

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

ID MCSOC Prix sur demande Durée 5 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

### Malware

- Current cyber threat situation and known incidents
- Introduction to function and analysis of malware
- Practice: Use of tools for malware analysis

### SIEM, Level 1

- Security Information and Event Management (SIEM) Introduction
- SIEM architectures
- Introduction Security Incident Management (SIM)
- Practice: Use of Splunk and predefined rules for attack detection

### Management of cyber crises, Level 1

- Good and bad examples
- Core process for crisis management
- Situation center and situation pictures
- Practice: Managing a serious cyber incident

### Network forensics

- Recap: TCP/IP protocol family
- Secure network architectures
- Introduction to protocol analysis tools
- Practice: Detecting network-level attacks

### SIEM, Level 2

- Practice: Creating your own rules based on attacks

### SOC Management and Reporting

- SOC processes and roles
- Practice: SIM process creation
- KPI reporting

### Management of cyber crises, Level 2

- Introduction to TIBER-DE
- Crisis communication
- Practice: Creation of own cyber crisis exercises

### Team exercise

- Joint defense of a realistic cyber incident from detection to management

# 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](mailto:info@flane.ch), <https://www.flane.ch>