CompTIA SY0-701 Online Practice Test (CompTIA-SY0-701-Practice-Test)


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)

DOWNLOAD the newest ITexamReview SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1zLlCF1l4D_nvMoIFtlcBYCyW-AMvl5O0

By analyzing the syllabus and new trend, our SY0-701 practice engine is totally in line with this exam for your reference. So grapple with this chance, our SY0-701 learning materials will not let you down. With our SY0-701 Study Guide, not only that you can pass you exam easily and smoothly, but also you can have a wonderful study experience based on the diversed versions of our SY0-701 training prep.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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.

Valid SY0-701 Exam Tutorial - Pass SY0-701 Guide

As long as you have a try on our products you will find that both the language and the content of our SY0-701 practice braindumps are simple. The language of our SY0-701 study materials is easy to be understood and suitable for any learners. The content emphasizes the focus and seizes the key to use refined SY0-701 Exam Questions And Answers to let the learners master the most important information by using the least amount of them.

CompTIA Security+ Certification Exam Sample Questions (Q520-Q525):

NEW QUESTION # 520
Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A. Jailbreaking
- B. Memory injection
- C. Side loading
- D. Resource reuse

Answer: C

Explanation:
Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. Reference = Sideloading - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers - CompTIA Security+ SY0-501 - 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

NEW QUESTION # 521
Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Decommissioning
- B. Isolation
- C. Hardening
- D. Segmentation

Answer: C

Explanation:
A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and

compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats.
One of the best ways to handle a legacy server running a critical business application is to harden it.
Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability.
Hardening a legacy server may involve steps such as:
Applying patches and updates to the operating system and the application, if available Removing or disabling unnecessary services, features, or accounts Configuring firewall rules and network access control lists to restrict inbound and outbound traffic Enabling encryption and authentication for data transmission and storage Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible.

NEW QUESTION # 522
A security analyst needs to propose a remediation plan 'or each item in a risk register. The item with the highest priority requires employees to have separate logins for SaaS solutions and different password complexity requirements for each solution. Which of the following implementation plans will most likely resolve this security issue?

- A. Securing access to each SaaS by using a single wildcard certificate
- B. Integrating each SaaS solution with the Identity provider
- C. Creating a unified password complexity standard
- D. Configuring geofencing on each SaaS solution

Answer: B

Explanation:
Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

NEW QUESTION # 523
A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A. SLA
- B. MOA
- C. SOW
- D. MOU

Answer: A

Explanation:
A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and amemorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

NEW QUESTION # 524

An organization is required to maintain financial data records for three years and customer data for five years. Which of the following data management policies should the organization implement?

- A. Retention
- B. Inventory
- C. Certification
- D. Destruction

Answer: A

Explanation:
The organization should implement a retention policy to ensure that financial data records are kept for three years and customer data for five years. A retention policy specifies how long different types of data should be maintained and when they should be deleted.
Retention: Ensures that data is kept for a specific period to comply with legal, regulatory, or business requirements.
Destruction: Involves securely deleting data that is no longer needed, which is part of the retention lifecycle but not the primary focus here.
Inventory: Involves keeping track of data assets, not specifically about how long to retain data.
Certification: Ensures that processes and systems meet certain standards, not directly related to data retention periods.

NEW QUESTION # 525
.....

Overall we can say that SY0-701 certification can provide you with several benefits that can assist you to advance your career and achieve your professional goals. Are you ready to gain all these personal and professional benefits? Looking for a sample, is smart and quick for SY0-701 Exam Dumps preparation? If your answer is yes then you do not need to go anywhere, just download ITexamReview SY0-701 Questions and start SY0-701 exam preparation with complete peace of mind and satisfaction.