2111N790

Candidate's Seat No :_____

IMBA (CSM) Sem.-9 Examination
CSM-MBA-501
Security Monitoring
November-2025

Time : 2-30 Hours] **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Explain the primary Security Goals (CIA Triad). Describe each component with suitable examples. 7Marks

ii. Define Security and Control. How do control mechanisms contribute to strengthening an organization's security framework? 7Marks

OR

i. Discuss the trade-off between Reliability and Security. Provide real-world examples where improving one may impact the other. 7Marks

ii. Explain the importance of Monitoring and Incident Response in a SOC environment. How do these functions improve organizational resilience? 7Marks

Question 2 Answer the following questions:

i. Describe the key components of a Log Management Infrastructure. How do they work together to collect, store, and analyze log data? 7Marks

ii. Explain the role of a Centralized Log Server in a log management system. What advantages does centralization offer over distributed logging? 7Marks

OR

i. Differentiate between Real-time Log Monitoring and Periodic Log Review. What are the benefits and limitations of each approach? 7Marks

ii. Explain the challenges of Log Management in large-scale enterprise environments. How can automation and SIEM tools help address these issues? 7Marks

Question 3 Answer the following questions:

i. Define SIEM (Security Information and Event Management). Explain its role in modern cybersecurity operations. 7Marks

ii. List and describe various Log Formats. Discuss their advantages and common use cases. 7Marks

OR

i. What is Log Baselining? Explain how establishing a baseline helps in identifying abnormal system behaviour. 7Marks

ii. Explain Event Collection in a SIEM environment. Include the types of data sources and collection methods used. 7Marks

Questions 4 Answer the following questions:

i. Discuss the importance of Communicating the Incident. Who should be notified, and what communication protocols should be followed? 7Marks

ii. Describe the process of Incident Classification and Investigation. What criteria are used to determine the severity and scope of an incident? 7Marks

OR

i. Explain the Containment and Response Strategy Formulation phase. How does this step help limit damage and plan remediation? 7Marks

ii. Explain the role of Data Collection, Forensic Analysis, and Evidence Protection during an investigation. Why is chain-of-custody important? 7Marks

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. What is the primary objective of a Security Operations Center?
2. What is usability in security context?
3. List a challenge in integrating security controls.
4. Give one reason for documentation in SOC.
5. Name a technique for baseline establishment.
6. What is the purpose of feedback loop in monitoring?
7. What is on-premise infrastructure
8. What does SOC infrastructure refer to?
9. What is a corrective measure in SOC?
10. What is system reliability?
11. Define proactive monitoring in security operations.
12. What is risk management?

.....X.....X.....