Security Operations and Administration Practice Test Questions and Answers

1. What is the primary purpose of a Security Operations Center (SOC)?

A) Physical building security
B) Monitoring and responding to cybersecurity incidents
C) Employee background checks
D) Financial auditing

2. Which tool is commonly used for centralized log management and analysis?

A) SIEM (Security Information and Event Management)
B) CRM (Customer Relationship Management)
C) ERP (Enterprise Resource Planning)
D) HRM (Human Resource Management)

3. What does the acronym "IOC" stand for in cybersecurity?

A) Internet Operations Center
B) Incident Operations Command
C) Indicator of Compromise
D) Information Operations Control

4. Which phase comes first in the incident response process?

A) Containment
B) Identification
C) Recovery
D) Lessons learned

Answers: 1-B 2-A 3-C 4-B