New SY0-701 Authentic Exam Hub Pass Certify | Latest Valid Test SY0-701 Braindumps: CompTIA Security+ Certification Exam

DOWNLOAD the newest GetValidTest SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1uwifuXVFOLBoCxrlSXc36XB034o1ikMq

GetValidTest's SY0-701 exam training materials evoke great repercussions in the examinees, and has established a very good reputation, which means that choosing GetValidTest SY0-701 exam training materials is to choose success. After you buy our SY0-701 VCE Dumps, if you fail to pass the certification exam or there are any problems of learning materials, we will give a full refund. What's more, after you buy our SY0-701 exam, we will provide one year free renewal service.

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	• 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	• 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	• 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	• 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.

>> SY0-701 Authentic Exam Hub <<

Valid Test SY0-701 Braindumps & SY0-701 Certification Cost

All three CompTIA SY0-701 exam dumps formats are ready for download. Just select the best CompTIA SY0-701 exam questions type and download it after paying an affordable SY0-701 exam questions charge and start preparation today. We offer you the most accurate SY0-701 Exam Answers that will be your key to pass the certification exam in your first try.

CompTIA Security+ Certification Exam Sample Questions (Q829-Q834):

NEW QUESTION # 829
Which of the following must be considered when designing a high-availability network? (Choose two).

- A. Attack surface
- B. Physical isolation
- C. Ability to patch
- D. Ease of recovery
- E. Responsiveness
- F. Extensible authentication

Answer: A,D

Explanation:
A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors12:
Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.
Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.
The other options are not directly related to high-availability network design:
Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.
Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.
Responsiveness: This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.
Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.
Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer.

NEW QUESTION # 830
An organization is required to provide assurance that its controls are properly designed and operating effectively. Which of the following reports will best achieve the objective?

- A. Red teaming
- B. Independent audit
- C. Vulnerability assessment
- D. Penetration testing

Answer: C

NEW QUESTION # 831
A security analyst reviews domain activity logs and notices the following:
Which of the following is the best explanation for what the security analyst has discovered?

- A. A keylogger is installed on [smith's workstation
- B. An attacker is attempting to brute force ismith's account.
- C. The user jsmith's account has been locked out.
- D. Ransomware has been deployed in the domain.

Answer: B

Explanation:
Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes - SY0-601 CompTIA Security+ : 1.1

NEW QUESTION # 832
Which of the following phases of the incident response process attempts to minimize disruption?

- A. Recovery
- B. Preparation
- C. Containment
- D. Analysis

Answer: C

Explanation:
Containment is the phase where an organization attempts to minimize the damage caused by a security incident. This may involve isolating affected systems, blocking malicious traffic, or temporarily shutting down compromised services to prevent further impact.
Recovery (A) focuses on restoring normal operations after an incident.
Preparation (C) involves planning and readiness before an incident occurs.
Analysis (D) involves investigating the root cause and assessing the damage.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

NEW QUESTION # 833
A company tested and validated the effectiveness of network security appliances within the corporate network. The IDS detected a high rate of SQL injection attacks against the company's servers, and the company's perimeter firewall is at capacity. Which of the following would be the best action to maintain security and reduce the traffic to the perimeter firewall?

- A. Convert the firewall to a WAF and use IPSec tunnels to increase throughput.
- B. Set the appliance to IPS mode and place it in front of the company firewall.
- C. Set the firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.
- D. Configure the firewall to perform deep packet inspection and monitor TLS traffic.

Answer: B

Explanation:
Given the scenario where an Intrusion Detection System (IDS) has detected a high rate of SQL injection attacks and the perimeter firewall is at capacity, the best action would be to set the appliance to Intrusion Prevention System (IPS) mode and place it in front of the company firewall. This approach has several benefits:
Intrusion Prevention System (IPS): Unlike IDS, which only detects and alerts on malicious activity, IPS can actively block and

prevent those activities. Placing an IPS in front of the firewall means it can filter out malicious traffic before it reaches the firewall, reducing the load on the firewall and enhancing overall security.
Reducing Traffic Load: By blocking SQL injection attacks and other malicious traffic before it reaches the firewall, the IPS helps maintain the firewall's performance and prevents it from becoming a bottleneck.
Enhanced Security: The IPS provides an additional layer of defense, identifying and mitigating threats in real-time.
Option B (Convert the firewall to a WAF and use IPSec tunnels) would not address the primary issue of reducing traffic to the firewall effectively. Option C (Set the firewall to fail open) would compromise security. Option D (Deep packet inspection) could be resource-intensive and might not alleviate the firewall capacity issue effectively.

NEW QUESTION # 834
.....

The CompTIA Security+ Certification Exam exam is one of the most valuable certification exams. The CompTIA CompTIA Security+ Certification Exam exam opens a door for beginners or experienced GetValidTest professionals to enhance in-demand skills and gain knowledge. SY0-701 Exam credential is proof of candidates' expertise and knowledge. After getting success in the CompTIA CompTIA Security+ Certification Exam exam, candidates can put their careers on the fast route and achieve their goals in a short period of time.