MERSENNE CYBERCOUNSELLORS LLP

Course Syllabus: Incident Response and Threat Hunting

Course Overview:
This course provides an in-depth understanding of cyber threats, incident response (IR), and proactive threat-hunting techniques. Participants will learn how to identify, analyze, and mitigate cyber threats using industry-standard methodologies and tools. The course follows best practices from NIST, MITRE ATT&CK, and SANS frameworks.

Course Details:

- **Duration:** 6 Weeks
- **Fee:** ₹12,000
- **Mode:** Online/Offline (as applicable)
- **Prerequisites:** Basic understanding of networking and cybersecurity concepts
- **Certification:** Upon successful completion, participants will receive a certification from Mersenne Cybercounsellors LLP

Week 1: Introduction to Cyber Threats and Incident Response

- Understanding the Cyber Threat Landscape
- Cyber Attack Vectors and the Cyber Kill Chain
- Incident Response (IR) Basics and Frameworks (NIST, SANS, MITRE ATT&CK)
- Role of Security Operations Centers (SOC) in Incident Response

Week 2: Incident Handling & Digital Forensics

- Phases of Incident Response: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned
- Identifying Indicators of Compromise (IoCs) and Attack Patterns
- Basics of Digital Forensics and Evidence Handling
- Analyzing Real-World Cybersecurity Incidents

Week 3: Threat Intelligence & Hunting Methodologies

- Introduction to Cyber Threat Intelligence (CTI)
- OSINT (Open-Source Intelligence) Techniques
- Proactive vs. Reactive Threat Hunting Approaches
- MITRE ATT&CK for Threat Hunting

Week 4: Hands-on Threat Hunting Techniques

- Host-Based and Network-Based Threat Hunting
- Analyzing System and Network Logs (SIEM, EDR, XDR)
- Malware Analysis and Reverse Engineering Fundamentals
- Utilizing Threat Hunting Tools (YARA, Sigma, Velociraptor, Suricata)

Week 5: Incident Containment, Mitigation, and Recovery

- Containment Strategies for Different Types of Threats
- Malware Eradication & Ransomware Recovery
- Insider Threat Management and Data Exfiltration Prevention
- Developing an Incident Response Playbook

Week 6: Adversary Simulation & Final Capstone Project

- Red Team vs. Blue Team Operations
- Adversary Simulation and Purple Teaming
- SOC Operations and Crisis Management
- **Final Project:** Simulated Cyberattack and Response Exercise

---

Assessment & Certification:

- Weekly quizzes and hands-on assignments
- Final capstone project evaluation
- Certification of Completion from Mersenne Cybercounsellors LLP

Target Audience:

- Cybersecurity professionals and analysts
- SOC teams and IT security personnel
- Network and system administrators
- Students and professionals aspiring to enter the cybersecurity field

Learning Outcomes:

- Develop a strong foundation in incident response methodologies
- Gain hands-on experience in threat hunting and analysis
- Understand real-world cyber threats and adversarial tactics
- Learn to use industry-standard security tools effectively
- Build an incident response strategy and playbook

MERSENNE CYBERCOUNSELLORS LLP

For inquiries and enrollment,

contact us at : **7499076330**

email at : info.cybercounsellors@gmail.com