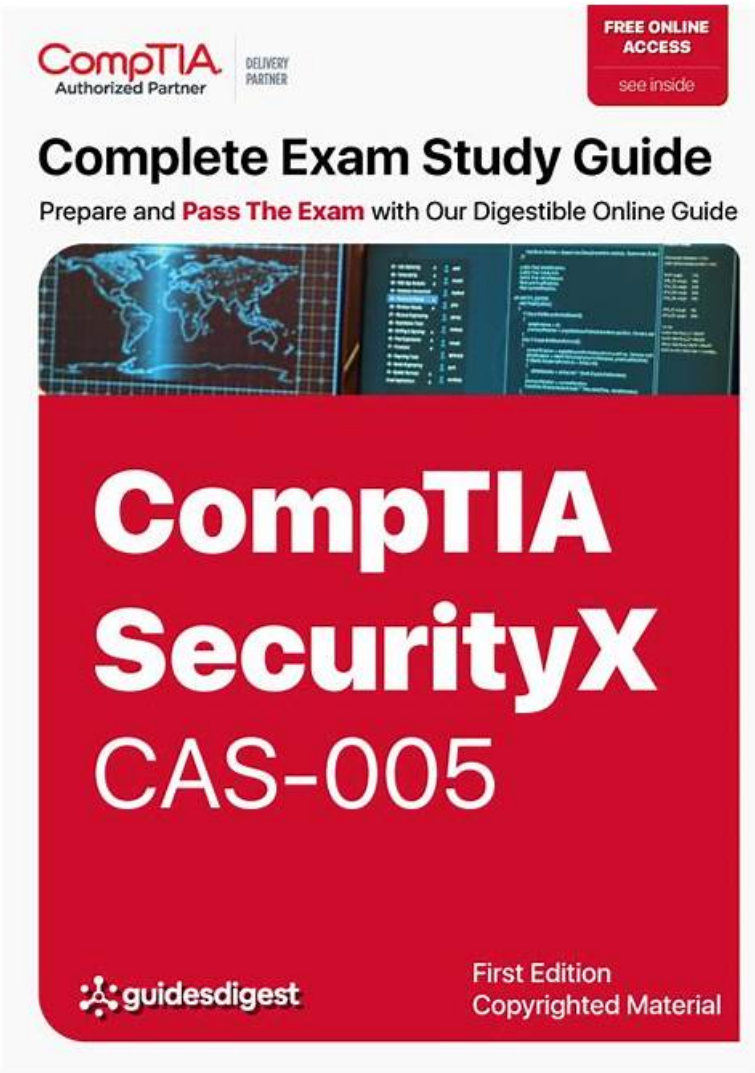
最受歡迎的CAS-005熱門考古題，免費下載CAS-005考試資料得到妳想要的CompTIA證書



數千家公司均依託 CompTIA 標準來提供一個可靠的員工業績評估。此外，數十家擁有自己認證專案的公司也非常信賴 CompTIA 認證，以確保員工具備扎實的技能功底。此舉可以為公司節省大量的時間和開銷。要想順利的一次通過 CAS-005 認證，選擇一部優秀的題庫非常必要，Fast2test 的專家一直致力於為客戶提供 CompTIA 認證的全真考題及認證學習資料,助您一次通過 CompTIA CAS-005 認證考試。

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	• 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 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	• 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.

>> CAS-005熱門考古題 <<

最新版的CAS-005熱門考古題，提前為CompTIA SecurityX Certification Exam CAS-005考試做好準備

如果你要參加CompTIA的CAS-005認定考試，Fast2test的CAS-005考古題是你最好的準備工具。這個資料可以幫助你輕鬆地通過考試。這是一個評價很高的資料，有了它，你就不用再擔心你的考試了。因為這個考古題可以解決你在準備考試時遇到的一切難題。在購買Fast2test的CAS-005考古題之前，你還可以下載免費的考古題樣本作為試用。這樣你就可以自己判斷這個資料是不是適合自己。

最新的 CompTIA CASP CAS-005 免費考試真題 (Q298-Q303):

問題 #298
During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a comprised web server Given the following portion of the code:

Which of the following best describes this incident?

- A. SQL injection
- B. XSRF attack
- C. Stored XSS
- D. Command injection

答案：C

解題說明：
The provided code snippet shows a script that captures the user's cookies and sends them to a remote server. This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.
A . XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.
B . Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.
C . Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends the user's cookies to the attacker's server.
D . SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.
Reference:
CompTIA Security+ Study Guide
OWASP (Open Web Application Security Project) guidelines on XSS
"The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

問題 #299
An organization is implementing advanced security controls associated with the execution of software applications on corporate endpoints. The organization must implement a deny-all, permit-by-exception approach to software authorization for all systems

regardless of OS. Which of the following should be implemented to meet these requirements?

- A. Block list
- B. SELinux
- C. Atomic execution
- D. MDM
- E. XDR

答案：A

解題說明：
Comprehensive and Detailed Step by Step Explanation:
* Understanding the Scenario: The organization wants a strict application control policy: deny all software execution by default and only allow specifically authorized applications. This must be enforced across all operating systems. It is implied that they mean an Allow list, but Block List is the only reasonable answer.
* Analyzing the Answer Choices:
* A. SELinux (Security-Enhanced Linux): SELinux is a security module for the Linux kernel that provides Mandatory Access Control (MAC). While it can enforce application control, it's specific to Linux and doesn't meet the "regardless of OS" requirement.

問題 #300
A security analyst reviews the following report:

	Location	Chassis manufacturer	OS	Application developer	Vendor
Product A	United States	Local company A	Debian 11	Unknown	Charlie Security Consulting
Product B	United States	Global company B	Red Hat Enterprise Linux	Developer B	BigBox Vulnerabilities

Which of the following assessments is the analyst performing?

- A. Quantitative
- B. System
- C. Supply chain
- D. Organizational

答案：C

解題說明：
The table shows detailed information about products, including location, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.
Why Supply Chain Assessment?
* Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.
* Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.
* Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third-party components or insecure development practices.
Other types of assessments do not align with the detailed supplier and component information provided:
* A. System: Focuses on individual system security, not the broader supply chain.
* C. Quantitative: Focuses on numerical risk assessments, not supplier information.
* D. Organizational: Focuses on internal organizational practices, not external suppliers.
References:
* CompTIA SecurityX Study Guide
* NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
* "Supply Chain Security Best Practices," Gartner Research

問題 #301
An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry. Which of the following should the security analyst use to perform threat modeling?

- A. OWASP
- B. ATT&CK
- C. CAPEC
- D. STRIDE

答案：B

解題說明：
The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry.
Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.
Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.
Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.

問題 #302
A company hired an email service provider called my-email.com to deliver company emails. The company started having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmarc include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Choose two.)

- A. The srv01 A record must be changed to a type CNAME record pointing to the web01 server
- B. The email CNAME record must be changed to a type A record pointing to 192.168.1.11
- C. The srvo1 A record must be changed to a type CNAME record pointing to the email server
- D. The TXT record must be changed to "v=dkim ip4:l92.168.1.11 include my-email.com -ell"
- E. The TXT record must be Changed to "v=dmarc ip4:192.168.1.10 include:my-email.com -all"
- F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"
- G. The email CNAME record must be changed to a type A record pointing to 192.168.1.10

答案：E,G

解題說明：
The security engineer should modify the following to fix the email migration issues:
Email CNAME Record: The email CNAME record must be changed to a type A record pointing to 192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.
TXT Record for DMARC: The TXT record must be changed to "v=dmarc ip4:192.168.1.10 include .com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.
DMARC: Ensuring the DMARC record is correctly set up helps in preventing email spoofing and phishing, aligning with email security best practices.

問題 #303
.....

Fast2test是個可以滿足很多客戶的需求的網站。有些使用我們類比測試軟體已經通過相關IT認證考試的人成為了Fast2test的回頭客。Fast2test可以提供領先的CompTIA 培訓技術助你通過CompTIA CAS-005 認證考試。

CAS-005最新題庫資源: https://tw.fast2test.com/CAS-005-premium-file.html