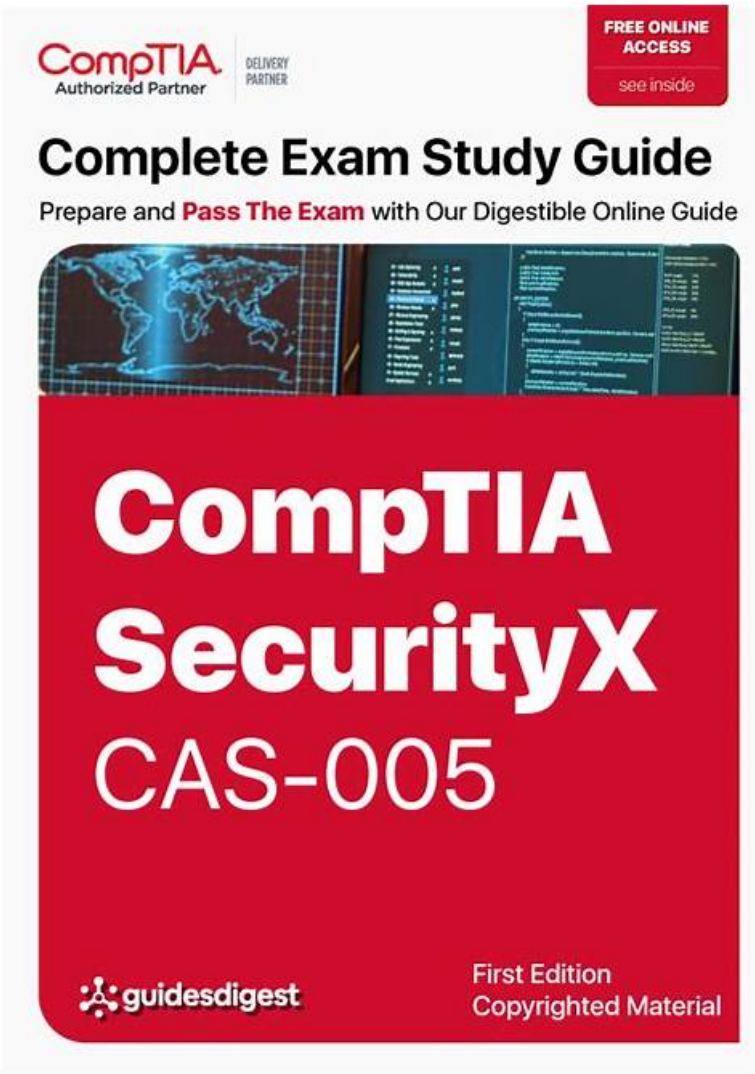
CAS-005證照指南，CAS-005考題寶典



從Google Drive中免費下載最新的KaoGuTi CAS-005 PDF版考試題庫：https://drive.google.com/open?id=1IpzJr6s9k2fEJpySERFyVqwJZovIzuFt

CAS-005認證考試是一個很難的考試。但是即使這個考試很難，報名參加考試的人也很多。如果要說為什麼，那當然是因為CAS-005考試是一個非常重要的考試。對IT職員來說，沒有取得這個資格那麼會對工作帶來不好的影響。這個考試的認證資格可以給你的工作帶來很多有益的幫助，也可以幫助你晉升。總之這是一個可以給你的職業生涯帶來重大影響的考試。这么重要的考试，你也想参加吧。

CompTIA CAS-005 考試大綱：

主題	簡介
主題 1	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
主題 2	• 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 3	• 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.
主題 4	• 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.

CAS-005考題寶典 - CAS-005软件版

敢於追求，才是精彩的人生，如果有一天你坐在搖晃的椅子上，回憶起自己的往事，會發出會心的一笑，那麼你的人生是成功的。 你想要成功的人生嗎？那就趕緊使用KaoGuTi CompTIA的CAS-005考試培訓資料吧，它包括了試題及答案，對每位IT認證的考生都非常使用，它的成功率高達100%，心動不如行動，趕緊購買吧。

最新的 CompTIA CASP CAS-005 免費考試真題 (Q217-Q222):

問題 #217
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:

	OS	Externally available?	Behind WAF?	IIS installed?
Host 1	Windows 2019	Yes	Yes	Yes
Host 2	Windows 2008 R2	No	N/A	No
Host 3	Windows 2012 R2	Yes	Yes	Yes
Host 4	Windows 2022	Yes	No	Yes
Host 5	Windows 2012 R2	No	N/A	No
Host 6	Windows 2019	Yes	No	No

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：D

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 securityanalyst 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 toEnterprise Patch Management Technologies CIS Controls: Control 3 - Continuous Vulnerability Management

問題 #218
A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is Identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within

seconds. The tablets are configured as follows to meet hospital policy:
- Full disk encryption is enabled
- "Always On" corporate VPN is enabled
- ef-use-backed keystore is enabled'ready.
- Wi-Fi 6 is configured with SAE.
- Location services is disabled.
- Application allow list is configured

- A. Configuring the application allow list to only per mil emergency calls
- B. Performing cryptographic obfuscation
- C. Returning on the device's solid-state media to zero
- D. Revoking the user certificates used for VPN and Wi-Fi access
- E. Using geolocation to find the device

答案：C

解題說明：
To mitigate the risk of data loss on a lost or stolen tablet quickly, the most effective strategy is to return the device's solid-state media to zero, which effectively erases all data on the device.
Immediate Data Erasure: Returning the solid-state media to zero ensures that all data is wiped instantly, mitigating the risk of data loss if the device is lost or stolen.
Full Disk Encryption: Even though the tablets are already encrypted, physically erasing the data ensures that no residual data can be accessed if someone attempts to bypass encryption.
Compliance and Security: This method adheres to best practices for data security and compliance, ensuring that sensitive patient data cannot be accessed by unauthorized parties.

問題 #219
After a company discovered a zero-day vulnerability in its VPN solution, the company plans to deploy cloud-hosted resources to replace its current on-premises systems. An engineer must find an appropriate solution to facilitate trusted connectivity. Which of the following capabilities is the most relevant?

- A. Microsegmentation
- B. Secure access service edge
- C. Container orchestration
- D. Conditional access

答案：B

解題說明：
Comprehensive and Detailed
The scenario involves replacing an on-premises VPN solution, which has a zero-day vulnerability, with cloud-hosted resources while ensuring trusted connectivity. Trusted connectivity in a cloud environment implies secure, scalable, and modern access control that goes beyond traditional VPNs. Let's analyze the options:
A . Container orchestration: This refers to managing and automating containerized workloads (e.g., Kubernetes). While useful for application deployment, it doesn't directly address secure connectivity to cloud resources.
B . Microsegmentation: This involves creating fine-grained security policies within a network to limit lateral movement. It's valuable for internal security but isn't a complete solution for trusted connectivity to cloud-hosted resources.
C . Conditional access: This ensures access based on conditions (e.g., user identity, device health). It's relevant for identity management but lacks the broader networking and security scope needed here.

問題 #220
Consultants for a company learn that customs agents at foreign border crossings are demanding device inspections. The company wants to:
* Minimize the risk to its data by storing its most sensitive data inside of a security container.
* Obfuscate containerized data on command.
Which of the following technologies is the best way to accomplish this goal?

- A. UEFI
- B. vTPM

- C. eFuse
- D. SED
- E. MicroSD HSM

答案：D

解題說明：
The best solution is to use Self-Encrypting Drives (SEDs). SEDs automatically encrypt all data stored on the disk and can be rapidly sanitized or obfuscated by deleting or altering the encryption keys. This provides immediate and secure protection if customs agents demand device access, as the sensitive data inside containers becomes unreadable without the decryption key.
Option B (eFuse) and C (UEFI) are hardware mechanisms unrelated to dynamic data protection. Option D (vTPM) provides virtualized key storage but does not obfuscate data quickly under inspection conditions. Option E (MicroSD HSM) is useful for key storage but does not protect all data at scale.
CAS-005 highlights hardware-based encryption solutions like SEDs for protecting sensitive data during travel, ensuring both regulatory compliance and rapid response capabilities under hostile conditions.

問題 #221
Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process. Which of the following is the best strategy for the engineer to use?

- A. Employing shielding lo prevent LMI
- B. Managing key material on a HSM
- C. Managing secrets on the vTPM hardware
- D. Disabling the BIOS and moving to UEFI

答案：B

解題說明：
The best strategy for securely managing cryptographic material is to use a Hardware Security Module (HSM). Here's why:
Security and Integrity: HSMs are specialized hardware devices designed to protect and manage digital keys. They provide high levels of physical and logical security, ensuring that cryptographic material is well protected against tampering and unauthorized access.
Centralized Key Management: Using HSMs allows for centralized management of cryptographic keys, reducing the risks associated with decentralized and potentially insecure key storage practices, such as on personal laptops.
Compliance and Best Practices: HSMs comply with various industry standards and regulations (such as FIPS 140-2) for secure key management. This ensures that the organization adheres to best practices and meets compliance requirements.
Reference:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-57: Recommendation for Key Management
ISO/IEC 19790:2012: Information Technology - Security Techniques - Security Requirements for Cryptographic Modules

問題 #222
.....

www.newdumpspdf.com]上搜索CAS-005題庫最新資訊

- 免費PDF CompTIA CAS-005證照指南是行業領先材料＆實用的CAS-005：CompTIA SecurityX Certification Exam 􀐩 進入▷ tw.fast2test.com◁搜尋➽ CAS-005 􀐩免費下載最新CAS-005考證
- CAS-005 PDF題庫 􀐩 CAS-005最新考題 􀐩 CAS-005題庫最新資訊 􀐩 複製網址➤ www.newdumpspdf.com 􀐩打開並搜索􀐩 CAS-005 􀐩免費下載CAS-005考試備考經驗
- CAS-005學習資料 􀐩 CAS-005考試備考經驗 ☎ CAS-005考題資源 ↩ 透過【 www.pdfexamdumps.com 】搜索【 CAS-005 】免費下載考試資料CAS-005考古題介紹
- 免費PDF CompTIA CAS-005證照指南是行業領先材料＆實用的CAS-005：CompTIA SecurityX Certification Exam 􀐩 （ www.newdumpspdf.com ）是獲取􀐩 CAS-005 􀐩免費下載的最佳網站CAS-005熱門考題
- CAS-005測試 􀐩 CAS-005熱門考題 􀐩 CAS-005最新題庫 􀐩 [www.pdfexamdumps.com]上搜索➤ CAS-005 􀐩輕鬆獲取免費下載CAS-005最新考證
- CAS-005考試資料 􀐩 CAS-005測試引擎 􀐩 CAS-005考試資料 􀐩 到➥ www.newdumpspdf.com 􀐩搜索✔ CAS-005 􀐩✔􀐩輕鬆取得免費下載CAS-005最新考題
- CAS-005 PDF題庫 􀐩 最新CAS-005考證 􀐩 CAS-005考古題介紹 􀐩 立即在➠ www.kaoguti.com 􀐩上搜尋▷ CAS-005 ◁並免費下載CAS-005認證
- myportal.utt.edu.tt, 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, www.wcs.edu.eu, 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, Disposable vapes

BONUS!!! 免費下載KaoGuTi CAS-005考試題庫的完整版：https://drive.google.com/open?id=1IpzJr6s9k2fEJpySERFyVqwJZovIzuFt