**Course – 6 Cyber Threat Intelligence**

1. Introduction to Cyber Threat Intelligence:

- Fundamentals: Understanding the basics of cyber threats, including malware, vulnerabilities, and attack vectors.

- Role in Cybersecurity: Recognizing the significance of threat intelligence in identifying and mitigating cyber threats.

2. Types of Threat Intelligence:

- Indicators of Compromise (IoCs): Identifying signs of potential security incidents.

- Tactics, Techniques, and Procedures (TTPs): Analyzing patterns and methodologies used by threat actors.

3. Collection and Analysis:

- Data Sources: Identifying and collecting data from various sources, including logs, network traffic, and external threat feeds.

- Analysis Techniques: Employing tools and methodologies to analyze collected data for actionable intelligence.

4. Cyber Threat Actors:

- Profiling Threat Actors: Understanding motivations, capabilities, and objectives of different threat actors.

- Attribution Challenges: Recognizing the complexities and limitations of attributing cyber attacks to specific actors.

5. Incident Response and Threat Hunting:

- Integration: Integrating threat intelligence into incident response processes.

- Proactive Threat Hunting: Proactively searching for signs of threats within an environment.

6. Frameworks and Standards:

- Cyber Kill Chain: Understanding the stages of a cyber attack and how intelligence can be applied at each stage.

- STIX/TAXII: Exploring standardized formats for threat intelligence sharing.

7. Information Sharing:

- ISACs and ISAOs: Understanding Information Sharing and Analysis Centers and Information Sharing and Analysis Organizations.

- Sharing Platforms: Exploring platforms for sharing threat intelligence with the broader cybersecurity community.

8. Tools and Technologies:

- Threat Intelligence Platforms (TIPs): Utilizing tools for aggregating, correlating, and analyzing threat data.

- Automation and Orchestration: Streamlining processes through automation for efficient threat intelligence management.

9. Legal and Ethical Considerations:

- Privacy and Compliance: Addressing legal and regulatory aspects of handling threat intelligence data.

- Ethical Responsibilities: Emphasizing ethical considerations in gathering and sharing threat intelligence.