Cortex™ XDR 3.2: Prevention and Deployment

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.

Prerequisites

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

Course Duration

3 days

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 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

Course Outline

1. Cortex XDR Overview
2. Cortex XDR Main Components
3. Cortex XDR Management Console
4. Profiles and Policy Rules
5. Malware Protection
6. Exploit Protection
7. Cortex XDR Alerts
8. Tuning Policies Using Exceptions
9. Response Actions
10. Basic Agent Troubleshooting
11. Broker VM Overview
12. Deployment Considerations

Who Should Attend

Cybersecurity analysts and engineers and security operations specialists, as well as administrators and product deployers.