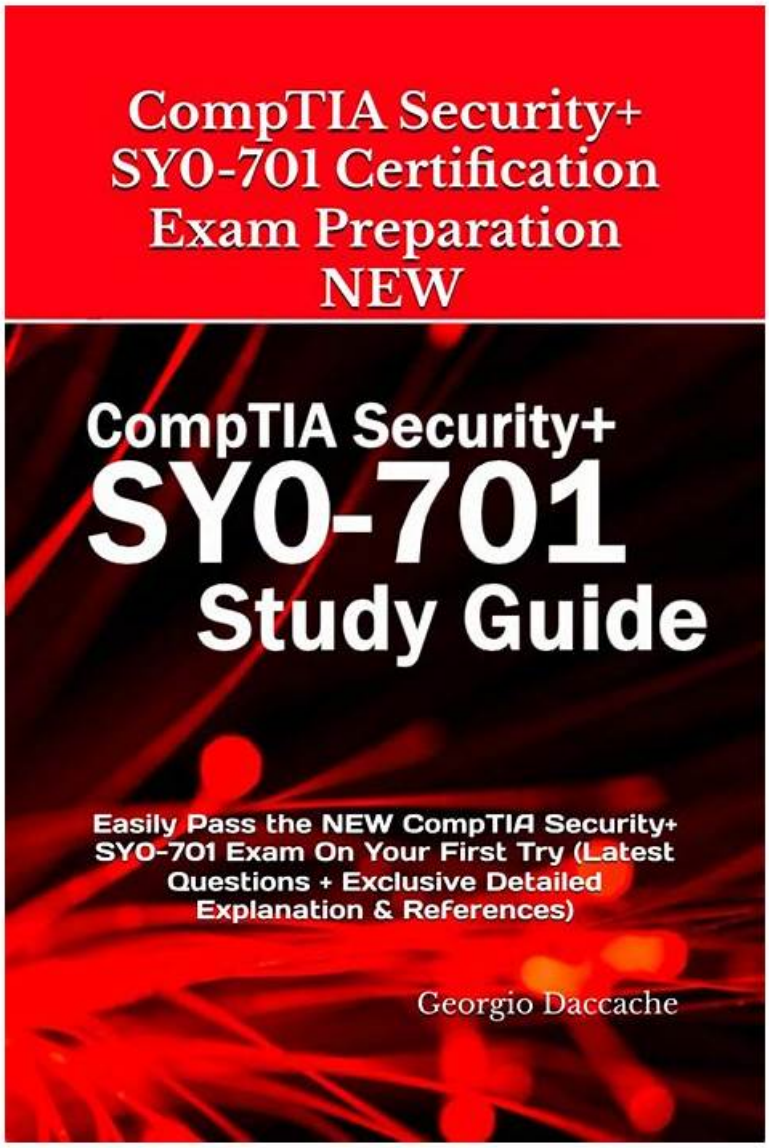
Exam SY0-701 Preparation - SY0-701 Latest Exam Duration



BONUS!!! Download part of ITExamSimulator SY0-701 dumps for free: https://drive.google.com/open?id=1kaHqX4gB0BMkIddu20j2Zv7FeqVjqatT

They can try a free demo for satisfaction before buying our CompTIA SY0-701 dumps. And a 24/7 support system assists them whenever they are stuck in any problem or issue. This CompTIA Security+ Certification Exam (SY0-701) questions is a complete package and a blessing for candidates who want to prepare quickly for the SY0-701 exam. Buy It Now!

Now in such society with a galaxy of talents, stabilizing your job position is the best survival method. But stabilizing job position is not so easy. When others are fighting to improve their vocational ability, if you still making no progress and take things as they are, then you will be eliminated. In order to stabilize your job position, you need to constantly improve your SY0-701 professional ability and keep up with the pace of others to let you not fall far behind others.

>> Exam SY0-701 Preparation <<

SY0-701 Latest Exam Duration - Updated SY0-701 Testkings

The ITExamSimulator is one of the top-rated and renowned platforms that has been offering real and valid CompTIA Security+

Certification Exam (SY0-701) exam practice test questions for many years. During this long time period countless CompTIA Security+ Certification Exam (SY0-701) exam candidates have passed their dream certification and they are now certified CompTIA professionals and pursuing a rewarding career in the market.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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 5	• 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.

CompTIA Security+ Certification Exam Sample Questions (Q290-Q295):

NEW QUESTION # 290
A systems administrator is working on a solution with the following requirements:
* Provide a secure zone.
* Enforce a company-wide access control policy.
* Reduce the scope of threats.
Which of the following is the systems administrator setting up?

- A. CIA
- B. Zero Trust
- C. AAA
- D. Non-repudiation

Answer: B

Explanation:
Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.
Reference:
5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.
8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

NEW QUESTION # 291
A company is discarding a classified storage array and hires an outside vendor to complete the disposal. Which of the following should the company request from the vendor?

- A. Certification
- B. Inventory list
- C. Classification
- D. Proof of ownership

Answer: A

Explanation:
The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel involved.
Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

NEW QUESTION # 292
An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

- A. DLP
- B. ACL
- C. IDS
- D. IPS

Answer: D

Explanation:
An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

NEW QUESTION # 293
Which of the following steps in the risk management process involves establishing the scope and potential risks involved with a project?

- A. Risk monitoring and review
- B. Risk identification
- C. Risk mitigation
- D. Risk treatment

Answer: B

Explanation:
Risk identificationis the first step in the risk management process, where potential threats and vulnerabilities are analyzed to understand their impact on an organization. This includesidentifying assets, evaluating threats, and assessing potential vulnerabilities.
Risk mitigation: Reducing risk by implementing controls.
Risk treatment: Determining how to handle identified risks.
Risk monitoring and review: Ongoing evaluation of risk controls.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

NEW QUESTION # 294
Which of the following is required for an organization to properly manage its restore process in the event of system failure?

- A. SDLC
- B. IRP
- C. DRP
- D. RPO

Answer: C

Explanation:
A disaster recovery plan (DRP) 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. A DRP typically includes the following elements:
A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.
A business impact analysis that prioritizes the recovery of the most essential functions and data.
A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.
A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss. Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

NEW QUESTION # 295
.....

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, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of ITExamSimulator SY0-701 dumps from Cloud Storage: https://drive.google.com/open?id=1kaHqX4gB0BMkIddu20j2Zv7FeqVjqatT