

Cortex™ XSOAR: Automation and Orchestration (EDU-380)

ID EDU-380 Prix sur demande Durée 4 jours

A qui s'adresse cette formation

Ingénieurs sécurité-opérations (SecOps), ou sécurité, orchestration, automatisation et réponse (SOAR), fournisseurs de services de sécurité gérés (MSSP), partenaires de prestation de services, intégrateurs de systèmes et ingénieurs de services professionnels. partenaires de prestation de services, intégrateurs de systèmes et ingénieurs de services professionnels.

Pré-requis

Les participants doivent suivre la formation digitale Cortex XSOAR Analyst. Les participants qui ont une expérience de l'écriture de scripts, de l'utilisation de Python et de JavaScript, et de l'utilisation d'objets de données JSON seront probablement en mesure d'appliquer ce qu'ils apprennent plus rapidement que les participants sans cette expérience. Toutefois, il n'est pas nécessaire de maîtriser le code pour suivre ce cours.

Objectifs

Cette formation est conçue pour permettre à un ingénieur SOC, CERT, CSIRT ou SOAR de commencer à travailler avec les intégrations Cortex XSOAR, les playbooks, les mises en page des incidents et d'autres fonctionnalités du système pour faciliter l'orchestration des ressources, l'automatisation des processus, la gestion des cas et le flux de travail des analystes.

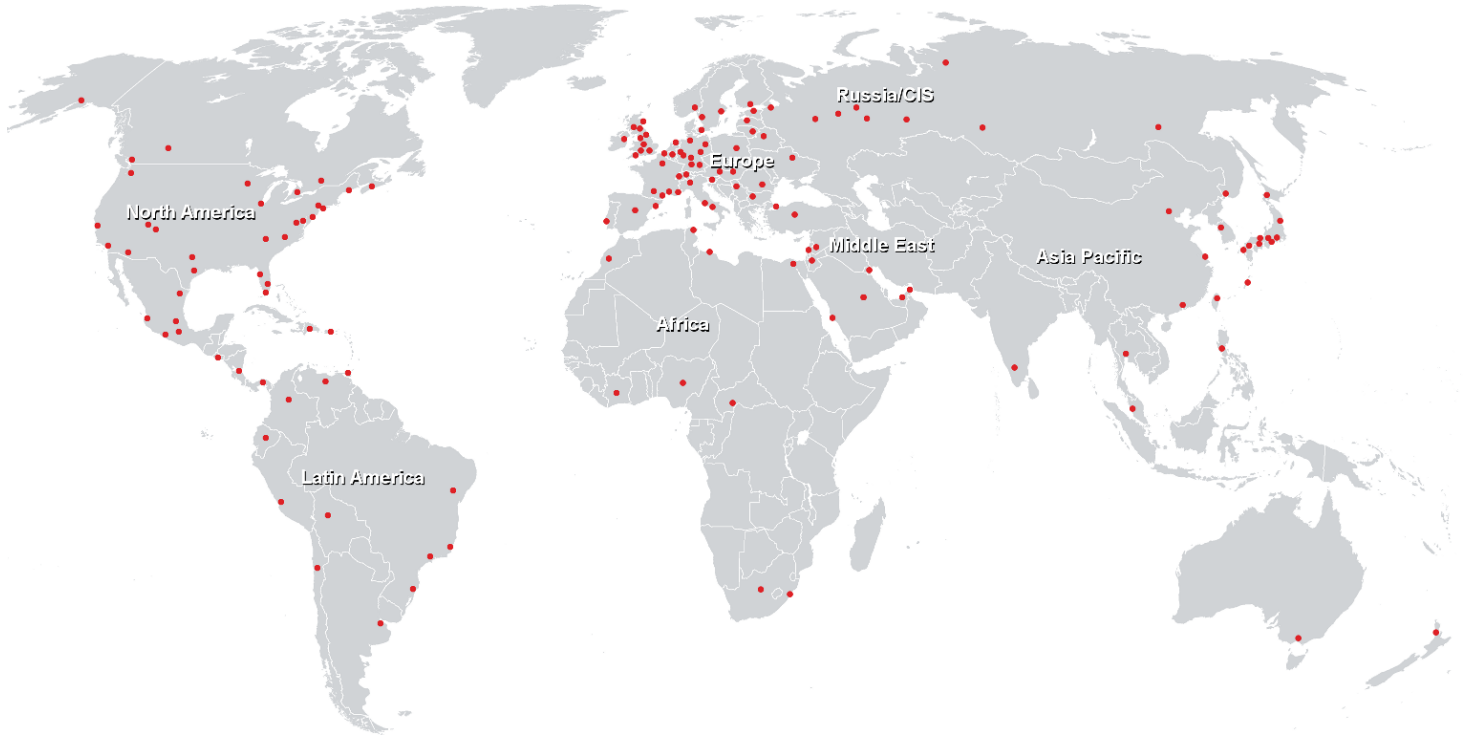
Le troisième module du cours présente un processus complet de développement de playbooks pour l'automatisation d'un flux de travail typique d'un analyste pour traiter les incidents de phishing. Cette vue de bout en bout du processus de développement fournit un cadre pour des discussions plus ciblées sur des sujets individuels qui sont couverts dans les modules suivants.

Contenu

- Fonctionnalités de base et ensembles de caractéristiques.
- Activation et configuration des intégrations.

- Développement de Playbook.
- Classification et mappage.
- Constructeur de mise en page.
- Architecture de la solution.
- Docker.
- Développement de l'automatisation et débogage.
- Gestion du contenu.
- Indicateurs.
- Jobs et planification des tâches.
- Gestion des utilisateurs et des rôles.
- Développement de l'intégration

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>