Trellix

XDR Administration

Instructor-Led Training

Duration

2 days

Prerequisites

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.

Introduction

This course is a primer on XDR, covering XDR features, benefits, deployment options, basic administration, and core functionality. Learners will discover the unique strengths of XDR, and understand how XDR enables real-time situational awareness of known and unknown threats.

Hands-on activities include searching log events, triaging XDR alerts and investigating security incidents using XDR.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components needed for XDR deployment
- Determine which data sources are most useful for detection and investigation
- Search log events across the enterprise
- Locate and use critical information in an XDR alert to assess a potential threat

Who Should Attend

Network security professionals, incident responders and Trellix administrators and analysts who use XDR 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. Data Sources

- Data Source Visibility
- Cloud Data Sources
- On-premises Data Sources
- Data Source Configuration
- Unparsed Data
- Trellix Audit Data
- Audit Policies

3. Search and Trellix Query Language (TQL)

- Searchable fields
- Anatomy of an TQL search
- TQL search, directories, and transform clauses

4. Custom Dashboards, Reports, and Lists

- Custom Dashboards
- Reports
- Lists

Day 2

1. Threat Trends, Data Source Selection, and Mitre ATT&CK

- 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

- Best practices for writing rules
- Creating and enabling rules
- Creating and using lists
- Using regular expressionin rules
- Multi-stage rules

3. Initial Alerts

- Threats and Alert correlations
- Helix Alerts
- Building Alert Context
- Intel Hits
- Trellix Detections
  - MVision
  - Endpoint Security (HX)
  - MVX and Network Security (NX)

4. Helix Case Management

- Creating a case in Helix
- Adding events to a case
- Case workflow

Trellix

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.

062023-07