Famous CAS-005 Training Quiz Bring You the Topping Exam Questions - RealVCE

BONUS!!! Download part of RealVCE CAS-005 dumps for free: https://drive.google.com/open?id=1mXzcI3zmqIKzdBR4bnHFZJAggydc3bWO

Do you feel that you are always nervous in your actual CAS-005 exam and difficult to adapt yourself to the real exam? If you answer is yes, I think you can try to use the software version of our CAS-005 exam quiz. I believe the software version of our CAS-005 trianing guide will be best choice for you, because the software version can simulate real test environment, you can feel the atmosphere of the CAS-005 exam in advance by the software version.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
Topic 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.
Topic 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.
Topic 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.

>> Valid CAS-005 Test Cram <<

Offer you Actual Valid CAS-005 Test Cram to Help Pass CAS-005

Being the most competitive and advantageous company in the market, our CAS-005 practice quiz have help tens of millions of exam candidates realize their dreams all these years. If you are the dream-catcher, we are willing to offer help with our CAS-005 Study Guide like always. And if you buy our CAS-005 exam materials, then you will find that passing the exam is just a piece of cake in front of you.

CompTIA SecurityX Certification Exam Sample Questions (Q139-Q144):

NEW QUESTION # 139
While investigating a security event an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the next step the analyst should take after reporting the incident to the management team?

- A. Request that the affected servers be restored immediately
- B. Notify law enforcement
- C. Isolate the servers to prevent the spread
- D. Pay the ransom within 48 hours

Answer: C

Explanation:
The immediate action after discovering ransomware is toisolate the affected serversto prevent further spread of the malware to other systems in the network. Paying the ransom is not recommended as it does not guarantee data recovery and encourages criminal behavior. Notifying law enforcement is necessary, but containment must happen first to limit damage. Requesting server restoration should only occur after containment and a thorough investigation to ensure no remnants of ransomware remain.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Execute incident response procedures to contain and mitigate incidents.

NEW QUESTION # 140
A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password.
Which of the following models should the company implement to solve this issue?

- A. Context-based
- B. Time-based
- C. Rule based
- D. Role based

Answer: A

Explanation:
Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

NEW QUESTION # 141
A company's internal network is experiencing a security breach, and the threat actor is still active. Due to business requirements, users in this environment are allowed to utilize multiple machines at the same time. Given the following log snippet:

Time	User	Process	Status	Machine
10:11	user-a	.exe	blocked	machine02
10:15	user-b	setup.exe	blocked	machine02
10:15	user-A	appwiz.exe	blocked	machine01
10:16	user-c	appwiz.CPL	blocked	machine03
11:17	user-c	cmd.exe	blocked	machine03
11:18	user-h	msconfig.exe	blocked	machine04
11:19	user-d	firefox.exe	blocked	machine04
11:19	user-d	cmd.com	blocked	machine01

Which of the following accounts should a security analyst disable to best contain the incident without impacting valid users?

- A. user-b
- B. user-d
- C. user-a
- D. user-c

Answer: D

Explanation:
Useruser-cis showinganomalous behavior across multiple machines, attempting to run administrative tools such as cmd.exe and appwiz.CPL, which are commonly used by attackers for system modification. The activity pattern suggests a lateral movement attempt, potentially indicating a compromised account.
user-a (A)anduser-b (B)attempted to run applications but only on one machine, suggesting less likelihood of compromise.
user-d (D)was blocked running cmd.com, but user-c's pattern is more consistent with an attack technique.

NEW QUESTION # 142
An ISAC supplied recent threat intelligence information about pictures used on social media that provide reconnaissance of systems in use in secure facilities. In response, the Chief Information Security Officer (CISO) wants several configuration changes implemented via the MDM to ensure the following:
* Camera functions and location services are blocked for corporate mobile devices.
* All social media is blocked on the corporate and guest wireless networks.
Which of the following is the CISO practicing to safeguard against the threat?

- A. Open-source intelligence
- B. Social engineering
- C. Adversary emulation
- D. Operational security

Answer: D

Explanation:
The actions described fall under Operational Security (OPSEC), which is the practice of identifying critical information, analyzing potential adversary intelligence collection, and implementing measures to protect sensitive details from disclosure. In this case, the ISAC report highlights how adversaries may use photos shared on social media as reconnaissance, revealing details about technology or configurations inside secure facilities.
By disabling cameras and location services on corporate devices and blocking access to social media from corporate and guest networks, the CISO is reducing the chance of inadvertent information disclosure. This prevents employees from unintentionally leaking images or metadata that adversaries could exploit.
Adversary emulation (A) involves simulating threat actors' tactics in controlled exercises, which is not what is occurring here. Open-source intelligence (C) is the method adversaries use to gather data, not the defensive practice the CISO is implementing. Social engineering (D) describes manipulative attacks against humans, but this control is preventive, not reactive.
Thus, these measures are clear examples of Operational Security to limit information exposure.

NEW QUESTION # 143
A company's internal network is experiencing a security breach, and the threat actor is still active. Due to business requirements, users in this environment are allowed to utilize multiple machines at the same time. Given the following log snippet:

Time	User	Process	Status	Machine
10:11	user-a	.exe	blocked	machine02
10:15	user-b	setup.exe	blocked	machine02
10:15	user-A	appwiz.exe	blocked	machine01
10:16	user-c	appwiz.CPL	blocked	machine03
11:17	user-c	cmd.exe	blocked	machine03
11:18	user-h	msconfig.exe	blocked	machine04
11:19	user-d	firefox.exe	blocked	machine04
11:19	user-d	cmd.com	blocked	machine01

Which of the following accounts should a security analyst disable to best contain the incident without impacting valid users?

- A. user-b
- B. user-d
- C. user-a
- D. user-c

Answer: D

Explanation:
User user-c is showing anomalous behavior across multiple machines, attempting to run administrative tools such as cmd.exe and appwiz.CPL, which are commonly used by attackers for system modification. The activity pattern suggests a lateral movement attempt, potentially indicating a compromised account.
user-a (A) and user-b (B) attempted to run applications but only on one machine, suggesting less likelihood of compromise.
user-d (D) was blocked running cmd.com, but user-c's pattern is more consistent with an attack technique.

NEW QUESTION # 144
......

CAS-005 ” for free by simply searching on ▹ www.pdfvce.com ◃ CAS-005 Reliable Test Pattern

- Test CAS-005 Preparation Pass4sure CAS-005 Exam Prep Vce CAS-005 Test Simulator Search for 《 CAS-005 》 on ▸ www.exam4labs.com ◂ immediately to obtain a free download Test CAS-005 Topics Pdf
- Free CAS-005 Brain Dumps Valid CAS-005 Test Simulator CAS-005 Real Torrent Easily obtain free download of （ CAS-005 ） by searching on “ www.pdfvce.com ” New CAS-005 Test Materials
- Selecting Valid CAS-005 Test Cram - No Worry About CompTIA SecurityX Certification Exam The page for free download of “ CAS-005 ” on ⇛ www.prep4sures.top ⇚ will open immediately CAS-005 Reliable Test Test
- www.stes.tyc.edu.tw, 2.999moli.com, ncon.edu.sa, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, zenwriting.net, rcmspace.com, www.stes.tyc.edu.tw, capitalcollege.ac.ug, Disposable vapes

2025 Latest RealVCE CAS-005 PDF Dumps and CAS-005 Exam Engine Free Share: https://drive.google.com/open?id=1mXzcI3zmqIKzdBR4bnHFZJAggydc3bWO