy threats that may have evaded detection by security tools. Threat hunting requires a combination of skills, tools, and methodologies, such as hypothesis generation, data collection and analysis, threat intelligence, and incident response. Threat hunting can also help improve the security posture of an organization by providing feedback and recommendations for security improvements. References = CompTIA Security+ Certification Exam Objectives, Domain 4.1: Given a scenario, analyze potential indicators of malicious activity. CompTIA Security+ Study Guide (SY0-701), Chapter 4: Threat Detection and Response, page 153. Threat Hunting - SY0-701 CompTIA Security+ : 4.1, Video 3:18.

CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 3.

**NEW QUESTION # 548**
An employee who was working remotely lost a mobile device containing company data. Which of the following provides the best solution to prevent future data loss?

- A. EDR
- B. MDM
- C. FDE
- D. DLP

**Answer: B**

Explanation:
MDM enables centralized control over mobile devices, allowing administrators to enforce security policies such as device encryption, remote wipe/lock, and access controls. If a device is lost or stolen, MDM can remotely erase corporate data to prevent unauthorized access.
MDM also supports Data Loss Prevention (DLP) policies, restricting data sharing and copying between apps, and controlling app permissions, which further protects sensitive information on mobile devices.

**NEW QUESTION # 549**
Which of the following are the best methods for hardening end user devices? (Select two)

- A. Segmentation
- B. Endpoint protection
- C. Proxy server
- D. Full disk encryption
- E. Group-level permissions
- F. Account lockout

**Answer: B,D**

Explanation:
The best methods for hardening end user devices are Full Disk Encryption (FDE) and Endpoint Protection.
FDE (A) protects data at rest on laptops and workstations, ensuring that data remains unreadable if devices are lost or stolen-an explicit best practice in Security+ SY0-701.
Endpoint protection (D), including EDR/anti-malware, hardens devices by preventing, detecting, and responding to malicious activity at the host level. Together, these controls provide strong baseline protection for confidentiality and threat prevention.
Group-level permissions (B) and account lockout (C) are important access controls but do not comprehensively harden devices against malware and data exposure. Proxy servers (E) and segmentation (F) are network controls rather than endpoint hardening measures.
Therefore, the correct selections are A: Full disk encryption and D: Endpoint protection.
Explanation (Security+ SY0-701 aligned):
Deception technologies-such as honeypots, honeynets, honeyfiles, and honeytokens-are designed to intentionally lure attackers into controlled, monitored environments. Their primary purpose is not to block attacks outright or replace preventive controls, but to observe attacker behavior, techniques, and tools in a safe way. This allows organizations to collect high-value threat intelligence without exposing real production systems or sensitive data.
In the Security+ SY0-701 objectives (General Security Concepts), deception and disruption technologies are highlighted as tools that increase attacker cost and uncertainty while improving defender visibility. When an attacker interacts with a honeypot or accesses a honeyfile, it generates a strong indicator of malicious intent because legitimate users should never touch these resources. This makes deception technologies extremely valuable for early detection and analysis of attacks.
Why the other options are incorrect:
* A. Preventing malware installation is the role of endpoint protection platforms (EPP/EDR), not deception technologies.
* B. Blocking all external traffic before it reaches critical systems describes perimeter defenses like firewalls or gateways, not deception.
* D. Detecting insider threats by monitoring privileged accounts is handled by IAM controls, logging, and UEBA, not deception systems.
In short, deception technologies are proactive detection and intelligence-gathering tools. They don't stop attackers at the gate; instead, they trick attackers into revealing themselves and their methods, giving defenders insight that strengthens the overall security

strategy.
Explanation (Security+ SY0-701 aligned):
To ensure an organization can review the controls and performance of a service provider or vendor, it should include a right-to-audit clause in its contract. A right-to-audit clause explicitly grants the customer the legal authority to inspect, assess, or audit the vendor's security controls, processes, and compliance posture. This is a key concept under Security Program Management and Oversight, particularly within third-party risk management.
In the SY0-701 objectives, third-party risk management emphasizes the importance of contractual controls that allow organizations to verify that vendors are meeting security, privacy, and compliance obligations. A right-to-audit clause enables activities such as reviewing policies, examining control effectiveness, validating compliance with standards (for example, SOC reports), and confirming that agreed-upon safeguards are actually in place. Without this clause, the organization may have no formal mechanism to independently verify vendor claims.
Why the other options are incorrect:
* A. Service-level agreement (SLA): SLAs define performance metrics like uptime, response time, and availability. They do not usually grant audit authority over security controls.
* B. Memorandum of agreement (MOA): An MOA outlines general responsibilities and cooperation between parties but typically lacks enforceable audit rights.
* D. Supply chain analysis: This is a risk assessment activity, not a contractual mechanism that provides audit access.
From a Security+ perspective, the right-to-audit clause is the most effective and direct way to ensure ongoing visibility and assurance over vendor security controls and performance.

**NEW QUESTION # 550**
.....