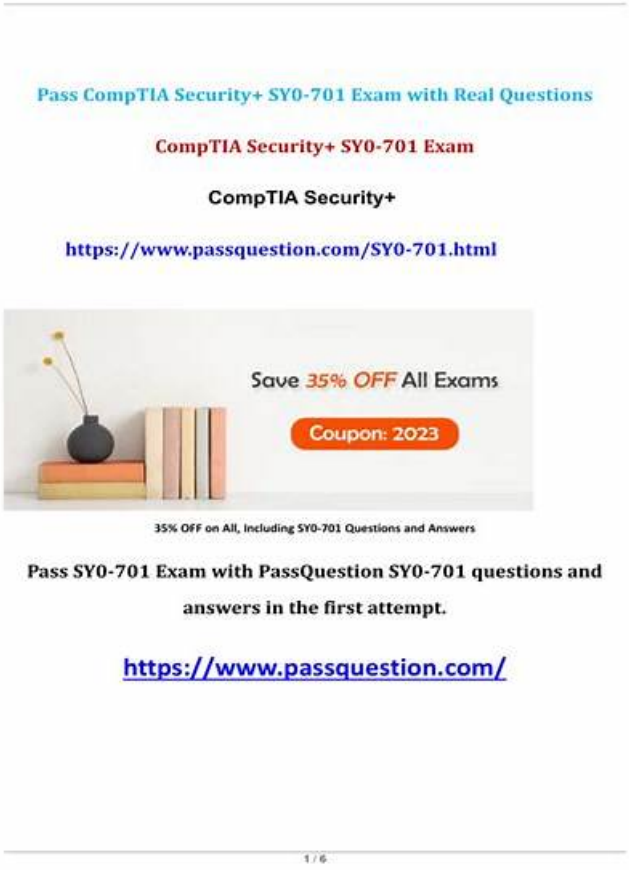
Valid CompTIA SY0-701 Test Dumps, SY0-701 Valid Practice Questions



What's more, part of that TroytecDumps SY0-701 dumps now are free: https://drive.google.com/open?id=1WuUQdNIIHFTIXOQQrUQUIP9GojSq7N9U

To save resources of our customers, we offer Real SY0-701 Exam Questions that are enough to master for SY0-701 certification exam. Our CompTIA SY0-701 Exam Dumps are designed by experienced industry professionals and are regularly updated to reflect the latest changes in the CompTIA Security+ Certification Exam exam content.

CompTIA SY0-701 Exam Syllabus Topics:

Section	Weight	Objectives

Governance, Risk & Compliance	14%	- Explain regulations, standards, and frameworks that impact cybersecurity • 1. Public and private sector compliance requirements • 2. Regulations, standards, and frameworks - Explain privacy and sensitive data concepts in relation to security • 1. Privacy and data protection regulations • 2. Data classification and handling • 3. Privacy-enhancing technologies - Given a scenario, apply risk management strategies • 1. Risk identification and assessment • 2. Risk monitoring and reporting • 3. Risk mitigation and treatment - Compare and contrast the various types of controls • 1. Control types • 2. Control categories
Threats, Attacks & Vulnerabilities	24%	- Compare and contrast different types of security threats and attacks • 1. Network attacks • 2. Supply chain attacks • 3. Social engineering attacks • 4. Insider threats • 5. Malware types • 6. Application/web-based attacks - Given a scenario, analyze indicators of malicious activity • 1. Indicators of compromise • 2. Attack framework concepts • 3. Indicators of attack - Explain penetration testing and vulnerability scanning concepts • 1. Remediation and mitigation • 2. Vulnerability scanning • 3. Penetration testing methodologies

Architecture & Design	21%	- Given a scenario, implement secure network architecture concepts • 1. Network segmentation • 2. Secure network designs • 3. Network device placement • 4. Network monitoring - Given a scenario, implement secure application and protocol concepts • 1. Hardening techniques • 2. Application protocols • 3. Secure application development - Explain the concept of the attack surface and network architecture • 1. Zero Trust • 2. Network architecture • 3. Virtualization and cloud concepts • 4. Physical security controls - Explain the importance of cryptographic solutions • 1. Symmetric and asymmetric cryptography • 2. Cryptographic standards and protocols • 3. Public key infrastructure (PKI) • 4. Hashing and digital signatures - Explain the importance of embedded and specialized systems security • 1. Specialized systems • 2. Security constraints • 3. Embedded systems
Operations & Incident Response	16%	- Given a scenario, apply incident response and recovery procedures • 1. Incident response procedures • 2. Business continuity and disaster recovery • 3. Incident investigation and digital forensics - Describe the collection and use of threat intelligence • 1. Threat intelligence sources • 2. Threat intelligence analysis - Explain the use of frameworks, policies, procedures, and controls • 1. Governance and compliance frameworks • 2. Security policies and procedures • 3. Security controls - Given a scenario, use the appropriate tool to assess organizational security • 1. Log analysis and packet capture • 2. Cybersecurity automation and orchestration • 3. Network reconnaissance and discovery • 4. Vulnerability scanning and remediation

Implementation	25%	- Given a scenario, implement appropriate environmental and physical controls • 1. Environmental controls • 2. Composite risks • 3. Physical security controls - Given a scenario, implement identity and access management (IAM) solutions • 1. Identity and access management concepts • 2. Directory services and federation • 3. Access control models • 4. Authentication factors and methods - Given a scenario, implement appropriate controls for mobile and embedded devices • 1. Mobile device deployment • 2. Mobile device management • 3. Mobile device enforcement and monitoring - Given a scenario, implement cybersecurity resilience solutions • 1. Redundancy and fault tolerance • 2. Resiliency and continuity measures • 3. Backup and recovery strategies

SY0-701 Valid Practice Questions & SY0-701 Exam Cram

The 24/7 support team is just an e-mail away for our customers so that they can contact us anytime. Our team will solve all of their issues as quickly as possible. Free demos and up to 1 year of free updates of our Sitecore Exams are also available at TroytecDumps. Buy updated and Real SY0-701 Exam Questions now and earn your dream SY0-701 certification with TroytecDumps!

CompTIA Security+ Certification Exam Sample Questions (Q1025-Q1030):

NEW QUESTION # 1025
An employee from the accounting department logs in to the website used for processing the company ' s payments. After logging in, a new desktop application automatically downloads on the employee ' s computer and causes the computer to restart. Which of the following attacks has occurred?

- A. Typosquatting
- B. Watering hole
- C. XSS
- D. Buffer overflow

Answer: B

Explanation:
A watering hole attack occurs when attackers compromise a website that is frequently visited by targeted users-in this case, the payment processing site used by employees. The compromised site then delivers malicious payloads to visitors, such as downloading malicious applications without user consent.
XSS (Cross-Site Scripting) attacks inject malicious scripts into web pages but typically do not cause automatic application downloads leading to restarts. Typosquatting (C) involves malicious websites mimicking legitimate ones via misspelled URLs. Buffer overflow (D) is an attack targeting software memory but doesn't typically involve website compromise and automatic downloads. This attack type is detailed in the Threats, Vulnerabilities, and Mitigations domain of SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#.

NEW QUESTION # 1026
A security audit of an organization revealed that most of the IT staff members have domain administrator credentials and do not change the passwords regularly. Which of the following solutions should the security learn propose to resolve the findings in the most complete way?

- A. Reviewing the domain administrator group, removing all unnecessary administrators, and rotating all passwords
- B. Securing domain administrator credentials in a PAM vault and controlling access with role-based access control
- C. Integrating the domain administrator's group with an IdP and requiring SSO with MFA for all access
- D. Creating group policies to enforce password rotation on domain administrator credentials

Answer: B

Explanation:
Using a Privileged Access Management (PAM) vault to secure domain administrator credentials and enforcing role-based access control (RBAC) is the most comprehensive solution. PAM systems help manage and control access to privileged accounts, ensuring that only authorized personnel can access sensitive credentials. This approach also facilitates password rotation, auditing, and ensures that credentials are not misused or left unchanged. Integrating PAM with RBAC ensures that access is granted based on the user's role, further enhancing security.
Reference =
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 # 1027
A database engineer needs sample customer data for testing purposes. Which of the following can prevent unauthorized viewing or disclosure of PII?

- A. Filtering
- B. RBAC
- C. Tokenization
- D. Masking

Answer: D

Explanation:
Data masking replaces real PII with realistic but fictional values in non-production environments, ensuring testers can't view or disclose actual sensitive information.

NEW QUESTION # 1028
A company uses multiple providers to send its marketing, internal, and support emails. Many of the emails are marked as spam. Which of the following changes should the company make to ensure legitimate emails are validated?

- A. Implement DMARC with a " reject " policy to enforce sender validation.
- B. Disable DKIM to avoid signature conflicts.
- C. Update the SPF record to include all authorized sending sources.
- D. Replace the domain ' s MX record with the marketing provider ' s services.

Answer: C

Explanation:
The best answer is D. Update the SPF record to include all authorized sending sources.
SPF (Sender Policy Framework) is used to identify which mail servers and third-party services are authorized to send email on behalf of a domain. In this scenario, the company uses multiple providers for marketing, internal, and support emails. If all of those sending sources are not properly listed in the domain's SPF record, receiving mail servers may treat some valid messages as suspicious or spam.
Updating the SPF record to include all legitimate sending providers helps recipient systems validate that the email came from an approved source. This directly addresses the problem of legitimate emails being flagged.
Why the other options are incorrect:
* A. Disable DKIM to avoid signature conflicts.This is incorrect because DKIM helps validate message authenticity by using digital signatures. Disabling it would weaken email validation rather than improve it.

* B. Implement DMARC with a " reject " policy to enforce sender validation.DMARC is important, but a reject policy can cause legitimate messages to fail if SPF and DKIM are not configured correctly first.
DMARC builds on SPF and DKIM; it does not replace the need to authorize all sending sources.
* C. Replace the domain ' s MX record with the marketing provider ' s services.MX records control where incoming email is received, not which systems are authorized to send email. This would not solve the validation issue for outbound messages.
From a Security+ perspective, this question focuses on email security controls and proper configuration of SPF, DKIM, and DMARC. The most direct fix for multiple legitimate senders is to ensure the SPF record includes every authorized provider.

NEW QUESTION # 1029
A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

- A. Transfer
- B. Mitigate
- C. Accept
- D. Avoid

Answer: A

Explanation:
Explanation
Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of-service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions. Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A risk register is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization. The four common risk mitigation strategies are:
Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high.
Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk.
Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk.
This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable.
Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high.
By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack. Therefore, the correct answer is B.
Transfer. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377.
Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).

NEW QUESTION # 1030
.....

- Get SY0-701 Exam Questions To Achieve High Score □ Search on （ www.exam4labs.com ） for " SY0-701 " to obtain exam materials for free download ♣SY0-701 Exam Cost
- SY0-701 Dump □ SY0-701 Test Testking □ SY0-701 Valid Dumps Ppt ⤴ Immediately open 【 www.pdfvce.com 】 and search for ➠ SY0-701 □ to obtain a free download □SY0-701 Dump
- SY0-701 Valid Dumps Ppt □ Question SY0-701 Explanations □ SY0-701 Exam Vce Free □ Search for ▹ SY0-701 ◃ and download exam materials for free through □ www.pdfdumps.com □ □SY0-701 Exam Vce Free
- SY0-701 Dump □ SY0-701 Dump ☎ SY0-701 Exam Vce Free □ Download ⇛ SY0-701 ⇚ for free by simply entering ▸ www.pdfvce.com ◂ website □SY0-701 Prepaway Dumps
- SY0-701 Exam Cost □ SY0-701 Exam Vce Free □ SY0-701 Valid Braindumps Book □ Easily obtain free download of 【 SY0-701 】 by searching on ➥ www.prepawaypdf.com □ □SY0-701 Valid Braindumps Book
- Where To Find Real CompTIA SY0-701 Exam Questions □ Download ➤ SY0-701 □ for free by simply entering 《 www.pdfvce.com 》 website □SY0-701 Valid Dumps Ppt
- CompTIA - Latest SY0-701 - Valid CompTIA Security+ Certification Exam Test Dumps □ ➤ www.verifieddumps.com □ is best website to obtain 《 SY0-701 》 for free download □SY0-701 Valid Dumps Ppt
- wefunder.com, www.stes.tyc.edu.tw, 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, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, tooter.in, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 CompTIA SY0-701 dumps are available on Google Drive shared by TroytecDumps: https://drive.google.com/open?id=1WuUQdNIIHFTIXOQQrUQUIP9GojSq7N9U