Investigations with Helix, Network and Endpoint Bundle (Helix, HX, NX)

Instructor-Led Training

Highlights

Duration

4 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.

This four-day primer on Helix, Network, and Endpoint covers the XDR workflow, extended detection via Trellix Helix, Trellix Network Security, and Trellix Endpoint Security (HX), and investigation and response using Helix, Network, and Endpoint tools.

Hands-on activities include writing MQL searches, creating rules, analyzing and validating alerts from Helix, Network Security, and Endpoint Security (HX), deep analysis of endpoint data collections, and response actions through Endpoint Security (HX) such as collecting data from across the enterprise and containing endpoints.

Learning Objectives

After completing this course, learners should be able to:

- Identify the components needed to deploy Trellix Helix, Network Security, and Endpoint Security (HX)
- Determine which data sources are most useful for Helix detection and investigation
- Locate and use critical information in a Helix alert to assess a potential threat
- Comfortably pivot from the Helix web console to native Trellix tools for deep analysis
- Validate Network Security and Endpoint Security (HX) alerts
- Use specialized features of Network Security and Endpoint Security (HX) to investigate and respond to potential threats across enterprise systems and endpoints

Who Should Attend

Incident response team members, threat hunters and information security professionals.

Course Outline

Day 1

1. Helix Fundamentals
   - Helix overview
   - Features and capabilities
   - Searching and pivoting
   - 3rd party data sources
   - Custom dashboards
2. Search, Mandiant Query Language (MQL), and Lists
   - Searchable fields
   - Anatomy of an MQL search
   - MQL search, directive, and transform clauses
   - Creating and using lists

Day 2

1. Rules
   - Creating and enabling rules
   - Using regular expressions in rules
   - Helix analytics
   - Multi-stage rules
2. Initial Alerts
   - Helix alerts
   - Guided investigations
   - Endpoint Security (HX) alerts
   - Network Security alerts
3. Helix Case Management
   - Creating a case in Helix
   - Adding events to a case
   - Case workflow

Day 3

1. Data Sources, Trends and the Attack Lifecycle
   - Threat landscape
   - Attack motivations
   - MITRE ATT&CK framework
   - Emerging threat actors
2. Using Audit Viewer and Redline®
   - Access triage and data collections for hosts
   - Navigate a triage collection or acquisition using Audit Viewer
   - Apply tags and comments to a triage collection to identify key events
3. Windows telemetry and acquisitions
   - Live forensic overview
   - Windows telemetry
     - Memory artifacts
     - System information
     - Processes
     - File system
     - Configuration files
     - Services
     - Scheduled tasks
     - Logging
   - Acquiring data

Day 4

1. Investigation Methodology
   - MITRE ATT&CK framework
   - Mapping evidence to attacker activity
     - Evidence of initial compromise
     - Evidence of persistence
     - Evidence of lateral movement
     - Evidence of internal reconnaissance
     - Evidence of data exfiltration
2. Capstone: Capture the Flag (CTF)

Elective Content

For private delivery, 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.

1. Deployment, Administration, and IAM
2. Helix API
3. Endpoint Security: Extended Capabilities
    - Open IOC Editor
    - HXTool
    - GoAuditParser
    - Endpoint Security REST API