Cortex XDR: Investigation and Response (EDU-262)

ID EDU-262 **Prix** sur demande **Durée** 2 jours

A qui s'adresse cette formation

- Analystes et Ingénieurs en cybersécurité et les personnes travaillant dans un SOC

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 être familiarisés avec l'analyse d'événements de sécurité.

Objectifs

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

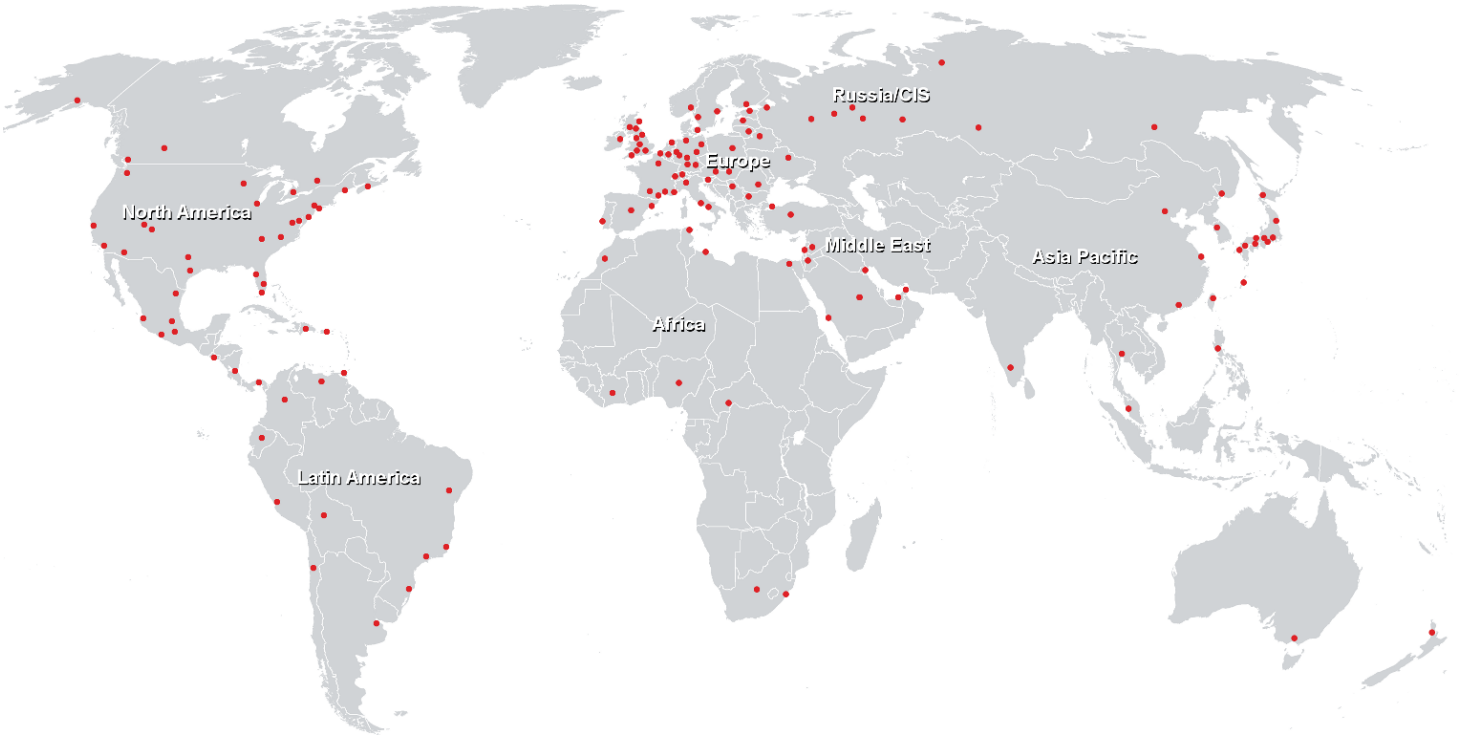
- Enquêter et gérer les incidents
- Décrire la causalité Cortex XDR et les concepts analytiques
- Analyser les alertes à l'aide des vues Causalité et Chronologie
- Travailler avec les actions Cortex XDR Pro telles que l'exécution de scripts à distance
- Créer et gérer des requêtes de recherche à la demande et les planifier dans le Centre de requêtes
- Créer et gérer les règles Cortex XDR BIOC et IOC
- Travailler avec les actifs et les inventaires Cortex XDR
- Écrire des requêtes XQL pour rechercher des ensembles de données et visualiser les ensembles de résultats
- Travailler avec la collecte de données externes de Cortex XDR

Contenu

- Module 1 : Incidents Cortex XDR
- Module 2 : Concepts de causalité et d'analyse
- Module 3 : Analyse de causalité des alertes
- Module 4 : Actions de réponses avancées
- Module 5 : Créer des requêtes de recherche
- Module 6 : Construire des règles XDR
- Module 7 : Actifs Cortex XDR
- Module 8 : Introduction à XQL
- Module 9 : Collecte de données externes

Cortex XDR: Investigation and Response (EDU-262)

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