Course Title:

Threat Hunting and Compromise Assessment

Course Duration:

5 Days (40 Hours)

Day-Wise Content Breakdown

Day 1: Introduction to Threat Hunting and Compromise Assessment

1. Overview of Threat Hunting and Compromise Assessment
    - Objectives and Scope
    - Key Concepts and Definitions
2. Understanding the Cyber Threat Landscape
    - Threat Actor Profiles
    - Tactics, Techniques, and Procedures (TTPs)
3. Threat Hunting Frameworks and Approaches
    - Introduction to MITRE ATT&CK Framework
    - Cyber Kill Chain in Threat Hunting
4. Overview of Tools and Technologies
    - SIEM and EDR Overview
    - Role of Threat Intelligence in Threat Hunting

Day 2: Methods and Techniques of Threat Hunting

1. Types of Threat Hunting Approaches
    - Hypothesis-Based Threat Hunting
    - IoC and IoA-Driven Hunting
    - Behavioral Analytics Approach
2. Techniques for Data Collection and Analysis
    - Log Analysis and Anomaly Detection
    - Threat Intelligence Correlation
3. Indicators and Signals for Threat Detection
    - Identifying IoCs and IoAs

    - Tracking Lateral Movement and Data Exfiltration
4. Organizational Requirements for Threat Hunting Programs
    - Structure and Team Roles

Day 3: Implementation Guidelines for Threat Hunting

1. Developing a Threat Hunting Strategy
    - Setting Objectives and KPIs
    - Defining Scope and Coverage
2. Steps for Effective Threat Hunting
    - Pre-Hunt Preparation
    - Execution Phase
    - Post-Hunt Analysis
3. Integration with Incident Response (IR) Processes
    - Role of IR in Threat Hunting
    - Escalation and Communication Protocols
4. Challenges and Solutions in Threat Hunting
    - Common Pitfalls and How to Overcome Them

Day 4: Compromise Assessment Techniques

1. Introduction to Compromise Assessment
    - Objectives and Key Differences from Threat Hunting
    - When and Why to Perform Compromise Assessments
2. Steps in Compromise Assessment
    - Scoping and Baseline Establishment
    - Analysis of Artifacts and Logs
3. Key Techniques for Detection
    - Identifying Persistent Threats and Hidden Backdoors
    - Detecting Credential Abuse and Privilege Escalation
4. Implementation Frameworks
    - Guidelines for Conducting Organization-Wide Assessments

---

Day 5: Operationalizing Threat Hunting and Compromise Assessment

1. Reporting and Documentation Best Practices
    - Structure of Threat Hunting and Compromise Reports
    - Presentation Techniques for Stakeholders
2. Building a Threat Hunting Culture
    - Training and Awareness within the Organization
    - Continuous Improvement in Threat Hunting Processes
3. Future Trends and Developments in Threat Hunting
    - AI/ML in Threat Detection
    - Threat Hunting in Cloud and Hybrid Environments
4. Closing Remarks and Course Recap
    - Summary of Key Learning Points
    - Q&A