Centre for Machine Learning and Intelligence

Generic Elective

Cyber Intelligence

(Applicable for the UG Students admitted from 2023 – 2024 onwards)

Semester:1,3,4,6 **Hours of Instruction/Week:**

5+1Subject Code : 23BAIGE2 **No. ofCredits: 6**

Objectives:

1. To understand the concept of cyber intelligence and its significance in military and security operations.
2. To explore different types of cyber intelligence, and its role in real word problem
3. To familiarize with various cyber threat intelligence and fraud prevention.

Unit 1: Introduction to Cyber Intelligence **- 15Hrs**

Need for cyber Intelligence – Application of Cyber Intelligence in military – Types of Intelligence – HUMINT Intelligence – IMIST Intelligence – (Open Source Intelligence)* – Electronic Intelligence – Technical Intelligence – Medical Intelligence. Intelligence Development - Introduction to Intelligent cycle – Intelligent cycle steps.

Unit 2: Cyber Threat Intelligence **-15 Hrs**

Introduction to cyber Threat Intelligence – Two types of Cyber Threat Intelligence – Operational Threat Intelligence – Strategic Threat Intelligence – Role of Threat Data Feeds. Threat Intelligence for Security Operations – Responsibilities of the SOC Team - Overwhelming Volume of Alerts - (Context is Kings)*.

Unit 3: Intelligence for Security Leaders, Risk Analysis and Fraud Prevention-15Hrs

Risk Management – Mitigation: People - Processes and Tools – Investments – Communication - Supporting Security Leaders - the security skills gaps - Intelligent to Manage Better. Risk Analysis – The FAIR Risk Model – Threat Intelligence and Threat Probabilities – Threat Intelligence and the Cost Attacks. Fraud Prevention – Stand and Deliver! – Know your Enemy – Criminal Communities and Dark Web – Connecting the Dots for Fraud Prevention – (use case: Payment fraud)*.

Unit 4: Cyber Threat Intelligence Framework -15Hrs

Intelligence frameworks –Why cyber threat frameworks? - Cyber threat framework architecture and operating model - Lockheed Martin's Cyber Kill Chain framework - Integrating the Cyber Kill Chain model into an intelligence project - Benefits of the Cyber Kill Chain framework - MITRE's ATT&CK knowledge-based framework - ATT&CK model mapping - Integrating the MITRE ATT&CK framework - Benefits of the ATT&CK framework – (Diamond model of intrusion analysis framework)*

Unit 5: Cyber Intelligence Active Defense **-15Hrs**

An introduction to active defense – Understanding cyber kill chain – General Principles of active defense – Enticement and entrapment in active defense Scenario A and Scenario B– (Types of active defense – Manual and Automatic)*- An application of tactical level Active Defense.

*** Indicates Self - Study Component**

Total Hours: 75

Reference Books:

1. Wilson Bautista Jr.(2018) "***Practical Cyber Intelligence***", **Packt Publishing**
2. Zane Pokorney. (2019) "***The Threat Intelligence Handbook Second Edition Moving Toward a Security Intelligence Program***", CyberEdge Group, LLC
3. Christopher Ahlberg. (2020) "***The Security Intelligence Handbook Third Edition How to Disrupt Adversaries and Reduce Risk With Security Intelligence***" CyberEdge Group, LLC

E-Learning Resources:

1. **https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/**

Course Outcomes:

CO1: Understand the cyber intelligence and its different types in military and security scenarios.

CO2: Familiarize with cyber threat intelligence to enhance security operations and effectively manage threats.

CO3: Analyze risks, implement mitigation strategies, and prevent fraud using intelligence-driven approaches.

CO4: Evaluate and apply cyber threat intelligence frameworks to enhance intelligence project and defense strategies.

CO5: Demonstrate an understanding of active defense principles, and understand in using the manual and automatic active defense.