COURSE TITLE	**CYBER SECURITY ANALYTICS**
COURSE CODE	**01CY0219**
COURSE CREDITS	**4**

Objective:

1 The objective of this course is to equip learners with advanced knowledge and practical skills in Cyber Security Analytics by integrating threat intelligence, machine learning, big data processing, and adversarial defense techniques. This intermediate to advanced-level curriculum focuses on real-world application of analytics in detecting, interpreting, and responding to sophisticated cyber threats. Through hands-on labs, red vs. blue team simulations, and the development of scalable detection systems, students will gain the capability to design, evaluate, and deploy intelligent security analytics solutions in enterprise environments, while aligning with frameworks like MITRE ATT&CK and leveraging modern AI/ML tools for proactive defense.

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

1 Analyze advanced cyber threats using behavioural, temporal, and adversarial patterns.
2 Evaluate machine learning models for detecting complex cyber intrusions.
3 Design scalable data pipelines for real-time threat detection and analytics.
4 Perform forensic investigations through red-blue team data and log correlation.
5 Create& Integrate analytics-driven detection into SIEM and SOAR for automated response.

Pre-requisite of course: Basic knowledge of networking, cybersecurity fundamentals, Python programming, and familiarity with system logs and SIEM tools.

Teaching and Examination Scheme

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

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
1	**Advanced Threat Modeling and Attack Surface Analytics** Cyber Threat Landscape and Adversary Profiling, Nation-state vs. cybercrime groups, APT campaigns and case studies (e.g., APT28, Lazarus), Threat Intelligence standards (STIX, TAXII, MISP), Attribution and intent analysis,Threat actor mapping using MITRE ATT&CK, Kill Chain & ATT&CK-Driven Threat Modeling Lockheed Martin Cyber Kill Chain vs. MITRE ATT&CK, TTP tracking from logs,Simulating kill chain phases with log datasets, Attack path mapping in enterprise networks,Detection rule crafting per ATT&CK technique, Attack Surface Enumeration at Scale Asset discovery automation (Nmap, Amass, Shodan),Web/app/API enumeration techniques, Shadow IT and unmanaged devices risk analytics,Cloud attack surface visibility (AWS, Azure),Continuous monitoring strategies, Risk Scoring and Threat Prioritization CVSS-based risk scoring vs. ML-based risk scoring,Asset criticality weighting models, Exposure scoring based on external threat feeds,Business impact-driven threat modelling,Prioritization frameworks (DREAD, PASTA)	8
2	**Anomaly & Behavioral Analytics at Scale User and Entity Behaviour Analytics (UEBA)** Behavioral baselining and deviation analysis,Privileged user monitoring techniques, Identity compromise indicators,Peer group comparison techniques,Case study: UEBA for lateral movement detection, Time-Series Anomaly Detection Seasonality, trend, and drift in security data,ARIMA, Holt-Winters, Prophet for log data,LSTM-based sequence modelling, Real-time alerting based on anomalies,Root cause traceability with temporal mapping, Graph-Based Threat Detection Graph construction from network/session data, Detecting island hopping and pivoting behaviour,Community detection in graph anomalies, Temporal graph evolution in attack patterns,Visual threat hunting using graph analytics, Insider Threat and Fraud Detection Behavioral fingerprinting for insider abuse, Session hijacking and account misuse analytics, Anomaly detection in file access patterns,Credential sharing detection,Advanced SOC alert correlation for insider threats	8
3	**Machine Learning & Adversarial AI in Cyber Defense** Machine Learning Pipelines for Threat Classification, Unsupervised & Semi-supervised Techniques, Adversarial Machine Learning (AML),AI-Driven Detection Systems	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
4	**Big Data Pipelines and Security Log Analytics ,Big Data Security Architectures** Apache Kafka for real-time ingestion, Spark Streaming vs. Flink for stream analytics, Time-windowed stream processing,Storage: HDFS, ElasticSearch, Druid, Architecting scalable log analytics systems, Scalable Threat Detection Techniques High-throughput anomaly scoring, CEP (Complex Event Processing) in Spark/Flink, Window-based correlation for pattern detection,Threat detection in multi-tenant environments,Managing backpressure in streaming pipelines, SIEM and SOAR Integration, ELK/Splunk integration with Kafka/Spark,Custom detection rules and dashboards, Auto-remediation using SOA playbooks,Automated alert prioritization models, ase study: Threat detection on ELK with Python, Threat Hunting with Query and Analytics, Log query optimization (Lucene/Splunk SPL),IOC pivoting across log sources, Threat chaining and incident reconstruction, YARA + Sigma-based hunting queries,, Case: Detecting APT lateral movement from logs	8
5	**Red-Blue Team Analytics, Incident Forensics & Capstone** Red vs. Blue Team Analytics, Red team TTP simulation using Atomic Red Team, Log collection and analysis of simulated attacks, Mapping attack telemetry to detection rules,MITRE ATT&CK coverage evaluation,Purple team exercise: attack vs. detection mapping, Incident Timeline Reconstruction, Log stitching and timeline visualization, Process tree and session correlation,Windows/Linux log forensic analysis, Artifact extraction and context mapping,Automated timeline generation tools (e.g., Timesketch), Security Decision Automation Scoring models for alerts (confidence, severity, urgency), Rule-based vs. ML-based automation,Risk-based ticket triaging systems, Integrating ML decisions into SOAR workflows,Case: Building a detection-decision-action loop	8
Total Hours		**40**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Practical Name: Network Threat Pattern Analysis using Wireshark Objective: To capture and analyze suspicious network traffic using filters to identify anomalies such as port scans or DNS tunneling.	2
2	**Practical 2** Practical Name: Detecting Brute Force Attacks using Splunk Objective: To create detection rules in Splunk that identify brute force login attempts from log files based on failed authentication patterns.	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
3	**Practical 3** Practical Name: Visualizing Lateral Movement with MITRE ATT&CK Navigator Objective: To map an attacker's lateral movement using MITRE ATT&CK tactics and techniques and visualize it with the ATT&CK Navigator tool.	2
4	**Practical 4** Practical Name: Anomaly Detection with Isolation Forest in Python Objective: To build and run an anomaly detection model using Isolation Forest to identify outlier events in synthetic security log data.	2
5	**Practical 5** Practical Name: Building a Custom Log Parser with Python Objective: To extract and normalize key fields (e.g., IPs, usernames, timestamps) from raw syslog or Windows Event Log files using Python.	2
6	**Practical 6** Practical Name: Threat Hunting with Sigma Rules Objective: To write basic Sigma detection rules for suspicious PowerShell activity and test them against sample logs using Sigma CLI tools.	2
7	**Practical 7** Practical Name: Real-Time Log Monitoring using ELK Stack Objective: To set up an ELK stack, ingest system logs, and create a dashboard to visualize security events like failed logins or unusual file access.	2
8	**Practical 8** Practical Name: Phishing Domain Detection using Passive DNS Data Objective: To analyze passive DNS data to identify potential phishing domains based on TTL values, domain age, and registrar patterns.	2
9	**Practical 9** Practical Name: Create a Risk Scorecard for Network Devices Objective: To assess assets based on open ports, known vulnerabilities (CVEs), and business value to assign dynamic risk scores.	2
10	**Practical 10** Practical Name: Log Correlation to Detect Data Exfiltration Objective: To correlate outbound traffic logs with file access logs to detect suspicious data exfiltration events to unauthorized destinations.	2
Total Hours		**20**

Textbook :

1 Intrusion Detection and Big Heterogeneous Data: A Survey. Journal of Big Data, Zuech, R., Khoshgoftaar, T. M., & Wald, R, -, 2015

References:

1 Guide to Intrusion Detection and Prevention Systems (IDPS), Guide to Intrusion Detection and Prevention Systems (IDPS), Scarfone, K., & Mell, P., NIST Special Publication, 2007

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 Privacy and Security in Online Social Media : https://nptel.ac.in/courses/106106146

2 Cybersecurity Analytics and Operations Specialization – Penn State

3 https://www.coursera.org/specializations/cybersecurity-analytics-operations

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

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