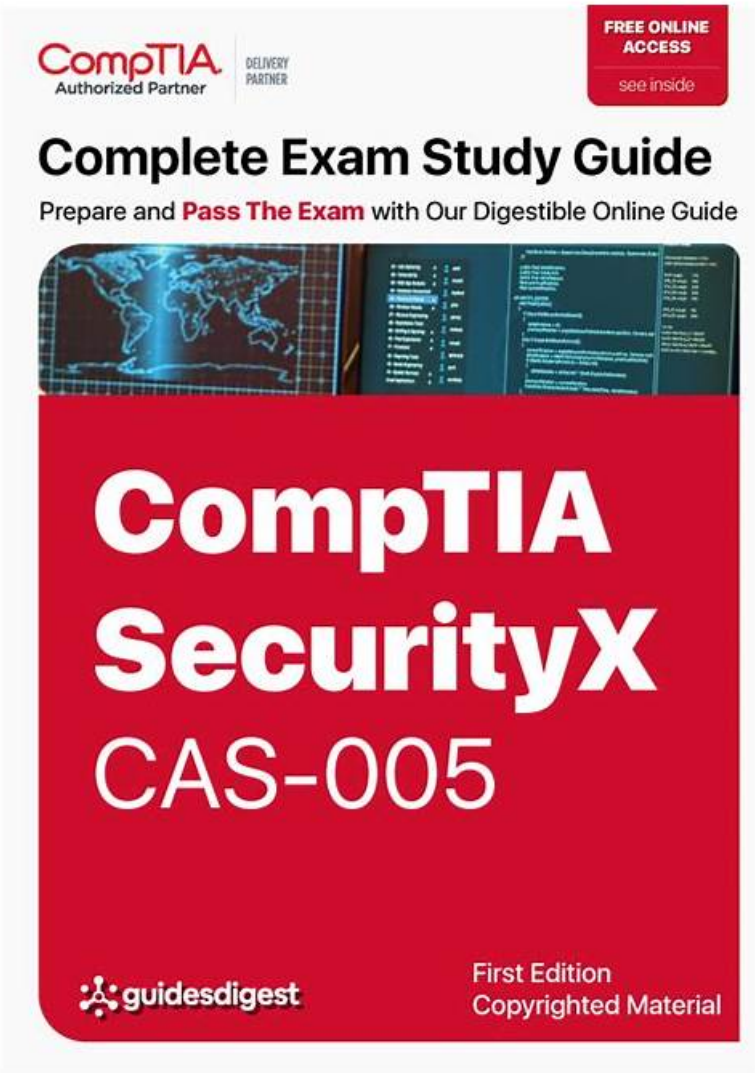
CompTIA CAS-005認定デベロッパー & CAS-005試験復習赤本



P.S. JPTestKingがGoogle Driveで共有している無料かつ新しいCAS-005ダンプ：https://drive.google.com/open?id=1aWSos-tb40QQQMHk1R4atjM8P_SDDB0o

JPTestKingあなたは自分の仕事の能力が認められない、またはあなたが長い間昇進していないと不満を言うかもしれません。ただし、CAS-005試験に合格しようとすると、高収入で良い仕事を見つける可能性が高くなります。そのため、CAS-005の質問トレントを購入することをお勧めします。 CAS-005試験の教材を購入して学習すると、試験に合格してより良い仕事を得るための簡単なものであることがわかります。購入前にCAS-005試験問題の概要を注意深くお読みください。私たちはあなたに最高のサービスを提供し、あなたが満足することを願っています。

CompTIA CAS-005 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.

トピック 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.
トピック 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.
トピック 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試験復習赤本、CAS-005関連試験

受験者の多くは、CAS-005試験問題のソフトバージョンが好きです。 CAS-005ガイドトレントのソフトウェアは、さまざまな自己学習および自己評価機能を強化して、学習の結果を確認します。このCompTIAソフトウェアは、学習者が脆弱なリンクを見つけて対処するのに役立ちます。 CAS-005試験問題は、タイミング機能と試験を刺激する機能を高めます。当社の製品はタイマーを設定して試験を刺激し、速度を調整してアラートを維持します。そのため、CAS-005試験問題を購入する価値があります。

CompTIA SecurityX Certification Exam 認定 CAS-005 試験問題 (Q423-Q428):

質問 # 423
Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Select two).
Implementing DLP controls preventing sensitive data from leaving Company B's network

- A. Performing an architectural review of Company B's network
- B. Reviewing the privacy policies currently adopted by Company B
- C. Documenting third-party connections used by Company B
- D. Forcing a password reset requiring more stringent passwords for users on Company B's network
- E. Requiring data sensitivity labeling tor all files shared with Company B

正解：B、C

解説：
To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:
A: Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.
E: Performing an architectural review of Company B's network: This review will identify vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface.
These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.
References:
* CompTIA SecurityX Study Guide: Emphasizes the importance of understanding third-party connections and conducting architectural reviews during acquisitions.
* NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems": Recommends comprehensive reviews and documentation of third-party connections.
* "Mergers, Acquisitions, and Other Restructuring Activities" by Donald DePamphilis: Discusses the importance of security assessments during acquisitions.

質問 # 424
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not normally send traffic to those sites. The technician will define this threat as:

- A. A decrypting RSA using an obsolete and weakened encryption attack.
- B. An advanced persistent threat.
- C. An on-path attack.
- D. A zero-day attack.

正解：B

解説：
The scenario describes a prolonged, stealthy operation where files were exfiltrated over three months via secure channels (TLS-protected HTTP) from unexpected systems, then ceased. This aligns with anAdvanced Persistent Threat (APT), characterized by long-term, targeted attacks aimed at data theft or surveillance, often using sophisticated methods to remain undetected.
* Option A:Decrypting RSA with weak encryption implies a cryptographic attack, but TLS suggests modern encryption was used, and there's no evidence of decryption here.
* Option B:A zero-day attack exploits unknown vulnerabilities, but the duration and cessation suggest a planned operation, not a single exploit.
* Option C:APT fits perfectly-slow, persistent exfiltration from unusual systems indicates a coordinated, stealthy threat actor.
* Option D:An on-path (man-in-the-middle) attack intercepts traffic, but there's no indication of interception; the focus is on unauthorized transfers.

質問 # 425
SIMULATION
During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.
INSTRUCTIONS
Review each of the events and select the appropriate analysis and remediation options for each IoC.

正解：

解説：
See the complete solution below in Explanation
Explanation:
Analysis and Remediation Options for Each IoC:
IoC 1:
Evidence:
Source: Apache_httpd
Type: DNSQ
Dest: @10.1.1.1:53,@10.1.2.5
Data: update.s.domain, CNAME 3a129sk219r9slmfkzzz000.s.domain, 108.158.253.253 Analysis:
Analysis: The service is attempting to resolve a malicious domain.
Reason: The DNS queries and the nature of the CNAME resolution indicate that the service is trying to resolve potentially harmful domains, which is a common tactic used by malware to connect to command-and-control servers.
Remediation:
Remediation: Implement a blocklist for known malicious ports.
Reason: Blocking known malicious domains at the DNS level prevents the resolution of harmful domains, thereby protecting the network from potential connections to malicious servers.
IoC 2:
Evidence:
Src: 10.0.5.5
Dst: 10.1.2.1, 10.1.2.2, 10.1.2.3, 10.1.2.4, 10.1.2.5
Proto: IP_ICMP
Data: ECHO
Action: Drop
Analysis:

Analysis: Someone is footprinting a network subnet.
Reason: The repeated ICMP ECHO requests to different addresses within a subnet indicate that someone is scanning the network to discover active hosts, a common reconnaissance technique used by attackers.
Remediation:
Remediation: Block ping requests across the WAN interface.
Reason: Blocking ICMP ECHO requests on the WAN interface can prevent attackers from using ping sweeps to gather information about the network topology and active devices.
IoC 3:
Evidence:
Proxylog:
GET /announce?info_hash=%01dff%27f%21%10%c5%wp%4e%1d%6f%63%3c%49%6d&peer_id%3dxJFS Uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started User-Agent: RAZA 2.1.0.0 Host: localhost Connection: Keep-Alive HTTP200 OK Analysis:
Analysis: An employee is using P2P services to download files.
Reason: The HTTP GET request with parameters related to a BitTorrent client indicates that the employee is using peer-to-peer (P2P) services, which can lead to unauthorized data transfer and potential security risks.
Remediation:
Remediation: Enforce endpoint controls on third-party software installations.
Reason: By enforcing strict endpoint controls, you can prevent the installation and use of unauthorized software, such as P2P clients, thereby mitigating the risk of data leaks and other security threats associated with such applications.
Reference:
CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.
CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.
Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.
By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

質問 # 426
A systems administrator needs to improve the security assurance in a company's cloud storage environment. The administrator determines that the best approach is to identify whether any data has been maliciously or inadvertently modified. Which of the following techniques should the systems administrator periodically use?

- A. Hashing
- B. Antitampering
- C. Journaling
- D. Interference

正解：A

解説：
Hashing is the best technique for identifying whether data has been maliciously or inadvertently modified. By generating and storing hash values for files or data, the administrator can periodically recheck the hashes to ensure that the data has not been altered. If the hash value changes, it indicates that the data has been modified. This technique provides an efficient and secure way to ensure data integrity.

質問 # 427
A security engineer is assisting a DevOps team that has the following requirements for container images:
Ensure container images are hashed and use version controls.
Ensure container images are up to date and scanned for vulnerabilities.
Which of the following should the security engineer do to meet these requirements?

- A. Enable audits on the container image and monitor for configuration changes.
- B. Enable clusters on the container image and configure the mesh with ACLs.
- C. Enable pulling of the container image from the vendor repository and deploy directly to operations.
- D. Enable new security and quality checks within a CI/CD pipeline.

正解：D

解説：
Implementing security and quality checks in a CI/CD pipeline ensures that:
Container images are scanned for vulnerabilities before deployment.
Version control is enforced, preventing unauthorized changes.
Hashes validate image integrity.
Other options:
A (Configuring ACLs on mesh networks) improves access control but does not ensure scanning.
C (Audits on container images) detect changes but do not enforce best practices.
D (Pulling from a vendor repository) does not ensure vulnerability scanning.

質問 # 428
.....

JPTestKingはCompTIAのCAS-005認定試験に対して問題集を提供しておるサイトで、現場のCompTIAのCAS-005試験問題と模擬試験問題集を含みます。ほかのホームページに弊社みたいな問題集を見れば、あとでみ続けて、弊社の商品を盗作することとよくわかります。JPTestKingが提供した資料は最も全面的で、しかも更新の最も速いです。

CAS-005試験復習赤本: https://www.jptestking.com/CAS-005-exam.html

- CAS-005 PDF問題サンプル □ CAS-005模擬モード □ CAS-005テスト参考書 □ サイト✔ www.jptestking.com □✔□で□ CAS-005 □問題集をダウンロードCAS-005認定テキスト
- CAS-005復習資料 □ CAS-005関連復習問題集 □ CAS-005問題サンプル □ URL □ www.goshiken.com □をコピーして開き、[CAS-005]を検索して無料でダウンロードしてくださいCAS-005試験勉強攻略
- CAS-005模擬試験サンプル □ CAS-005専門トレーリング □ CAS-005試験合格攻略 □ ウェブサイト✔ www.topexam.jp □✔□から《 CAS-005 》を開いて検索し、無料でダウンロードしてくださいCAS-005試験合格攻略
- CAS-005 CompTIA SecurityX Certification Examテスト実用的な情報 □ 「 www.goshiken.com 」サイトにて⇒ CAS-005 ⇐問題集を無料で使おうCAS-005復習問題集
- CAS-005試験準備 □ CAS-005復習問題集 □ CAS-005試験合格攻略 □ ▹ www.shikenpass.com ◃から簡単に《 CAS-005 》を無料でダウンロードできますCAS-005模擬問題
- 100％合格率のCAS-005認定デベロッパー一回合格-権威のあるCAS-005試験復習赤本 □ 今すぐ➡ www.goshiken.com □□□を開き、“CAS-005 ”を検索して無料でダウンロードしてくださいCAS-005関連復習問題集
- CAS-005復習問題集 □ CAS-005復習問題集 □ CAS-005問題サンプル □ ➠ www.passtest.jp □を開き、[CAS-005]を入力して、無料でダウンロードしてくださいCAS-005模擬問題
- CAS-005関連復習問題集 □ CAS-005試験合格攻略 □ CAS-005 PDF問題サンプル □ ▸ www.goshiken.com ◂に移動し、□ CAS-005 □を検索して、無料でダウンロード可能な試験資料を探しますCAS-005模擬問題
- 100％合格率のCAS-005認定デベロッパー一回合格-権威のあるCAS-005試験復習赤本 □ ▸ www.topexam.jp ◂には無料の“CAS-005 ”問題集がありますCAS-005専門トレーリング
- CAS-005試験解説問題 □ CAS-005キャリアパス □ CAS-005関連復習問題集 □ 今すぐ➡ www.goshiken.com □□□で【 CAS-005 】を検索し、無料でダウンロードしてくださいCAS-005テスト参考書
- 100％合格率のCAS-005認定デベロッパー一回合格-権威のあるCAS-005試験復習赤本 □ ▸ www.passtest.jp ◂は、{ CAS-005 }を無料でダウンロードするのに最適なサイトですCAS-005 PDF問題サンプル
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, excelelearn.com, 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.stes.tyc.edu.tw, Disposable vapes

無料でクラウドストレージから最新のJPTestKing CAS-005 PDFダンプをダウンロードする：https://drive.google.com/open?id=1aWSos-tb40QQQMHk1R4atjM8P_SDDB0o