COURSE TITLE	**MITRE FRAMEWORK**
COURSE CODE	**01CY0217**
COURSE CREDITS	**4**

Objective:

1 To equip students with practical and analytical skills in advanced threat detection, using MITRE ATT&CK, D3FEND, and real-world telemetry. The course focuses on threat hunting, CTI-driven defense, and simulation of persistent threats in enterprise networks.

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

1 Design and execute threat hunting operations based on MITRE ATT&CK techniques.

2 Simulate adversary behavior using open-source red teaming frameworks.

3 Correlate security telemetry with MITRE-based detection logic.

4 Develop and evaluate defensive coverage using MITRE D3FEND and Detection Maturity Models.

5 Produce threat reports and dashboards for SOC/Purple Team visibility.

Pre-requisite of course: Completion of MITRE Framework or equivalent knowledge of ATT&CK, SIEM, and threat modeling

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	**Threat Hunting with ATT&CK** Introduction to Threat Hunting Methodologie, Hypothesis-driven Hunting, Hunting Maturity Model (HMM),, ATT&CK use in Hunt Scenarios.	7
2	**Advanced Simulation and Emulation Tools** Adversary Simulation Frameworks:, Caldera, Atomic Red Team, Infection Monkey, Emulating APT Campaigns (e.g., Emotet, Cobalt Strike, Log4Shell)	7
3	**Security Telemetry and Data Analytics** Parsing Logs: Sysmon, EDR, Firewall, DNS, Proxy, Sigma Rules and mapping to ATT&CK, Behavioral vs Signature Detection	7
4	**MITRE-Based Defensive Engineering** Coverage and Detection Engineering with ATT&CK Navigator, Detection Engineering with ATT&CK Navigator, Risk, Threat type, detection rules D3FEND Mapping and Implementation,, Detection Maturity and Gaps	8

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
5	**SOC & Purple Team Analytics and Reporting** Purple Teaming Exercise Planning, CTI-led Dashboards (e.g., Kibana, PowerBI), ATT&CK Evaluations and Defense Benchmarking	7
6	**Practical 6** Map threat actor techniques using CTI reports and ATT&CK	2
Total Hours		**38**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Simulate attack chain using Caldera on a virtual lab	2
2	**Practical 2** Perform behavioral hunting for persistence using Sysmon logs	2
3	**Practical 3** Design and test Sigma rules for detecting MITRE technique T1059	2
4	**Practical 4** Map coverage of MITRE techniques in your simulated SOC setup	2
5	**Practical 5** Use ATT&CK Navigator to identify visibility gaps	2
6	**Practical 7** Build a detection dashboard using Kibana or Splunk	2
7	**Practical 8** red/blue team simulation using Atomic Red Team	2
8	**Practical 9** MITRE-based detection coverage in heatmap format	2
9	**Practical 10** Present purple team case study with gaps and recommendations	2
Total Hours		**18**

Textbook :

1 “MASTER MITRE ATT&CK: Mapping Strategies for Offensive and Defensive Techniques for Security Teams, Diego Rodrigues & StudioD21 Smart Tech Content, Independently Published, 2025

References:

1 Automating the MITRE ATT&CK Framework: Improve Your Organisation’s Security Posture, Automating the MITRE ATT&CK Framework: Improve Your Organisation’s Security Posture, -, Amazon Digital Services LLC, 2024

2 The Threat Hunter Playbook, The Threat Hunter Playbook, Roberto Rodriguez, Packt Publishing, 2021

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

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

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

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 black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
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, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1. ATT&CK Workbench
2. Splunk ESCU & MITRE Apps
3. ELK Stack & OpenSearch dashboards
4. Detection-as-Code (DAST/Sigma/Osquery)
5. Threat Intelligence feeds (MISP, ATT&CK CTI, OTX)

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

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