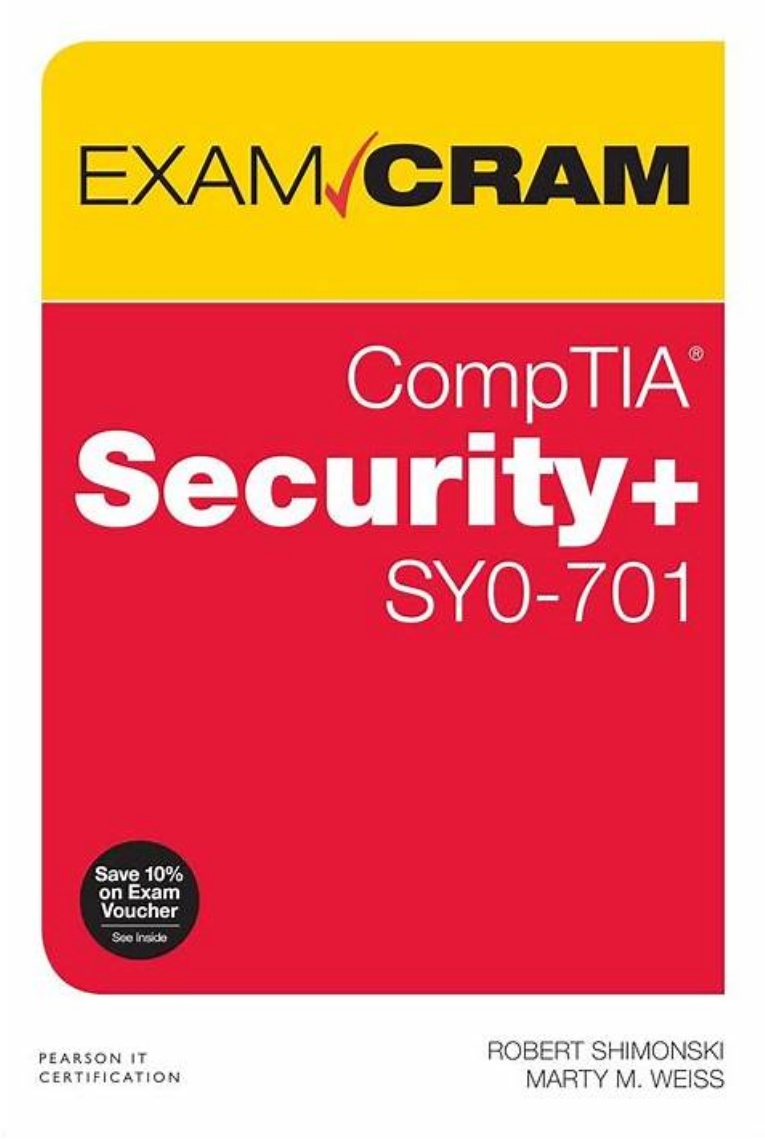
SY0-701 Latest Braindumps Files - SY0-701 Valid Exam Cram



DOWNLOAD the newest Test4Cram SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1nwgFmmnkRW5YC8Dyfmk580327Eb_IMuz

If you want to be a part of a great company, such as SY0-701, preparing and taking the exam with SY0-701 study guide will be your best choice, because there have been more and more big companies to pay real attention to these people who have passed the SY0-701 Exam and have got the related certification in the past years. It is a generally accepted fact that the SY0-701 exam has attracted more and more attention and become widely acceptable in the past years.

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 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 3	• 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 4	• 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 5	• 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.

CompTIA SY0-701 Valid Exam Cram, SY0-701 Reliable Test Preparation

Life is beset with all different obstacles that are not easily overcome. For instance, SY0-701 exams may be insurmountable barriers for the majority of population. However, with the help of our exam test, exams are no longer problems for you. The reason why our SY0-701 training materials outweigh other study prep can be attributed to three aspects, namely free renewal in one year, immediate download after payment and simulation for the software version. Now that using our SY0-701 practice materials have become an irresistible trend, why don't you accept SY0-701 learning guide with pleasure?

CompTIA Security+ Certification Exam Sample Questions (Q778-Q783):

NEW QUESTION # 778
Which of the following data roles is responsible for identifying risks and appropriate access to data?

- A. Owner
- B. Steward
- C. Custodian
- D. Controller

Answer: A

Explanation:
The data owner is the role responsible for identifying risks to data and determining who should have access to that data. The owner has the authority to make decisions about the protection and usage of the data, including setting access controls and ensuring that appropriate security measures are in place.

NEW QUESTION # 779
A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis Which of the following types of controls is the company setting up?

- A. Detective
- B. Corrective
- C. Deterrent

- D. Preventive

Answer: A

Explanation:
A detective control is a type of security control that monitors and analyzes events to detect and report on potential or actual security incidents. A SIEM system is an example of a detective control, as it collects, correlates, and analyzes security data from various sources and generates alerts for security teams. Corrective, preventive, and deterrent controls are different types of security controls that aim to restore, protect, or discourage security breaches, respectively. References: CompTIA Security+ Study Guide: Exam SY0-701,
9th Edition, page 33; What is Security Information and Event Management (SIEM)?

NEW QUESTION # 780
A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.
Which of the following is the most important consideration during development?

- A. Availability
- B. Cost
- C. Scalability
- D. Ease of deployment

Answer: A

Explanation:
Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of-service attacks, and have backup and recovery plans in case of failures2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

NEW QUESTION # 781
A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring. Which of the following strategies would best accomplish this goal?

- A. Enabling full packet capture for traffic entering and exiting the servers
- B. Deploying network traffic sensors on the same subnet as the servers
- C. Logging all NetFlow traffic into a SIEM
- D. Logging endpoint and OS-specific security logs

Answer: A

Explanation:
Explanation
Full packet capture is a technique that records all network traffic passing through a device, such as a router or firewall. It allows for detailed analysis and investigation of network events, such as SQLi attacks, by providing the complete content and context of the packets. Full packet capture can help identify the source, destination, payload, and timing of an SQLi attack, as well as the impact on the server and database. Logging NetFlow traffic, network traffic sensors, and endpoint and OS-specific security logs can provide some information about network activity, but they do not capture the full content of the packets, which may limit the scope and depth of the investigation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page
372-373

NEW QUESTION # 782
An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions over the phone to use a new account. Which of the following would most likely prevent this activity in the future?

- A. Implementing insider threat detection measures
- B. Executing regular phishing campaigns

- C. Updating processes for sending wire transfers
- D. Standardizing security incident reporting

Answer: C

Explanation:
Comprehensive and Detailed In-Depth Explanation:Updating wire transfer processes to include verification steps (such as requiring dual approval or verifying account changes via a secondary communication method) canprevent fraudulent transactions. Attackers often use business email compromise (BEC) or pretexting to trick employees into transferring funds to fraudulent accounts.
* Standardizing security incident reportingis useful for tracking security events but does not prevent fraud in real time.
* Executing regular phishing campaignsimproves awareness but does not enforce a verification process for financial transactions.
* Implementing insider threat detectionfocuses on internal risks but does not specifically prevent external fraud.
Amore secure wire transfer processwith additional verification steps is the most effective measure against fraudulent transactions.

NEW QUESTION # 783
.....

CompTIA SY0-701 certification is indeed a better idea before you start with the interviews. CompTIA SY0-701 certification will add up to your excellence in your field and leave no space for any doubts in the mind of the hiring team. But, have you thought about how can you prepare for the CompTIA SY0-701 Exam Questions? Do you have any idea how we can crack the nut to give wings to our dreams?