Latest Version: 47.0

Question: 1

Which of the following is the MOST relevant security check to be performed before embedding third-parry libraries in developed code?

A. Check to see if the third party has resources to create dedicated development and staging environments.
B. Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.
C. Assess existing vulnerabilities affecting the third-parry code and the remediation efficiency of the libraries' developers.
D. Read multiple penetration-testing reports for environments running software that reused the library.

Answer: C

Question: 2

The Chief Information Security Officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data. Which of the following would be BEST for the third-party vendor to provide to the CISO?

A. GDPR compliance attestation
B. Cloud Security Alliance materials
C. SOC 2 Type 2 report
D. NIST RMF workbooks

Answer: C

Question: 3

A recent audit cited a risk involving numerous low-criticality vulnerabilities created by a web application using a third-party library. The development staff state there are still customers using the application even though it is end of life and it would be a substantial burden to update the application for compatibility with more secure libraries. Which of the following would be the MOST prudent course of action?

A. Accept the risk if there is a clear road map for timely decommission
B. Deny the risk due to the end-of-life status of the application.
C. Use containerization to segment the application from other applications to eliminate the risk

D. Outsource the application to a third-party developer group

Answer: C

Question: 4

Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

A. EOL
B. SLA
C. MOU
D. EOSL

Answer: B

Question: 5

A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

A. DNS poisoning
B. MAC flooding
C. DDoS attack
D. ARP poisoning

Answer: C