Cortex XDR: Prevention and Deployment

Course code: EDU-260

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.

Who is the course for

Cybersecurity analysts and engineers

Security operations specialists

What we teach you

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 prioritize them using starring and exclusion policies
- Tune Security profiles using Cortex XDR exceptions
- Perform and track response actions in the Action Center
- 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 authorization

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

Course outline
- Cortex XDR Introduction
- Cortex XDR Main Components
- Cortex XDR Management Console
- Profiles and Policies
- Malware Protection
- Exploit Protection
- Cortex XDR Alerts
- Exclusions and Exceptions
- Response Actions
- Basic Troubleshooting
- Broker VM Overview
- Deployment Considerations

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.