Threat Intelligence

Duration: 16 hours

Module 1: Introduction to Threat Intelligence

- Fundamentals of Threat Intelligence
- Threat Intelligence Lifecycle
- Types and Classification of Threat Intelligence

Module 2: Cyber Threats and Attack Frameworks

- Overview of Cyber Threats and Actors
- Advanced Persistent Threats (APTs)
- Cyber Kill Chain Methodology
- MITRE ATT&CK Framework
- Diamond Model of Intrusion Analysis

Module 3: Requirements, Planning, Direction, and Review

- Understanding Threat Intelligence Requirements
- Planning and Direction Processes
- Review and Feedback Mechanisms

Module 4: Data Collection and Processing

- Threat Intelligence Data Sources and Feeds
- Open-Source Intelligence (OSINT) Techniques
- Cyber Counterintelligence (CCI) Basics
- Indicators of Compromise (IoCs) and Malware Analysis

Day 2 (8 Hours)

Module 5: Intelligence Reporting and Dissemination

- Threat Intelligence Reporting Standards
- Methods for Sharing Intelligence Reports
- Threat Intelligence Platforms (TIPs)

Module 6: Threat Hunting and Detection

- Introduction to Threat Hunting Concepts
- Threat Hunting Methodologies and Process

- Automation in Threat Hunting
- Tools and Techniques for Threat Detection

Module 7: Threat Intelligence in SOC Operations, Incident Response, and Risk Management

- Role of Threat Intelligence in SOC Operations
- Integration into Incident Response Plans
- Risk Mitigation Strategies