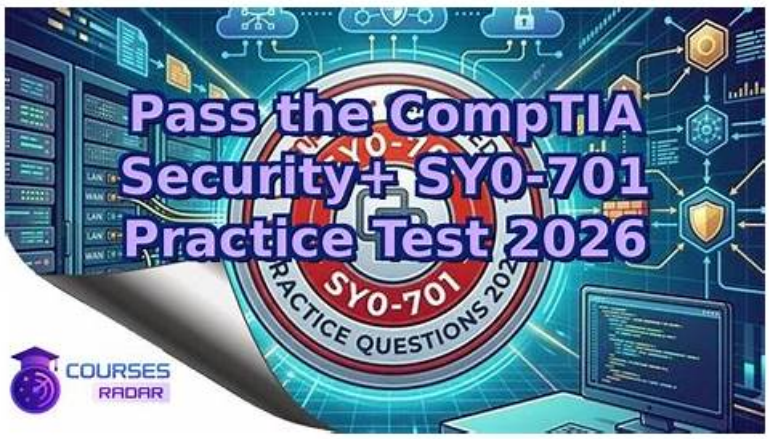
# Get CompTIA SY0-701 Practice Test To Gain Brilliant Result [2026]




DOWNLOAD the newest Pass4cram SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=11xhcRmSfyzC-kcXEQy5PWRPJ4wQM4g1w

How to let our customers know the applicability of the virtual products like SY0-701 exam software before buying? We provide the free demo of SY0-701 exam software so that you can directly enter our Pass4cram to free download the demo to check. If you have any question about it, you can directly contact with our online service or email us. When you decide to choose our product, you have already found the shortcut to success in SY0-701 Exam Certification.

## CompTIA SY0-701 Exam Overview:

| | |
|---|---|
| Certification Vendor: | CompTIA |
| Exam Name: | CompTIA Security+ Certification Exam (SY0-701) |
| Exam Number: | SY0-701 |
| Available Languages: | English, Japanese, Portuguese, Spanish, German |
| Related Certifications: | CompTIA A+<br>CompTIA Network+<br>CompTIA CySA+ |
| Exam Price: | USD $404 (may vary by region) |
| Passing Score: | 750 (on a scale of 100–900) |
| Exam Duration: | 90 minutes |
| Certificate Validity Period: | 3 years |
| Real Exam Qty: | Maximum 90 questions |
| Exam Format: | Multiple-choice, Multiple-response, Performance-based questions (PBQs) |
| Recommended Training: | Professor Messer Security+ Training<br>CompTIA CertMaster Learn Security+ |
| Exam Registration: | CompTIA Official Certification Registration<br>Pearson VUE Exam Booking |
| Sample Questions: | CompTIA SY0-701 Sample Questions |
| Exam Way: | Online proctored or in-person at Pearson VUE test centers |
| Pre Condition: | No mandatory prerequisites, recommended: CompTIA Network+ or equivalent knowledge |
| Official Syllabus URL: | https://www.comptia.org/certifications/security |

**>> SY0-701 Passed <<**

## Latest SY0-701 Test Notes & SY0-701 Exam Fee

Our company has employed a lot of leading experts in the field to compile the SY0-701 exam question. Our system of team-based working is designed to bring out the best in our people in whose minds and hands the next generation of the best SY0-701 exam torrent will ultimately take shape. Our company has a proven track record in delivering outstanding after sale services and bringing innovation to the guide torrent. Your success is guaranteed for our experts can produce world class SY0-701 Guide Torrent for our customers. You will be bound to pass the SY0-701 exam.

## CompTIA SY0-701 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • 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 2 | • 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. |
| Topic 3 | • 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 4 | • 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 5 | • 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. |

## CompTIA Security+ Certification Exam Sample Questions (Q315-Q320):

**NEW QUESTION # 315**
A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?

- A. Network segmentation
- B. Strong authentication policies
- C. Visualization and isolation of resources
- D. Data encryption

**Answer: C**

Explanation:
When hosting an on-premises software application in a cloud-based service, ensuring visualization and isolation of resources is crucial for maintaining security best practices. This involves using virtualization techniques to create isolated environments (e.g., virtual machines or containers) for different applications and services, reducing the risk of cross-tenant attacks or resource leakage.
* Network segmentation is important but pertains more to securing network traffic rather than isolating computing resources.
* Data encryption is also essential but doesn't specifically address resource isolation in a cloud environment.
* Strong authentication policies are critical for access control but do not address the need for isolating resources within the cloud environment.

**NEW QUESTION # 316**

A security analyst learns that an attack vector, which was used as a part of a recent incident, was a well-known IoT device exploit. The analyst needs to review logs to identify the time of initial exploit. Which of the following logs should the analyst review first?

- A. Wireless access point
- B. NAC
- C. Firewall
- D. Switch

**Answer: C**

Explanation:
The firewall is the choke point that records every inbound/outbound session to the IoT device; its timestamps on the first suspicious connection will most reliably show when the exploit traffic first hit the network. Reviewing those entries pinpoints the initial compromise time before diving into more granular device or segment logs.

**NEW QUESTION # 317**
Which of the following is the greatest advantage that network segmentation provides?

- A. Decreased resource utilization
- B. Enhanced endpoint protection
- C. Security zones
- D. End-to-end encryption
- E. Configuration enforcement

**Answer: C**

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The greatest advantage of network segmentation is the creation of security zones, which isolate systems into separate logical or physical network sections. According to CompTIA Security+ SY0-701, segmentation is a foundational security architecture practice used to reduce the attack surface, restrict lateral movement, enforce least privilege, and contain breaches. By dividing the network into zones-such as DMZ, internal, restricted, and guest-administrators can apply tailored access controls, firewall rules, IDS/IPS placement, and monitoring boundaries.
Segmentation provides defense-in-depth by preventing attackers from reaching critical systems even if they compromise a less-secure device. It also limits broadcast domains and improves traffic visibility. End-to-end encryption (A) protects confidentiality but is unrelated to segmentation. Decreased resource utilization (B) is not a primary benefit. Enhanced endpoint protection (C) applies to host controls, not network topology.
Configuration enforcement (D) is a benefit of centralized management, not segmentation.
Therefore, the correct answer is Security zones, the core outcome and highest-value advantage of segmentation.

**NEW QUESTION # 318**
A security analyst receives an alert that an employee has clicked on a phishing email and exposed their credentials. Which of the following should the analyst do?

- A. Lock the employee's account to prevent further unauthorized access.
- B. Wait for the confirmation from the employee before making any changes to their account.
- C. Notify all employees about the phishing attack and instruct them to avoid suspicious emails
- D. Reimage the employee's workstation to ensure no malware is present.

**Answer: A**

Explanation:
Locking the compromised account immediately prevents attackers from using the exposed credentials to gain unauthorized access, containing the incident quickly.

**NEW QUESTION # 319**
An MSSP manages firewalls for hundreds of clients. Which of the following tools would be most helpful to create a standard configuration template in order to improve the efficiency of firewall changes?

- A. Benchmarks
- B. Netflow
- C. SNMP
- D. SCAP

**Answer: A**

Explanation:
Benchmarks provide standardized security configuration baselines or templates (such as CIS Benchmarks) for systems including firewalls. Using benchmarks helps MSSPs apply consistent and secure configurations across many clients efficiently.
SNMP (A) is for network device management, Netflow (C) is for traffic analysis, and SCAP (D) is a framework for vulnerability and compliance management but not directly for template creation.
Benchmarks are fundamental for configuration management in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

**NEW QUESTION # 320**
.....