Training Course

Cortex XDR 2: Prevention, Analysis and Response (EDU-260)

Duration: 3 Days **Product Version:** Cortex XDR 2

Description

This course combines instructor-led topics and hands-on lab activities to cover installation and management activities for the following:

- Activate the Cortex XDR instance, create and install Cortex XDR agent packages Create security policies and profiles to protect endpoints against multi-stage, fileless attacks that use combinations of malware and exploits
- Behavioural threat analysis, log stitching, agent-provided enhanced endpoint data and causality analysis

They will also learn how to:

- Investigate and triage attacks using the incident management page of Cortex XDR
- Analyse alerts through Causality and Timeline analysis views
- Use API to insert alerts
- Create BIOC rules and search a lead in raw data sets using Cortex XDR Query Builder
- Learn about the new features added in Cortex XDR 2.7 and 2.8 releases.

Target Audience

The Cortex XDR 2: Prevention, Analysis & Response (EDU-260) course is intended for Cybersecurity analysts and engineers, and security operations specialists. This can also include security engineers and security administrators

Prerequisite Requirements

The following is required when attending the course:

- Familiarity with the enterprise security concepts

Certification

There is a Micro Credential for XDR - “Micro-Credential Cortex XDR Consultant” that complements this course. It is now available in the Palo Alto Networks “Beacon” Portal.

Course Outline

Day 1

- Cortex XDR Family Overview
- Working with Cortex Apps
- Getting Started with Endpoint Protection
- Malware Protection
- Exploit Protection

Day 2

- Exceptions and Response Actions
- Basic Troubleshooting
- Behavioural Threat Analysis
- Cortex XDR Rules
- Incident Management

Day 3

- Alert Analysis Views
- Search and Investigate
- Investigation Views
- Host Insights
- Cortex XDR 2.7 and 2.8 New Features

+ Course details are subject to change