2/36

2111N789

Candidate's Seat No :_____

IMSc (CSF) Sem.-9 Examination

ICSF-501

Security Monitoring

November-2025

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

Question 1 Answer the following questions:

i. What is meant by "Finding the Sweet Spot" in security operations? Describe how organizations balance usability, performance, and security in practical scenarios. 7Marks

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

OR

i. Identify and explain some Typical Security Flaws found in system design and implementation. Suggest possible mitigation strategies. 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. Discuss the steps involved in Log Management Planning. What factors should an organization consider when designing a log management policy? 7Marks

OR

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

ii. Describe the Log Management Operational Process. Include stages such as log collection, transmission, analysis, and retention. 7Marks

Question 3 Answer the following questions:

i. Describe the key components of SIEM Architecture. Explain how data flows from log sources to dashboards and alerts. 7Marks

ii. Explain the process of Understanding Logs. What critical information can security analysts extract from log data? 7Marks

OR

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

P.T.O

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. List and discuss the key Requirements of an effective Incident Response Plan. Include both technical and organizational aspects. 7Marks

ii. Explain the process of Incident Recording and Initial Response. Why are accurate documentation and quick action vital during this stage? 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. Mention one role of automation in SOC monitoring.
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. What is on-premise infrastructure?
12. What is risk management?

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