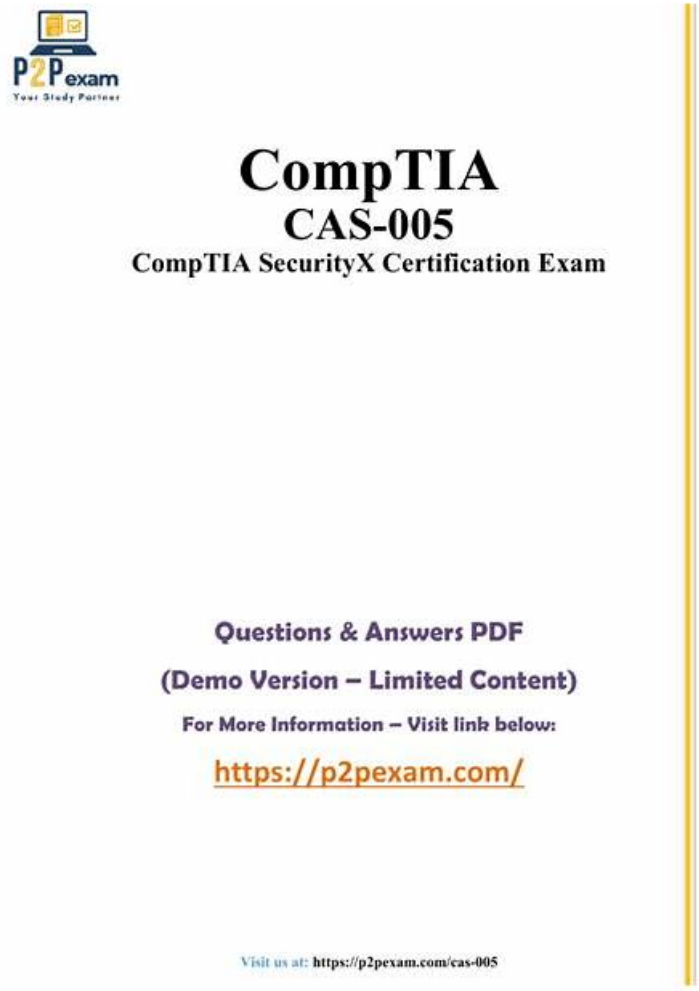
Free Demo Version and Free Updates of Real CompTIA CAS-005 Questions



P.S. Free & New CAS-005 dumps are available on Google Drive shared by PDF4Test: https://drive.google.com/open?id=1EDSpTTNArSdcBI_FhmlZeMJpaCVzDMUS

CompTIA provides the most reliable and authentic CompTIA CAS-005 Exam prep material there is. The 3 kinds of CompTIA CAS-005 Preparation formats ensure that there are no lacking points in a student when he attempts the actual CAS-005 exam.

For candidates who are going to buy CAS-005 study guide materials online, the safety for the website is important. We have professional technicians to examine the website at times. If you choose us, we will provide you with a clean and safe online shopping environment. Besides, we offer you free demo for CAS-005 exam materials for you to have a try, so that you can know the mode of the complete version. You can enjoy free update for one year for CAS-005 Exam Materials, so that you can know the latest version for the exam timely. The update version for CAS-005 exam materials will be sent to your email automatically.

>> CAS-005 Valid Test Pattern <<

CAS-005 Exam Question | Reliable CAS-005 Exam Online

The pass rate of the CAS-005 exam braindumps is 98.75%, and pass guarantee and money back guarantee, if you indeed fail in the exam by using CAS-005 exam dumps of us , we will refund your money or if you need to attend other exam, we will replace other 2 valid exam dumps for free. Besides, the CAS-005 Exam Dumps contain both quality and certain quantity, it is good for you to practice and pass the exam successfully.

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	• 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 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.

CompTIA SecurityX Certification Exam Sample Questions (Q366-Q371):

NEW QUESTION # 366
Which of the following best explains why AI output could be inaccurate?

- A. Output handling
- B. Social engineering
- C. Model poisoning
- D. Prompt injections

Answer: C

NEW QUESTION # 367
An organization has deployed a cloud-based application that provides virtual event services globally to clients. During a typical event, thousands of users access various entry pages within a short period of time. The entry pages include sponsor-related content that is relatively static and is pulled from a database. When the first major event occurs, users report poor response time on the entry pages. Which of the following features is the most appropriate for the company to implement?

- A. Caching
- B. Vertical scalability
- C. Containerization
- D. Horizontal scalability
- E. Static code analysis

Answer: A

Explanation:
Since the entry pages contain sponsor-related content that is relatively static and pulled from a database, implementing caching would be the most appropriate solution. Caching stores frequently accessed data in a location that is faster to access than querying the database repeatedly. This reduces the load on the database and improves response times for users, especially during high-traffic events. By caching the static content (like sponsor information), the application can serve those pages faster and handle large numbers of users more efficiently.

NEW QUESTION # 368
A security analyst is reviewing the following event timeline from an COR solution:

Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

Which of the following most likely has occurred and needs to be fixed?

- A. An EDR bypass was utilized by a threat actor and updates must be installed by the administrator.
- B. A potential insider threat is being investigated and will be addressed by the senior management team.
- C. The DlP has failed to block malicious exfiltration and data tagging is not being utilized property
- D. A logic law has introduced a TOCTOU vulnerability and must be addressed by the COR vendor

Answer: D

Explanation:
The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of-Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.
Reference:
CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations": Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
"The Art of Software Security Assessment" by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

NEW QUESTION # 369
An organization hires a security consultant to establish a SOC that includes a threat-modeling function.
During initial activities, the consultant works with system engineers to identify antipatterns within the environment. Which of the following is most critical for the engineers to disclose to the consultant during this phase?

- A. Results from the most recent infrastructure access review
- B. A listing of unpatchable IoT devices in use in the data center
- C. Results from the most recent software composition analysis
- D. Network and data flow diagrams covering the production environment
- E. A current inventory of cloud resources and SaaS products in use

Answer: D

Explanation:
In the context of establishing a Security Operations Center (SOC) with a threat-modeling function, it's crucial to understand how data flows within the organization's systems. Network and data flow diagrams provide a visual representation of the system's architecture, illustrating how data moves between components, which is essential for identifying potential security weaknesses and antipatterns. Antipatterns are common responses to recurring problems that are ineffective and risk-inducing. By analyzing these diagrams, the consultant can pinpoint areas where security controls may be lacking or misconfigured, thereby facilitating the development of effective threat models.
While other options like unpatchable IoT devices (Option B) and inventories of cloud resources (Option E) are important for comprehensive security assessments, they are more pertinent during later stages, such as vulnerability management and asset inventory. The initial phase of threat modeling focuses on understanding the system's structure and data flows to identify potential threats, making network and data flow diagrams the most critical information at this stage.

NEW QUESTION # 370
While reviewing recent modem reports, a security officer discovers that several employees were contacted by the same individual

who impersonated a recruiter. Which of the following best describes this type of correlation?

- A. Threat modeling
- B. Red team assessment
- C. Spear-phishing campaign
- D. Attack pattern analysis

Answer: C

Explanation:
The situation where several employees were contacted by the same individual impersonating a recruiter best describes a spear-phishing campaign. Here's why:
* Targeted Approach: Spear-phishing involves targeting specific individuals within an organization with personalized and convincing messages to trick them into divulging sensitive information or performing actions that compromise security.
* Impersonation: The use of impersonation, in this case, a recruiter, is a common tactic in spear-phishing to gain the trust of the targeted individuals and increase the likelihood of a successful attack.
* Correlated Contacts: The fact that several employees were contacted by the same individual suggests a coordinated effort to breach the organization's security by targeting multiple points of entry through social engineering.
* References:
* CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
* NIST Special Publication 800-61: Computer Security Incident Handling Guide
* OWASP Phishing Cheat Sheet

NEW QUESTION # 371
.....

BONUS!!! Download part of PDF4Test CAS-005 dumps for free: https://drive.google.com/open?id=1EDSpTTNArSdcBI_FhmlZeMJpaCVzDMUS