Pass Guaranteed Quiz CompTIA - SY0-701 - CompTIA Security+ Certification Exam Perfect Valid Test Answers


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)

2026 Latest ExamBoosts SY0-701 PDF Dumps and SY0-701 Exam Engine Free Share: https://drive.google.com/open?id=1CD-sXJlwn0UaoxeMdRZrnp8GuqJuJ8qz

Firmly believe in an idea, the SY0-701 exam questions are as long as the user to follow our steps, follow our curriculum requirements, users can be good to achieve their goals, to obtain the SY0-701 qualification certificate of the target. Before you make your decision to buy our SY0-701 learning guide, you can free download the demos to check the quality and validity. Then you can know the SY0-701 training materials more deeply.

Choose SY0-701 premium files, you will pass for sure. Each questions & answers of SY0-701 free training pdf are edited and summarized by our specialist with utmost care and professionalism. The CompTIA SY0-701 latest online test is valid and really trustworthy for you to rely on. The highly relevant content & best valid and useful SY0-701 Exam Torrent will give you more confidence and help you pass easily.

>> Valid SY0-701 Test Answers <<

PDF SY0-701 Cram Exam | Detail SY0-701 Explanation

Your purchase with ExamBoosts is safe and fast. We use Paypal for payment and committed to keep your personal information secret and never share your information to the third part without your permission. In addition, our CompTIA SY0-701 practice exam torrent can be available for immediate download after your payment. Besides, we guarantee you 100% pass for SY0-701 Actual Test, in case of failure, you can ask for full refund. The refund procedure is very easy. You just need to show us your SY0-

701 failure certification, then after confirmation, we will deal with your case.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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 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	• 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 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.

CompTIA Security+ Certification Exam Sample Questions (Q664-Q669):

NEW QUESTION # 664
Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

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

Answer: C

Explanation:
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. References = 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 # 665
An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?

- A. Authentication
- B. Application
- C. Network
- D. System

Answer: C

Explanation:
To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would provide information on outbound and inbound traffic, allowing the analyst to see if the user's system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.

NEW QUESTION # 666
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. Scheduled downtime
- B. Impact analysis
- C. Backout plan
- D. Change management boards

Answer: A

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.

NEW QUESTION # 667
A utility company is designing a new platform that will host all the virtual machines used by business applications. The requirements include:
- A starting baseline of 50% memory utilization
- Storage scalability
- Single circuit failure resilience
Which of the following best meets all of these requirements?

- A. Transitioning the platform to an IaaS provider
- B. Deploying multiple large NAS devices for each host
- C. Connecting dual PDUs to redundant power supplies
- D. Configuring network load balancing for multiple paths

Answer: A

Explanation:
This option addresses the 50% memory utilization baseline, provides scalable storage, and typically includes built-in redundancy to handle single circuit failures. IaaS providers offer flexible resource allocation, easy scalability, and robust infrastructure with multiple layers of redundancy.

NEW QUESTION # 668
After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

- A. Web-based administration
- B. VLANs
- C. Console access
- D. Routing protocols

Answer: A

Explanation:
Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANs).

NEW QUESTION # 669
.....

- Exam SY0-701 Questions Exam SY0-701 Questions Valid SY0-701 Exam Pass4sure Search for ➤ SY0-701 and download exam materials for free through ▶ www.validtorrent.com ◀ New SY0-701 Test Cram
- Brilliantly Updated CompTIA SY0-701 Exam Dumps Search for ☀ SY0-701 ☀ and easily obtain a free download on ➤ www.pdfvce.com Reliable SY0-701 Exam Syllabus
- SY0-701 Dumps Discount SY0-701 Real Dump SY0-701 Dumps Discount Search for 「SY0-701」 on ➻ www.easy4engine.com immediately to obtain a free download SY0-701 Actual Questions
- Exam SY0-701 Questions Exam SY0-701 Questions Reliable SY0-701 Exam Syllabus Search for SY0-701 and obtain a free download on 《www.pdfvce.com》 Valid SY0-701 Exam Pass4sure
- Brilliantly Updated CompTIA SY0-701 Exam Dumps Search for ➥ SY0-701 and obtain a free download on www.vce4dumps.com SY0-701 Reliable Practice Questions
- Get 100% Passing Success With True SY0-701 Exam Search on www.pdfvce.com for [SY0-701] to obtain exam materials for free download ✳SY0-701 Real Dump
- Exam SY0-701 Questions ↕ SY0-701 Test Simulator Reliable SY0-701 Exam Syllabus Download ➻ SY0-701   for free by simply entering ➤ www.prepawaypdf.com website SY0-701 Reliable Practice Questions
- SY0-701 Reliable Practice Questions New SY0-701 Test Cram SY0-701 Actual Questions Search for 《SY0-701》 and easily obtain a free download on 「www.pdfvce.com」 SY0-701 Actual Questions
- Latest SY0-701 Test Blueprint New SY0-701 Test Sims Guaranteed SY0-701 Success Search for "SY0-701" and download it for free on ☀ www.prepawaypdf.com ☀ website SY0-701 Actual Questions
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

What's more, part of that ExamBoosts SY0-701 dumps now are free: https://drive.google.com/open?id=1CD-sXJlwn0UaoxeMdRZrnp8GuqJuJ8qz