

# Isaca

*Cybersecurity-Fundamentals*  
*ISACA Cybersecurity Fundamentals*

**For More Information – Visit link below:**

<https://www.examsempire.com/>

**Product Version**

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

---

# Latest Version: 6.0

## Question: 1

What is a primary consideration when implementing role-based access control (RBAC) in an organization?

Response:

- A. The physical locations of users
- B. The job functions and responsibilities of users
- C. The operating system versions users are working with
- D. The personal preferences of the organization's leadership

**Answer: B**

## Question: 2

In incident response, what is the primary purpose of the containment phase?

Response:

- A. To eliminate the threat from the network
- B. To identify the source of the breach
- C. To prevent the spread of an incident
- D. To recover data lost during the incident

**Answer: C**

## Question: 3

'Zero Trust' architecture relies on which core principle?

Response:

- A. Trust no entity and verify every interaction
- B. Trust is based on the network location
- C. Zero security breaches are possible
- D. Trust can be established through biometrics alone

**Answer: A**

---

### Question: 4

Who is typically responsible for identifying and analyzing emerging threats in an organization's threat landscape?

Response:

- A. Human resources department
- B. External regulatory bodies
- C. Threat intelligence team
- D. All employees indiscriminately

**Answer: C**

### Question: 5

How do Advanced Persistent Threats (APTs) typically gain initial access to a network?

Response:

- A. Through physical access by a malicious insider
- B. By exploiting vulnerabilities in publicly accessible systems
- C. Through a large-scale, indiscriminate phishing campaign
- D. Using brute force attacks on network passwords

**Answer: B**

### Question: 6

During which phase of incident response are actions taken to prevent the spread of an incident?

Response:

- A. Preparation
- B. Detection and Analysis
- C. Containment, Eradication, and Recovery
- D. Post-Incident Activity

**Answer: C**

### Question: 7

---

Which principle of information security is primarily concerned with preventing unauthorized data disclosure?

Response:

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Non-repudiation

**Answer: C**

### Question: 8

Which of the following best defines the role of a SIEM system in a Security Operations Center (SOC)?

Response:

- A. To manage the organization's firewalls and intrusion prevention systems
- B. To provide real-time analysis of security alerts generated by network hardware and applications
- C. To conduct vulnerability assessments and penetration testing
- D. To offer a framework for regulatory compliance management

**Answer: B**

### Question: 9

Advanced Persistent Threats (APTs) are distinguished by which of the following characteristics?

(Choose Two)

Response:

- A. Their use of highly sophisticated hacking techniques and technologies
- B. Their focus on a specific target over an extended period
- C. Their reliance on large-scale automated exploits
- D. Their goal to disrupt rather than gather intelligence

**Answer: A,B**

### Question: 10

When should a security operations center (SOC) escalate incident response procedures?

Response:

- A. When the incident is resolved

- 
- B. When there is minimal impact on business operations
  - C. When an incident exceeds predefined thresholds
  - D. When external media become aware of the incident

**Answer: C**

**Thank You for Trying Our Product**

**Special 16 USD Discount Coupon: **NSZUBG3X****

**Email:** [support@examsempire.com](mailto:support@examsempire.com)

**Check our Customer Testimonials and ratings  
available on every product page.**

**Visit our website.**

**<https://examsempire.com/>**