# Cortex XDR: Investigation and Response (EDU-262)

**ID** EDU-262 **Price** CHF 1,980.—(excl. VAT) **Duration** 2 days

## Who should attend

- Cybersecurity analysts and engineers
- Security operations specialists

## This course is part of the following Certifications

Palo Alto Networks XDR Engineer (PXDRE)

## Prerequisites

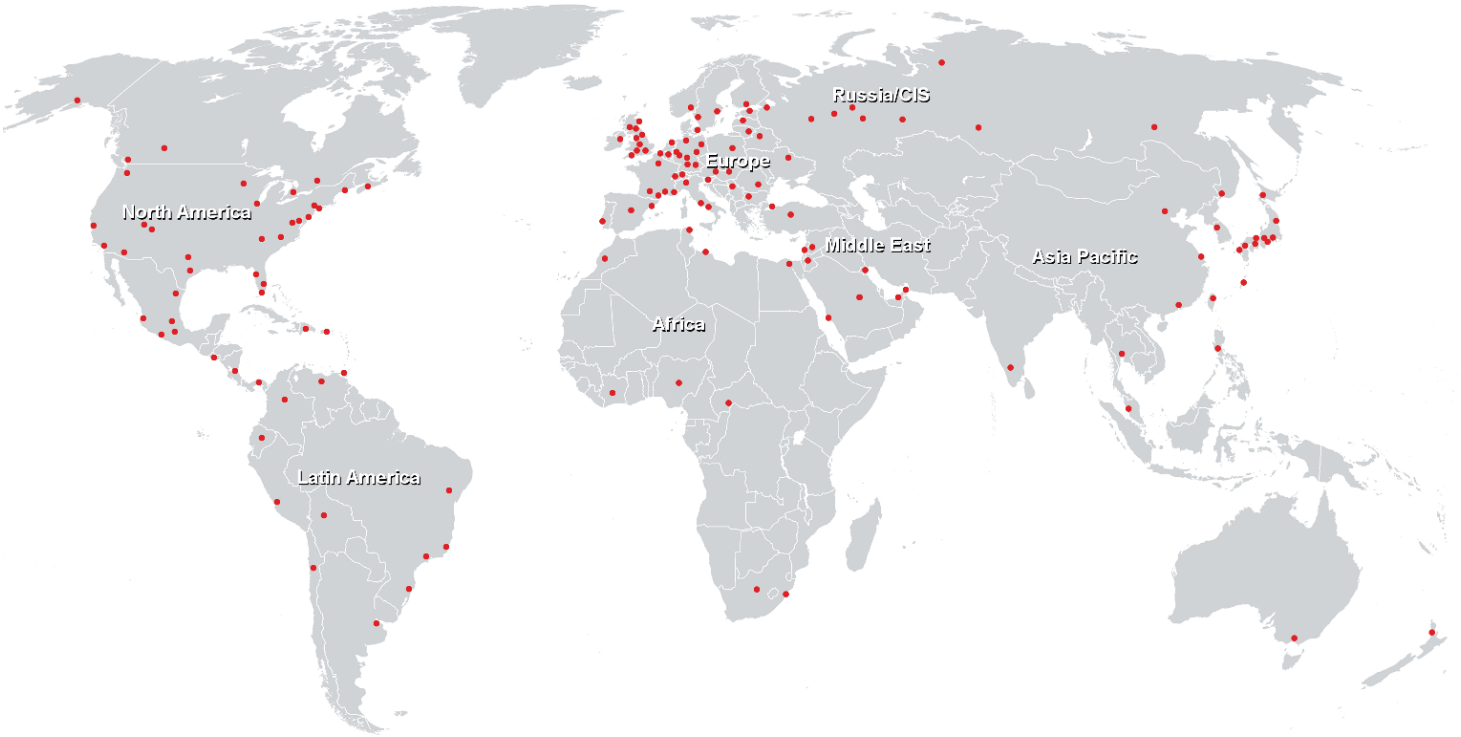
Participants must have completed the Cortex XDR: Prevention and Deployment (EDU-260) course.

## Course Objectives

Successful completion of this instructor-led course with hands-on lab activities should enable the students to:

- Investigate and manage incidents
- Describe the Cortex XDR causality and analytics concepts
- Analyze alerts using the Causality and Timeline Views
- Work with Cortex XDR Pro actions such as remote script execution
- Create and manage on-demand and scheduled search queries in the Query Center
- Create and manage the Cortex XDR rules BIOC and IOC
- Working with Cortex XDR assets and inventories
- Write XQL queries to search datasets and visualize the result sets
- Work with Cortex XDR's external-data collection

### Training Centres worldwide






**Fast Lane Institute for Knowledge Transfer (Switzerland) AG**

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

**info@flane.ch, https://www.flane.ch**