Cortex XSIAM for Security Operations and Automation (EDU-270)

ID EDU-270 **Price** on request **Duration** 4 days

Who should attend

SOC/CERT/CSIRT/XSIAM engineers and managers, MSSPs and service delivery partners/system integrators, internal and external professional-services consultants and sales engineers, incident responders and threat hunters.

Prerequisites

Participants must be familiar with enterprise product deployment, networking, and security concepts.

Course Objectives

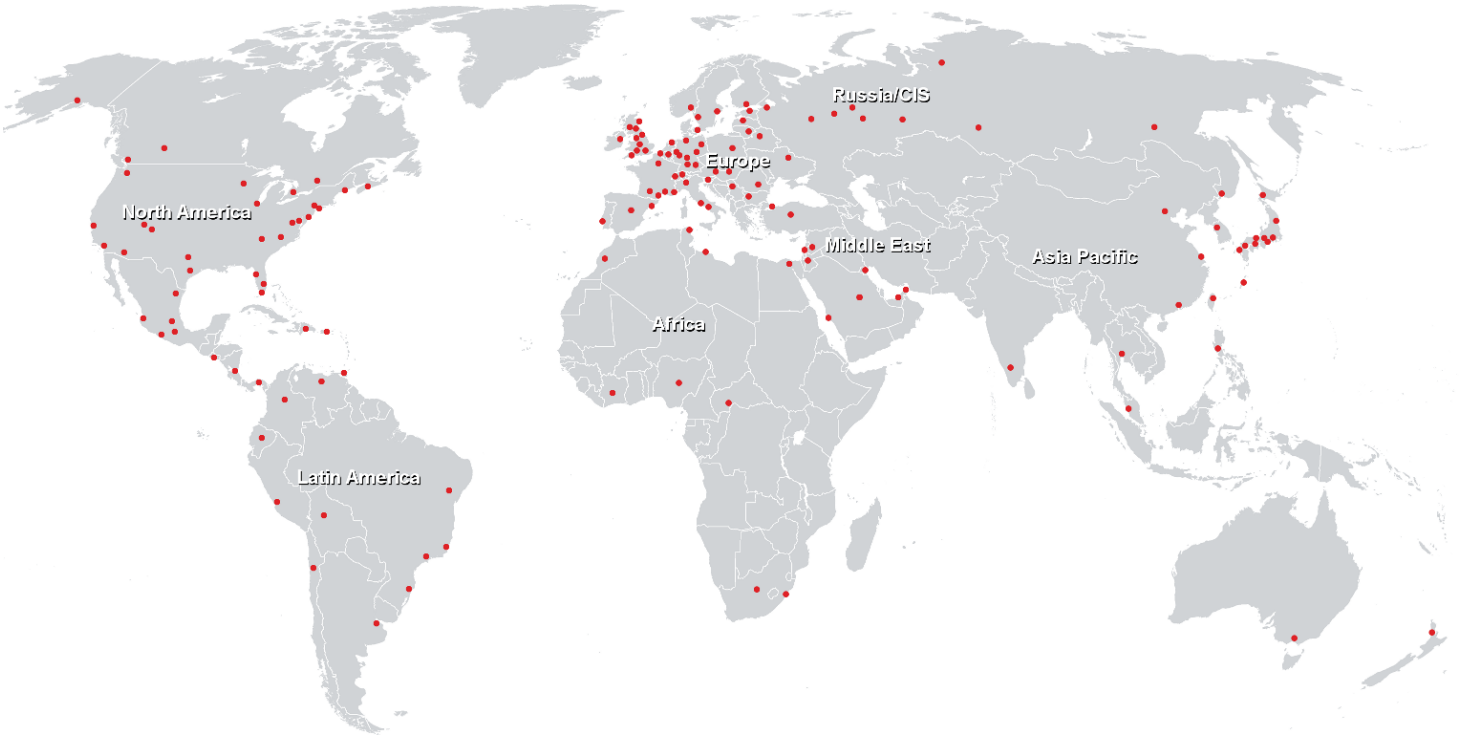
The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Engineering roles, to use XSIAM. The course reviews XSIAM intricacies, from fundamental components to advanced strategies and automation techniques, including skills needed to navigate incidenthandling, optimize log sources, and orchestrate cybersecurity excellence.

Course Content

Course Modules

- 1 - Introduction to Cortex XSIAM
- 2 - Elements of Security Operations
- 3 - Maturity Model
- 4 - Agent Deployment and Configuration
- 5 - Data Source Ingestion
- 6 - Visibility
- 7 - Data Model
- 8 - Analytics
- 9 - Alerting and Detecting
- 10 - Attack Surface Management
- 11 - Automation
- 12 - Incident Handling / SOC

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