CISM$^{\text{Q\&As}}$

Certified Information Security Manager

Pass Isaca CISM Exam with 100% Guarantee

QUESTION 1

Which of the following is the PRIMARY objective of incident triage?

A. Coordination of communications

B. Mitigation of vulnerabilities

C. Categorization of events

D. Containment of threats

Correct Answer: C

The primary objective of incident triage is to categorize events based on their severity, impact, urgency, and priority. Incident triage helps the security operations center (SOC) to allocate the appropriate resources, assign the relevant roles and responsibilities, and determine the best course of action for each event. Incident triage also helps to filter out false positives, reduce noise, and focus on the most critical events that pose a threat to the organization\\'s information security. Coordination of communications, mitigation of vulnerabilities, and containment of threats are important tasks that are performed during the incident response process, but they are not the primary objective of incident triage. Coordination of communications ensures that the relevant stakeholders are informed and updated about the incident status, roles, actions, and outcomes. Mitigation of vulnerabilities addresses the root causes of the incident and prevents or reduces the likelihood of recurrence. Containment of threats isolates and stops the spread of the incident and minimizes the damage to the organization\\'s assets and operations. These tasks are dependent on the outcome of the incident triage, which determines the scope, severity, and priority of the incident.

QUESTION 2

For event logs to be acceptable for incident investigation, which of the following is the MOST important consideration to establish chain of evidence?

A. Centralized logging

B. Time clock synchronization

C. Available forensic tools

D. Administrator log access

Correct Answer: B

QUESTION 3

Which of the following should be of MOST concern to an information security manager reviewing an organization\\'s data classification program?

A. The program allows exceptions to be granted.

B. Labeling is not consistent throughout the organization.

C. Data retention requirement are not defined.

D. The classifications do not follow industry best practices.

Correct Answer: B

QUESTION 4

When messages are encrypted and digitally signed to protect documents transferred between trading partners, the GREATEST concern is that:

A. trading partners can repudiate the transmission of messages.

B. hackers can eavesdrop on messages.

C. trading partners can repudiate the receipt of messages.

D. hackers can introduce forgery messages.

Correct Answer: D

QUESTION 5

An IS manager has decided to implement a security system to monitor access to the Internet and prevent access to numerous sites. Immediately upon installation, employees Hood the IT helpdesk with complaints of being unable to perform business functions on Internet sites. This is an example of:

A. conflicting security controls with organizational needs.

B. strong protection of information resources.

C. implementing appropriate controls to reduce risk.

D. proving information security\\'s protective abilities.

Correct Answer: A

The needs of the organization were not taken into account, so there is a conflict. This example is not strong protection; it is poorly configured. Implementing appropriate controls to reduce risk is not an appropriate control as it is being used. This does not prove the ability to protect, but proves the ability to interfere with business.