

# Endpoint Detection and Response Essentials Self-Paced Online Training

### / Highlights

#### Duration

4-hours

#### Who Should Attend

This course is intended for system and network administrators, security personnel, auditors, and/ or consultants concerned with network and system security.

#### Prerequisites

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

#### How to Register

This course is available for purchase at <a href="https://trellix-training.netexam.com">https://trellix-training.netexam.com</a>

This course provides instruction on the design, setup, configuration, and management of Trellix Endpoint Detection and Response (EDR). In addition, students will learn how to effectively leverage EDR in their environment.

## **Learning Objectives**

- Identify the EDR capabilities
- Define EDR components
- Distinguish how EDR helps the SOC Mission
- Describe 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
- Recall the first steps for adding EDR to your environment
- Check in the required product extension(s)
- Deploy the EDR Client to endpoints
- Recall EDR dashboards and their purposes

## Agenda at a Glance

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

- 8. Real-time Search
- 9. Catalog
- 10. Investigating
- 11. Action History and Performance Metrics
- 12. Basic Troubleshooting
- 13. Use Cases



## Visit <u>Trellix.com</u> 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 <a href="https://trellix.com">https://trellix.com</a>.