CAS-003Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

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

https://www.passapply.com/cas-003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A security analyst has been asked to create a list of external IT security concerns, which are applicable to the organization. The intent is to show the different types of external actors, their attack vectors, and the types of vulnerabilities that would cause business impact. The Chief Information Security Officer (CISO) will then present this list to the board to request funding for controls in areas that have insufficient coverage.

Which of the following exercise types should the analyst perform?

A. Summarize the most recently disclosed vulnerabilities.

B. Research industry best practices and latest RFCs.

C. Undertake an external vulnerability scan and penetration test.

D. Conduct a threat modeling exercise.

Correct Answer: D

QUESTION 2

A security architect has designated that a server segment of an enterprise network will require each server to have secure and measured boot capabilities. The architect now wishes to ensure service consumers and peers can verify the integrity of hosted services. Which of the following capabilities must the architect consider for enabling the verification?

A. Centralized attestation server

B. Enterprise HSM

C. vTPM

D. SIEM

Correct Answer: B

QUESTION 3

A security analyst works for a defense contractor that produces classified research on drones. The contractor faces nearly constant attacks from sophisticated nation-state actors and other APIs. Which of the following would help protect the confidentiality of the research data?

A. Use diverse components in layers throughout the architecture

B. Implement non-heterogeneous components at the network perimeter

C. Purge all data remnants from client devices\\' volatile memory at regularly scheduled intervals

D. Use only in-house developed applications that adhere to strict SDLC security requirements

Correct Answer: A

QUESTION 4

A security engineer is working on a large software development project. As part of the design of the project, various stakeholder requirements were gathered and decomposed to an implementable and testable level.

Various security requirements were also documented.

Organize the following security requirements into the correct hierarchy required for an SRTM.

Requirement 1: The system shall provide confidentiality for data in transit and data at rest.

Requirement 2: The system shall use SSL, SSH, or SCP for all data transport.

Requirement 3: The system shall implement a file-level encryption scheme.

Requirement 4: The system shall provide integrity for all data at rest.

Requirement 5: The system shall perform CRC checks on all files.

A. Level 1: Requirements 1 and 4; Level 2: Requirements 2, 3, and 5

B. Level 1: Requirements 1 and 4; Level 2: Requirements 2 and 3 under 1, Requirement 5 under 4

C. Level 1: Requirements 1 and 4; Level 2: Requirement 2 under 1, Requirement 5 under 4; Level 3: Requirement 3 under 2

D. Level 1: Requirements 1, 2, and 3; Level 2: Requirements 4 and 5

Correct Answer: B

Confidentiality and integrity are two of the key facets of data security. Confidentiality ensures that sensitive information is not disclosed to unauthorized users; while integrity ensures that data is not altered by unauthorized users. These are

Level 1 requirements.

Confidentiality is enforced through encryption of data at rest, encryption of data in transit, and access control. Encryption of data in transit is accomplished by using secure protocols such as PSec, SSL, PPTP, SSH, and SCP, etc.

Integrity can be enforced through hashing, digital signatures and CRC checks on the files.

In the SRTM hierarchy, the enforcement methods would fall under the Level requirement.

References:

Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley and Sons, Indianapolis, 2012, pp. 17-19, 20, 27-29

QUESTION 5

Which of the following may indicate a configuration item has reached end-of-life?

A. The device will no longer turn on and indicated an error.

B. The vendor has not published security patches recently.

C. The object has been removed from the Active Directory.

D. Logs show a performance degradation of the component.

Correct Answer: B