

Branch Name:	MCA
Program Code:	CS201
Course Name:	Security Monitoring Practical
Course Code:	4CS2010306P
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	
-	-	4	2	-	-	25	25	50

LAB/ Practical:

Note: The practical list provided beneath is for reference only. The course teacher may Change/formulate it as per his/her methodology and requirement.

Sr. No	Practical Experiments
1	Prepare a Case Study on the Event Logs, Activity Logs & Information Logs in a proper Document.
2	Installation & Configuration of Splunk Universal Forwarder in Windows Virtual Machine with all the necessary & required Fields.
3	To Perform the Log management & Analysis bi Identifying the sources types & to perform Log Correlation & Anomaly Detection.
4	To Identify various Log Events using their Event Code from Windows Security.
5	To Perform Alert Generation using Splunk.
6	To View Results in Statistics Tab using Splunk.
7	To Perform Basic Searches & Find the Search Results in Splunk.

8	To create Dashboard & Panel in Splunk
9	To enable the field Lookups in Splunk.
10	Perform Threat Hunting using Splunk.

Text Books:

- Security Operations Center: Building, Operating, and Maintaining Your SOC**
– Joseph Muniz, Gary McIntyre, Nadhem AlFardan
- The Modern Security Operations Center** – Joseph Muniz (Advanced SOC concepts, automation, real-world operations)
- 11 Strategies of a World-Class Cybersecurity Operations Center** – Carson Zimmerman, Kathryn Knerler, Ingrid Parker (Best practices and strategies for SOC improvement)
- Effective Threat Investigation for SOC Analysts** – Mostafa Yahia (Focus on threat analysis, logs, investigation techniques)
- Open-Source Security Operations Center (SOC)** – Alfred Basta, Nadine Basta, Waqar Anwar (Modern SOC using open-source tools & practical implementation)

References Books:

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