Cortex XDR: Prevention and Deployment (EDU-260)

Course Description

This instructor-led training enables you to prevent attacks on your endpoints. After an overview of the Cortex XDR components, the training introduces the Cortex XDR management console and demonstrates how to install agents on your endpoints and how to create Security profiles and policies.

The training enables you to perform and track response actions, tune profiles, and work with Cortex XDR alerts. It concludes by discussing basic troubleshooting of the agent, the on-premises Broker VM component, and Cortex XDR deployment.

Objectives

Successful completion of this instructor-led course with hands-on lab activities should enable you to:

› **Describe the architecture and components of the Cortex XDR family**

› **Use the Cortex XDR management console, including reporting**

› **Create Cortex XDR agent installation packages, endpoint groups, and policies**

› **Deploy Cortex XDR agents on endpoints**

› **Create and manage Exploit and Malware Prevention profiles**

› **Investigate alerts and prioritise them using starring and exclusion policies**

› **Tune Security profiles using Cortex XDR exceptions**

› **Perform and track response actions in the Action Centre**

› **Perform basic troubleshooting related to Cortex XDR agents**

› **Deploy a Broker VM and activate the Local Agents Settings applet**

› **Understand Cortex XDR deployment concepts and activation requirements**

› **Work with the Customer Support Portal and Cortex XDR Gateway for authentication and authorisation**

Target Audience

› **Cybersecurity Analysts and Engineers**

› **Cybersecurity Engineers**

› **Security Operations Specialists**

› **Administrators**

› **Product deployers**

Prerequisites

Participants must be familiar with enterprise product deployment, networking, and security concepts.

Course Outline:

Day 1

› **Cortex XDR Overview**
› **Cortex XDR Main Components**
› **Cortex XDR Management Console**
› **Profiles and Policy Rules**

Day 2

› **Malware Protection**
› **Exploit Protection**
› **Cortex XDR Alerts**
› **Tuning Policies using Exceptions**

Day 3

› **Response Actions**
› **Basic Agent Troubleshooting**
› **Broker VM Overview**
› **Deployment Considerations**

Scope

› **Level:** Intermediate
› **Duration:** 3 days
› **Format:** Lecture and hands-on labs
› **Platform support:** Cortex XDR Pro per Endpoint

Palo Alto Networks Education

The technical curriculum developed and authorised by Palo Alto Networks and delivered by Exclusive Networks as a Palo Alto Networks Authorised Training Partner helps provide the knowledge and expertise that prepare you to protect our digital way of life. These trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks and safely enable applications.

View our latest training schedule.

› Visit: **https://training.exclusive-networks.com/**
› Select your country in the top right
› Choose Palo Alto Networks in the Vendor options, and hit search.