Subject: Cyber Threat Intelligence and Incident Response								
Program: M.Sc. in CyberSecurity			**Subject Code:**			**Semester: II**		
Teaching Scheme				**Examination Evaluation Scheme**				
Lecture	**Tutorial**	**Practical**	**Credits**	**University Theory Examination**	**University Practical Examination**	**Continuous Internal Evaluation (CIE)- Theory**	**Continuous Internal Evaluation (CIE)- Practical**	**Total**
4	**0**	**2**	**5**	**40**	**40**	**60**	**60**	**200**

COURSE OBJECTIVES:

Content

Course Content

W - Weightage (%) , **T** - Teaching hours

Sr.	Topics	W	T
1	**Introduction to Cyber Threat Intelligence (CTI)** Introduction to CTI and its importance in cybersecurity Frameworks for CTI and their applications Intelligence cycle and its phases Threat actors and their motives Threat intelligence sources and collection methods	**25**	**10**
2	**Cyber Threat Hunting** Introduction to cyber threat hunting Cyber threat hunting methodologies Threat hunting tools and techniques Adversary emulation and simulation Threat hunting in cloud environments	**25**	**10**
3	**Intelligence Analysis for CTI** Intelligence analysis process Techniques for data analysis and visualization Indicators of compromise (IOCs) and their analysis Analyzing threat intelligence reports and feeds CTI sharing and collaboration	**25**	**11**
4	**Threat Intelligence Operations** CTI operational planning and management CTI tools and platforms	**25**	**15**

	Threat intelligence automation and orchestration Threat hunting operations Incident response and remediation **Emerging Trends in CTI and Cyber Threat Hunting** Current and emerging cyber threats Emerging CTI technologies and techniques CTI and threat hunting for IoT and SCADA systems Ethics and legal considerations in CTI and threat hunting		

TEXTBOOKS and REFERENCE BOOKS:

1. Cyber Threat Intelligence: A Comprehensive Guide to Identify, Analyze, and Mitigate Threats to Your Digital Enterprise by Alexandre Dulaunoy, Clément Onymus, and Bertrand Waltisperger
2. Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks by Roger A. Grimes
3. The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence by Recorded Future
4. Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure by Eric D. Knapp and Raj Samani
5. Cybersecurity Operations Handbook by J.W. Rittiaghouse and William M. Hancock

List of Practicals:

1. To understand the concepts and importance of cyber threat intelligence and hunting.
2. To gain knowledge about frameworks, tools, and techniques for CTI and threat-hunting operations.
3. To develop skills in intelligence analysis, IOCs, and CTI sharing and collaboration.
4. To learn about CTI and threat hunting operations and incident response planning.
5. To gain awareness of emerging trends and ethical considerations in CTI and threat hunting.
6. Conducting a phishing simulation and analyzing the results to identify potential threats
7. Conducting a network reconnaissance operation and identifying potential attack vectors
8. Conducting a social engineering attack and analyzing the results to identify vulnerabilities
9. Developing custom IOCs based on specific threat scenarios and testing their effectiveness
10. Conducting a red team exercise to simulate a real-world attack and identifying weaknesses in defensive strategies