Cortex XDR: Investigation and Response (EDU-262)

ID EDU-262 **Prix** CHF 1 980,– (Hors Taxe) **Durée** 2 jours

A qui s'adresse cette formation

Ce cours s'adresse à un large éventail de professionnels de la sécurité, notamment :

- les analystes SOC, CERT, CSIRT et XDR
- les responsables
- les intervenants en cas d'incident
- les chasseurs de menaces.
- les consultants en services professionnels
- les ingénieurs commerciaux
- les partenaires de prestation de services.

Cette formation prépare à la/aux certifications

Palo Alto Networks XDR Engineer (PXDRE)

Pré-requis

Il est vivement recommandé par l'éditeur pour les participants d'avoir suivi la formation Cortex XDR: Prevention and Deployment (EDU-260) Les participants doivent avoir une compréhension fondamentale des principes de cybersécurité et une expérience dans l'analyse des incidents et l'utilisation d'outils de sécurité pour les enquêtes.

Objectifs

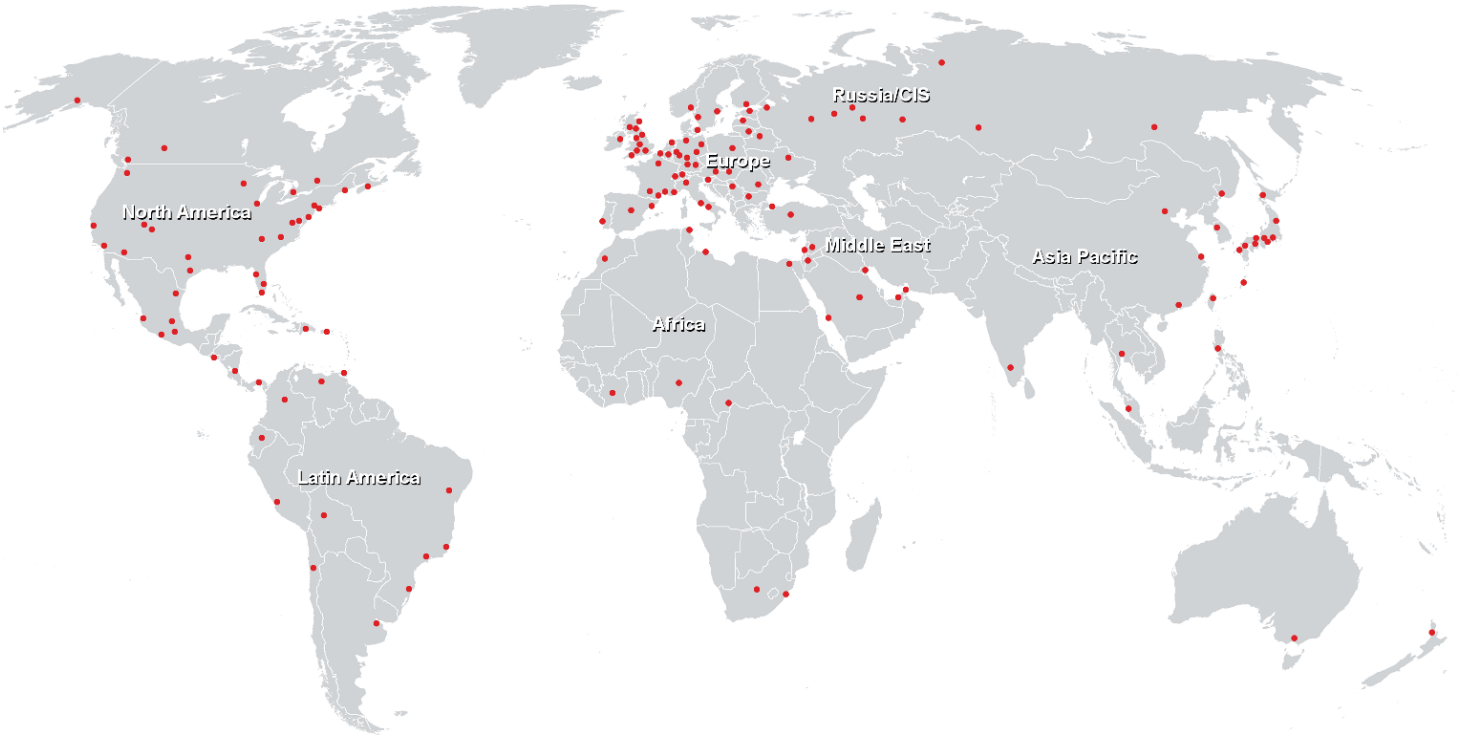
À l'issue de ce cours, vous serez capable de :

- Enquêter sur les cas, analyser les actifs et artefacts clés, et interpréter la chaîne de causalité.
- Interroger et analyser les journaux à l'aide de XQL afin d'en extraire des informations pertinentes.
- Utiliser des outils et ressources avancés pour une analyse complète des cas.

Contenu

- Module 1 : Introduction à Cortex XDR
- Module 2 : Terminaux
- Module 3 : XQL
- Module 4 : Alertes et détection
- Module 5 : Vulnérabilité et analyse forensic
- Module 6 : Automatisation de la plateforme
- Module 7 : Gestion des cases
- Module 8 : Tableaux de bord et rapports

Centres de formation dans le monde entier





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