

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



**Days:** 3

**Course Overview:** Palo Alto Networks Cortex XDR is the world's first detection and response app that natively integrates network, endpoint and cloud data to stop sophisticated attacks. Cortex XDR accurately detects threats with behavioral analytics and reveals the root cause to speed up investigations. Tight integration with enforcement points accelerates containment, enabling you to stop attacks before the damage is done.

**Prerequisites:** Participants must be familiar with enterprise security concepts.

## **Audience:**

- Cybersecurity analysts and engineers
- Security operations specialists

**Course Objectives:** Successful completion of this instructor-led course with hands-on lab activities should enhance the student's understanding of how to activate a Cortex XDR instance; create agent installation packages to install the Cortex XDR agents; create security policies and profiles to protect endpoints against multi-stage, fileless attacks built using malware and exploits; respond to attacks using response actions; understand behavioral threat analysis, log stitching, agent-provided enhanced endpoint data, and causality analysis; investigate and triage attacks using the incident management page of Cortex XDR and analyze alerts using the Causality and Timeline analysis views; use API to insert alerts; create BIOC rules, and search a lead in raw data sets in Cortex Data Lake using Cortex XDR Query Builder.

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

- Differentiate the architecture and components of the Cortex XDR family
- Describe Cortex, Cortex Data Lake, the Customer Support Portal, and the hub
- Activate Cortex XDR, deploy the agents, and work with the management console
- Work with the Cortex XDR management console, describe a typical management page, and work with the tables and filters
- Create Cortex XDR agent installation packages, endpoint groups, policies, and profiles
- Create and manage exploit and malware profiles, and perform response actions
- Describe detection challenges with behavioral threats
- Differentiate the Cortex XDR rules BIOC and IOC, and create and manage them
- Describe the Cortex XDR causality analysis and analytics concepts
- Triage and investigate alerts and incidents, and create alert starrng and exclusion policies
- Work with the Causality and Timeline Views and investigate threats in the Query Center

## **OUTLINE:**

This class is comprised of the following modules:

- Module 1 - Cortex XDR Family Overview
- Module 2 - Working with the Cortex Apps
- Module 3 - Getting Started with Endpoint Protection

Baton Rouge | Lafayette | New Orleans

[www.lantecctc.com](http://www.lantecctc.com)

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

- Module 4 - Malware Protection
- Module 5 - Exploit Protection
- Module 6 - Exceptions and Response Actions
- Module 7 - Behavioral Threat Analysis
- Module 8 - Cortex XDR Rules
- Module 9 - Incident Management
- Module 10 - Alert Analysis Views
- Module 11 - Search and Investigate
- Module 12 - Basic Troubleshooting