Overview

The Cortex XDR self-paced digital learning course describes activation, deployment, and operation of Cortex XDR solution, and how security analysts can perform triage. The course contains about 2.0 hours of narrated modules, demonstrations, knowledge check questions, and hands-on practice.

The Cortex XDR course will help the learner to:

- Describe the function and role of Cortex XDR in a cybersecurity platform
- Differentiate the components and their roles involved in a Cortex XDR deployment
- Explain preparation requirements for a Cortex XDR deployment
- List the steps involved in activating the Cortex XDR service
- Triage and interpret Cortex XDR alerts

The course will cover the following modules.

- Module 1: Introduction to Cortex XDR
- Module 2: Preparation for Cortex XDR Deployment
- Module 3: Activating the Cortex XDR Service
- Module 4: Cortex XDR Alert Triage

Course Objectives

This course should help students understand the role of Cortex XDR in cybersecurity and the Palo Alto Networks Security Operating System and provides information about the advanced threat protection capabilities of Cortex XDR. The course will demonstrate the hands-on steps necessary to prepare an environment for Cortex XDR and how to activate the Cortex XDR service. The course provides information about the different approaches available to prioritize and interpret Cortex XDR security alerts.

Scope

- Course level: Beginner
- Course duration: 1.5 hours
- Course format: Digital learning with interactive video
- Platform support: Cortex XDR is a cloud-based service.

Target Audience

Cybersecurity Analysts and Security Operations Specialists

Prerequisites

Students should have a basic familiarity with security concepts, including sophisticated threat approaches. They also should be familiar with how to license and activate cloud services.

This digital learning course is available at the Learning Center.