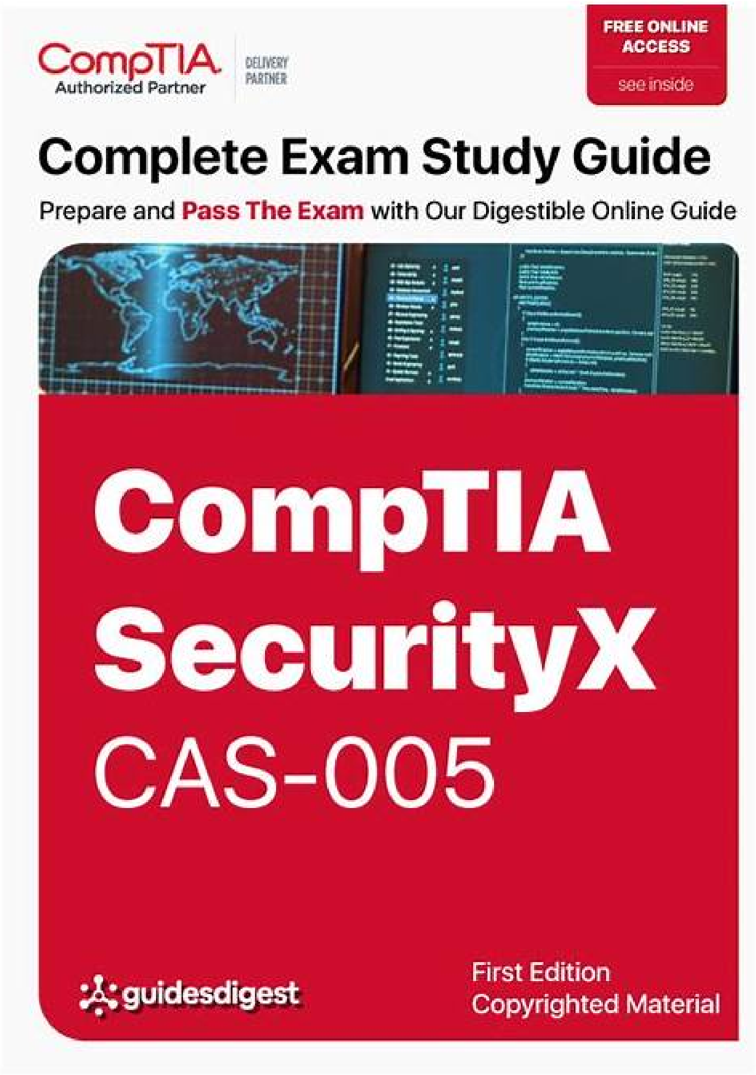
New CompTIA CAS-005 Exam Preparation, CAS-005 Valid Test Papers



P.S. Free 2026 CompTIA CAS-005 dumps are available on Google Drive shared by BraindumpStudy: https://drive.google.com/open?id=1RjDWSYAXxZvOl24QFW8ocCzB3Hp_Zzra

The BraindumpStudy is committed to providing the best possible study material to succeed in the CompTIA SecurityX Certification Exam (CAS-005) exam. With actual PDF questions, customizable practice exams, and 24/7 support, customers can be confident that they are getting the best possible prep material. The BraindumpStudy CAS-005 is an excellent choice for anyone looking to advance their career with the certification. Buy Now.

As we all know, examination is a difficult problem for most students, but getting the test CAS-005 certification and obtaining the relevant certificate is of great significance to the workers in a certain field, so the employment in the new period is under great pressure. Fortunately, however, you don't have to worry about this kind of problem anymore because you can find the best solution on a powerful Internet - CAS-005 Study Materials. With our technology, personnel and ancillary facilities of the continuous investment and research, our company's future is a bright, the CAS-005 study materials have many advantages, and now I would like to briefly introduce.

>> New CompTIA CAS-005 Exam Preparation <<

Quiz 2026 CompTIA CAS-005: CompTIA SecurityX Certification Exam Latest New Exam Preparation

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

CompTIA SecurityX Certification Exam Sample Questions (Q76-Q81):

NEW QUESTION # 76
During DAST scanning, applications are consistently reporting code defects in open-source libraries that were used to build web applications. Most of the code defects are from using libraries with known vulnerabilities. The code defects are causing product deployment delays. Which of the following is the best way to uncover these issues earlier in the life cycle?

- A. Modifying the WAF policies to block against known vulnerabilities
- B. Using a software dependency management solution
- C. Directing application logs to the SIEM for continuous monitoring
- D. Completing an IAST scan against the web application

Answer: B

Explanation:
Comprehensive and Detailed
SecurityX CAS-005 exam content emphasizes integrating security into the SDLC and using automated tools to identify vulnerabilities early.
Software dependency management solutions track and analyze libraries and components for known vulnerabilities before deployment, using vulnerability databases such as NVD or OSS Index.
IAST scanning still requires the application to be running and may detect issues later.
WAF policies help block attacks in production but do not prevent vulnerable code from being deployed.

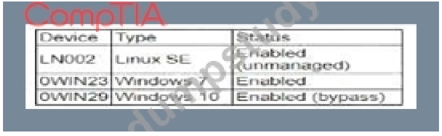
NEW QUESTION # 77
An endpoint security engineer finds that a newly acquired company has a variety of non-standard applications running and no defined ownership for those applications. The engineer needs to find a solution that restricts malicious programs and software from running in that environment, while allowing the non-standard applications to function without interruption. Which of the following application control configurations should the engineer apply?

- A. MAC list
- B. Deny list
- C. Audit mode
- D. Allow list

Answer: C

Explanation:
Comprehensive and Detailed Step-by-Step Explanation:
Option A: Deny list
* Deny lists block specific applications or processes identified as malicious.
* This approach is reactive and may inadvertently block the non-standard applications that are currently in use without proper ownership.
Option B: Allow list
* Allow lists permit only pre-approved applications to run.
* While secure, this approach requires defining all non-standard applications, which may disrupt operations in an environment where ownership is unclear.
Option C: Audit mode
* Correct Answer.
* Audit mode allows monitoring and logging of applications without enforcing restrictions.
* This is ideal in environments with non-standard applications and undefined ownership because it enables the engineer to observe the environment and gradually implement control without interruption.
* Audit mode provides critical visibility into the software landscape, ensuring that necessary applications remain functional.
Option D: MAC list
* Mandatory Access Control (MAC) lists restrict access based on classification and clearance levels.
* This does not align with application control objectives in this context.
CompTIA CASP+ Study Guide - Chapters on Endpoint Security and Application Control.
CASP+ Objective 2.4: Implement appropriate security controls for enterprise endpoints.

NEW QUESTION # 78
During a security assessment using an CDR solution, a security engineer generates the following report about the assets in me system:



Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
OWIN23	Windows 7	Enabled
OWIN29	Windows 10	Enabled (bypass)

After five days, the EDR console reports an infection on the host 0WIN23 by a remote access Trojan Which of the following is the most probable cause of the infection?

- A. The EDR has an unknown vulnerability that was exploited by the attacker.
- B. 0W1N29 spreads the malware through other hosts in the network
- C. OW1N23 uses a legacy version of Windows that is not supported by the EDR
- D. LN002 was not supported by the EDR solution and propagates the RAT

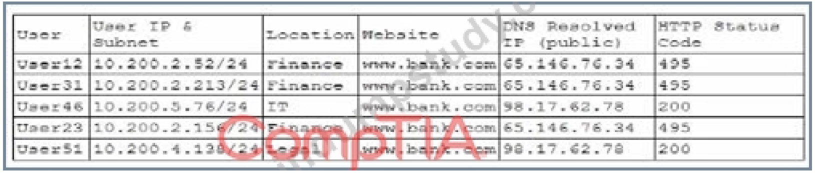
Answer: C

Explanation:
OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).
A: OWIN23 uses a legacy version of Windows that is not supported by the EDR: This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.
B: LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.
C: The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.
D: OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.
References:
CompTIA Security+ Study Guide
NIST SP 800-53, "Security and Privacy Controls forInformation Systems and Organizations" Microsoft's Windows 7 End of

Support documentation

NEW QUESTION # 79

A company's help desk is experiencing a large number of calls from the finance department slating access issues to www bank com The security operations center reviewed the following security logs:



User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.138/24	Legal	www.bank.com	98.17.62.78	200

Which of the following is most likely the cause of the issue?

- A. The DNS record has been poisoned.
- B. Recursive DNS resolution is failing
- C. The DNS was set up incorrectly.
- D. DNS traffic is being sinkholed.

Answer: D

Explanation:
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.
In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.
Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.
DNS poisoning (B) could result in users being directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.
Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.
By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.
Reference:
CompTIA SecurityX study materials on DNS security mechanisms.
Standard HTTP status codes and their implications.

NEW QUESTION # 80

A security engineer must ensure that sensitive corporate information is not exposed if a company laptop is stolen. Which of the following actions best addresses this requirement?

- A. Using explicit allow lists of specific IP addresses and deploying single sign-on
- B. Updating security mobile reporting policies and monitoring data breaches
- C. Utilizing desktop as a service for all company data and multifactor authentication
- D. Deploying mobile device management and requiring stronger passwords

Answer: C

Explanation:
To prevent sensitive corporate information from being exposed if a laptop is stolen, the solution must ensure that data is not stored locally and access is tightly controlled. According to the CompTIA SecurityX CAS-005 study guide (Domain 4: Governance, Risk, and Compliance, 4.3), Desktop as a Service (DaaS) hosts data and applications in the cloud, reducing the risk of data exposure on physical devices. Combining DaaS with multifactor authentication (MFA) ensures that even if a laptop is stolen, unauthorized access to the cloud environment is prevented.
Option B: IP allow lists and SSO do not address data stored locally on the laptop, which could be accessed offline.
Option C: MDM and stronger passwords help but do not prevent data exposure if the device is compromised (e.g., via offline attacks).
Option D: Updating policies and monitoring breaches are reactive measures that do not directly protect data on a stolen laptop.
Option A: DaaS ensures no sensitive data resides on the device, and MFA secures access, making it the best solution.

Reference:
CompTIA SecurityX CAS-005 Official Study Guide, Domain 4: Governance, Risk, and Compliance, Section 4.3: "Implement secure data handling through cloud-based solutions like DaaS." CAS-005 Exam Objectives, 4.3: "Analyze solutions for protecting sensitive data on endpoints."

NEW QUESTION # 81

......

It is well acknowledged that people who have a chance to participate in the simulation for the real CAS-005 exam, they must have a fantastic advantage over other people to get good grade in the CAS-005 exam. Now, it is so lucky for you to meet this opportunity once in a blue. We offer you the simulation test with the Software version of our CAS-005 Preparation dumps in order to let you be familiar with the environment of test as soon as possible.

CAS-005 Valid Test Papers: https://www.braindumpstudy.com/CAS-005_braindumps.html

- New CAS-005 Exam Preparation 100% Pass | High Pass-Rate CAS-005 Valid Test Papers: CompTIA SecurityX Certification Exam □ Copy URL { www.dumpsmaterials.com } open and search for { CAS-005 } to download for free □ □Reliable CAS-005 Test Experience
- Latest CAS-005 Exam Cost □ Exam CAS-005 Reviews □ Valid CAS-005 Test Syllabus □ Go to website ⇛ www.pdfvce.com ⇚ open and search for ▹ CAS-005 ◃ to download for free □CAS-005 Dumps Collection
- 100% Pass 2026 CompTIA CAS-005: Newest New CompTIA SecurityX Certification Exam Exam Preparation □ Immediately open ⇛ www.vce4dumps.com ⇚ and search for ☀ CAS-005 □☀□ to obtain a free download □CAS-005 Exam Details
- Exam CAS-005 Reviews □ Valid CAS-005 Test Syllabus □ CAS-005 Test Price □ Copy URL ➥ www.pdfvce.com □ open and search for " CAS-005 " to download for free □Study CAS-005 Center
- Real CompTIA SecurityX Certification Exam Test Questions - CAS-005 Actual Torrent - CompTIA SecurityX Certification Exam Pdf Questions □ Open ✔ www.pass4test.com □✔□ and search for ☀ CAS-005 □☀□ to download exam materials for free □CAS-005 Exam Details
- CAS-005 Valid Test Notes □ CAS-005 Valid Braindumps □ CAS-005 Exam □ Search for 【 CAS-005 】 and easily obtain a free download on ➥ www.pdfvce.com □ □CAS-005 Exam Quizzes
- Valid CAS-005 Test Syllabus □ CAS-005 Valid Braindumps □ PDF CAS-005 Download □ Download ✔ CAS-005 □✔□ for free by simply searching on ☀ www.practicevce.com □☀□ □Dumps CAS-005 Questions
- Study CAS-005 Center □ PDF CAS-005 Download □ CAS-005 Exam Details □ Search for ⇛ CAS-005 ⇚ and easily obtain a free download on ➻ www.pdfvce.com □ □CAS-005 Valid Test Sims
- Professional New CAS-005 Exam Preparation - Easy and Guaranteed CAS-005 Exam Success □ Search for ➡ CAS-005 □□□ and download exam materials for free through { www.practicevce.com } □Latest CAS-005 Exam Cost
- CAS-005 Exam Demo □ Latest CAS-005 Exam Cost □ CAS-005 Test Price □ Easily obtain free download of ➠ CAS-005 □ by searching on □ www.pdfvce.com □ □CAS-005 Valid Test Cost
- CAS-005 Valid Test Cost □ Latest CAS-005 Exam Cost □ Dumps CAS-005 Questions □ The page for free download of " CAS-005 " on 「 www.prepawayexam.com 」 will open immediately □CAS-005 Valid Test Cost
- 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, Disposable vapes

DOWNLOAD the newest BraindumpStudy CAS-005 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1RjDWSYAXxZvOl24QFW8ocCzB3Hp_Zzra