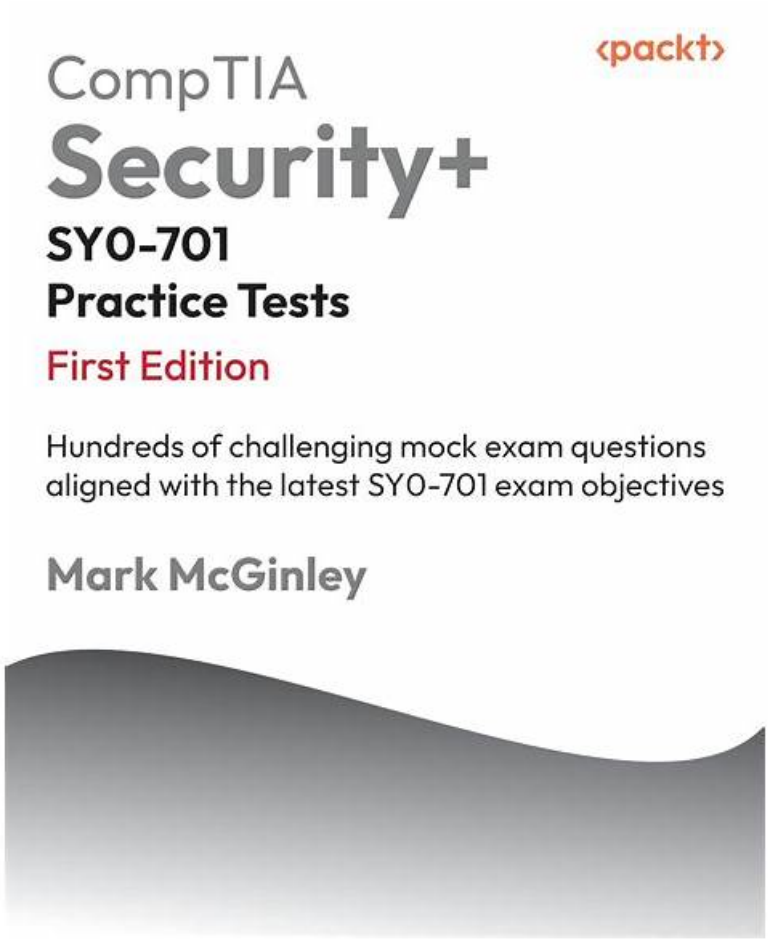
Latest SY0-701 Exam Materials - SY0-701 Test Fee



2026 Latest LatestCram SY0-701 PDF Dumps and SY0-701 Exam Engine Free Share: https://drive.google.com/open?id=1R51qKHkvVMvkZXVAWy3z8JO1odqJ-v4S

When you know you will enjoy one year free update after purchase, you may consider how to get the latest CompTIA SY0-701 exam torrent. Here, we will tell you, the LatestCram system will send the update SY0-701 exam dumps to you automatically. You can pay attention to your payment email. If you find there is update and do not find any update email, do not worry, you can check your spam. If there is still not, please contact us by email or online chat. Besides, if you have any questions about CompTIA SY0-701, please contact us at any time. Our 7/24 customer service will be always at your side and solve your problem at once.

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	• 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 3	• 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 4	• 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 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.

Latest SY0-701 Exam Materials High Hit Rate Questions Pool Only at LatestCram

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 Security+ Certification Exam Sample Questions (Q252-Q257):

NEW QUESTION # 252
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Answer:

Explanation:
Explanation:
Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification
A screenshot of a computer program Description automatically generated with low confidence

NEW QUESTION # 253
Which of the following should a security analyst use to prioritize the remediation of a vulnerability?

- A. CVSS
- B. CVE
- C. IoC
- D. OSINT

Answer: A

Explanation:
The Common Vulnerability Scoring System (CVSS) provides a standardized severity score for vulnerabilities, enabling analysts to prioritize remediation efforts based on risk impact.

NEW QUESTION # 254
A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

- A. GPO
- B. FIM
- C. NAC
- D. SPF

Answer: B

Explanation:
FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.
Some of the benefits of FIM are:
It can prevent data tampering and corruption by verifying the checksums or hashes of the files.
It can identify the source and time of the changes by logging the user and system actions.
It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.
It can support forensic analysis and incident response by providing evidence and audit trails of the changes.

NEW QUESTION # 255
A security analyst is evaluating a SaaS application that the human resources department would like to implement. The analyst requests a SOC 2 report from the SaaS vendor. Which of the following processes is the analyst most likely conducting?

- A. Attestation
- B. Penetration testing
- C. Internal audit
- D. Due diligence

Answer: D

NEW QUESTION # 256
Which of the following security control types does an acceptable use policy best represent?

- A. Detective
- B. Preventive
- C. Compensating
- D. Corrective

Answer: B

Explanation:
Explanation
An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network1.
An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or administrative in nature2.
Some examples of preventive controls are:
Locks, fences, or guards that prevent unauthorized physical access to a facility or a device Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors by users or employees An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or

availability of the network or the system, such as:
Downloading or installing unauthorized or malicious software
Accessing or sharing sensitive or confidential information without authorization or encryption Using the network or the system for personal, illegal, or unethical purposes Bypassing or disabling security controls or mechanisms Connecting unsecured or unapproved devices to the network By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions3.
References = 1: How to Create an Acceptable Use Policy - CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A Corporate Acceptable Use Policy - CompTIA

NEW QUESTION # 257
.....

Are you preparing for the CompTIA SY0-701 certification exam? Whether you're an experienced professional CompTIA SY0-701 looking to take your career to the next level or a recent graduate trying to break into the tech field, the road to CompTIA SY0-701 Certification can be a long and challenging one. The good news is that you do not have to navigate it alone.

What's more, part of that LatestCram SY0-701 dumps now are free: https://drive.google.com/open?id=1R51qKHkvVMvkZXVAWy3z8JO1odqJ-v4S