COURSE TITLE	**THREAT INTELLIGENCE AND MALWARE ANALYSIS**
COURSE CODE	**01CY0113**
COURSE CREDITS	**4**

Objective:

1 To gain comprehensive knowledge and practical skills in Cyber Threat Intelligence (CTI) by understanding the cyber threat landscape, identifying threat actors and their TTPs, mastering threat detection and analysis techniques, and utilizing cyber security tools for effective threat detection and incident response

Course Outcomes: After completion of this course, student will be able to:

1 Demonstrate a comprehensive understanding of cyber threat intelligence concepts, including types of threat intelligence and their applications

2 Acquire skills in analyzing malware and other indicators of compromise (IOCs).

3 Apply threat intelligence to enhance proactive threat detection and response capabilities within an organization.

4 Critical Thinking and Problem-Solving to analyze and interpret complex cyber security incidents and threats and apply critical thinking skills to prioritize and respond to incidents based on their severity and potential impact

5 Recognize the importance of continuous learning and adaptation in response to evolving cyber threats.

Pre-requisite of course: Fundamental Knowledge of Cyber security, OS basic knowledge, Critical Thinking and Analytical Skills

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Cyber Threat Intelligence (CTI)** Introduction to CTI and its importance in cyber security, Frameworks for CTI and their applications, Intelligence cycle and its phases, Threat actors and their motives, Threat intelligence sources and collection methods	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.	9

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
3	**Intelligence Analysis for CTI** Intelligence analysis process, Techniques for data analysis and visualization, Indicators of compromise (IOCs) and their analysis, nalyzing threat intelligence reports and feeds, CTI sharing and collaboration	8
4	**Introduction to Malware** Introduction to Malware, Types of Malware, Introduction to x86 architecture, The difference between source code and compiled code, Introduction to disassemblers and decompilers, Obfuscation techniques, Analysis of File format.	9
5	**Malware Analysis& Tools** Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging, Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation,, Kernel vsUser mode debugging, Basic static, dynamic& hybrid analysis,, Portable executable file format, PE header and sections, Introduction to DLLs and Handles	10
Total Hours		**46**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Use OSINT Framework in order to understand Threat Intelligence Tools Required: Shodan, Spiderfoot, OSINT Framework	2
2	**Practical 2** Use OSINT Framework to identify IOC in the organization Tools Required: Phishing (zphisher), DDOS (Hping3)	2
3	**Practical 3** Explain the benefits of the COSO framework in Large-scale Technical Organizations in order to understand Risk Avoidance & Transfer Techniques/ Tools Required:COSO Framework	2
4	**Practical 4** Explain how ISO 270001 framework is useful in any Technical Organization in order to understand Risk Analysis & Identification Techniques/ Tools Required:ISO 270001 framework	2
5	**Practical 5** Create a Keylogger in python language in order to understand the concept of spyware malware concept and also analyse it’s behaviour to understand the dynamic analysis concept, Techniques/ Tools Required:Python Language, Kali Linux	2
6	**Practical 6** Use malicious pcap file for wireshark analysis in order to understand static malware analysis concept, Techniques/ Tools Required:Wireshark, Pcap file	2

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
7	**Practical 7** Use steghide tool to understand the concept of steganography and also hide malicious file using steghide to understand the data hiding concept Techniques/ Tools Required:Steghide, kali linux	2
8	**Practical 8** Create a malware in any language, run it and analyse to see it's impact in the machine (4 prank malware, 4 dangerous malware) Techniques/ Tools Required:kali linux, github	2
9	**Practical 9** Use volatility framework to analyse memory dump of any sample file in order to understand the concept of hybrid malware analysis Techniques/ Tools Required:kali linux, Volatility2	2
10	**Practical 10** Use metasploit framework to exploit the target machine using reverse_tcp concept to understand the IOC and IOA concept for malware threat analysis, Techniques/ Tools Required:kali linux, metasploitable2, mitre framework	2
Total Hours		**20**

Textbook :

1 "The Threat Intelligence Handbook" A Practical Guide for Security Teams to Unlocking the Power of Intelligence by Recorded Future, Mika Karjalainen, Tero Kokkonen, Tuomo Sipola, Springer International Publishing, 2022

References:

1 Cybersecurity Operations Handbook, Cybersecurity Operations Handbook, J.W. Rittiaghouse and William M. Hancock, Elsevier Science, 2003

2 Introduction to Network Security, Introduction to Network Security, Neal Krawetz, CENGAGE Learning, 2009

3 Practical Malware Analysis, Practical Malware Analysis, Michael Sikorski, Andrew Honig, No Starch Press, 2012

4 Evasive Malware, Evasive Malware, Kyle Cucci, No Starch Press, 2024

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	0.00	30.00	30.00	30.00	10.00

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Instructional Method:

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by blackboard, may also use any of tools such as demonstration ,role play Quiz, brain storming, MOOC set c.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTELvideos, e-courses, Virtual Laboratory

Supplementary Resources:

1. "Cyber Threat Intelligence: From Adversary Tracking to Zero-Day Vulnerability Management" by Tyler W. Bort, Steven W. Bort
2. "Cyber Threat Intelligence: A Comprehensive Guide to CTI, Tools, Tactics, and Techniques" by Bob Stasio, Jacob G. Oakley, Matthew J. Flick
3. “The IDA Pro Book, 2nd Edition: The Unofficial Guide to the World’s Most Popular Disassembler” by Chris Eagle

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)