Cortex XDR: Prevention and Deployment (EDU-260)

ID EDU-260 **Prix** CHF 2 730,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

Ce cours est recommandé pour les :

- Ingénieurs SOC
- Analystes en cybersécurité
- Administrateurs Système
- les personnes en charge du déploiement.

Cette formation prépare à la/aux certifications

Palo Alto Networks XDR Engineer (PXDRE)

Pré-requis

Les participants doivent être familiarisés avec les déploiements d'entreprise, le réseau et les bases de la sécurité.

Objectifs

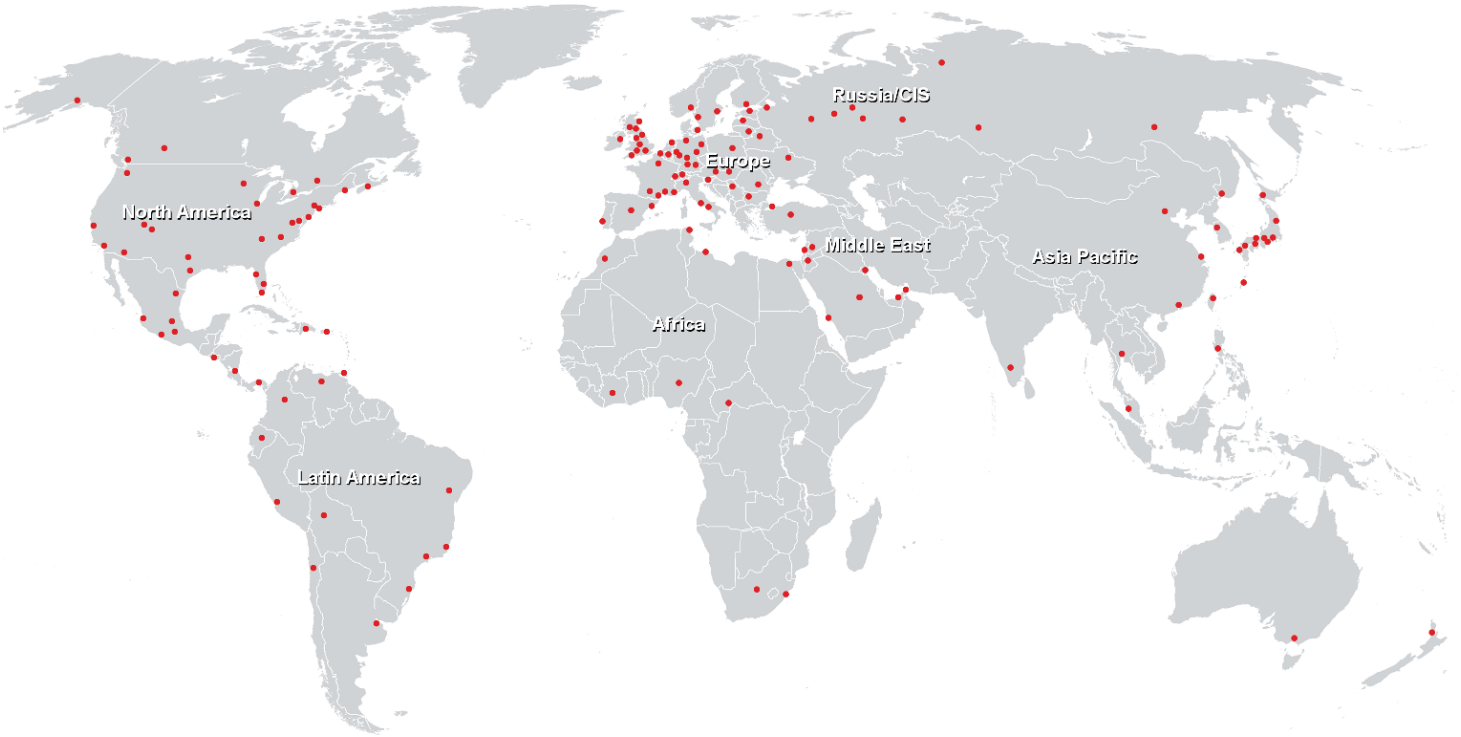
L'alternance des modules de cours avec des sessions de labs devrait vous permettre de :

- Configurer les composants de Cortex XDR, y compris les agents, les collecteurs XDR, les pare-feux de nouvelle génération (NGFW) et les Broker VM
- Utiliser XQL pour interroger et analyser les journaux afin de permettre une ingestion efficace des données et la détection des menaces.
- Mettre en place des workflows pour optimiser les opérations de sécurité.
- Appliquer des listes dynamiques externes (EDL) et des règles d'indicateurs pour faire respecter les politiques de sécurité.

Contenu

- Module 0 : Présentation du cours
- Module 1 : Présentation de Cortex XDR
- Module 2 : Composants logiciels
- Module 3 : Intégrations
- Module 4 : XQL
- Module 5 : Outils de détection
- Module 6 : Optimisation du système
- Module 7 : 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