6/36

2611N874

Candidate's Seat No :_____

IMSc (CSF) Sem.-9 Examination

ICSF-504 (EA)

SOC

November-2025

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

Question 1 Answer the following questions:

i. Describe the key roles within a SOC, focusing on duties of SOC analysts, incident responders, and SOC managers. 7Marks

ii. Illustrate typical SOC architecture, outlining its main components and layout. 7Marks

OR

i. Discuss various types of cyber threats and their attack vectors, providing examples. 7Marks

ii. Describe the typical workflow for incident escalation in a SOC. 7Marks

Question 2 Answer the following questions:

i. Discuss the importance of log management and various types of logs used for security monitoring. 7Marks

ii. Analyze the integration process of threat intelligence with SIEM, providing examples of use cases. 7Marks

OR

i. Explain challenges faced in managing large-scale log data in modern SOCs. 7Marks

ii. Describe the process of log correlation and its significance in threat detection. 7Marks

Question 3 Answer the following questions:

i. Compare and contrast indicator-based (IOC) and behavioural-based (IOA) detection techniques in SOC. 7Marks

ii. Explain threat actor profiling and discuss its significance in threat mitigation. 7Marks

OR

i. Describe the process of mapping security alerts to MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs). 7Marks

ii. Evaluate common challenges in implementing SOAR and automation in large SOCs. 7Marks

Questions 4 Answer the following questions:

i. Explain key performance indicators (KPIs) and metrics for measuring SOC effectiveness. 7Marks

ii. Analyze the purpose and implementation of ISO27001 in SOCs. 7Marks

OR

P.T.O

i. Outline legal considerations that SOCs must be aware of during incident response. 7Marks

ii. Assess the role of reporting and documentation in achieving and maintaining SOC compliance. 7Marks

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

1. List any two common cyber-attack vectors.
2. Name two responsibilities of a SOC manager.
3. List any two roles within a SOC.
4. Give an example of a log source in a SOC environment.
5. What is the purpose of integrating threat intelligence into SOC operations?
6. Define "correlation" in the context of SIEM.
7. What is SOAR in SOC operations?
8. List two advantages of incident response automation.
9. Name a common data source used during threat hunting.
10. Why are SOC metrics important?
11. Define a key legal consideration for SOCs.
12. What is meant by 'audit trail' in SOC monitoring?

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

2611N874 -3 Candidate's Seat No :_____

IMSc (CSF) Sem.-9 Examination

ICSF-504 (EB)

Digital Forensics

November-2025

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

Question 1 Answer the following questions:

i. Describe the history and evolution of digital forensics from the 1980s to the present. 7Marks

ii. What is the Chain of Custody? Write the steps involved and their importance in court. 7Marks

OR

i. Explain the process of evidence collection and preservation in digital forensics. 7Marks

ii. Write a short note on any two forensic tools, such as FTK, Autopsy, or myFRT. 7Marks

Question 2 Answer the following questions:

i. Define file system forensics and explain its objectives and importance in digital investigations. 7Marks

ii. Explain file carving. Discuss its three main techniques: header–footer carving, fragment recovery, and content-based carving. 7Marks

OR

i. Write short notes on four tools used for file carving in digital forensics. 7Marks

ii. Differentiate between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) with examples. 7Marks

Question 3 Answer the following questions:

i. Describe the process of data acquisition in cloud forensics for IaaS, PaaS, and SaaS models with suitable examples. 7Marks

ii. Define IoT Forensics. Explain its ecosystem and challenges related to device diversity, data storage, and proprietary protocols. 7Marks

OR

i. What is an Advanced Persistent Threat (APT)? Describe its key characteristics and objectives in cyberattacks. 7Marks

ii. Classify APT threats based on origin, attack vector, objectives, and target sector with relevant examples. 7Marks

P.T.O

N874-4

Questions 4 Answer the following questions:

i. Write short notes on three famous digital forensic cases and the lessons learned from each. 7Marks

ii. Network Intrusion Case: A university detects abnormal traffic and suspects a data breach. Discuss how you would investigate this incident using network forensic tools and prepare findings for legal submission. 7Marks

OR

i. Email Investigation: A company suspects that an employee has leaked confidential data through email. As a digital forensic investigator, describe the steps you would take to collect, analyse, and report the evidence. 7Marks

ii. Explain the importance of documentation and the chain of custody in a digital forensic investigation. Why are these steps essential for court admissibility? 7Marks

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

1. Why is a write blocker used in digital forensics?
2. What is the main difference between live acquisition and dead acquisition?
3. What is meant by volatile data? Give one example.
4. What is the purpose of hashing in evidence handling?
5. Define file carving in digital forensics.
6. What is the Volatility framework used for?
7. What is the main purpose of network forensics?
8. What is memory forensics?
9. Name any two challenges faced in cloud forensics.
10. What is the main purpose of a forensic report?
11. Name any two types of digital evidence commonly analysed in case studies.
12. What is the importance of documentation in forensic investigations?

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

2611N874-5

Candidate's Seat No :_____

IMSc (CSF) Sem.-9 Examination
ICSF-504 (EC)
Cloud Security
November-2025

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

Question 1 Answer the following questions:

i. Explain the different types of cloud services (IaaS, PaaS, SaaS) with suitable examples. 7Marks

ii. Compare and contrast the security features offered by AWS, Azure, and Google Cloud. 7Marks

OR

i. Illustrate how cloud service providers implement shared responsibility models in security. 7Marks

ii. Describe the importance and usage of API security in cloud services. 7Marks

Question 2 Answer the following questions:

i. Discuss the authentication and authorization methods used in the cloud, providing examples. 7Marks

ii. Illustrate best practices for IAM policy design in cloud platforms. 7Marks

OR

i. Describe the challenges of integrating on-premises IAM with cloud IAM. 7Marks

ii. Illustrate how zero trust models are implemented using cloud IAM. 7Marks

Question 3 Answer the following questions:

i. Discuss common misconfiguration risks in cloud environments and strategies to mitigate them. 7Marks

ii. Analyze the concept of policy-as-code and its benefits for automated cloud governance. 7Marks

OR

i. Describe how encryption-in-transit and encryption-at-rest are implemented in the cloud,with examples. 7Marks

ii. Discuss the role of CSPM in supporting regulatory compliance. 7Marks

Questions 4 Answer the following questions:

i. Discuss the role of audit logging (with reference to AWS CloudTrail) in cloud compliance. 7Marks

P.T.O

N 824-6

ii. Describe the key elements of a Service Level Agreement (SLA) for cloud security and risk management. 7Marks

OR

i. Analyze SLA management in ensuring compliance for sensitive cloud workloads. 7Marks

ii. Discuss the effect of shared responsibility models on compliance efforts in cloud computing. 7Marks

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

1. Name any one component of NIST SP 800-53.
2. What is the difference between audit log and event log in the cloud?
3. What is meant by "cloud risk management"?
4. Explain "least-privilege" as applied to key management.
5. Give one use of a Hardware Security Module (HSM).
6. Name a policy-as-code tool.
7. What is OAuth?
8. List any one best practice for IAM management.
9. Name a key difference between authentication and authorization.
10. Name any one Google Cloud security tool.
11. What is the main benefit of PaaS?
12. What is multi-tenancy?

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