Newest Exam CAS-005 Forum Supply you Unparalleled Reliable Study Materials for CAS-005: CompTIA SecurityX Certification Exam to Prepare casually

BONUS!!! Download part of DumpsKing CAS-005 dumps for free: https://drive.google.com/open?id=1B-gTQXWvavEcguf3sptacmUGcQVjjt-q

Our CAS-005 exam simulation is selected many experts and constantly supplements and adjust our questions and answers. When you use our CAS-005 study materials, you can find the information you need at any time. When we update the CAS-005 preparation questions, we will take into account changes in society, and we will also draw user feedback. If you have any thoughts and opinions in using our CAS-005 Study Materials, you can tell us. We hope to grow with you and the continuous improvement of CAS-005 training engine is to give you the best quality experience.

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

>> Exam CAS-005 Forum <<

CAS-005 Reliable Study Materials | Valid Exam CAS-005 Braindumps

Our CompTIA SecurityX Certification Exam (CAS-005) exam dumps comes in three formats: CompTIA CAS-005 PDF dumps file, desktop-based practice test software, and a web-based practice exam. These versions are specially designed to make CompTIA SecurityX Certification Exam (CAS-005) preparation for users easier. CAS-005 Questions in these formats of DumpsKing's material are enough grasp every test topic in the shortest time possible.

CompTIA SecurityX Certification Exam Sample Questions (Q153-Q158):

NEW QUESTION # 153
During a recent security event, access from the non-production environment to the production environment enabled unauthorized users to:
* Install unapproved software
* Make unplanned configuration changes
During the investigation, the following findings were identified:
* Several new users were added in bulk by the IAM team
* Additional firewalls and routers were recently added
* Vulnerability assessments have been disabled for more than 30 days
* The application allow list has not been modified in two weeks
* Logs were unavailable for various types of traffic
* Endpoints have not been patched in over ten days
Which of the following actions would most likely need to be taken to ensure proper monitoring? (Select two)

- A. Configure firewall rules to only allow production-to-non-production traffic
- B. Routinely update all endpoints and network devices as soon as new patches/hot fixes are available
- C. Extend log retention for all security and network devices to 180 days for all traffic
- D. Ensure all network and security devices are sending relevant data to the SIEM
- E. Disable bulk user creations by the IAM team
- F. Review the application allow list daily

Answer: B,D,E

Explanation:
Comprehensive and Detailed Explanation:
* Understanding the Security Event:
* Unauthorized users gained access from non-production to production.
* IAM policies were weak, allowing bulk user creation.
* Vulnerability assessments were disabled, and patching was delayed.
* Logs were unavailable, making incident response difficult.
* Why Options A, D, and E are Correct:
* A (Disable bulk user creation by IAM team) # Prevents unauthorized mass user account creation, which could be exploited by attackers.
* D (Routine updates for endpoints & network devices) # Patch management ensures vulnerabilities are not left open for attackers.
* E (Ensure all security/network devices send logs to SIEM) # Helps with real-time monitoring and detection of unauthorized activities.
* Why Other Options Are Incorrect:
* B (180-day log retention) # While log retention is good, real-time monitoring is the priority.
* C (Review application allow list daily) # Reviewing it daily is impractical. Regular audits are better.
* F (Restrict production-to-non-production traffic) # The issue is unauthorized access, not traffic routing.

NEW QUESTION # 154
A security engineer wants to stay up-to-date on new detections that are released on a regular basis. The engineer's organization uses multiple tools rather than one specific vendor security stack. Which of the following rule-based languages is the most appropriate to use as a baseline for detection rules with the multiple security tool setup?

- A. Rita
- B. YARA
- C. Sigma
- D. Snort

Answer: C

Explanation:
Sigma is a rule-based detection language that is vendor-agnostic, meaning it can be used across different SIEM (Security Information and Event Management) tools.

NEW QUESTION # 155
An organization recently migrated data to a new file management system. The architect decides to use a discretionary authorization model on the new system. Which of the following best explains the architect's choice?

- A. The legacy file management system did not support modern authentication techniques despite the business requirements.
- B. The data custodians were selected by business stakeholders to ensure backups of the file management system are maintained off site.
- C. The responsibility of migrating data to the new file management system was outsourced to the vendor providing the platform.
- D. The permissions were not able to be migrated to the new system, and several stakeholders were made responsible for granting appropriate access.

Answer: D

Explanation:
Comprehensive and Detailed Explanation:
In a Discretionary Access Control (DAC) model, the data owner or an assigned stakeholder has the authority to determine who can access resources. SecurityX CAS-005 IAM objectives describe DAC as user- or owner-controlled, where permissions can be granted or revoked at the owner's discretion.
In this scenario, because permissions from the legacy system could not be migrated, multiple stakeholders were made responsible for assigning and managing access-matching the DAC model's characteristics.
* Option A relates to outsourcing, which does not define an access control model.
* Option C is about authentication limitations, unrelated to the choice of DAC.
* Option D describes backup responsibilities, which are operational tasks, not access control.

NEW QUESTION # 156
A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform This collaboration gives partner organizations theability to obtain and share data associated with emerging threats from a variety of adversaries Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

- A. ATTACK
- B. STIX
- C. YAKA
- D. CWPP
- E. JTAG
- F. TAXII

Answer: B,F

Explanation:
D:STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.
E: TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.
Other options:
A: CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.
B: YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.
C: ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.
F: JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.

NEW QUESTION # 157
A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?

- A. Fragility and other availability attacks
- B. Non-conformance to accepted manufacturing standards
- C. Physical Implants and tampering
- D. Ability to obtain components during wartime

Answer: C

Explanation:
The allow list for specific countries of origin as a risk mitigation indicates that the central bank is focused on preventing physical implants and tampering in hardware. This is a form of supply chain attack where malicious actors may insert malicious hardware components into devices, leading to potential compromises in security. By restricting the countries of origin, the bank is likely aiming to prevent such vulnerabilities.

NEW QUESTION # 158
.....

Compared with the education products of the same type, some users only for college students, some only provide for the use of employees, these limitations to some extent, the product covers group, while our CAS-005 study dumps absorbed the lesson, it can satisfy the different study period of different cultural levels of the needs of the audience. For example, if you are a college student, you can study and use online resources through the student column of our CAS-005 learning guide, and you can choose to study in your spare time. On the other hand, the research materials of CAS-005 can make them miss the peak time of college students' use, so that they can make full use of their time to review after work. The range of people covered greatly enhances the core competitiveness of our products and maximizes the role of our CAS-005 exam materials.

What's more, part of that DumpsKing CAS-005 dumps now are free: https://drive.google.com/open?id=1B-gTQXWvavEcguf3sptacmUGcQVjjt-q