Course Type	Course Code	Name of Course	L	T	P	Credit
DE	OCSD605	Practical Cyber Security for Cyber Security Practitioners	3	0	0	3

Course Objective

As we interact with various industry and their needs for cyber security, they often complain that the courses at academic institutions provide students with the fundamentals of cyber security, but the students are often not familiar with the practical issues associated with running a cyber security operation in a real organization. Also, while a lot of the theses at master's level or dissertation at the PhD level are based on theoretical exploration of techniques, algorithms, or mathematical modeling of cyber security problems, there is a dearth of dissertation and thesis on the practical aspects of running cyber security operations.

Learning Outcomes

Understand various and very interesting problems to be solved for practical cyber security which also requires a great deal of fundamental thinking, reasoning, and concerns about human cognition of the inputs the operators and leaders receive from cyber security tools, dashboards, policy formulations but then in the crowd of details, fundamentals are lost, reasoning is replaced by ad hoc decisions. To change that, we need workforce, as well as academics who can abstract out the fundamentals from such practical problems are develop various practically oriented methods, methodologies, policy frameworks, and decision processes which would simplify cyber operations. This course is meant to be a first step towards that line of thinking, modeling, and methodology development

Unit No.	Topics To be covered	No of Lecture Video	Video Time (Minutes)	Learning Outcome
1	Introduction: Cyber Security Posture, Maturity, and Continuous Improvement Strategies What is CKC, steps involved in CKC, identify the targets, prepare the operation.	2	90	Evaluate enterprise cybersecurity posture and maturity models to establish continuous improvement strategies for proactive threat defense. Examine the Cyber Kill Chain (CKC) framework and its multi-stage execution lifecycle to model cyber threat progression from initial intrusion to objective completion. Analyze early-stage attacker operations—specifically target identification, reconnaissance, and campaign preparation—to implement effective pre-exploitation disruption controls.
2	Knowing your attacker: MITRE ATT&CK Framework Launch and Operation, Gain Access to victim, establish beach head at the victim, remotely control the implants, Mission`s goal. Course on action matrix and examples	3	139	Utilize the MITRE ATT&CK framework and Course of Action matrix to map adversary tactics, techniques, and procedures (TTPs) for threat-informed defensive planning. Analyze attack execution lifecycles—from initial operation launching and victim compromise to establishing persistent beachheads within target networks. Evaluate command-and-control (C2) mechanisms for remotely managing implants and assess post-exploitation tactics used by attackers to fulfill mission goals.
3	Knowing your attacker: MITRE ATT&CK Framework Attackers Techniques, Tactics and procedures. What is ATT & CK? Spear phishing, APT Groups, Mitigation and use case of ATT & CK. Gap Analysis, CTI, C2C	3	144	Examine the architecture and practical use cases of the MITRE ATT&CK framework to systematically categorize adversary Tactics, Techniques, and Procedures (TTPs) and perform defense gap analyses. Analyze advanced attack vectors—such as targeted spear phishing and Command-and-Control (C2) communication infrastructure—utilized by Advanced Persistent Threat (APT) groups. Integrate Cyber Threat Intelligence (CTI) with ATT&CK-mapped mitigation strategies to enhance threat visibility, incident response, and proactive network defense.
4	Cyber Kill Chains: Lockheed Martin Cyber Kill Chain and Unified Kill Chain Store and display mapped ATT & CK behavior, APT 28 & 29 Techniques, comparing layers in ATT & CK navigator, making defensive recommendation. Applying Technique intelligence to defense. determine and research techniques.	3	139	Compare the 7-stage linear Lockheed Martin Cyber Kill Chain with the expanded 18-stage, multi-phase Unified Kill Chain (Initial Foothold, Network Propagation, Action on Objectives) to model modern cyber intrusion lifecycles. Map and analyze threat actor TTPs using MITRE ATT&CK Navigator layers, contrasting specific campaigns like APT28 (Fancy Bear) and APT29 (Cozy Bear/Nobelium) to identify overlapping techniques. Translate technique-level threat intelligence into actionable defensive recommendations, prioritizing mitigations and detection analytics to proactively disrupt adversarial behaviors.
5	Defending Yourself: MITRE DEF3ND Framework Introduction to unified kill chain, why another kill chain, basic assumption in LM	3	134	Evaluate the MITRE D3FEND framework to systematically map defensive counter-measures, architecture components, and technical security controls against adversarial techniques.

	CKC, what is unified kill chain is good for? Design of unified kill chain, intermediate goals, initial foot hold, network propagation, action on objectives,			Analyze the structural assumptions and limitations of the Lockheed Martin Cyber Kill Chain to justify the necessity and advantages of a more comprehensive model. Examine the design and tactical phases of the Unified Kill Chain—Infiltration (Initial Foothold), Network Propagation, and Action on Objectives—to model intermediate adversary goals across end-to-end intrusion lifecycles.
6	Securing your Configurations: STIG Benchmarking Introduction to MITRE DEF3ND Framework, Origin of DEF3ND framework, its tactics and techniques, digital objects and artifacts, Deep dive into MITRE DEF3ND framework-I, credential hardening, message hardening, Platform hardening, File analysis, NTA, process analysis	3	144	Examine the origin, tactics, techniques, and artifact model of the MITRE D3FEND framework to establish a standardized baseline for defensive counter-measure mapping. Implement technical hardening matrices across core operational domains—including STIG benchmarking, credential management, platform configurations, and message security. Apply deep defense techniques—such as file analysis, process behavior tracking, and Network Traffic Analysis (NTA)—to detect, isolate, and evict threat activity.
7	Sharing Threat Intelligence: STIX and TAXII 2.0 MITRE DEF3ND Framework Conclusion & Introduction to Risk Identification and Assessment. Deep dive into Risk Assessment-I Deep dive into Risk Assessment-II	3	192	Utilize STIX and TAXII 2.0 standards to structure, automate, and securely exchange actionable Cyber Threat Intelligence (CTI) across enterprise security ecosystems. Synthesize technical defensive controls from the MITRE D3FEND framework to transition from operational engineering into strategic risk identification and threat exposure mapping. Execute qualitative and quantitative risk assessment methodologies to evaluate asset criticality, threat likelihood, business impact metrics, and mitigation strategies.
8	Cyber Security Risk Management Introduction to cyber crisis management. Cyber Crisis Conclusion and Introduction to Cyber Resilience, Deep dive into Cyber Resilience -I	3	150	Formulate comprehensive Cyber Security Risk Management frameworks to identify, assess, prioritize, and mitigate technical and operational enterprise threats. Develop and execute Cyber Crisis Management strategies to ensure rapid incident response, stakeholder communication, and organizational continuity during major security breaches. Design and implement robust Cyber Resilience controls to ensure systems continuously adapt to, withstand, and rapidly recover from emerging cyber disruptions and systemic failures.
9	Cyber Resilience Assessment Deep dive into Cyber Resilience -II Cyber Resilience review	2	105	Execute comprehensive Cyber Resilience Assessments using industry frameworks to evaluate an organization's capability to anticipate, withstand, recover from, and adapt to adverse cyber events. Formulate advanced recovery, operational continuity, and adaptive response strategies to minimize downtime and business impact during persistent cyber disruptions. Conduct structured cyber resilience reviews to identify capability gaps, measure maturity metrics, and continuously improve defensive postures.
10	Cyber Security Policy Formulation Cyber Threat Intelligence Sharing-STIX Tutorial-Part 1 Cyber Threat Intelligence Sharing-STIX Tutorial-Part 2	2	129	Formulate robust cybersecurity policies and regulatory compliance frameworks to govern organizational risk, data protection, and incident response procedures. Master the STIX 2.1 data model to represent threat intelligence using STIX Domain Objects (SDOs), Cyber Observables (SCOs), and Relationship Objects (SROs). Apply practical threat intelligence techniques to construct, parse, and automate machine-readable STIX JSON payloads for threat hunting and SOC integration.
11	Cyber Security Policy Formulation Introduction to SCAP, CVE and CCE Deep Dive into CVE, CCE, CPE, CVSS Scoring, XCCDF, OVAL Languages	2	93	Integrate Security Content Automation Protocol (SCAP) standards into cybersecurity policy formulation using CVE, CCE, and CPE for standardized asset, configuration, and vulnerability identification. Evaluate software and configuration vulnerabilities using the Common Vulnerability Scoring System (CVSS) framework to quantify risk severity and prioritize security patching. Automate security benchmarking and vulnerability auditing across enterprise endpoints using Extensible Configuration Checklist Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL).

12	Cyber Crisis Management Plan and Cyber Incident Management Plan	2	83	Formulate a Cyber Crisis Management Plan (CCMP) to coordinate executive decision-making, business continuity, strategic communications, and regulatory compliance during severe cyber disruptions. Develop an operational Cyber Incident Management Plan (CIMP) outlining technical protocols for detection, containment, eradication, and recovery across the incident lifecycle. Align CCMP and CIMP frameworks to ensure seamless escalation from technical containment at the Incident Command level to strategic crisis response at the executive level.
Total No of video lectures & Video time		**31**	**1542**	

Text books

No Textbook available on the course topic as yet. All material will be made available via the NPTEL course website

Reference books:

No Reference book available on the course topic as yet. All material will be made available via the NPTEL course website

Link of NPTEL Course:

https://nptel.ac.in/courses/106104467