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

ID MCSOC **Preis** auf Anfrage **Dauer** 5 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

Malware

- Aktuelle Cyberbedrohungslage und bekannt gewordene Vorfälle
- Einführung in Funktion und Analyse von Malware
- Praxis: Einsatz von Tools zur Malware-Analyse

SIEM, Level 1

- Security Information and Event Management (SIEM) Einführung
- SIEM-Architekturen
- Einführung Security Incident Management (SIM)
- Praxis: Nutzung von Splunk und vorgefertigten Regeln zur Angriffserkennung

Management von Cyberkrisen, Level 1

- Gute und schlechte Beispiele
- Kernprozess zum Krisenmanagement
- Lagezentrum und Lagebilder
- Praxis: Bewältigung eines schwerwiegenden Cybervorfalls

Netzwerk-Forensik

- Recap: TCP/IP-Protokollfamilie
- Sichere Netz-Architekturen
- Einführung in Protokoll-Analyse-Tools
- Praxis: Erkennung von Angriffen auf Netzwerk-Ebene

SIEM, Level 2

- Praxis: Erstellung eigener Rules auf Basis von Angriffen

SOC Management und Reporting

- SOC-Prozesse und -Rollen
- Praxis: SIM-Prozess-Erstellung
- KPI-Reportings

Management von Cyberkrisen, Level 2

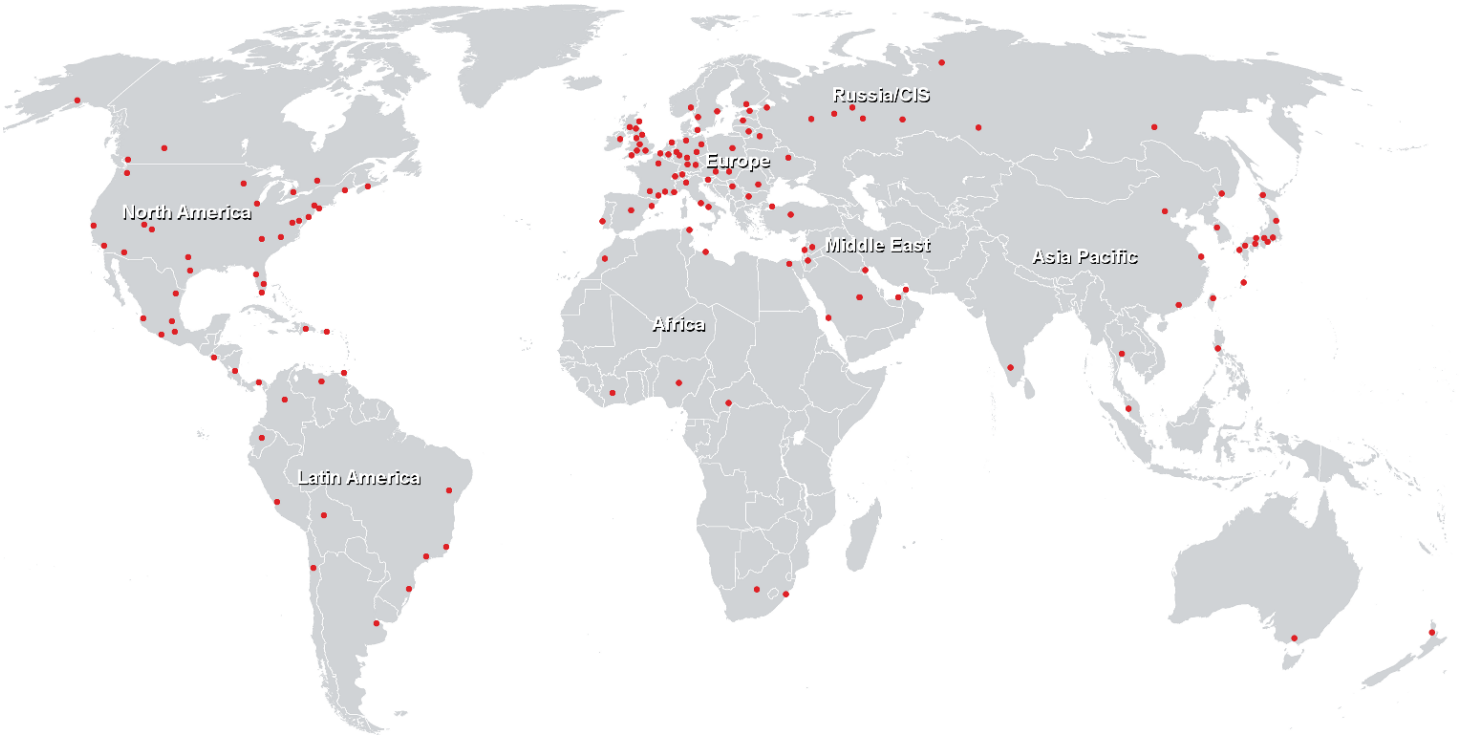
- Einführung in TIBER-DE
- Krisenkommunikation
- Praxis: Erstellung eigener Cyberkrisen-Übungen

Team-Übung

- Gemeinsame Abwehr eines realistischen Cybervorfalls von der Erkennung bis zur Bewältigung

Master Class: SOC – Security Operations Center – Hands On Cyber Attack Simulation

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