Trellix EDUCATION SERVICES

Helix Administration

Instructor-Led Training

Highlights

Duration

2 days

Prerequisites

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

How to Register

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

This course covers the Trellix Helix workflow, triaging Helix alerts, and creating and scoping cases from an alert. 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
- Leverage Trellix WISE to efficiently triage security cases by leveraging AI-driven alert analysis and risk prioritization

Who Should Attend

This course is intended for network security professionals, incident responders, and Trellix administrators and analysts who use Helix to analyze data in noisy event streams.

Course Outline

1. Welcome
2. Helix Fundamentals
3. Search and TQL
4. Data Sources / Integration Hub
5. Custom Dashboards, Reports, and Lists
6. Detection Rules
7. Tags
8. Initial Alerts
9. Case Management
10. Legacy Features

Visit Trellix.com to learn more.

022024-15