

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

ID MCSOC Price 6,990.— €(excl. tax) **Duration 5 days**

Course Overview

Analysis of past incidents shows repeatedly: Human error is the most common cause of delays and serious failures when dealing with cybersecurity incidents. In our SOC Master Class, we prepare you for the dynamics and complexity of such situations with numerous learning and practice elements.

In the training, participants are introduced to the essential technologies and processes for detecting and remediating cyberattacks. The knowledge acquired is then practiced in each case by means of the participants' own handling of simulated live attacks. For this purpose, an arena is used in which participants can safely practice various tactics for defense and remediation. In particular, cross-functional collaboration is also addressed. The exercises include technical elements as well as elements of incident, emergency and crisis management.

The Master Class is conducted by a facilitator ("White Team Trainer") and accompanied by an attacker ("Red Team Trainer").

Who should attend

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

Prerequisites

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

Course Content

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



About Fast Lane



Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center



Worldwide Presence
with high-end training centers
around the globe



Multiple Awards
from vendors such as AWS,
Microsoft, Cisco, Google, NetApp,
VMware



Experienced SMEs
with over 19.000 combined
certifications

Germany

Fast Lane Institute for Knowledge
Transfer GmbH

Tel. +49 40 25334610

info@flane.de / www.flane.de

Austria

ITLS GmbH

(Partner of Fast Lane)

Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Switzerland

Fast Lane Institute for Knowledge
Transfer (Switzerland) AG

Tel. +41 44 8325080

info@flane.ch / www.flane.ch