Latest Version: 33.0

Question: 1

Which of the following would be the MOST effective countermeasure against malicious programming that rounds down transaction amounts and transfers them to the perpetrator's account?

A. Apply the latest patch programs to the production operating systems.
B. Implement controls for continuous monitoring of middleware transactions.
C. Set up an agent to run a virus-scanning program across platforms.
D. Ensure that proper controls exist for code review and release management.

Answer: B

Question: 2

A measure of the effectiveness of the incident response capabilities of an organization is the:

A. reduction of the annual loss expectancy (ALE).
B. time to closure of incidents.
C. number of employees receiving incident response training.
D. number of incidents detected.

Answer: B

Question: 3

The BEST indication of a change in risk that may negatively impact an organization is an increase

A. security incidents reported by staff to the information security team.
B. alerts triggered by the security information and event management (SIEM) solution.
C. events logged by the intrusion detection system (IDS).
D. malware infections detected by the organization's anti-virus software.

Answer: B

Question: 4

Which of the following is the MAIN objective of a risk management program?

A. Reduce costs associated with incident response.
B. Reduce risk to the maximum extent possible.
C. Reduce risk to the level of the organization’s risk appetite.
D. Reduce corporate liability for information security incidents.

Answer: C

Question: 5

Which of the following should an information security manager do FIRST after a new cybersecurity regulation has been introduced?

A. Update the information security policy.
B. Conduct a cost-benefit analysis.
C. Consult corporate legal counsel.
D. Perform a gap analysis.

Answer: D