SOC – Security Operations Center – Hands On Cyber Attack Simulation (MCSOC)

ID MCSOC **Preis** CHF 2'490.– (exkl. MwSt.) **Dauer** 3 Tage

Zielgruppe

Führungskräfte, Manager und Auditoren für IT- und Informationssicherheit, Mitarbeiter aus den Bereichen IT und Informationssicherheit

Voraussetzungen

Die Master Class setzt kein Spezialwissen über bestimmte Technologien voraus. Kenntnisse über Grundsätze der IT-Sicherheit und des Informationssicherheitsmanagements sollten vorhanden sein.

Kursinhalt

Im Bereich Malware werden aktuelle Bedrohungen sowie Grundlagen der Analyse vermittelt und praktisch angewendet.

Im Kontext SIEM lernen die Teilnehmer Architekturen, Log-Analyse und Security Incident Management kennen und arbeiten mit Splunk zur Angriffserkennung.

Die Netzwerk-Forensik umfasst die Analyse von Netzwerkverkehr und die Erkennung von Angriffen auf Protokollebene.

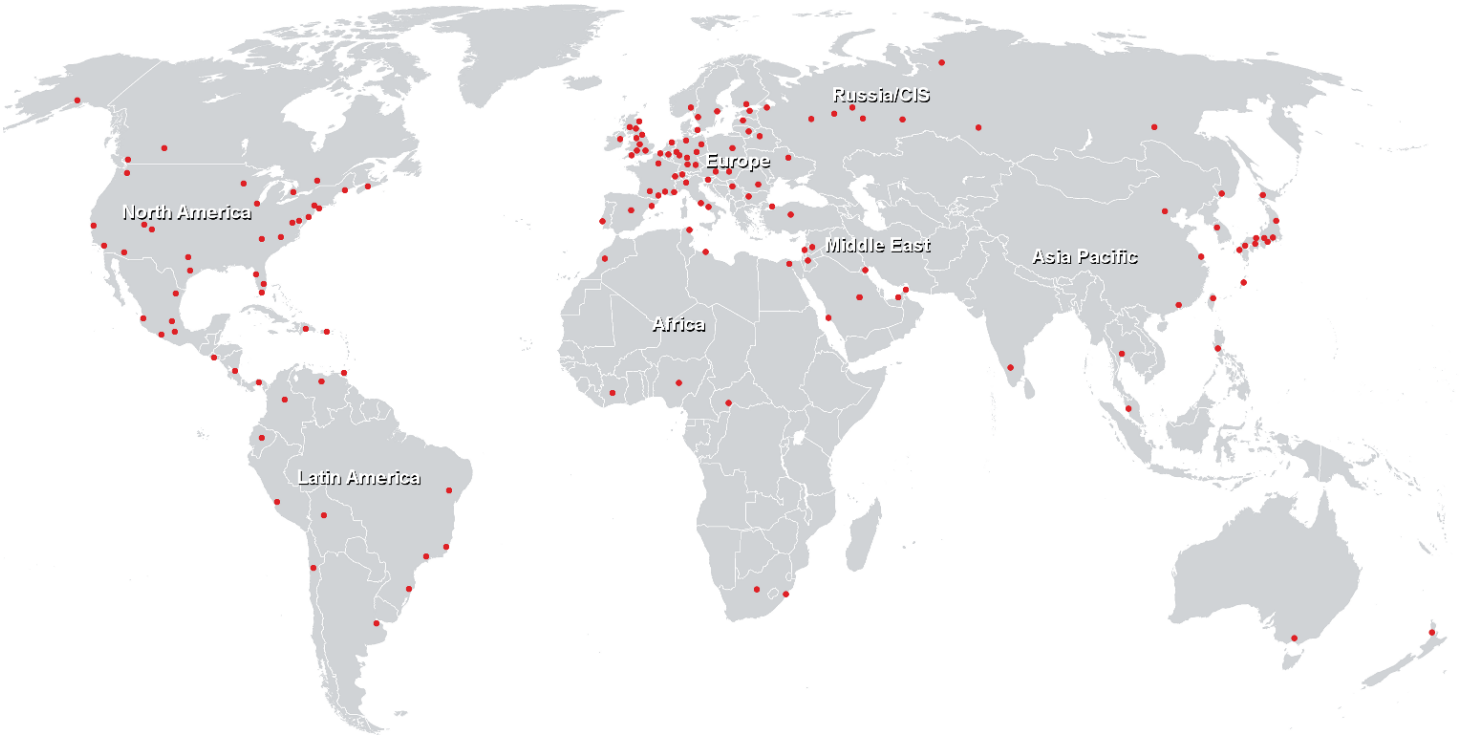
In der vertiefenden SIEM-Praxis erstellen und optimieren die Teilnehmer eigene Detection-Regeln auf Basis realer Szenarien.

SOC-Prozesse und Reporting behandeln Rollen, Abläufe und die Erstellung strukturierter Auswertungen.

Die Übungen sind durchgehend integraler Bestandteil aller Module und basieren auf realistischen Angriffsszenarien. KI-Tools werden dabei gezielt zur Unterstützung von Analyse- und Entscheidungsprozessen eingesetzt.

SOC – Security Operations Center – Hands On Cyber Attack Simulation (MCSOC)

Weltweite Trainingscenter





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