

Branch Name:	Bachelor of Technology (Computer Engineering / Information Technology)
Program Code:	ET103/ET105
Course Title:	Elective -V Practical: Cybersecurity Operating and Monitoring Practical
Course Code:	2ET1030707P
Pre-requisite Course:	Basic knowledge of Computer Networks, Operating Systems

Course Objectives: To provide students with practical knowledge of Security Operations Center (SOC) processes, security monitoring, and log management using SIEM technologies. The course aims to develop skills in collecting, analyzing, correlating, and visualizing security events using Splunk, as well as performing threat hunting and incident detection activities to support cybersecurity operations.

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.	
1	-	-	2	2	-	-	-	-	10	25	10	25	50

List of Experiments:

S.N.	Practical Exercise
1	Prepare a Case Study on the Event Logs, Activity Logs & Information Logs in a proper Document.
2	Install and configure Splunk Universal Forwarder on a Windows virtual machine for centralized log collection and monitoring.
3	Perform log management, source type identification, event correlation, and anomaly detection using Splunk.
4	Investigate Windows Security Event Logs and interpret event codes to identify security-related activities and incidents.
5	Configure and generate security alerts in Splunk based on predefined detection rules and suspicious activities.
6	Utilize Splunk statistical analysis features to summarize, visualize, and interpret security-related data.
7	Perform basic and intermediate SPL (Search Processing Language) queries to retrieve and analyze security events.
8	Design and develop interactive dashboards and visualization panels for security monitoring and reporting.
9	Implement field lookups in Splunk to enrich log data and improve security event analysis.
10	Conduct threat hunting activities using Splunk to identify indicators of compromise and potential security threats.

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 Cybersecurity Framework (NIST CSF)
2. MITRE ATT&CK Framework
3. OWASP Top 10
4. CIS Critical Security Controls
5. SANS Incident Response Guidelines

Course Outcomes (CO):

Course Outcomes	Description	Bloom's Taxonomy Level
CO1	Explain the role of logs, SIEM platforms, and Security Operations Centers in cybersecurity monitoring.	Understand (2)
CO2	Configure Splunk components and manage log collection from different sources.	Apply (3)
CO3	Perform log analysis, event correlation, and security event investigation using Splunk.	Analyze (4) Apply (3)
CO4	Develop alerts, dashboards, reports, and data enrichment mechanisms for effective security monitoring.	Apply (3) Create (6)
CO5	Conduct threat hunting and evaluate security events to identify indicators of compromise and potential threats.	Evaluate (5) Analyze (4)

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