Trellix EDUCATION SERVICES

Endpoint Security (HX) for Analysts

Self-Paced Online Training

Highlights

Duration

2 - 2.5 hours

Prerequisites

Students taking this course should have a working understanding of networking and network security, the Windows operating system, file system, registry, and use of the command line interface (CLI).

How to Register

This course is available for purchase at https://trellix-training.netexam.com

This entry-level course covers core functionality of Trellix Endpoint Security (HX), including features, operational workflows, alert analysis, and containment.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components of Trellix Endpoint Security (HX)
- Describe the communication between the Endpoint Security (HX) Server and the Trellix Endpoint agent
- Describe the function of the ring buffer
- Create hosts sets
- Create custom threat indicators
- Identify critical information in an Endpoint Security (HX) alert
- Request and approve hosts for containment
- Use Enterprise Search to find artifacts on managed hosts
- Acquire files and triages from hosts
- Review a triage or acquisition using Audit Viewer

Who Should Attend

Analysts and Incident Responders who use Trellix Endpoint Security (HX).

Course Outline

1. **Introduction to Endpoint Security (HX)**
2. **Fundamentals of Endpoint Security (HX)**
   - Trellix Ecosystem
   - Trellix Endpoint Agent
   - Ring buffer
   - Detection Engines
   - Host Sets
3. **Threat Management**
   - Rules
   - Endpoint Security (HX) Alerts
   - Triage summary
4. **Containment**
   - Containment process
   - Roles for Containment
5. **Searches and Acquisitions**
   - Enterprise Search
   - Exhaustive Search
   - Acquiring files and triage packages
   - Audit Viewer

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.