Trellix

EDUCATION SERVICES

Cyber Threat Hunting

Instructor-Led Training

Highlights

Duration

2 days

Prerequisites

Students taking this course should have a working knowledge of Windows operating systems, networking and network security, file system, registry, and regular expressions. Scripting experience with Python or PowerShell is beneficial. Completion of Endpoint Investigations instructor-led course is also required.

Recommended Pre Training

One of the following:

- Investigations with Endpoint Security (HX
- Network Traffic Analysis with Network Forensics

How to Register

Public sessions are listed at https://trellix-training.netexam.com.

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://trellix-training.netexam.com.

This course covers the fundamentals of Cyber 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 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 leave the course with critical information for establishing hunt programs within their organization, templates that can be used to document hunt missions, and 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 Trellix Endpoint Security (HX); learners attending the course do not need a prior knowledge of specific Trellix technology to benefit from the instruction, however, lab activities are leveraged on the following Trellix technologies: Helix, Endpoint Security (HX) and Trellix Network Forensics. For example, endpoint hunting use cases leverage either 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
- Understand how to identify key stakeholders within an organization
- 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
- Use relevant threat models to implement a hunt mission by acquiring and analyzing relevant data
- Identify areas of the hunt process that can be automated

Who Should Attend

This is a fast-paced technical course that is designed to provide hands-on experience hunting for attackers in modern enterprise environments, including collecting and analyzing endpoint and network evidence. The content and pace is intended for students with some background in incident response, forensic analysis, network traffic analysis, log analysis, security assessments, and/or penetration testing. It is also well suited for those managing incident response or hunt teams or who are in roles that require oversight of cyber threat hunting and other investigative tasks.

Course Outline

1. **Hunting Fundamentals**
   - Types of hunting
   - Hunting process
   - Defining hunt missions
   - Creating a hunt program
   - Identifying key stakeholders
   - Defining and leveraging cyber threat intelligence
   - Effecting threat modeling
2. **Acquiring and Analyzing Endpoint Data at Scale**
   - Operating system technology review
   - Malware hiding techniques
   - Uncovering internal reconnaissance
   - Uncovering lateral movement
   - Data acquisition techniques
3. **Acquiring and Analyzing Network Data at Scale**
   - Network technology review
   - Tunneling techniques
   - Exfiltration techniques
   - Suspicious HTTP traffic
   - Data acquisition techniques

Hunting Use Cases

This course includes a variety of hunting use cases, for example, indicator removal on hosts, DNS protocol abuse, 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. Each use case has the following format:

- Real-world Threats
- Technology Review
- Hunt Mission: Hypothesis Development
- Hunt Mission: Data Acquisition
- Hunt Mission: Analysis
- Refining the Hunt Mission

Trellix

Visit Trellix.com to learn more.

092023-13