CAS-005 Q&As

CompTIA SecurityX Exam

Pass CompTIA CAS-005 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cas-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpomts:

1.

Full disk encryption

2.

Host-based firewall

3.

Time synchronization

4.

Password policies

5.

Application allow listing

6.

Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

A. CASB

B. SBoM

C. SCAP

D. SASE

E. HIDS

Correct Answer: CD

To address the specific OS benchmark configurations, the following solutions are most appropriate:

C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies. D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data. These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures. NIST Special Publication 800-126, "The Technical Specification for the Security Content

Automation

Protocol (SCAP)": Details SCAP\\'s role in security automation. "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

QUESTION 2

A security engineer evaluates the overall security of a custom mobile gaming application and notices that developers are bringing in a large number of open-source packages without appropriate patch management. Which of the following would the engineer most likely recommend for uncovering known vulnerabilities in the packages?

A. Leverage an exploitation framework to uncover vulnerabilities.

B. Use fuzz testing to uncover potential vulnerabilities in the application.

C. Utilize a software composition analysis tool to report known vulnerabilities.

D. Reverse engineer the application to look for vulnerable code paths.

E. Analyze the use of an HTTP intercepting proxy to dynamically uncover issues.

Correct Answer: C

QUESTION 3

Which of the following best explains the business requirement a healthcare provider fulfills by encrypting patient data at rest?

A. Securing data transfer between hospitals

B. Providing for non-repudiation data

C. Reducing liability from identity theft

D. Protecting privacy while supporting portability.

Correct Answer: D

Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this

practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is

maintained even if the storage media are compromised. Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are

in place.

References:

CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.

HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.

"Health Informatics: Practical Guide for Healthcare and Information Technology Professionals" by Robert E. Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.

QUESTION 4

Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

A. Encryption systems based on large prime numbers will be vulnerable to exploitation

B. Zero Trust security architectures will require homomorphic encryption.

C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques

D. Quantum computers will enable malicious actors to capture IP traffic in real time

Correct Answer: A

Advancements in quantum computing pose a significant threat to current encryption systems, especially those based on the difficulty of factoring large prime numbers, such as RSA. Quantum computers have the potential to solve these

problems exponentially faster than classical computers, making current cryptographic systems vulnerable.

Why Large Prime Numbers are Vulnerable:

Shor\\'s Algorithm: Quantum computers can use Shor\\'s algorithm to factorize large integers efficiently, which undermines the security of RSA encryption. Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that

encrypted data, which relies on the hardness of this mathematical problem, can be decrypted.

Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:

B. Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms. C. Perfect forward secrecy: It enhances security but is not the main reason for new encryption

algorithms.

D. Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.

References:

CompTIA SecurityX Study Guide

NIST Special Publication 800-208, "Recommendation for Stateful Hash-Based Signature Schemes"

"Quantum Computing and Cryptography," MIT Technology Review

QUESTION 5

Company A and Company D ate merging Company A\\'s compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed.

Which of the following should me analyst cons