Trellix

EDUCATION SERVICES

Trellix Endpoint Detection and Response with Forensics On-Prem Analyst

Instructor-Led Training

Highlights

Duration

2 days

Prerequisites

Students taking this course should have proficiency in Windows, Linux, and macOS system administration, specifically regarding process management, registry structures (Windows), and system logging (Syslog/Event Logs).

Basic understanding of computer security, command line syntax, malware/anti-malware, virus/anti-virus, and web technologies is recommended. Prior experience or working knowledge of ePolicy Orchestrator is also highly recommended.

Students should also have a familiarity with the MITRE ATT&CK Framework and its tactics, techniques, and procedures (TTPs), as well as the Cyber Kill Chain, to effectively contextualize and analyze host-centric endpoint alerts.

This course equips Security Analysts and Incident Responders to detect, investigate, and remediate endpoint threats using Trellix EDR with Integrated Forensics On-Premises (EDRF On-Prem). Designed for air-gapped, high-security, or regulated environments, it covers a localized three-server topology: ePolicy Orchestrator (ePO) On-Premises, Forensics HX Controller, and EDRF Telemetry Store (OpenSearch cluster) connected via Data Exchange Layer (DXL). Core topics include monitoring host alerts, threat hunting with Historical Search, Enterprise Search, Process and Logon Trackers, obtaining forensic acquisitions (File, Triage, Data), auditing evidence via Audit Viewer, and localized containment with remote shell remediation. This course also includes usage of the ETS Explorer and HX Tool.

Learning Objectives

After completing this course, learners should be able to:

- Navigate effectively through the Trellix Forensics (HX) Server UI.
- Use alert details, process trees, and Storytime visualization to quickly analyze threats and prioritize action.
- Perform threat hunting actions by searching across real-time and historical data using key product features that include Process Tracker, Logon Tracker, Enterprise Search, and Historical Search.
- Create and manage custom Indicators of Compromise (IOC) rules to trigger localized alerts.
- Leverage forensics features such as File, Triage, and Data acquisitions to gather comprehensive endpoint artifacts.
- Analyze acquired forensic data (registry, event logs, file activity) via the local web-based Audit Viewer and offline using Redline.
- Enforce host containment and remote endpoint remediation using containment controls and secure remote shell access.

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/

Who Should Attend

This course is intended for Security Analysts, Incident Responders, and Threat Hunters concerned with endpoint security and forensic investigation.

Course Outline

DAY 1

- **Welcome**
- **EDRF On-Prem Product Overview**
- **Analyst Views and Host Alerts**
- **Threat Hunting with EDRF On-Prem**

DAY 2

- **Threat Hunting with EDRF On-Prem (continued)**
- **Advanced Acquisitions and Offline Forensics**
- **Responding to Threats with EDRF On-Prem**

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.

Copyright © 2026 Musarubra US LLC

022024-15