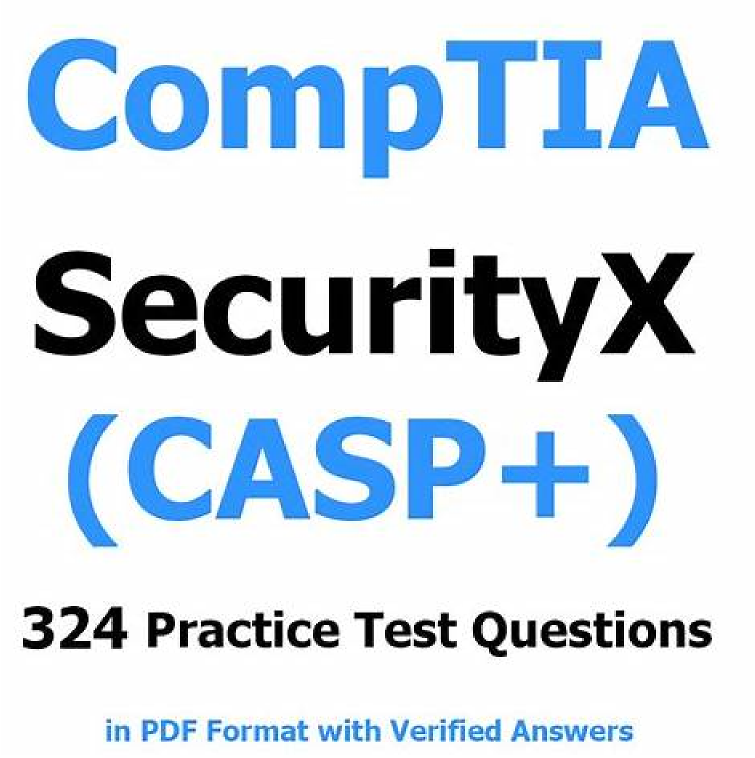
Free PDF 2026 CompTIA CAS-005–Efficient Exam Actual Questions


CompTIA
SecurityX
(CASP+)
324 Practice Test Questions
in PDF Format with Verified Answers

BTW, DOWNLOAD part of Exams-boost CAS-005 dumps from Cloud Storage: https://drive.google.com/open?id=19696nlCLlcX2fYpz6k2YA76BiyP5CKbd

Our CAS-005 study materials are compiled and tested by our expert. CAS-005 try hard to makes CAS-005 exam preparation easy with its several quality features. We send learning information in the form of questions and answers, and our CAS-005 study materials are highly relevant to what you need to pass CAS-005 certification exam. Our free demo will show you the actual CAS-005 Certification Exam. You can learn about real exams in advance by studying our CAS-005 study materials and improve your confidence in the exam so that you can pass CAS-005 exams with ease. This is also the reason that has been popular by the majority of candidates.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 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.
Topic 3	• 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.

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

>> CAS-005 Exam Actual Questions <<

CompTIA CAS-005 Pass-Sure Exam Actual Questions

Our CAS-005 study materials are compiled by domestic first-rate experts and senior lecturer and the contents of them contain all the important information about the test and all the possible answers of the questions which maybe appear in the test. You can use the practice test software to check your learning outcomes. Our CAS-005 study materials' self-learning and self-evaluation functions, the statistics report function, the timing function and the function of stimulating the test could assist you to find your weak links, check your level, adjust the speed and have a warming up for the real exam. You will feel your choice to buy CAS-005 Study Materials are too right.

CompTIA SecurityX Certification Exam Sample Questions (Q241-Q246):

NEW QUESTION # 241
A company wants to use loT devices to manage and monitor thermostats at all facilities The thermostats must receive vendor security updates and limit access to other devices within the organization Which of the following best addresses the company's requirements"

- A. Configuring IoT devices to always allow automatic updates
- B. Only allowing operation for loT devices during a specified time window
- C. Operating lot devices on a separate network with no access to other devices internally
- D. Only allowing Internet access to a set of specific domains

Answer: C

Explanation:
The best approach for managing and monitoring IoT devices, such as thermostats, is to operate them on a separate network with no access to other internal devices. This segmentation ensures that the IoT devices are isolated from the main network, reducing the risk of potential security breaches affecting other critical systems. Additionally, this setup allows for secure vendor updates without exposing the broader network to potential vulnerabilities inherent in IoT devices.
References:
* CompTIA SecurityX Study Guide: Recommends network segmentation for IoT devices to minimize security risks.
* NIST Special Publication 800-183, "Network of Things": Advises on the isolation of IoT devices to enhance security.
* "Practical IoT Security" by Brian Russell and Drew Van Duren: Discusses best practices for securing IoT devices, including network segmentation.

NEW QUESTION # 242
A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?

- A. Threat intelligence platform
- B. Continuous adversary emulation
- C. Honeypots
- D. Dark web monitoring

Answer: A

Explanation:
Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.
Why a Threat Intelligence Platform?
Data Integration: It consolidates data from multiple sources, including dark web monitoring and honeypots, making it easier to analyze and derive actionable insights.

Actionable Insights: Provides real-time alerts and reports on potential threats, helping the organization take proactive measures.
Operational Efficiency: Streamlines the process of threat detection and response, allowing the security team to focus on critical issues.
Research and Development: Facilitates the operationalization of research output by providing a platform for continuous monitoring and analysis of emerging threats.
Other options, while valuable, do not offer the same level of integration and operationalization capabilities:
A: Dark web monitoring: Useful for specific threat intelligence but lacks comprehensive operationalization.
C: Honeypots: Effective for detecting and analyzing specific attack vectors but not for broader threat intelligence.
D: Continuous adversary emulation: Important for testing defenses but not for integrating and operationalizing threat intelligence.

NEW QUESTION # 243
An analyst reviews a SIEM and generates the following report:
Only HOST002 is authorized for internet traffic. Which of the following statements is accurate?

- A. The HOST002 host is under attack, and a security incident should be declared.
- B. The VM002 host is misconfigured and needs to be revised by the network team.
- C. The network connection activity is unusual, and a network infection is highly possible.
- D. The SIEM platform is reporting multiple false positives on the alerts.

Answer: C

Explanation:
Comprehensive and Detailed
Understanding the Security Event:
HOST002 is the only device authorized for internet traffic. However, the SIEM logs show that VM002 is making network connections to web.corp.local.
This indicates unauthorized access, which could be a sign of lateral movement or network infection.
This is a red flag for potential malware, unauthorized software, or a compromised host.
Why Option D is Correct:
Unusual network traffic patterns are often an indicator of a compromised system.
VM002 should not be communicating externally, but it is.
This suggests a possible breach or malware infection attempting to communicate with a command-and-control (C2) server.
Why Other Options Are Incorrect:
A (Misconfiguration): While a misconfiguration could explain the unauthorized connections, the pattern of activity suggests something more malicious.
B (Security incident on HOST002): The issue is not with HOST002. The suspicious activity is from VM002.
C (False positives): The repeated pattern of unauthorized connections makes false positives unlikely.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide: Chapter on SIEM & Incident Analysis MITRE ATT&CK Tactics: Lateral Movement & Network-based Attacks

NEW QUESTION # 244
A company's security policy states that any publicly available server must be patched within 12 hours after a patch is released A recent IIS 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

Answer: F

Explanation:
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

NEW QUESTION # 245
A security review revealed that not all of the client proxy traffic is being captured. Which of the following architectural changes best enables the capture of traffic for analysis?

- A. Adding an additional proxy server to each segmented VLAN
- B. Enabling client device logging and system event auditing
- C. Setting up a reverse proxy for client logging at the gateway
- D. Configuring a span port on the perimeter firewall to ingest logs

Answer: D

Explanation:
Configuring a span port on the perimeter firewall to ingest logs is the best architectural change to ensure that all client proxy traffic is captured for analysis. Here's why:
Comprehensive Traffic Capture: A span port (or mirror port) on the perimeter firewall can capture all inbound and outbound traffic, including traffic that might bypass the proxy. This ensures that all network traffic is available for analysis.
Centralized Logging: By capturing logs at the perimeter firewall, the organization can centralize logging and analysis, making it easier to detect and investigate anomalies.
Minimal Disruption: Implementing a span port is a non-intrusive method that does not require significant changes to the network architecture, thus minimizing disruption to existing services.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-92: Guide to Computer Security Log Management OWASP Logging Cheat Sheet

NEW QUESTION # 246
......

We provide first-rate service on the CAS-005 learning prep to the clients and they include the service before and after the sale, 24-hours online customer service and long-distance assistance, the refund service and the update service. The client can try out our and download CAS-005 guide materials freely before the sale and if the client have problems about our product after the sale they can contact our customer service at any time. We provide 24-hours online customer service which replies the client's questions and doubts about our CAS-005 training quiz and solve their problems.

search for ➥ CAS-005 □ to download exam materials for free □Flexible CAS-005 Testing Engine

- CAS-005 Latest Braindumps □ Valid Test CAS-005 Bootcamp □ CAS-005 Reliable Practice Materials □ Search for □ CAS-005 □ and obtain a free download on ➥ www.pdfvce.com □ □New CAS-005 Exam Fee
- CAS-005 Question Explanations □ CAS-005 Exams Dumps □ Flexible CAS-005 Testing Engine □ ☀ www.prepawayexam.com □☀□ is best website to obtain ➥ CAS-005 □ for free download □CAS-005 Latest Test Dumps
- CAS-005 Exam Actual Questions | Professional CAS-005: CompTIA SecurityX Certification Exam ♥ Copy URL （ www.pdfvce.com ） open and search for ➡ CAS-005 □□□ to download for free □CAS-005 Pdf Exam Dump
- Track Your Progress with CompTIA CAS-005 Practice Test □ Open ▷ www.examcollectionpass.com ◁ and search for 「 CAS-005 」 to download exam materials for free □Exam CAS-005 Bible
- 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, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of Exams-boost CAS-005 dumps for free: https://drive.google.com/open?id=19696nlCLlcX2fYpz6k2YA76BiyP5CKbd