Trellix

EDUCATION SERVICES

Endpoint Detection and Response with Forensics - SaaS Administration

Instructor-Led Training

Highlights

Duration

3 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 required.

Familiarity with the MITRE ATT&CK Framework and the Cyber Kill Chain to contextualize EDR alerts within a broader attack lifecycle. .

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 provides IT Administrators, Security Analysts, and Incident Responders with the specialized knowledge required to deploy, configure, and utilize the Trellix EDRF ecosystem. The curriculum focuses on the integration of traditional EDR capabilities with deep-dive forensic artifacts. Key highlights include the leverage of Trellix Wise for automated investigations, the utilization of enhanced forensic collection modules (Command Shell, PowerShell, and Full Memory acquisition), and the implementation of advanced remediation workflows. Participants will learn to move beyond simple alert monitoring to proactive threat hunting using the specialized Endpoint Detection and Response and Forensics Workspaces.

Learning Objectives

After completing this course, learners should be able to:

- Utilize ePO - SaaS platform to deploy EDRF XClients to managed endpoints.
- Navigate effectively through the product dashboards.
- Use alert ranking and data visualization to quickly understand threats and prioritize action.
- Walk through guided investigations.
- Leverage forensics features such as IOC detections, custom IOCs, acquisitions, enterprise search, enrichment and triage.
- Perform threat hunting actions by searching across real time and historical data using key artifacts (IP, hash, process) and logical operators.
- Create custom collectors and reactions, and perform investigative search activities.
- Detect advanced device threats, fully investigate them, and quickly respond.

- Leverage best practices and product performance recommendations.
- Synthesize diagnostic data and system configurations to troubleshoot, validate, and manage endpoint-to-cloud communication.

Who Should Attend

This course is intended for IT Administrators, Security Analysts, and Incident Responders concerned with system endpoint security.

Course Outline

1. **Welcome**
2. **EDRF Product and Architecture Overview**
3. **EDRF Setup and Deployment**
4. **Threat Detection with EDRF**
5. **Threat Hunting with EDRF**
6. **Investigations with EDRF**
7. **Responding to Threats with EDRF**
8. **Troubleshooting**

Trellix

Visit Trellix.com to learn more.

022024-15