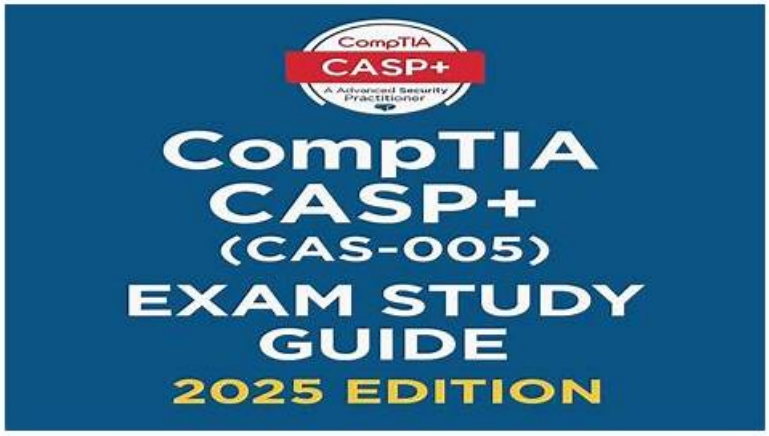
Valid CAS-005 Exam Answers & CAS-005 Exam Vce Format



BONUS!!! Download part of Actual4Cert CAS-005 dumps for free: https://drive.google.com/open?id=1XdVc5kINvwkRa3SxoJ6D_IH-6hjyx16R

These CompTIA CAS-005 practice tests simulate the real CompTIA SecurityX Certification Exam (CAS-005) exam pattern, track your progress, and help you overcome mistakes. Our CompTIA SecurityX Certification Exam (CAS-005) desktop software is compatible with Windows. Whereas, the web-based CompTIA CAS-005 Practice Exam works online on iOS, Linux, Android, Windows, and Mac. Additionally, the web-based CompTIA SecurityX Certification Exam (CAS-005) practice exam is also compatible with MS Edge, Internet Explorer, Opera, Firefox, Safari, and Chrome.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 4	• Security Architecture: This domain focuses on analyzing requirements to design resilient systems, including the configuration of firewalls and intrusion detection systems.

>> Valid CAS-005 Exam Answers <<

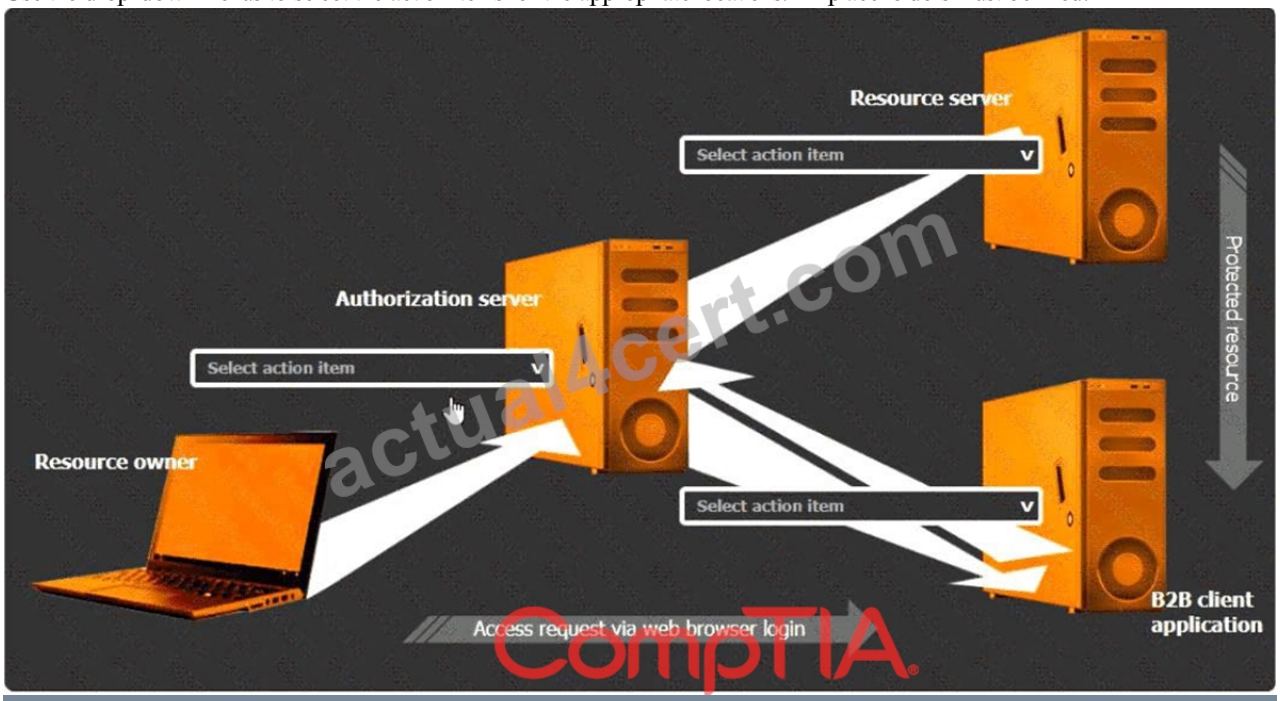
Valid CAS-005 Exam Answers | High Pass-Rate CAS-005: CompTIA SecurityX Certification Exam

Do you want to pass your exam with the least time? If you do, then we will be your best choice. CAS-005 training materials are

edited and verified by experienced experts in this field, therefore the quality and accuracy can be guaranteed. Besides CAS-005 exam materials contain both questions and answers, and it's convenient for you to have a check after practicing. We have online and offline chat service, if you have any questions about CAS-005 Training Materials, you can consult us, we will give you reply as quickly as possible.

CompTIA SecurityX Certification Exam Sample Questions (Q80-Q85):

NEW QUESTION # 80
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 theHTTP 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, desktopapplications, 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 # 81
During a periodic internal audit, a company identifies a few new, critical security controls that are missing.
The company has a mature risk management program in place, and the following requirements must be met:
* The stakeholders should be able to see all the risks.
* The risks need to have someone accountable for them.
Which of the following actions should the GRC analyst take next?

- A. Add the risk to the risk register and assign the owner and severity.
- B. Mitigate the risk and change the status to accepted.
- C. Change the risk appetite and assign an owner to it.

- D. Review the risk to decide whether to accept or reject it.

Answer: A

Explanation:
A risk register is atool commonly used in risk management to document all identified risks, their assessment in terms of likelihood and impact, and the actions steps to manage them. By adding the newly identified risks to the risk register and assigning an owner and severity, the organization ensures that each risk is visible to stakeholders and has a designated individual responsible for its management. This aligns with the company's requirements for transparency and accountability in risk management.
Reference:CompTIA SecurityX CAS-005 Official Study Guide, Chapter 6: "Risk Management," Section 6.4: "Risk Register and Risk Ownership."

NEW QUESTION # 82
An organization recently implemented a purchasing freeze that has impacted endpoint life-cycle management efforts. Which of the following should a security manager do to reduce risk without replacing the endpoints?

- A. Dispose of end-of-support devices
- B. Remove unneeded services
- C. Deploy EDR
- D. Reimage the system

Answer: B

Explanation:
Removing unnecessary services from existing endpoints reduces the attack surface by minimizing the number of potential vulnerabilities attackers could exploit. This is a cost-effective method to harden devices without requiring new purchases, aligning perfectly with a purchasing freeze. Deploying new EDR solutions or disposing of devices would likely conflict with the resource freeze, and reimaging systems does not address minimizing services proactively.

NEW QUESTION # 83
An organization recently implemented a policy that requires all passwords to be rotated every 90 days. An administrator observes a large volume of failed sign-on logs from multiple servers that are often accessed by users. The administrator determines users are disconnecting from the RDP session but not logging off. Which of the following should the administrator do to prevent account lockouts?

- A. Extend the allowed session length.
- B. Enforce password complexity.
- C. Automate logout of inactive sessions.
- D. Increase the account lockout threshold.

Answer: C

Explanation:
When users disconnect from Remote Desktop Protocol (RDP) sessions without properly logging off, their sessions remain active on the server. If their passwords are changed due to the 90-day rotation policy, these lingering sessions may attempt to reauthenticate using outdated credentials, leading to multiple failed login attempts and potential account lockouts.
Automating the logout of inactive sessions ensures that disconnected or idle sessions are terminated after a specified period, preventing stale sessions from causing authentication issues. This approach aligns with best practices for session management and helps maintain security compliance.
Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 3.1: "Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment."

NEW QUESTION # 84
An organization recently implemented a purchasing freeze that has impacted endpoint life-cycle management efforts. Which of the following should a security manager do to reduce risk without replacing the endpoints?

- A. Dispose of end-of-support devices
- B. Remove unneeded services

- C. Deploy EDR
- D. Reimage the system

Answer: B

Explanation:
Removing unnecessary services from existing endpoints reduces the attack surface by minimizing the number of potential vulnerabilities attackers could exploit. This is a cost-effective method to harden devices without requiring new purchases, aligning perfectly with a purchasing freeze. Deploying new EDR solutions or disposing of devices would likely conflict with the resource freeze, and reimaging systems does not address minimizing services proactively.
Reference:CompTIA SecurityX CAS-005, Domain 3.0: Implement endpoint security controls and hardening techniques.

NEW QUESTION # 85
.....