

FACULTY OF COMPUTER SCIENCE
Master of Computer Application (Sem-III)
 In Effect from Academic Year 2025-26

Branch Name:	MCA
Program Code:	CS201
Course Name:	Security Monitoring
Course Code:	4CS2010306T
Pre-requisite Course:	Basics of Computer Networks, Operating Systems, and Fundamental Knowledge of Cybersecurity concepts with basic understanding of system logs and networking.

Course Objective:

1. The course aims to introduce the concepts of Security Operations Center (SOC) and security monitoring.
2. The course provides understanding of cybersecurity fundamentals, threats, and security principles.
3. This course covers security tools and technologies such as SIEM, IDS/IPS, and log management for threat detection.
4. This course enables learners to analyze security events and apply threat intelligence for effective monitoring.
5. The course equips learners with knowledge of SOC operations, incident response procedures, and real-world security practices.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture	Tutorial	Practical	Credit	Theory		Practical		Total
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
3	-	-	3	60	40	-	-	100

Subject Contents			
Sr. No	Topic	Total Hours	Weight (%)
1	1. INTRODUCTION OF SECURITY OPERATION CENTER • Definition of SOC, • What is SOC & Need of SOC, • Key Functions of a SOC, • How is a SOC Structured, • SOC Hub & Spoke Architecture, • Key SOC Roles and Responsibilities, • Which Tools Are used in a SOC, • SOC as a service (SOCaaS), • SIEM Solutions in a SOC • Security Analysts, • SOC Automation & Orchestration, • Compliance & Regulatory Considerations.	8	25
2	2. CYBERSECURITY FUNDAMENTALS • Overview of Cybersecurity Concepts & Importance, • Evolution of Cyber Threats & the current threat landscape,	8	25

	• Role of Cybersecurity in protecting Digital Assets & Sensitive Information, • Common Cyber Threats & Attack Vectors, • Security Principles & Attack Vectors, • Understanding Compliance Requirements & Regulatory Standards, • Mapping Cybersecurity Frameworks to Organizational Needs.		
3	3. SECURITY TOOLS & TECHNOLOGIES • Overview of the role of Security Tools in Cybersecurity • Importance of selecting appropriate Tools based on Organizational needs & Threat Landscape • Understanding SIEM Architecture & Components • Log Management & Correlation for Threat Detection • Use Cases & Benefits of SIEM in SOC Operations • Overview of IDS/IPS Technologies & Deployment Options • Signature-based vs Anomaly-based Detection Techniques • Configuring & Tuning IDS/IPS to detect & prevent Network Intrusions • Endpoint Detection & Response (EDR) Tools.	8	25
4	4. SECURITY MONITORING & THREAT INTELLIGENCE • Overview of Security Monitoring Concepts & Objectives • Importance of Continuous Monitoring for Detecting & Responding to Security Threats • Understanding the Importance of Logs in Security Monitoring • Log Collection, Normalization & Aggregation Techniques • Analyzing Log Data for Detecting Security Incidents & Anomalies • SIEM Systems and their Role in Security Monitoring • SIEM Architecture, Components & Deployment Considerations.	7	25
5	5. SOC OPERATIONS & PROCEDURES • Incident Triage • Incident Investigation • Incident Classification • Incident Response • Communication and Collaboration • Documentation and Reporting • Escalation Procedures • Continuous Monitoring & Threat Hunting • Incident Post-Mortem and Lessons Learned • Training and Skill Development.	8	25

Text Books:

1. **Security Operations Center: Building, Operating, and Maintaining Your SOC** – Joseph Muniz, Gary McIntyre, Nadhem AlFardan
2. **The Modern Security Operations Center** – Joseph Muniz (Advanced SOC concepts, automation, real-world operations)
3. **11 Strategies of a World-Class Cybersecurity Operations Center** – Carson Zimmerman, Kathryn Knerler, Ingrid Parker (Best practices and strategies for SOC improvement)
4. **Effective Threat Investigation for SOC Analysts** – Mostafa Yahia (Focus on threat analysis, logs, investigation techniques)

References Books:

1. “Security Operations Center: Building, Operating, and Maintaining your SOC” by Joseph Muniz (Author), Gary McIntyre (Author), Nadhem AlFardan (Author).
2. “11 Strategies of a World-Class Cybersecurity Operations Center” by Kathryn Knerler (Author), Ingrid Parker (Author), Carson Zimmerman (Author).
3. “Effective Threat Investigation for SOC Analysts: The ultimate guide to examining various threats and attacker techniques using security logs” by Mostafa Yahia (Author).
4. “Modern Security Operations Center, The 1st Edition” by Joseph Muniz (Author).

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom’s Taxonomy Level
CLO1	Understand the concepts, structure, and functions of a Security Operations Center (SOC).	2.Understand
CLO2	Explain fundamental cybersecurity concepts, threats, and security principles.	2.Understand
CLO3	Apply knowledge of security tools and technologies such as SIEM, IDS/IPS, and EDR.	3. Apply
CLO4	Analyze logs and security events for effective security monitoring and threat detection.	4. Analyze
CLO5	Apply threat intelligence techniques to identify and respond to cybersecurity incidents.	3. Apply
CLO6	Evaluate SOC operations and incident response procedures including escalation and reporting.	5.Evaluate

Mapping of CLOs with Pos & PSOs

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CLO1	H	L											H	M
CLO2	H	M											H	M
CLO3		H	M	M	H								H	H
CLO4		H		H	H								H	H
CLO5		M	H	H	H					M			H	H
CLO6			M	H	M					H			M	H

H: High, M: Medium, L: Low