Trellix

EDUCATION SERVICES

Helix Administration

Instructor-Led Training

Highlights

Duration

2 days

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

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 Trellix Helix workflow, triaging Helix alerts, creating and scoping cases from an alert, and using Helix during an investigation.

Hands-on activities include writing TQL searches, as well as analyzing and validating Helix alerts.

Learning Objectives

After completing this course, learners should be able to:

- Determine which data sources are most useful for Helix detection and investigation
- Search log events across the enterprise
- Locate and use critical information in a Helix alert to assess a potential threat
- Create a case from events of interest
- Create and manage IAM users

Who Should Attend

Network security professionals, incident responders and Trellix administrators and analysts who use Helix to analyze data in noisy event streams.

Course Outline

Day 1

1. **Helix Fundamentals**
   - Introducing Helix
   - Features and capabilities
   - Searching and pivoting
   - Event parsing
   - Custom dashboards
2. **Search and Trellix Query Language (TQL)**
   - Searchable fields
   - Anatomy of an TQL search
   - TQL search, directories, and transform clauses

Day 2

1. **Data Source Selection and the MITRE ATT&CK framework**
   - Data sources for detection and investigation
   - Attack models to frame data source selection
   - Using the MITRE ATT&CK framework
   - Mapping attacker activity to the stages of an APT attack
2. **Rules & Lists**
   - Best practices for writing rules
   - Creating and enabling rules
   - Creating and using lists
   - Using regular expression in rules
   - Multi-stage rules
3. **Initial Alerts**
   - Helix alerts
   - Guided Investigations
   - Trellix Network Security alerts
   - MVX engine
   - Trellix Endpoint Security alerts
   - Triage with Triage Summary
   - Run searches across all hosts in the enterprise
4. **Helix Case Management**
   - Creating a case in Helix
   - Adding events to a case
   - Case workflow

Elective Content

The following additional lessons are available at no extra fee. These lessons are not relevant for all audiences, and are provided upon customer request, if time permits. Please coordinate with your Trellix instructor.

1. **Deployment and IAM**
   - User Management
   - Role-based Access
   - Deployment scenarios
   - Configuring 3rd party event collection
2. **Helix API**

Trellix

Visit Trellix.com to learn more.