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 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 starring and exclusion policies
- Work with the Causality and Timeline Views and investigate threats in 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. **Alert Analysis Views**
11. **Search and Investigate**
12. **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 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.

Target Audience

Cybersecurity analysts and engineers, 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.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

edu-260-90-threat- prevention-ds-072020