EXCLUSIVE NETWORKS

TRAINING PALO ALTO NETWORKS CORTEX XDR 2: PREVENTION, ANALYSIS & RESPONSE (EDU-260)

INCREASE REVENUE AND CUSTOMER VALUE WITH EXCLUSIVE NETWORKS PROFESSIONAL & SUPPORT SERVICES

Exclusive Networks
Alresford House, Mill Lane, Alton, Hampshire, GU34 2QJ
Tel: +44 (0)845 521 7217 or +44 (0)1420 548248
Email: Training@exclusive-networks.com

INTRODUCTION

Exclusive Networks offers the highest standard of technical education on products and solutions in its portfolio. All courses are delivered by vendor accredited trainers with real world experience and practical insight, providing attendees with tangible capability as well as study book theory. Courses are designed to equip engineers with the skills needed to understand, configure, support, troubleshoot and manage products in their care. Knowledge transfer through the training programme helps both business partners and their customers become more effective in supporting/managing solutions. Exclusive Networks' high levels of accreditation and training credentials speak for themselves, through authorised training endorsements from the vendors in Exclusive Networks' product portfolio.

Exclusive Networks UK operates authorised training centres for:

Accredited training can be provided in accordance with the vendor courseware either from Exclusive Networks' training suites, at the customer's premises or a suitable location for all parties. Alternatively, bespoke training courses using selected material from the vendor courseware can be provided where necessary. Both accredited training and bespoke training include instructorled training and hands-on labs. Knowledge transfer sessions are also available which provide instruction and demonstration of customer selected topics.*

All of Exclusive Networks' trainers adopt a 'hands-on' approach, which means they teach course content with real-world practical experience, rather than simply facilitate how to achieve accreditation.

*Knowledge transfer sessions do not include courseware or hands-on labs.

COURSE NAME: 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

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.

PRE-REQUISITE(S)

The following is required when attending the course:

- Familiarity with the enterprise security concepts

CERTIFICATION

There is to be a new Micro Credential for XDR Analyst test that will complement this course. Release date to be confirmed by Palo Alto Networks.

COURSE OUTLINE

Day 1

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

Day 2

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

Day 3

- Alert Analysis Views
- Search and Investigate
- Basic Troubleshooting

+ Course details are subject to change