

Branch Name:	Bachelor of Technology (Computer Engineering / Information Technology)
Program Code:	ET103/ET105
Course Title:	Elective -V Theory: Cybersecurity Operating & Monitoring
Course Code:	2ET1030707T
Pre-requisite Course:	Basic knowledge of Computer Networks, Operating Systems

Course Objectives: To understand the principles of digital forensics, cybercrime investigation, evidence handling, and incident response & develop skills in forensic analysis, malware investigation, reporting, use of modern forensic tools and technologies.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weightage (%)
1	Introduction Of Security Operation Center: Definition of SOC, Purpose and Importance of Security Operations Centers, Core Functions of Security Operations Centers, SOC Organizational Structure and Design, SOC Deployment Models: Hub-and-Spoke Architecture, SOC Roles, Responsibilities, and Team Structure, SOC Technologies and Security Tools, SOC as a service (SOCaaS), SIEM Solutions in a SOC, Roles and Responsibilities of Security Analysts, SOC Automation and Security Orchestration, Compliance, Governance, and Regulatory Requirements in SOC Operations.	9	20%
2	Cybersecurity Fundamentals: Foundations of Cybersecurity, Evolution of Cyber Threats and Threat Landscape, Protection of Digital Assets and Sensitive Information, Cyber Threats and Attack Vectors, Fundamental Security Principles, Compliance Requirements and Regulatory Standards, Cybersecurity Frameworks and Organizational Alignment.	8	18%
3	Security Tools and Technologies: Overview of the role of Security Tools in Cybersecurity, Importance of selecting appropriate Tools based on Organizational needs & Threat Landscape, Understanding SIEM Architecture and Components, Log Management and Event Correlation, Use Cases & Benefits of SIEM in SOC Operations, Overview of IDS/IPS Technologies & Deployment Options, Signature-based vs Anomaly-based Detection Techniques, IDS/IPS Configuration and Optimization, Endpoint Detection & Response (EDR) Solutions.	12	26%
4	Security Monitoring and 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.	8	18%
5	SOC Operations and Procedures: Incident Triage Methodology, Incident Investigation, Incident Classification and Prioritization, Incident	8	18%

	Response, Communication and Collaboration, Documentation and Reporting, Escalation Management Procedures, Continuous Monitoring and Threat Hunting, Post Incident Review and Lessons Learned, SOC Workforce Development and Training		
--	--	--	--

Reference 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).
5. “Blue Team Handbook: Incident Response Edition” by Don Murdoch

List of Open-Source Software/learning website:

1. NIST SP 800-101, 800-86 <https://csrc.nist.gov/publications/sp800>
2. ISO/IEC 27037, 27041 <https://www.iso.org/standard/44381.html>
3. <https://cyberdefenders.org/>
4. <https://nptel.ac.in/courses/128106006>

Course Outcomes (CO):

Course Outcomes	Description	Bloom's Taxonomy Level
CO1	Understand the Basic Concept of Security Operation Center.	Understanding (2)
CO2	Acknowledge & Gain Knowledge of Cybersecurity Fundamentals.	Apply (3)
CO3	Develop & Gain Knowledge of Security Tools & Technologies.	Apply (3)
CO4	Analyse the Security Monitoring and Threat Intelligence.	Analyze (4)
CO5	Apply the Concept of SOC with Operations & Procedures.	Apply (3)

Mapping of CO with PO and PSO

Course Outcomes	Program Outcomes (POs)												Program Specific Outcomes (PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3	PSO 4
CO1	H	M	-	-	L	M	-	H	-	-	-	M	M	L	L	H
CO2	M	H	-	H	H	-	-	M	-	M	-		H	M	L	M
CO3	M	H	-	H	H	-	-	-	-	-	-	L	H	M	M	L
CO4	M	H	M	H	H	-	-	-	-	-	-	L	H	H	H	L
CO5	M	H	H	H	H	L	-	-	M	M	M	M	H	H	H	M

H: High, M: Medium, L: Low