Trellix

EDUCATION SERVICES

Endpoint Detection and Response Administration

Instructor-Led Training

Highlights

Duration

2 days

Prerequisites

Students taking this course should have a solid knowledge of networking and system administration concepts, computer security concepts, network security concepts and practices, as well as a working knowledge of malware analysis, forensics, tactics, and techniques. Students should also have a general understanding of networking and application software.

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.

Introduction

This course prepares SOC Analysts to understand, communicate, and use the features provided by Trellix Endpoint Detection and Response (EDR). Through hands-on lab exercises, you will learn how to detect advanced device threats, fully investigate, and quickly respond.

Learning Objectives

After completing this course, learners should be able to:

- Install EDR in an ePO-SaaS environment.
- Navigate effectively through the product dashboard, walk through guided investigations, and create custom collectors and reactions.
- Leverage EDR features to detect advanced device threats, fully investigate them, and quickly respond.
- Use alert ranking and data visualization to quickly understand threats and prioritize action.

Who Should Attend

This course is intended for customers acting as analysts and/or engineers, responsible for configuration, management, and monitoring activity on their systems, networks, databases, and applications using the EDR solution.

Course Outline

Day 1

1. Welcome
2. What is EDR?
3. Architecture
4. Setup and Deployment
5. Monitoring
6. Alerting
7. Device Search
8. Historical Search

Day 2

1. Real-time Search
2. Catalog
3. Investigating
4. Action History and Performance Metrics
5. Troubleshooting EDR
6. Use Cases

Trellix

Visit Trellix.com to learn more.

092024-05