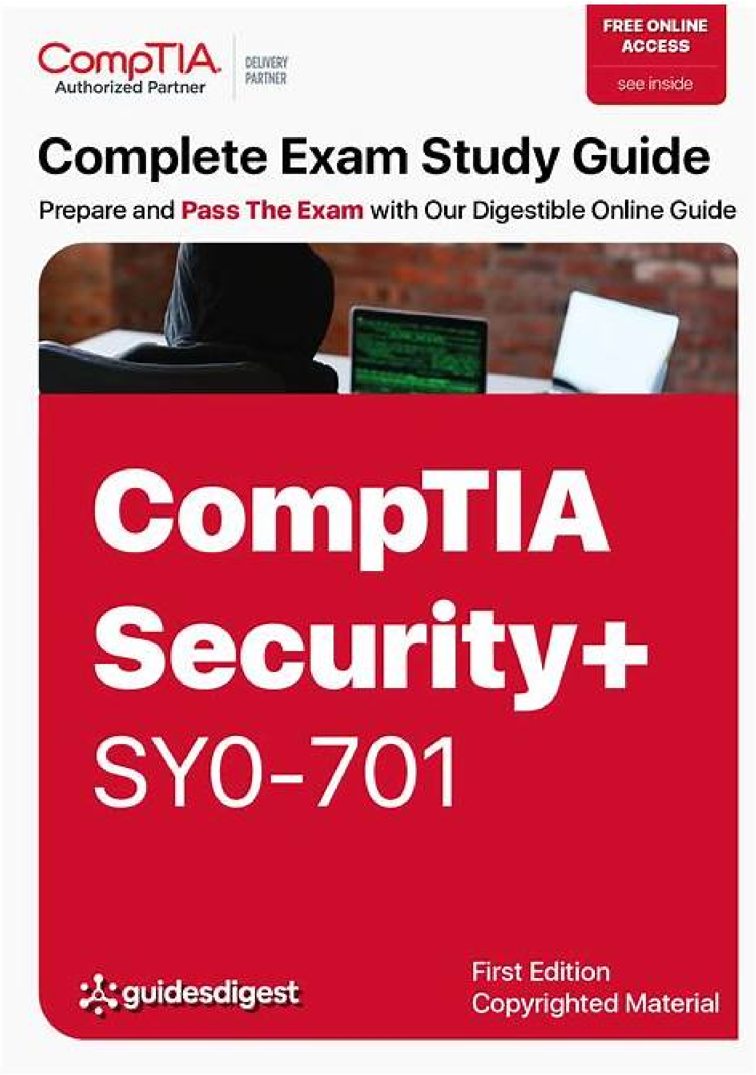
SY0-701學習筆記 - SY0-701考試內容



在CompTIA的SY0-701考試題庫頁面中，我們擁有所有最新的考古題，由Fast2test資深認證講師和經驗豐富的技術專家精心編輯而來，完整覆蓋最新試題。CompTIA的SY0-701考古題包含了PDF電子檔和軟件版，還有在線測試引擎，全新收錄了SY0-701認證考試所有試題，并根據真實的考題變化而不斷變化，適合全球考生通用。我們保證SY0-701考古題的品質，百分之百通過考試，對于購買我們網站SY0-701題庫的客戶，還可以享受一年更新服務。

CompTIA SY0-701 考試大綱：

主題	簡介
主題 1	• 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.
主題 2	• 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.

主題 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.
主題 4	- 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.
主題 5	- 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.

>> SY0-701學習筆記 <<

SY0-701考試內容 & SY0-701熱門考古題

在短短幾年中，CompTIA的SY0-701考試認證在日常生活中給人們造成了影響，但未來的關鍵問題是如何更有效的第一次通過CompTIA的SY0-701考試認證？回答這個問題就是利用Fast2test CompTIA的SY0-701考試培訓資料，有了它便實現了你的第一次通過考試認證，你還在等什麼，去獲得Fast2test CompTIA的SY0-701考試培訓資料，有了它將得到更多你想要的東西。

最新的 CompTIA Security+ SY0-701 免費考試真題 (Q125-Q130):

問題 #125
A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

- A. Dashboard
- B. Metadata
- C. Packet captures
- D. Vulnerability scans

答案：A

解題說明：
Explanation
A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria12.
A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors13.
A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter14.
Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards - SY0-601 CompTIA Security+: 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464:
CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

問題 #126

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 firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.
- C. Configure the firewall to perform deep packet inspection and monitor TLS traffic.
- D. Set the appliance to IPS mode and place it in front of the company firewall.

答案： D

解題說明：
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.

問題 #127

Which of the following are the most likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Choose two).

- A. Vendors/supply chain
- B. Use of penetration-testing utilities
- C. Outdated anti-malware software
- D. Included third-party libraries
- E. Certificate mismatch
- F. Weak passwords

答案： A,D

解題說明：
Software that is outsourced to vendors and third parties is vulnerable to malware being injected into the product from the supply chain.

問題 #128

Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Change management procedure
- B. Business continuity plan
- C. Disaster recovery plan
- D. Incident response procedure

答案： A

解題說明：
Explanation
A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network.

Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:

A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.

A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.

A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.

A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.

A change documentation that records the details and status of the change, as well as the lessons learned and best practices.

A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.

A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:

Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.

Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.

Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.

Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.

The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan 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. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

問題 #129

Which of the following best describe the benefits of a microservices architecture when compared to a monolithic architecture? (Choose two.)

- A. Reduced complexity of the system
- B. Improved scalability of the system
- C. Easier debugging of the system
- D. Increased compartmentalization of the system
- E. Reduced cost of ownership of the system
- F. Stronger authentication of the system

答案：B,D

問題 #130

......

Exam □ □ www.newdumpspdf.com □上的免費下載「 SY0-701 」頁面立即打開新版SY0-701題庫上線

- CompTIA SY0-701學習筆記和www.pdfexamdumps.com - 資格考試的領導者 □ 複製網址➥ www.pdfexamdumps.com □打開並搜索“ SY0-701 ”免費下載SY0-701熱門題庫
- SY0-701下載 □ SY0-701熱門考古題 □ SY0-701新版題庫上線 □ 在➽ www.newdumpspdf.com □搜索最新的➠ SY0-701 □題庫SY0-701考試大綱
- 可靠的SY0-701學習筆記和資格考試的領導者與更正的CompTIA CompTIA Security+ Certification Exam □ 透過⇛ www.newdumpspdf.com ⇚搜索□ SY0-701 □免費下載考試資料SY0-701考題資訊
- SY0-701熱門題庫 □ 新版SY0-701題庫 □ SY0-701考試大綱 □ 打開網站☀ www.newdumpspdf.com □☀□搜索▷ SY0-701 ◁免費下載最新SY0-701題庫
- 準確的SY0-701學習筆記和資格考試中的領先提供商＆可信賴的SY0-701考試內容 □ 在▷ www.kaoguti.com ◁網站上查找（ SY0-701 ）的最新題庫SY0-701熱門考古題
- 更新的SY0-701學習筆記＆保證CompTIA SY0-701考試成功，準備充分的SY0-701考試內容 □ 透過➠ www.newdumpspdf.com □搜索➽ SY0-701 □免費下載考試資料SY0-701考試內容
- SY0-701認證考試 □ SY0-701 PDF題庫 □ 新版SY0-701題庫 □ 在➡ www.kaoguti.com □□□搜索最新的（ SY0-701 ）題庫新版SY0-701題庫
- SY0-701 PDF題庫 □ SY0-701認證考試 □ SY0-701信息資訊 □ 請在「 www.newdumpspdf.com 」網站上免費下載「 SY0-701 」題庫SY0-701信息資訊
- 可靠的SY0-701學習筆記和資格考試的領導者與更正的CompTIA CompTIA Security+ Certification Exam □ 免費下載➽ SY0-701 □只需在▷ www.kaoguti.com ◁上搜索SY0-701認證考試
- 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, jptsexams3.com, study.stcs.edu.np, 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, lms.slikunedu.in, www.stes.tyc.edu.tw, lms.ait.edu.za, 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, Disposable vapes