

Cortex XDR 2: Prevention, Analysis, and Response (EDU 260)

This course is three days of instructor-led training that will help you to:

- Differentiate the architecture and components of Cortex XDR
- Describe the threat prevention concepts for endpoint protection
- Work with the Cortex XDR management console
- Differentiate exploit and malware attacks and describe how Cortex XDR blocks them
- Perform appropriate response actions
- Describe the Cortex XDR causality analysis and analytics concepts
- Triage and investigate alerts, and manage incidents
- Manage Cortex XDR rules and investigate threats through the Query Center

Course Modules

1. **Cortex XDR Family Overview**
2. **Working with the Cortex Apps**
3. **Getting Started with Endpoint Protection**
4. **Malware Protection**
5. **Exploit Protection**
6. **Exceptions and Response Actions**
7. **Behavioral Threat Analysis**
8. **Cortex XDR Rules**
9. **Incident Management**
10. **Search and Investigate**
11. **Basic Troubleshooting**

Scope

- **Level:** Intermediate
- **Duration:** 3 days
- **Format:** Lecture and hands-on labs
- **Platform support:** Palo Alto Networks Cortex XDR Pro per endpoint and Pro per TB

Objectives

Successful completion of this instructor-led course with hands-on lab activities should enhance the student's understanding of how to install Cortex XDR agents, manage content updates, configure and manage Cortex XDR from its management console to protect endpoints against exploits and malware-driven attacks, understand fileless attacks and behavioral threat protection to stop them, build policy rules and profiles, and work with incidents and alerts including triaging, analyzing, and investigating, and then respond to prevention and network alerts.

Target Audience

Cybersecurity analysts and security operations specialists

Prerequisites

Participants must be familiar with enterprise security concepts.

Palo Alto Networks Education

The technical curriculum developed and authorized by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise that prepare you to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks and safely enable applications.