100% Pass SY0-701 - Perfect CompTIA Security+ Certification Exam Valid Test Fee


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)

BONUS!!! Download part of Itcertkey SY0-701 dumps for free: https://drive.google.com/open?id=1BLmNh4V9UKWvg83kJoP1mJTyiVblLS7g

The SY0-701 would assist applicants in preparing for the CompTIA SY0-701 exam successfully in one go SY0-701 would provide SY0-701 candidates with accurate and real CompTIA Security+ Certification Exam (SY0-701) Dumps which are necessary to clear the SY0-701 test quickly. Students will feel at ease since the content they are provided with is organized rather than dispersed.

CompTIA SY0-701 Exam Syllabus Topics:

Section	Weight	Objectives

Topic 1: Governance, Risk & Compliance	14%	- Explain privacy and sensitive data concepts in relation to security • 1. Data classification and handling • 2. Privacy and data protection regulations • 3. Privacy-enhancing technologies - Explain regulations, standards, and frameworks that impact cybersecurity • 1. Regulations, standards, and frameworks • 2. Public and private sector compliance requirements - Given a scenario, apply risk management strategies • 1. Risk mitigation and treatment • 2. Risk monitoring and reporting • 3. Risk identification and assessment - Compare and contrast the various types of controls • 1. Control categories • 2. Control types
Topic 2: Operations & Incident Response	16%	- Explain the use of frameworks, policies, procedures, and controls • 1. Security controls • 2. Governance and compliance frameworks • 3. Security policies and procedures - Given a scenario, use the appropriate tool to assess organizational security • 1. Cybersecurity automation and orchestration • 2. Network reconnaissance and discovery • 3. Vulnerability scanning and remediation • 4. Log analysis and packet capture - Given a scenario, apply incident response and recovery procedures • 1. Business continuity and disaster recovery • 2. Incident response procedures • 3. Incident investigation and digital forensics - Describe the collection and use of threat intelligence • 1. Threat intelligence sources • 2. Threat intelligence analysis

Topic 3: Architecture & Design	21%	- Explain the importance of cryptographic solutions • 1. Cryptographic standards and protocols • 2. Hashing and digital signatures • 3. Public key infrastructure (PKI) • 4. Symmetric and asymmetric cryptography - Given a scenario, implement secure network architecture concepts • 1. Network segmentation • 2. Network monitoring • 3. Network device placement • 4. Secure network designs - Given a scenario, implement secure application and protocol concepts • 1. Secure application development • 2. Hardening techniques • 3. Application protocols - Explain the concept of the attack surface and network architecture • 1. Virtualization and cloud concepts • 2. Network architecture • 3. Zero Trust • 4. Physical security controls - Explain the importance of embedded and specialized systems security • 1. Specialized systems • 2. Embedded systems • 3. Security constraints
Topic 4: Threats, Attacks & Vulnerabilities	24%	- Explain penetration testing and vulnerability scanning concepts • 1. Remediation and mitigation • 2. Vulnerability scanning • 3. Penetration testing methodologies - Given a scenario, analyze indicators of malicious activity • 1. Indicators of compromise • 2. Attack framework concepts • 3. Indicators of attack - Compare and contrast different types of security threats and attacks • 1. Social engineering attacks • 2. Network attacks • 3. Supply chain attacks • 4. Application/web-based attacks • 5. Insider threats • 6. Malware types

Topic 5: Implementation	25%	- Given a scenario, implement appropriate environmental and physical controls • 1. Environmental controls • 2. Composite risks • 3. Physical security controls - Given a scenario, implement cybersecurity resilience solutions • 1. Redundancy and fault tolerance • 2. Backup and recovery strategies • 3. Resiliency and continuity measures - Given a scenario, implement identity and access management (IAM) solutions • 1. Access control models • 2. Directory services and federation • 3. Authentication factors and methods • 4. Identity and access management concepts - Given a scenario, implement appropriate controls for mobile and embedded devices • 1. Mobile device management • 2. Mobile device deployment • 3. Mobile device enforcement and monitoring

Study Material For CompTIA SY0-701 Exam Questions

Itcertkey presents you with their effective CompTIA Security+ Certification Exam (SY0-701) exam dumps as we know that the registration fee is very high (from $100-$1000). Itcertkey product covers all the topics with a complete collection of actual SY0-701 exam questions. We also offer free demos and up to 1 year of free CompTIA Dumps updates. So, our CompTIA SY0-701 prep material is the best to enhance knowledge which is helpful to pass CompTIA Security+ Certification Exam (SY0-701) on the first attempt.

CompTIA Security+ Certification Exam Sample Questions (Q821-Q826):

NEW QUESTION # 821
A user attempts to send an invoice to a customer. When the user follows up with the customer to see if the invoice was received, the customer informs the user that it went to the spam folder. The management team has asked the systems administrator to implement measures to reduce the likelihood of this happening again by implementing server authentication. Which of the following should the systems administrator implement?

- A. DMARC
- B. SPF
- C. XDR
- D. DNSSEC

Answer: B

Explanation:
SPF (Sender Policy Framework) lets the domain owner specify which mail servers are authorized to send email on its behalf. Publishing an SPF record in DNS helps recipient mail systems verify the sending server's legitimacy, reducing the chance that legitimate messages are marked as spam.

NEW QUESTION # 822
A security officer observes that a software development team is not complying with its corporate security policy on encrypting

confidential data. Which of the following categories refers to this type of non- compliance?

- A. Standard
- B. Regulation
- C. External
- D. Internal

Answer: D

Explanation:
Non-compliance with internal policies, such as corporate security policies, falls under internal non- compliance. These are rules created and enforced within the organization to maintain security standards.
External non-compliance (A) refers to violations of outside regulations or laws. Standards (B) are generally established best practices or industry guidelines, and regulation (C) refers to legal or governmental requirements.
Internal compliance management is a key focus area in the Security Program Management domain of SY0-701 #6:Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION # 823
A security administrator is configuring fileshares. The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties. Which of the following best describes why the administrator performed these actions?

- A. Least privilege
- B. Access control monitoring
- C. Data replication requirements
- D. Encryption standard compliance

Answer: A

Explanation:
The security administrator's actions of removing default permissions and adding permissions only for users who need access as part of their job duties best describe the principle of least privilege. This principle ensures that users are granted the minimum necessary access to perform their job functions, reducing the risk of unauthorized access or data breaches.
Least privilege: Limits access rights for users to the bare minimum necessary for their job duties, enhancing security by reducing potential attack surfaces.
Encryption standard compliance: Involves meeting encryption requirements, but it does not explain the removal and assignment of specific permissions.
Data replication requirements: Focus on duplicating data across different systems for redundancy and availability, not related to user permissions.
Access control monitoring: Involves tracking and reviewing access to resources, but the scenario is about setting permissions, not monitoring them.

NEW QUESTION # 824
Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Decommissioning
- B. Hardening
- C. Isolation
- D. Segmentation

Answer: B

Explanation:
A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats.
One of the best ways to handle a legacy server running a critical business application is to harden it.
Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability.

Hardening a legacy server may involve steps such as:
Applying patches and updates to the operating system and the application, if available Removing or disabling unnecessary services, features, or accounts Configuring firewall rules and network access control lists to restrict inbound and outbound traffic Enabling encryption and authentication for data transmission and storage Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible.
References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain
3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective:
Legacy systems 2

NEW QUESTION # 825
Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A. Impact analysis
- B. Change management boards
- C. Scheduled downtime
- D. Backout plan

Answer: C

Explanation:
Explanation
Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

NEW QUESTION # 826
.....

The main key to passing the SY0-701 exam is to use your time affectionately and grasp every topic so you can attempt the maximum number of questions in the actual SY0-701 Exam. By studying the questions mentioned in the prep material, the candidates have control over the exam anxiety in no time.

obtain a free download on ➤ www.pdfvce.com □ □Reliable SY0-701 Braindumps Ebook

- Real SY0-701 Dumps Free □ VCE SY0-701 Exam Simulator □ Test SY0-701 Dumps Free □ Download ⇛ SY0-701 ⇚ for free by simply entering ➽ www.practicevce.com □ website □Valid SY0-701 Test Question
- CompTIA Security+ Certification Exam pdf test - SY0-701 test dumps □ Search for ➡ SY0-701 □□□ on 《 www.pdfvce.com 》 immediately to obtain a free download □Valid Dumps SY0-701 Pdf
- VCE SY0-701 Exam Simulator □ Valid Dumps SY0-701 Pdf □ SY0-701 Exam Certification Cost □ Easily obtain ▶ SY0-701 ◀ for free download through 「 www.practicevce.com 」 □VCE SY0-701 Exam Simulator
-

P.S. Free & New SY0-701 dumps are available on Google Drive shared by Itcertkey: https://drive.google.com/open?id=1BLmNh4V9UKWvg83kJoP1mJTyiVblLS7g