

SY0-701 Test Objectives Pdf offer you accurate Reliable Dumps Ebook to pass CompTIA Security+ Certification Exam exam



CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-701



CompTIA Security+ SY0-701 Certification Exam: Exam Objectives version 5.0
Copyright © 2023 CompTIA, Inc. All rights reserved.

CompTIA

DOWNLOAD the newest NewPassLeader SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1tJd59DRFvVZ6f4y4zhBi_i2nwcMhZ4bw

In addition to the CompTIA SY0-701 PDF questions, we offer desktop CompTIA Security+ Certification Exam (SY0-701) practice exam software and web-based CompTIA Security+ Certification Exam (SY0-701) practice test to help applicants prepare successfully for the actual Building CompTIA Security+ Certification Exam (SY0-701) exam. These CompTIA Security+ Certification Exam (SY0-701) practice exams simulate the actual SY0-701 exam conditions and provide an accurate assessment of test preparation.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">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 2	<ul style="list-style-type: none"> • 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 3	<ul style="list-style-type: none"> • 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 4	<ul style="list-style-type: none"> • 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 5	<ul style="list-style-type: none"> • 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.

>> SY0-701 Test Objectives Pdf <<

100% Pass SY0-701 - Accurate CompTIA Security+ Certification Exam Test Objectives Pdf

NewPassLeader is a very good website for CompTIA certification SY0-701 exams to provide convenience. According to the research of the past exam exercises and answers, NewPassLeader can effectively capture the content of CompTIA Certification SY0-701 Exam. NewPassLeader's CompTIA SY0-701 exam exercises have a very close similarity with real examination exercises.

CompTIA Security+ Certification Exam Sample Questions (Q728-Q733):

NEW QUESTION # 728

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Incident response procedure
- B. Business continuity plan
- C. Change management procedure
- D. Disaster recovery plan

Answer: C

Explanation:

A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network. Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:

A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.

A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.

A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.

A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the

change.

A change documentation that records the details and status of the change, as well as the lessons learned and best practices.

A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.

A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:

Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.

Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.

Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.

Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.

The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest. Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

NEW QUESTION # 729

To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed. Which of the following best describe these types of controls? (Select two).

- A. **Detective**
- B. Corrective
- C. **Deterrent**
- D. Directive
- E. Compensating
- F. Preventive

Answer: A,C

Explanation:

The CCTV system and signs about the possibility of being filmed serve as both deterrent and detective controls.

Deterrent controls: Aim to discourage potential attackers from attempting unauthorized actions.

Posting signs about CCTV serves as a deterrent by warning individuals that their actions are being monitored.

Detective controls: Identify and record unauthorized or suspicious activity. The CCTV system itself functions as a detective control by capturing and recording footage that can be reviewed later.

Preventive controls: Aim to prevent security incidents but are not directly addressed by the CCTV and signs in this context.

Corrective controls: Aim to correct or mitigate the impact of a security incident.

Directive controls: Provide guidelines or instructions but are not directly addressed by the CCTV and signs.

Compensating controls: Provide alternative measures to compensate for the absence or failure of primary controls.

NEW QUESTION # 730

A security administrator observed the following in a web server log while investigating an incident:

□ Which of the following attacks did the security administrator most likely see?

- A. **Directory traversal**
- B. Privilege escalation
- C. Brute force
- D. Credential replay

Answer: A

NEW QUESTION # 731

Which of the following would a systems administrator follow when upgrading the firmware of an organization's router?

- A. Risk tolerance
- **B. Maintenance window**
- C. Certificate signing request
- D. Software development life cycle

Answer: B

Explanation:

When upgrading the firmware of an organization's router, a systems administrator would typically follow a maintenance window.

NEW QUESTION # 732

Which of the following is an example of a data protection strategy that uses tokenization?

- **A. Replacing sensitive data with surrogate values**
- B. Hashing sensitive data in critical systems
- C. Encrypting databases containing sensitive data
- D. Removing sensitive data from production systems

Answer: A

Explanation:

Detailed Explanation:

Tokenization replaces sensitive data with non-sensitive surrogate values that retain the necessary format but are meaningless without access to the original data. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Data Masking and Tokenization".

NEW QUESTION # 733

.....

With the rapid development of the world economy, it has been universally accepted that a growing number of people have longed to become the social elite. The SY0-701 latest study guide materials will be a shortcut for a lot of people who desire to be the social elite. If you try your best to prepare for the SY0-701 Exam and get the related certification in a short time, it will be easier for you to receive the attention from many leaders of the big company like us, and it also will be very easy for many people to get a decent job in the labor market with the help of our SY0-701 learning guide.

Reliable SY0-701 Dumps Ebook: <https://www.newpassleader.com/CompTIA/SY0-701-exam-preparation-materials.html>

- 2026 100% Free SY0-701 –Excellent 100% Free Test Objectives Pdf| Reliable SY0-701 Dumps Ebook ☐ Open 《 www.prepawaypdf.com 》 enter ☐ SY0-701 ☐ and obtain a free download ☐ SY0-701 Examinations Actual Questions
- Free PDF Quiz CompTIA - SY0-701 –Efficient Test Objectives Pdf ☐ [www.pdfvce.com] is best website to obtain ☐ SY0-701 ☐ for free download ☐ SY0-701 Study Plan
- SY0-701 Examinations Actual Questions * Exam SY0-701 Lab Questions ☐ SY0-701 Certification Sample Questions ☐ Open ➡ www.examcollectionpass.com ☐ enter 《 SY0-701 》 and obtain a free download ☐ SY0-701 Study Plan
- Questions SY0-701 Pdf ☐ SY0-701 Latest Exam Pass4sure ☐ Exam SY0-701 Lab Questions ☐ Search for ⇒ SY0-701 ⇐ and obtain a free download on (www.pdfvce.com) ☐ SY0-701 Study Plan
- 100% Pass 2026 Reliable SY0-701: CompTIA Security+ Certification Exam Test Objectives Pdf ☐ Download [SY0-701] for free by simply searching on ➡ www.troytecdumps.com ☐ ☐ SY0-701 Valid Exam Practice
- SY0-701 Valid Exam Materials ☐ Exam SY0-701 Lab Questions ☐ Exam SY0-701 Lab Questions ☐ Open ➡ www.pdfvce.com ☐ enter [SY0-701] and obtain a free download ☐ Exam Dumps SY0-701 Demo
- SY0-701 Valid Exam Materials ➤ SY0-701 Valid Exam Materials ☐ SY0-701 Valid Exam Materials ☐ Enter ➤ www.examcollectionpass.com ☐ and search for ➡ SY0-701 ☐ to download for free ☐ SY0-701 Valid Test Cost
- 2026 100% Free SY0-701 –Excellent 100% Free Test Objectives Pdf| Reliable SY0-701 Dumps Ebook ☐ ➡ www.pdfvce.com ☐ is best website to obtain ➤ SY0-701 ☐ for free download ☐ SY0-701 Valid Test Cost
- Accurate SY0-701 Test Objectives Pdf and Newest Reliable SY0-701 Dumps Ebook - Well-Prepared Reliable Exam

CompTIA Security+ Certification Exam Pass4sure ☐ Search for ✓ SY0-701 ☐ ✓ ☐ and download exam materials for free through 《 www.torrentvce.com 》 ☐ SY0-701 Reliable Study Guide

- SY0-701 Valid Exam Practice ☐ SY0-701 Valid Exam Practice ☐ SY0-701 Certification Sample Questions ☐ The page for free download of 《 SY0-701 》 on ☐ www.pdfvce.com ☐ will open immediately ☐ Questions SY0-701 Pdf
- SY0-701 Valid Exam Practice ☐ Exam SY0-701 Lab Questions ☐ Testing SY0-701 Center ☐ Easily obtain free download of ☐ SY0-701 ☐ by searching on ⇒ www.examcollectionpass.com ⇐ ☐ SY0-701 Valid Exam Practice
- bbs.t-firefly.com, www.stes.tyc.edu.tw, www.alreemsedu.com, mahademy.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

2026 Latest NewPassLeader SY0-701 PDF Dumps and SY0-701 Exam Engine Free Share: https://drive.google.com/open?id=1tJd59DRFvVZ6f4y4zhBi_i2nwcMhZ4bw