9/21

2611N875

Candidate's Seat No :_____

IMBA (CSM) Sem.-9 Examination

CSM-MBA-504 (EA)

SOC

November-2025

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

Question 1 Answer the following questions:

i. Explain the definition, purpose, and overall importance of a Security Operations Centre in modern organizations. 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. Compare the responsibilities of all SOC Tier analysts, giving relevant examples. 7Marks

Question 2 Answer the following questions:

i. Elaborate on the basics of threat intelligence and how it supports proactive detection in the SOC. 7Marks

ii. Compare different types of log sources and their relevance in detecting security incidents. 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. Describe the structure and application of the MITRE ATT&CK framework in a SOC environment. 7Marks

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

OR

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

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

Questions 4 Answer the following questions:

i. Discuss the differences among SOC1, SOC2, and SOC3, and their importance for organizations. 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

14 Marks

Questions 5: Attempt any Seven out of Twelve.

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.....

2611N875 –3 Candidate's Seat No :_____

IMBA (CSM) Sem.-9 Examination

CSM-MBA-504 (EB)

Digital Forensics

Time : 2-30 Hours] **November-2025** **[Max. Marks : 70**

Question 1: Answer the following questions:

i. Explain the term Digital Forensics. Discuss its importance in modern criminal and cyber investigations. 7Marks

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

OR

i. Differentiate between volatile and non-volatile data with examples of each. 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. Describe the main file system structures FAT, NTFS, EXT4, and HFS+ highlighting one key forensic feature of each. 7Marks

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

OR

i. What is the Volatility framework? Discuss its features, uses, and importance in analysing memory dumps. 7Marks

ii. Describe the steps in malware reverse engineering using static and dynamic analysis techniques. 7Marks

Question 3: Answer the following questions:

i. Describe the different acquisition methods in mobile forensics, such as logical, file system, physical, chip-off, and JTAG, including their advantages and limitations. 7Marks

ii. Explain the phases of the APT attack lifecycle and the corresponding forensic focus at each stage. 7Marks

OR

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

ii. Explain the steps involved in mobile device forensics seizure, preservation, extraction, analysis, and reporting. 7Marks

P.T.O

N875-4

Question 4: Answer the following questions:

i. Cyberbullying Case: A student reports receiving threatening messages on social media. Explain how you would perform a forensic analysis of the social media account and device to trace the sender. 7Marks

ii. Describe the main parts of a forensic report. How does a well-structured report help investigators and legal authorities understand the case? 7Marks

OR

i. Computer Crime Scene: During a corporate fraud investigation, you seize a laptop suspected of containing financial records. Describe the procedures you would follow from seizure to report preparation, ensuring the chain of custody is maintained. 7Marks

ii. What is the role of an expert witness in court? Describe how a forensic examiner presents digital evidence during testimony. 7Marks

Question 5: Attempt any seven out of twelve. 14 Marks

1. What is the full form of FTK?
2. What is the difference between analysis and reporting in forensics?
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.....