CAS-003 Q&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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security appliance vendor is reviewing an RFP that is requesting solutions for the defense of a set of web-based applications. This RFP is from a financial institution with very strict performance requirements. The vendor would like to respond with its solutions.

Before responding, which of the following factors is MOST likely to have an adverse effect on the vendor\\'s qualifications?

A. The solution employs threat information-sharing capabilities using a proprietary data model.

B. The RFP is issued by a financial institution that is headquartered outside of the vendor\\'s own country.

C. The overall solution proposed by the vendor comes in less that the TCO parameter in the RFP.

D. The vendor\\'s proposed solution operates below the KPPs indicated in the RFP.

Correct Answer: D

QUESTION 2

Following the most recent patch deployment, a security engineer receives reports that the ERP application is no longer accessible The security engineer reviews the situation and determines a critical secunty patch that was applied to the ERP server is the cause. The patch is subsequently backed out.

Which of the following security controls would be BEST to implement to mitigate the threat caused by the missing patch?

A. Anti-malware

B. Patch testing

C. HIPS

D. Vulnerability scanner

Correct Answer: C

A Host Intrusion Prevention System (HIPS) is newer than a HIDS, with the main difference being that a HIPS can take action toward mitigating a detected threat Reference: https://www.sciencedirect.com/topics/comDuter-science/host-intrusion-Drevention-svstem

QUESTION 3

A software development team has spent the last 18 months developing a new web-based front-end that will allow clients to check the status of their orders as they proceed through manufacturing. The marketing team schedules a launch party to present the new application to the client base in two weeks. Before the launch, the security team discovers numerous flaws that may introduce dangerous vulnerabilities, allowing direct access to a database used by manufacturing. The development team did not plan to remediate these vulnerabilities during development.

Which of the following SDLC best practices should the development team have followed?

A. Implementing regression testing

B. Completing user acceptance testing

C. Verifying system design documentation

D. Using a SRTM

Correct Answer: D

QUESTION 4

An application has been through a peer review and regression testing and is prepared for release. A security engineer is asked to analyze an application binary to look for potential vulnerabilities prior to wide release. After thoroughly analyzing the application, the engineer informs the developer it should include additional input sanitation in the application to prevent overflows. Which of the following tools did the security engineer MOST likely use to determine this recommendation?

A. Fuzzer

B. HTTP interceptor

C. Vulnerability scanner

D. SCAP scanner

Correct Answer: A

QUESTION 5

A company is in the process of outsourcing its customer relationship management system to a cloud provider. It will host the entire organization\\'s customer database. The database will be accessed by both the company\\'s users and its customers. The procurement department has asked what security activities must be performed for the deal to proceed. Which of the following are the MOST appropriate security activities to be performed as part of due diligence? (Select TWO).

A. Physical penetration test of the datacenter to ensure there are appropriate controls.

B. Penetration testing of the solution to ensure that the customer data is well protected.

C. Security clauses are implemented into the contract such as the right to audit.

D. Review of the organizations security policies, procedures and relevant hosting certifications.

E. Code review of the solution to ensure that there are no back doors located in the software.

Correct Answer: CD

Due diligence refers to an investigation of a business or person prior to signing a contract. Due diligence verifies information supplied by vendors with regards to processes, financials, experience, and performance. Due diligence should verify the data supplied in the RFP and concentrate on the following: Company profile, strategy, mission, and reputation Financial status, including reviews of audited financial statements Customer references, preferably from companies that have outsourced similar processes Management qualifications, including criminal background checks

Process expertise, methodology, and effectiveness

Quality initiatives and certifications Technology, infrastructure stability, and applications Security and audit controls

Legal and regulatory compliance, including any outstanding complaints or litigation

Use of subcontractors Insurance Disaster recovery and business continuity policies C and D form part of Security and audit controls.