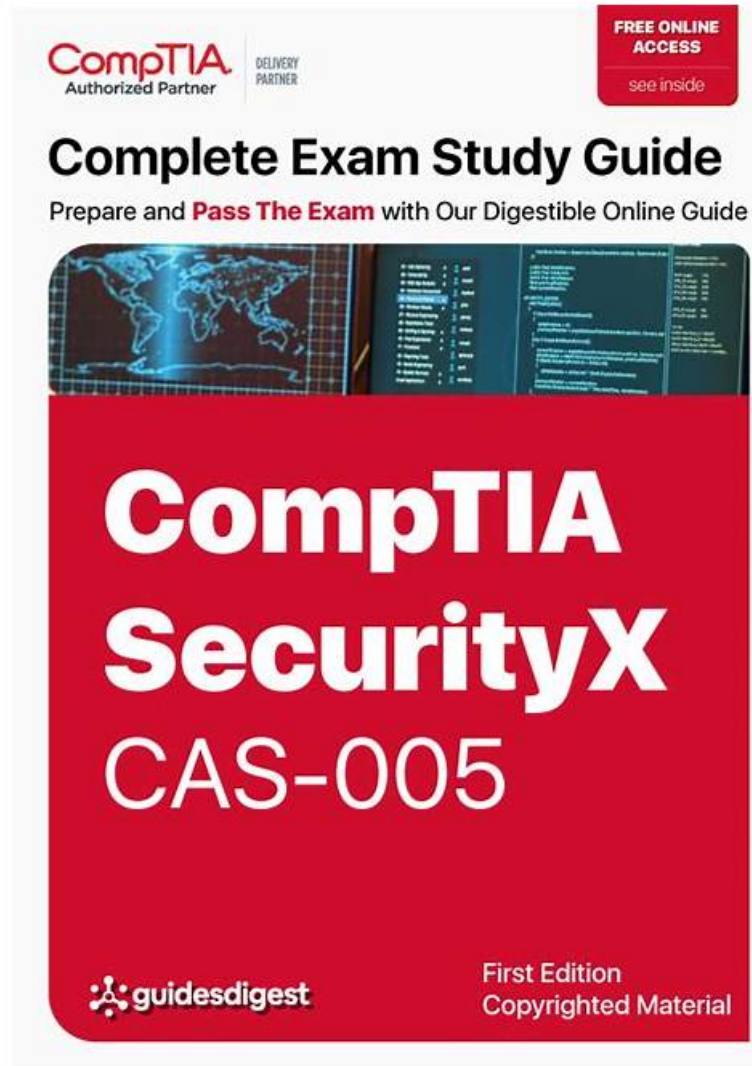# CAS-005 Exam Guide - CAS-005 Test Questions & CAS-005 Exam Torrent

DOWNLOAD the newest ValidExam CAS-005 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1_-xvVLnlGK4z1LqUPQCxl_OLibFr27Tt

We can proudly claim that you can successfully pass the exam just on the condition that you study with our CAS-005 preparation materials for 20 to 30 hours. And not only you will get the most rewards but also you will get an amazing study experience by our CompTIA SecurityX Certification Exam CAS-005 Exam Questions. For we have three different versions of our CompTIA CAS-005 study guide, and you will have different feelings if you have a try on them.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.
Topic 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 Exam Preview <<

CAS-005 Latest Dumps Files - CAS-005 Exam Blueprint

We now live in a world which needs the talents who can combine the practical abilities and knowledge to apply their knowledge into the practical working conditions. To prove that you are that kind of talents you must boost some authorized and useful certificate and the test CAS-005 certificate is one kind of these certificate. Passing the test CAS-005 Certification can prove you are that kind of talents and help you find a good job with high pay and if you buy our CAS-005 guide torrent you will pass the CAS-005 exam successfully. And our pass rate of CAS-005 exam prep is high as 99% to 100%.

CompTIA SecurityX Certification Exam Sample Questions (Q262-Q267):

NEW QUESTION # 262
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:
. The application does not need to know the users' credentials.
. An approval interaction between the users and the HTTP service must be orchestrated.
. The application must have limited access to users' data.
INSTRUCTIONS
Use the drop-down menus to select the action items for the appropriate locations. All placeholders must be filled.

Answer:

Explanation:
See the complete solution below in Explanation:
Explanation:
Select the Action Items for the Appropriate Locations:
Authorization Server:
Action Item: Grant access
The authorization server's role is to authenticate the user and then issue an authorization code or token that the client application can use to access resources. Granting access involves the server authenticating the resource owner and providing the necessary tokens for the client application.
Resource Server:
Action Item: Access issued tokens
The resource server is responsible for serving the resources requested by the client application. It must verify the issued tokens from the authorization server to ensure the client has the right permissions to access the requested data.
B2B Client Application:
Action Item: Authorize access to other applications
The B2B client application must handle the OAuth flow to authorize access on behalf of the user without requiring direct knowledge of the user's credentials. This includes obtaining authorization tokens from the authorization server and using them to request access to the resource server.
Detailed Explanation:
OAuth 2.0 is designed to provide specific authorization flows for web applications, desktop applications, mobile phones, and living

room devices. The integration involves multiple steps and components, including:
Resource Owner (User):
The user owns the data and resources that are being accessed.
Client Application (B2B Client Application):
Requests access to the resources controlled by the resource owner but does not directly handle the user's credentials. Instead, it uses tokens obtained through the OAuth flow.
Authorization Server:
Handles the authentication of the resource owner and issues the access tokens to the client application upon successful authentication.
Resource Server:
Hosts the resources that the client application wants to access. It verifies the access tokens issued by the authorization server before granting access to the resources.
OAuth Workflow:
The resource owner accesses the client application.
The client application redirects the resource owner to the authorization server for authentication.
The authorization server authenticates the resource owner and asks for consent to grant access to the client application.
Upon consent, the authorization server issues an authorization code or token to the client application.
The client application uses the authorization code or token to request access to the resources from the resource server.
The resource server verifies the token with the authorization server and, if valid, grants access to the requested resources.
References:
CompTIA Security+ Study Guide: Provides comprehensive information on various authentication and authorization protocols, including OAuth.
OAuth 2.0 Authorization Framework (RFC 6749): The official documentation detailing the OAuth 2.0 framework, its flows, and components.
OAuth 2.0 Simplified: A book by Aaron Parecki that provides a detailed yet easy-to-understand explanation of the OAuth 2.0 protocol.
By ensuring that each component in the OAuth workflow performs its designated role, the B2B client application can securely access the necessary resources without compromising user credentials, adhering to the principle of least privilege.

NEW QUESTION # 263
During a gap assessment, an organization notes that OYOD usage is asignificant risk. The organization implemented administrative policies prohibiting BYOD usage However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following solutions should the organization implement to b»« reduce the risk of OYOD devices? (Select two).

- A. PAM. to enforce local password policies
- B. Cloud 1AM to enforce the use of token based MFA
- C. NAC, to enforce device configuration requirements
- D. DLP, to enforce data protection capabilities
- E. Conditional access, to enforce user-to-device binding
- F. SD-WAN. to enforce web content filtering through external proxies

Answer: C,E

Explanation:
To reduce the risk of unauthorized BYOD (Bring Your Own Device) usage, the organization should implement Conditional Access and Network Access Control (NAC).
Why Conditional Access and NAC?
Conditional Access:
User-to-Device Binding: Conditional access policies can enforce that only registered and compliant devices are allowed to access corporate resources.
Context-Aware Security: Enforces access controls based on the context of the access attempt, such as user identity, device compliance, location, and more.
Network Access Control (NAC):
DeviceConfiguration Requirements: NAC ensures that only devices meeting specific security configurations are allowed to connect to the network.
Access Control: Provides granular control over network access, ensuring that BYOD devices comply with security policies before gaining access.
Other options, while useful, do not address the specific need to control and secure BYOD devices effectively:
A . Cloud IAM to enforce token-based MFA: Enhances authentication security but does not control device compliance.

D . PAM to enforce local password policies: Focuses on privileged account management, not BYOD control.

E . SD-WAN to enforce web content filtering: Enhances network performance and security but does not enforce BYOD device compliance.

F . DLP to enforce data protection capabilities: Protects data but does not control BYOD device access and compliance.

Reference:

CompTIA SecurityX Study Guide

"Conditional Access Policies," Microsoft Documentation

"Network Access Control (NAC)," Cisco Documentation

NEW QUESTION # 264

A security analyst notices a number of SIEM events that show the following activity:

10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop HinDctend

10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptidcasp.exe

10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell

10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell -> 40.90.23.154:443

Which of the following response actions should the analyst take first?

- A. Disable local administrator privileges on the endpoints
- B. Disable powershell.exe on all Microsoft Windows endpoints
- C. Configure the forward proxy to block 40.90.23.154
- D. Restart Microsoft Windows Defender

Answer: C

Explanation:

The first immediate action in an active incident is containment. Blocking the IP address (40.90.23.154) at the network edge prevents further communication with the malicious external server. Disabling PowerShell or removing local admin privileges are valid hardening steps, but containment by network control is the highest priority during an active compromise to stop data exfiltration or further command and control activity.

NEW QUESTION # 265

A cloud engineer wants to configure mail security protocols to support email authenticity and enable the flow of email security information to a third-party platform for further analysis. Which of the following must be configured to achieve these requirements? (Select two).

- A. DMARC
- B. SPF
- C. DKIM
- D. TLS
- E. MX
- F. DNSSEC

Answer: A,C

Explanation:

To support email authenticity and enable analysis by a third-party platform, the protocols must verify the sender's identity and provide metadata for inspection. According to the CompTIA SecurityX CAS-005 study guide (Domain 3: Cybersecurity Technology, 3.2):

* DMARC (Domain-based Message Authentication, Reporting, and Conformance): DMARC builds on SPF and DKIM to enforce policies for email authenticity and provides reporting mechanisms to share authentication results with third parties for analysis.

* DKIM (DomainKeys Identified Mail): DKIM adds a cryptographic signature to emails, allowing recipients to verify the sender's domain and ensure the email's integrity.

These two protocols are essential for authenticity and reporting.

* Option C (TLS): TLS ensures encryption during transmission but does not address authenticity or reporting.

* Option D (SPF): SPF verifies sender IP addresses but lacks reporting capabilities without DMARC.

* Option E (DNSSEC): DNSSEC secures DNS queries but is not specific to email authenticity.

* Option F (MX): MX records define mail servers, not authenticity or reporting.

Reference:

CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.2:

"Configure email security protocols, including DMARC and DKIM."
CAS-005 Exam Objectives, 3.2: "Implement technologies for email security and authenticity."

NEW QUESTION # 266
All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

- A. SAE
- B. Account federation with hardware tokens
- C. Key splitting
- D. Sating and hashing
- E. SSO with MFA

Answer: C

Explanation:
The technique that best addresses the issue of insider threats from employees who have individual access to encrypted material is key splitting.
Key Splitting: Key splitting involves dividing a cryptographic key into multiple parts and distributing these parts among different individuals or systems. This ensures that no single individual has complete access to the key, thereby mitigating the risk of insider threats.
Increased Security: By requiring multiple parties to combine their key parts to access encrypted material, key splitting provides an additional layer of security. This approach is particularly useful in environments where sensitive data needs to be protected from unauthorized access by insiders.
Compliance and Best Practices: Key splitting aligns with best practices and regulatory requirements for handling sensitive information, ensuring that access is tightly controlled and monitored.

NEW QUESTION # 267
......

Our CAS-005 exam pdf are regularly updated and tested according to the changes in the pattern of exam and latest exam information. There are free CAS-005 dumps demo in our website for you to check the quality and standard of our braindumps. We believe that our CAS-005 Pass Guide will be of your best partner in your exam preparation and of the guarantee of high passing score.

- CAS-005 Exam Preview - Realistic 2026 CompTIA CompTIA SecurityX Certification Exam Latest Dumps Files Pass Guaranteed 🔲 Easily obtain ☀ CAS-005 🔲☀🔲 for free download through ☀ www.practicevce.com 🔲☀🔲 🔲Test CAS-005 Practice
- quickeasyskill.com, 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, h20tradeskills.com, www.stes.tyc.edu.tw, learnup.center, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that ValidExam CAS-005 dumps now are free: https://drive.google.com/open?id=1_-xvVLnlGK4z1LqUPQCxl_OLibFr27Tt