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

ID MCSOC **Prix** CHF 2 490,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

Executives, managers and auditors for IT and information security, employees from the areas of IT and information security.

Pré-requis

The Master Class does not require specialized knowledge of specific technologies. Knowledge of IT security principles and information security management should be present.

Contenu

In the area of malware, students learn about current threats and the fundamentals of analysis, and apply this knowledge in practical exercises.

In the context of SIEM, participants will learn about architectures, log analysis, and security incident management, and will use Splunk for attack detection.

Network forensics involves the analysis of network traffic and the detection of attacks at the protocol level.

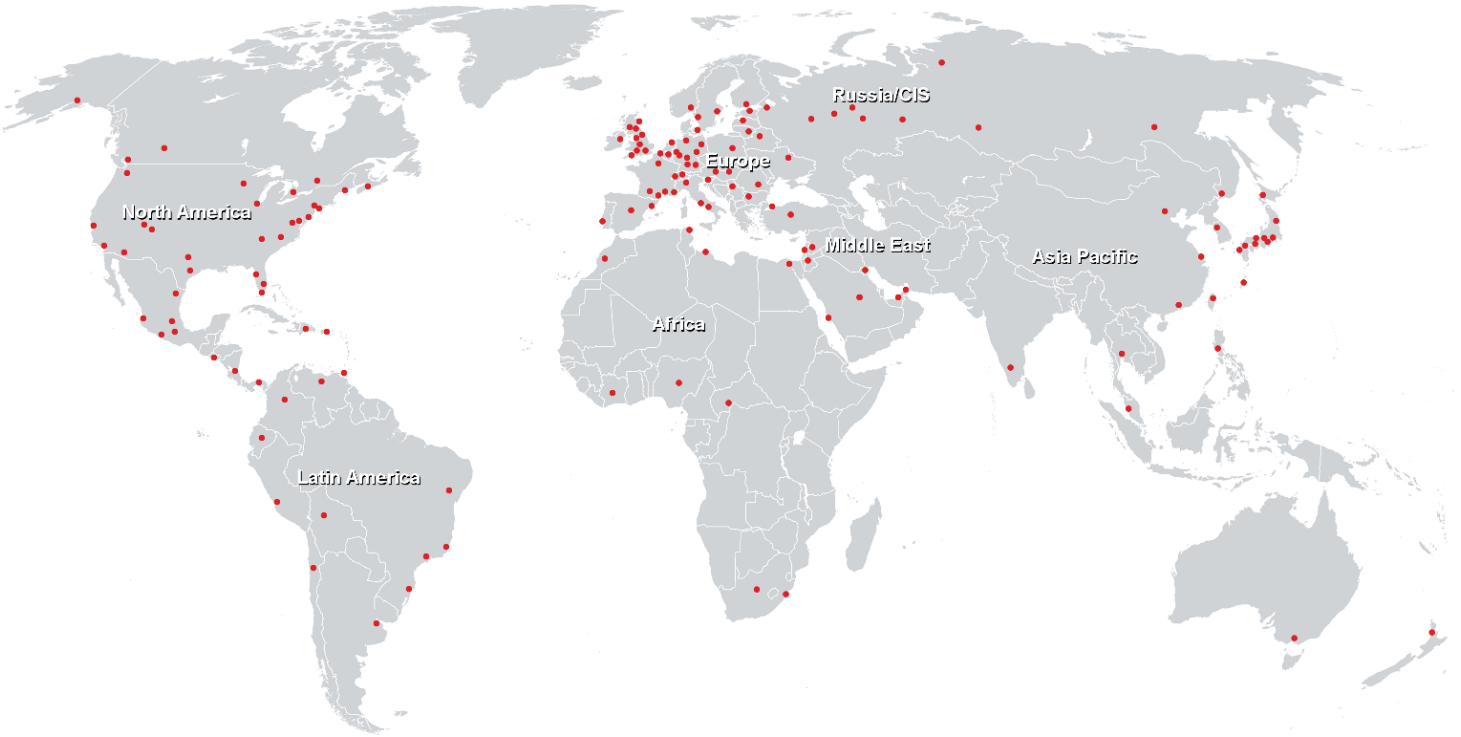
In this advanced SIEM workshop, participants will create and optimize their own detection rules based on real-world scenarios.

SOC processes and reporting cover roles, procedures, and the creation of structured reports.

The exercises are an integral part of all modules and are based on realistic attack scenarios. AI tools are specifically used to support analysis and decision-making processes.

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

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