Cyber Threat Hunting

Instructor-led training

This course covers the fundamentals of threat hunting, how to build out a hunt program in your own environment, and how to identify, define, and execute a hunt mission.

Cyber Threat Hunting is two-day in-class training on threat hunting. This course covers the fundamentals of threat hunting; how to build out a hunt program in your own environment; and how to identify, define, and execute a hunt mission. The course introduces essential concepts for network and endpoint hunting and then allows learners to apply techniques to hunt for anomalous patterns. Hands-on activities follow real-world use cases to identify attacker techniques. Learners will leave the course with concrete use cases that they can leverage to hunt in their own environment.

Throughout the course, instructors provide guidance on hunting across typical security toolsets such as SIEM, packet capture, and EDR; learners attending the course do not need a prior knowledge of specific FireEye technology to benefit from the instruction, however, lab activities are leveraged on the following FireEye technologies: FireEye Helix, FireEye Endpoint Security (HX) and FireEye Network Forensics (PX/IA). For example, Endpoint Hunting use cases leverage either FireEye Endpoint Security (HX), or Helix, or both, to acquire data used in the Hunt Mission.

**Learning Objectives**

After completing this course, learners should be able to:

- Define Cyber Threat Hunting and articulate its value to an organization
- Create or enhance an existing hunting program
- Leverage provided use cases for your Hunting Program
- Build hunt missions for threat hunting in your organization
- Leverage both endpoint and network data for successful hunting
- Implement a hunting mission to hunt, find, and automate the hunting process
Who Should Attend
Network security professionals and incident responders who will be using security and logging products to assist with their network and endpoint hunting responsibilities.

Course Outline

1. Introduction to Hunting
   - Types of Hunting
   - Hunting Process
   - Defining Hunt Missions
   - Creating a Hunt Program

2. Endpoint Hunting
   - Operating System Technology Review
   - Malware Hiding Techniques
   - Uncovering Internal Reconnaissance
   - Uncovering Lateral Movement
   - Data Acquisition Techniques

3. Network Hunting
   - Network Technology Review
   - Tunneling Techniques
   - Suspicious HTTP Traffic
   - Data Acquisition Techniques

Hunting Use Cases
This course includes six hunting use cases, for example, Event Log Clearing, RDP Tunneling and others. Each use case follows the hunting process by presenting a hunt mission and providing artifacts for hands-on analysis in a lab environment. Use cases are mainly separate hunt missions for network and endpoint with two use cases that require analysis in both areas. Each use case has the following format:

   - Technology Review
   - Real-world Threats
   - Hunt Mission
   - Data Collection and Hunt Execution
   - Analysis
   - Refining the Hunt Mission

Instructor-led sessions are typically a blend of lecture and hands-on lab activities.

For more details, or to view our full course catalog, please visit https://www.fireeye.com/services/training/