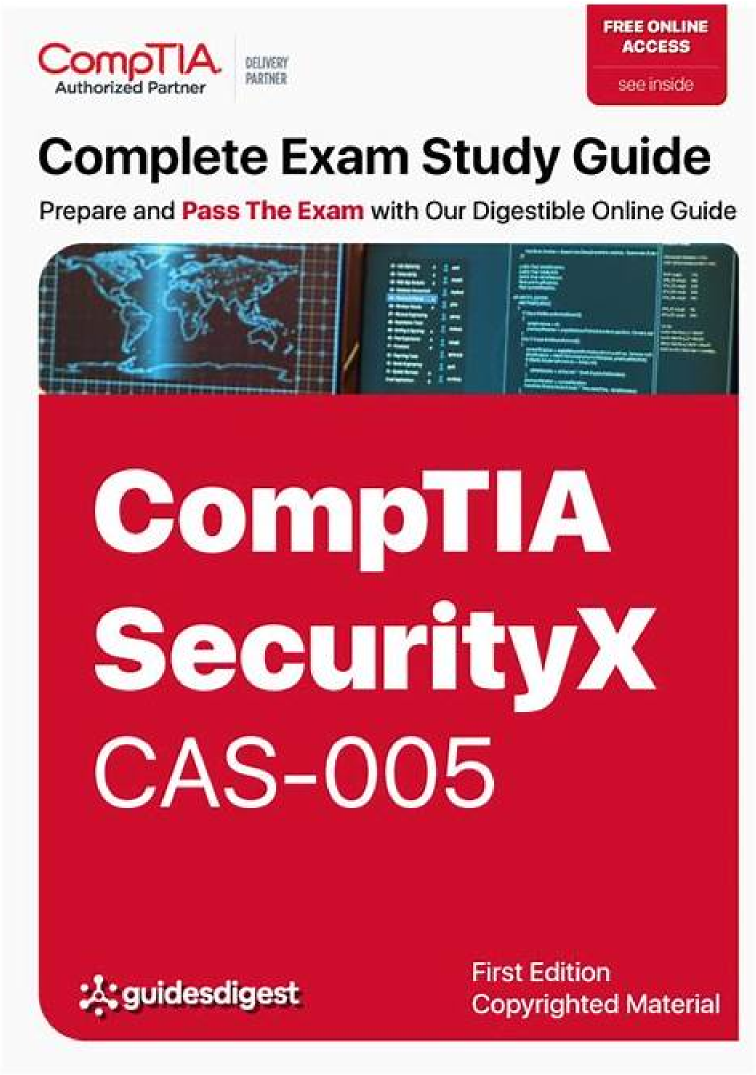
CAS-005題庫下載 -最新CAS-005考題



從Google Drive中免費下載最新的VCESoft CAS-005 PDF版考試題庫：https://drive.google.com/open?id=17wzCkvR5_NoMFba2FBG4JP4SQRN5YlAj

當你進入VCESoft網站，你看到每天進入VCESoft網站的人那麼多，不禁感到意外。其實這很正常的，我們VCESoft網站每天給不同的考生提供培訓資料數不勝數，他們都是利用了我們的培訓資料才順利通過考試的，說明我們的CompTIA的CAS-005考試認證培訓資料真起到了作用，如果你也想購買，那就不要錯過我們VCESoft網站，你一定會非常滿意的。

CompTIA CAS-005 考試大綱：

主題	簡介
主題 1	• Security Operations: This domain is designed for CompTIA security architects and covers analyzing data to support monitoring and response activities, as well as assessing vulnerabilities and recommending solutions to reduce attack surfaces. Candidates will apply threat-hunting techniques and utilize threat intelligence concepts to enhance operational security.
主題 2	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.

主題 3	- Governance, Risk, and Compliance: This section of the exam measures the skills of CompTIA security architects that cover the implementation of governance components based on organizational security requirements, including developing policies, procedures, and standards. Candidates will learn about managing security programs, including awareness training on phishing and social engineering.
主題 4	- Security Engineering: This section measures the skills of CompTIA security architects that involve troubleshooting common issues related to identity and access management (IAM) components within an enterprise environment. Candidates will analyze requirements to enhance endpoint and server security while implementing hardware security technologies. This domain also emphasizes the importance of advanced cryptographic concepts in securing systems.

>> CAS-005題庫下載 <<

最新CAS-005考題，CAS-005熱門考題

VCESoft是一個優秀的IT認證考試資料網站，在VCESoft您可以找到關於CompTIA CAS-005認證考試的考試心得和考試材料。您也可以在VCESoft免費下載部分關於CompTIA CAS-005考試的考題和答案。VCESoft還將及時免費為您提供有關CompTIA CAS-005考試材料的更新。並且我們的銷售的考試考古題資料都提供答案。我們的IT專家團隊將不斷的利用行業經驗來研究出準確詳細的考試練習題來協助您通過考試。總之，我們將為您提供你所需要的一切關於CompTIA CAS-005認證考試的一切材料。

最新的 CompTIA CASP CAS-005 免費考試真題 (Q322-Q327):

問題 #322
A security operations analyst is reviewing network traffic baselines for nightly database backups.
Given the following information:
Which of the following should the security analyst do next?

- A. Refer to the incident response playbook for the proper response.
- B. Quarantine PRDDB01 and then alert the database engineers.
- C. Consult with a network engineer to determine the impact of bandwidth usage.
- D. Review all the network logs for further data exfiltration.

答案：D

問題 #323
After an incident occurred, a team reported during the lessons-learned review that the team.
- Lost important Information for further analysis.
- Did not utilize the chain of communication
- Did not follow the right steps for a proper response
Which of the following solutions is the best way to address these findinds?

- A. Publishing the incident response policy and enforcing it as part of the security awareness program
- B. Building playbooks for different scenarios and performing regular table-top exercises
- C. Requesting budget for better forensic tools to Improve technical capabilities for Incident response operations
- D. Requiring professional incident response certifications tor each new team member

答案：B

解題說明：
Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review.
Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.
Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.

Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

問題 #324

A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent lIS zero-day vulnerability was discovered that affects all versions of the Windows Server OS:

Which of the following hosts should a security analyst patch first once a patch is available?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4
- F. 5

答案： C

解題說明：

Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the security analyst should patch Host 1 first. Here's why:

* Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.

* Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.

* Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.

* References:

* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

* NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies

* CIS Controls: Control 3 - Continuous Vulnerability Management

問題 #325

A network engineer must ensure that always-on VPN access is enabled Curt restricted to company assets Which of the following best describes what the engineer needs to do"

- A. Generate device certificates using the specific template settings needed
- B. Create a wildcard certificate for connections from public networks
- C. Add the VPN hostname as a SAN entry on the root certificate
- D. Modify signing certificates in order to support IKE version 2

答案： A

解題說明：

To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution.

These certificates ensure that only authorized devices can establish a VPN connection.

Why Device Certificates are Necessary:

* Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.

* Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.

* Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.

Other options do not provide the same level of control and security for always-on VPN access:

* B. Modify signing certificates for IKE version 2: While important for VPN protocols, it does not address device-specific authentication.

* C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.

* D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.

References:
* CompTIA SecurityX Study Guide
* "Device Certificates for VPN Access," Cisco Documentation
* NIST Special Publication 800-77, "Guide to IPsec VPNs"

問題 #326
A security engineer performed a code scan that resulted in many false positives. The security engineer must find a solution that improves the quality of scanning results before application deployment. Which of the following is the best solution?

- A. Limiting the tool to a specific coding language and tuning the rule set
- B. Using an application vulnerability scanner to identify coding flaws in production
- C. Performing updates on code libraries before code development
- D. Configuring branch protection rules and dependency checks

答案：A

解題說明：
To improve the quality of code scanning results and reduce false positives, the best solution is to limit the tool to a specific coding language and fine-tune the rule set. By configuring the code scanning tool to focus on the specific language used in the application, the tool can more accurately identify relevant issues and reduce the number of false positives. Additionally, tuning the rule set ensures that the tool's checks are appropriate for the application's context, further improving the accuracy of the scan results.
Reference:
CompTIA SecurityX Study Guide: Discusses best practices for configuring code scanning tools, including language-specific tuning and rule set adjustments.
"Secure Coding: Principles and Practices" by Mark G. Graff and Kenneth R. van Wyk: Highlights the importance of customizing code analysis tools to reduce false positives.
OWASP (Open Web Application Security Project): Provides guidelines for configuring and tuning code scanning tools to improve accuracy.

問題 #327
......

- 高效的CAS-005題庫下載 |高通過率的考試材料|專業的CAS-005：CompTIA SecurityX Certification Exam □ 到□ www.pdfexamdumps.com □搜尋➽ CAS-005 □以獲取免費下載考試資料CAS-005題庫
- www.skudci.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

此外，這些VCESoft CAS-005考試題庫的部分內容現在是免費的：https://drive.google.com/open?id=17wzCkvR5_NoMFba2FBG4JP4SQRN5YlAj