

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

ID EDU-380 Preis auf Anfrage Dauer 4 Tage

Zielgruppe

Security-Operations (SecOps) oder Security, Orchestration, Automation und Response (SOAR) Ingenieure, Managed Security Service Provider (MSSP), Service Delivery Partner, Systemintegratoren und Ingenieure für professionelle Dienstleistungen.

Voraussetzungen

Die Teilnehmer müssen das digitale Lernprogramm Cortex XSOAR Analyst absolvieren. Teilnehmer, die Erfahrung mit Skripting, der Verwendung von Python und JavaScript sowie der Verwendung von JSON-Datenobjekte werden das Gelernte wahrscheinlich schneller anwenden können als Teilnehmer ohne solche Erfahrungen. Der Abschluss des Kurses bedeutet jedoch nicht erfordern die Fähigkeit, Code zu schreiben.

Kursziele

Diese Schulung soll SOC-, CERT-, CSIRT- oder SOAR-Ingenieure in die Lage versetzen, mit Cortex XSOAR-Integrationen, Playbooks, Layouts für Vorfälle und andere Systemfunktionen zur Erleichterung der Ressourcenorganisation, der Prozessautomatisierung, des Fallmanagements und des Arbeitsablaufs von Analysten. Das dritte Modul des Kurses demonstriert einen kompletten Playbook-Entwicklungsprozess für die Automatisierung eines typischen Analysten-Workflows zur Behandlung von Phishing-Vorfällen. Diese Die End-to-End-Ansicht des Entwicklungsprozesses bietet einen Rahmen für gezieltere Diskussionen zu einzelnen Themen, die in den nachfolgenden Modulen behandelt werden.

Weltweite Trainingscenter



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>