APT and Malware Hunting

Duration: 5 Days (8 Hours per Day)

1: Foundations of APT and Malware Analysis

1. **Understanding Advanced Persistent Threats (APTs)**
    - Characteristics and objectives of APTs
    - The APT attack lifecycle
2. **Introduction to Malware**
    - Types of malware and their behaviors
    - Techniques used for persistence and evasion
3. **Recognizing Indicators of Compromise (IoCs)**
    - Identifying key signs of APT and malware activity

2: Principles of Threat Hunting

1. **Introduction to Threat Hunting**
    - Purpose and benefits of proactive threat hunting
    - Differences between threat hunting and traditional detection
2. **APT Hunting Strategies**
    - Network-focused approaches
    - Behavioral analysis techniques
3. **Approaches to Malware Detection**
    - Analyzing suspicious processes and files
    - Examining log data for anomalies

3: Advanced Malware Analysis Techniques

1. **Static Malware Analysis**
    - Examining file properties and structure
    - Recognizing malicious patterns
2. **Dynamic Malware Analysis**
    - Observing malware behavior during execution

- Monitoring system and network changes

3. **Introduction to Reverse Engineering**
    - Decoding malware functionality
    - Identifying command-and-control (C2) channels

4: APT Detection and Mitigation Strategies

1. **Identifying APT Activities**
    - Spotting lateral movement and privilege escalation
    - Uncovering stealth tactics used by attackers
2. **Responding to APT Incidents**
    - Steps for containment and eradication
    - Post-incident recovery and analysis
3. **Proactive Defense Against APTs**
    - Building resilience through network and system hardening
    - Implementing proactive threat detection strategies

5: Integration and Strategic Defense

1. **Developing a Threat Hunting Framework**
    - Establishing processes for continuous improvement
    - Incorporating threat intelligence
2. **Collaboration Between Teams**
    - Aligning red and blue team activities
    - Enhancing detection with combined efforts
3. **Practical Applications of APT and Malware Hunting**
    - Implementing best practices to secure the environment
    - Building long-term defensive strategies
4. **Q&A and Closing Discussions**
    - Summarizing key takeaways
    - Addressing queries and feedback