

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Incident Response and Threat Intelligence Practical
Course Code:	2ET2070105P
Pre-requisite Course:	Basic fundamental knowledge of cyber security

Course Objectives: After successful completion of the course, students will be able to

1. To learn how to define an incident relating to cyber security.
2. To learn protocols for first-on-crime scene investigations.
3. Obtain basic knowledge on dealing with system security-related incidents.
4. To learn basic fundamentals of cyber threat intelligence.
5. To demonstrate how cyber has changed the nature of intelligence collection.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (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

Course Contents:

Unit	Details	Contact Hours
1	- Incident Indicators and Incident Detection Analyzing Incidents - Vulnerability Detection Methods and Tools, System Model and Consequence analysis, Threat Intelligence, and Threat activation of Vulnerabilities	6
2	- Data Analytics support for Incident Response, - Backup and Recovery, Recovery from Incident Methods - Planning of a Cyber Security operation in an IT organization vs an OT/ICS - Planning and Risk Analysis	6

3	- Cloud Security, Cloud, and API security - Cyber Security Operations (CyOps), and integration of cyber security operations to software development and operation process (DevSecOps), and integration of relevant operations (MLops, AIops, DevOps)	6
4	- Continuing Challenges - A skills gap - Too many alerts, too little time - Time to response is rising - A piecemeal approach - The Reactivity Problem Minimizing Reactivity in Incident Response - Identification of probable threats Prioritization	7
5	- Strengthening Incident Response With Threat Intelligence - Threat Intelligence in Action - Use Case: Prepare processes in advance - Use Case: Scope and contain incidents - Use Case: Remediate data exposure and stolen assets - Abuse Case: Half measures are worse than nothing	7

Reference Books:

1. Murdoch Don, 2016, —Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, CreateSpace Independent Publishing Platform, 2.2 Edition , ISBN: 978-1500734756
2. Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Darkweb cyber threat intelligence mining. Cambridge University Press.

Course Outcomes:

At the end of the course, students will be able to:

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Obtain basic knowledge of dealing with system security.	Understanding (2)
COL2	Increase knowledge of potential defenses and countermeasures against common threat vectors/vulnerabilities.	Understanding (2)
COL3	Gain experience using tools and common processes in performing analysis of compromised systems and dynamic malware analysis.	Applying (3)
COL4	Examine the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collections.	Applying (3)
COL5	Threat Study1 the technique to Develop Cyber Threat Intelligence Requirements.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning 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	PS O1	PS O2	PS O3	PS O4
CL1	H	M	M		M											
CL2	H	M			M							L				
CL3	H	M	M		M											
CL4	M	M	M		M							L				

H: High, M: Medium, L: Low