DATASHEET

Trellix Endpoint Detection and Response Essentials Course

Education Services Instructor-led Training

Introduction

The Trellix EDR Essentials course from Education Services provides instruction on the design, setup, configuration, and management of this application. In addition, students will learn how to effectively leverage Trellix EDR in their environment. This course is roughly four hours in length.

Course Goals

- Identify the Trellix EDR capabilities
- Define Trellix EDR components
- Distinguish how Trellix EDR helps the SOC Mission
- escribe the MITRE ATT&CK Matrix
- Describe the product/solution architecture
- Distinguish deployment options
- Recall common log and product files
- Identify product/solution communication paths and ports

Audience

System and network administrators, security personnel, auditors, and/or consultants concerned with network and system security should take this course.

Recommended Pre-Work

It is recommended that students have a working knowledge of system administration concepts, computer security concepts, threat remediation, and a general understanding of networking.

Related Courses

- Trellix Intelligent Sandbox Administration
- Trellix Data Loss Prevention Endpoint Administration
- Trellix Endpoint Security Administration
- Trellix ePolicy Orchestrator – On-prem Essentials
- Trellix Agent Essentials
- Trellix ePolicy Orchestrator Advanced Topics

Ordering or Information

To order, or for further information, please email SecurityEducation@trellix.com

- Identify the supported platform, environment, or operating systems
- Recall the first steps for adding Trellix EDR to your environment
- Check in the required product extension(s)
- Deploy the Trellix EDR Client to endpoints
- Recall EDR dashboards and their purposes

Agenda at a Glance – 4 hours

- What is EDR? - An introduction and overview of the product and how it functions.
- Architecture - An overview of the software architecture and its functions

- Setup and Configuration – Covers the software deployment, installation, and configuration.
- Monitoring – View threat events in the Monitoring dashboard.
- Alerting - Leverage the Alerting dashboard to view the raw events from managed devices.
- Device Search – Use device data to assist with analyzing how a threat occurred in the system and what triggered it.
- Historical Search - Use the historical data to analyze a threat by tracing its behavior.
- Real-time Search - Obtain information about processes currently running on managed endpoints using real-time search queries.
- Catalog - Use the Catalog dashboard to view/create or delete custom collectors and reactions.
- Investigating - Analyze an investigation using the key findings and key artifacts discovered.
- Action History and Performance Metrics - View the details of actions performed through the Action History dashboard and View the Performance Metrics page to analyze the amount of time spent on resolving investigations.
- Basic Troubleshooting – Walk through multiple troubleshooting actions.
- Use Cases – Describe how different users put the EDR solution to use and for which events.

Trellix

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.