Cortex XDR: Investigation and Analysis (PCXDR-IA)

ID PCXDR-IA **Price** on request **Duration** 2 days

Who should attend

This course is for a wide range of security professionals, including SOC, CERT, CSIRT, and XDR analysts, managers, incident responders, and threat hunters. It is also well-suited for professional-services consultants, sales engineers, and service delivery partners.

Prerequisites

Participants should have a foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.

Course Objectives

This course is designed to enable you to:

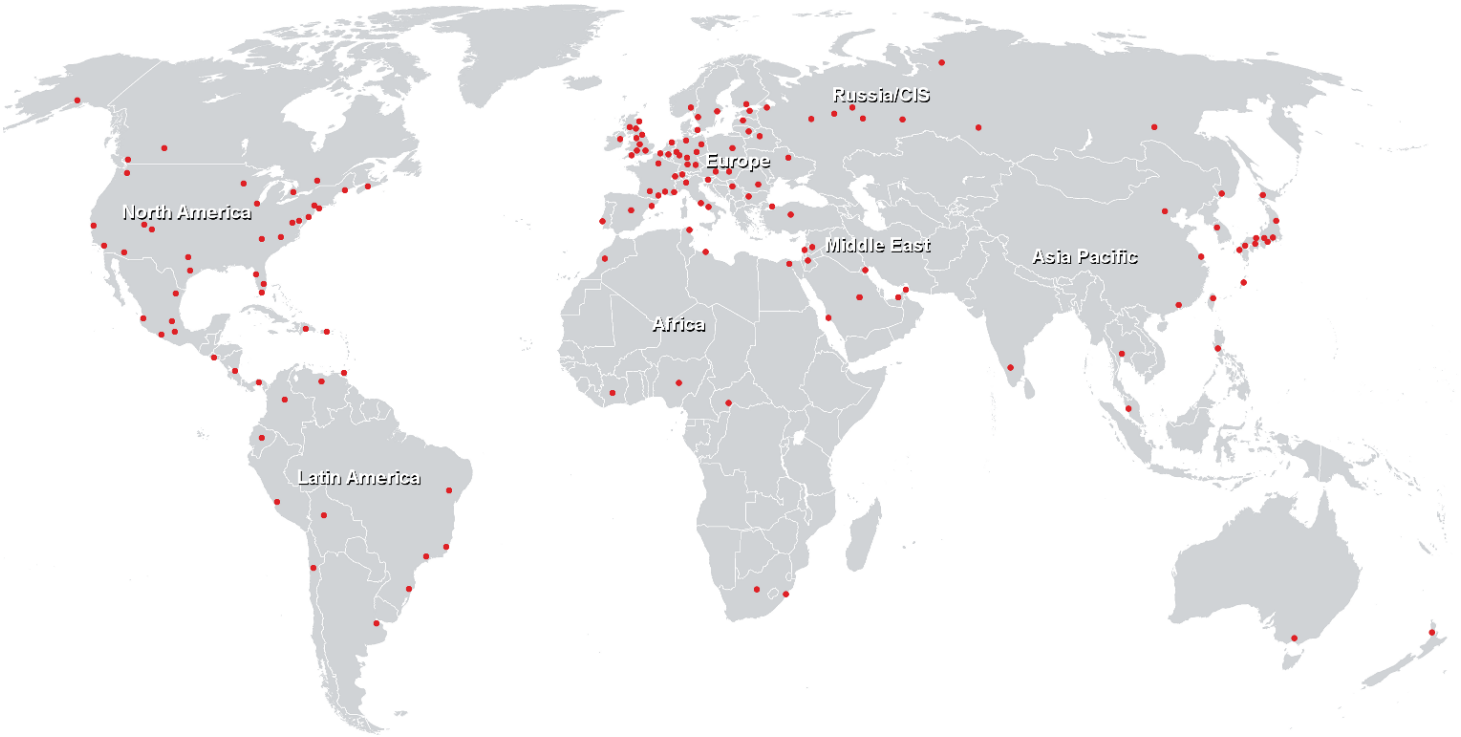
- Investigate cases, analyze key assets and artifacts, and interpret the causality chain.
- Query and analyze logs using XQL to extract meaningful insights.
- Utilize advanced tools and resources for comprehensive case analysis.

Course Content

Course Modules

- 1 - Introduction to Cortex XDR
- 2 - Endpoints
- 3 - XQL
- 4 - Alerting and Detection
- 5 - Vulnerability & Forensics
- 6 - Platform Automation
- 7 - Case Management
- 8 - Dashboards & Reports

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