Free PDF SY0-701 - CompTIA Security+ Certification Exam Latest Exam Preparation


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)

BONUS!!! Download part of TestPassKing SY0-701 dumps for free: https://drive.google.com/open?id=1N54FlIuNbjEVctBjOSEabUxII72-QfA-

As far as the price of CompTIA SY0-701 exam practice test questions is concerned, these exam practice test questions are being offered at a discounted price. Get benefits from CompTIA SY0-701 exam questions at discounted prices and download them quickly. Best of luck in SY0-701 Exam and career!!! Just choose the best SY0-701 exam questions format and start CompTIA SY0-701 exam preparation without wasting further time.

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	• 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	• 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 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.

Pass4sure SY0-701 Study Materials - New SY0-701 Test Blueprint

Our SY0-701 study materials are the product for global users. No matter which courtry you are in, you can buy and study our SY0-701 exam questions to pass the exam. And the standards in all aspects about our SY0-701 learning engine are also required by international standards. In terms of privacy that everyone values, we respect every user. Our company has always put the customer first as a development concept. It is very safe and easy to buy our SY0-701 Practice Braindumps!

CompTIA Security+ Certification Exam Sample Questions (Q513-Q518):

NEW QUESTION # 513
A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

- A. Aggregating
- B. Archiving
- C. Tuning
- D. Quarantining

Answer: C

Explanation:
Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope.
Therefore, this is the best answer among the given options. References = Security Alerting and Monitoring Concepts and Tools - CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

NEW QUESTION # 514
A company's web filter is configured to scan the URL for strings and deny access when matches are found.
Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. www.*.com
- B. encryption=off\
- C. :443
- D. http://

Answer: D

Explanation:
Explanation
A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling",
"porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or
443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.
To
prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks.
To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.
The other options are not correct because they do not match the protocol of non-encrypted web traffic.
Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page
69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

NEW QUESTION # 515
Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

- A. Net Flow
- B. SCAP
- C. DLP
- D. Antivirus

Answer: C

Explanation:
DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such asfiles), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions:
Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

NEW QUESTION # 516

Company A jointly develops a product with Company B, which is located in a different country.
Company A finds out that their intellectual property is being shared with unauthorized companies.
Which of the following has been breached?

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

Answer: B

Explanation:
A Memorandum of Agreement (MOA) outlines terms of cooperation, including restrictions on sharing intellectual property. A breach indicates the terms of the agreement were violated, compromising confidentiality or usage terms.

NEW QUESTION # 517
Which of the following scenarios describes a possible business email compromise attack?

- A. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
- B. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.
- C. Employees who open an email attachment receive messages demanding payment in order to access files.
- D. An employee receives a gift card request in an email that has an executive's name in the display field of the email.

Answer: D

Explanation:
A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data. The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to convince the victim to comply with the request12.
In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive's name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes. This is a common tactic used by BEC attackers to steal money from unsuspecting victims34.
Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key. Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority. Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company's email portal and capture their credentials. These are all types of cyberattacks, but they are not examples of BEC attacks. Reference = 1: Business Email Compromise - CompTIA Security+ SY0-701 - 2.2 2: CompTIA Security+ SY0-701 Certification Study Guide 3: Business Email Compromise: The 12 Billion Dollar Scam 4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

NEW QUESTION # 518
.....

701 ◂ and easily obtain a free download on { www.testkingpass.com } □Updated SY0-701 Dumps

- SY0-701 Valid Vce Dumps □ SY0-701 Study Test □ Exam SY0-701 Details □ Search for ⇛ SY0-701 ⇚ on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □Reliable SY0-701 Test Price
- SY0-701 Exam Questions - SY0-701 Guide Torrent -amp; CompTIA Security+ Certification Exam Test Guide □ Search for ➠ SY0-701 □ and download it for free immediately on ▸ www.torrentvce.com ◂ □Reliable SY0-701 Exam Sims
- Exam SY0-701 Details □ SY0-701 New Braindumps Questions □ SY0-701 PDF Guide □ ⇛ www.pdfvce.com ⇚ is best website to obtain " SY0-701 " for free download □SY0-701 Clearer Explanation
- SY0-701 Study Test □ SY0-701 New Braindumps Questions □ Exam SY0-701 Details □ Enter ▸ www.prepawaypdf.com ◂ and search for （ SY0-701 ） to download for free □Updated SY0-701 Dumps
- SY0-701 Exam Questions - SY0-701 Guide Torrent -amp; CompTIA Security+ Certification Exam Test Guide □ Search for [SY0-701] on （ www.pdfvce.com ） immediately to obtain a free download □SY0-701 Clearer Explanation
- New SY0-701 Exam Preparation | Latest CompTIA SY0-701: CompTIA Security+ Certification Exam 100% Pass !! □ www.exam4labs.com □ is best website to obtain ➠ SY0-701 □ for free download □Latest SY0-701 Test Format
- SY0-701 PDF Guide □ Reliable SY0-701 Exam Sims □ Practice SY0-701 Engine □ Enter （ www.pdfvce.com ） and search for □ SY0-701 □ to download for free □SY0-701 Download
- SY0-701 PDF Guide □ Valid SY0-701 Test Simulator □ Updated SY0-701 Dumps □ Go to website ➠ www.exam4labs.com □ open and search for " SY0-701 " to download for free □Certification SY0-701 Test Answers
- k12.instructure.com, notefolio.net, ddy.hackp.net, tooter.in, www.zazzle.com, blogfreely.net, www.intensedebate.com, www.stes.tyc.edu.tw, hhi.instructure.com, notefolio.net, Disposable vapes

BONUS!!! Download part of TestPassKing SY0-701 dumps for free: https://drive.google.com/open?id=1N54FlIuNbjEVctBjOSEabUxIl72-QfA-