

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

ID MCSOC Preis 4.499,- € (exkl. MwSt.) Dauer 5 Tage

Kursüberblick

Die Analysen vergangener Vorfälle zeigen immer wieder: menschliches Versagen ist bei der Bewältigung von Cybersicherheits-Vorfällen die häufigste Ursache von Verzögerungen und schwerwiegenden Fehlern. In unserer SOC Master Class bereiten wir Sie mit zahlreichen Lern- und Übungselementen auf die Dynamik und Komplexität derartiger Situationen vor.

In dem Training werden den Teilnehmern die wesentlichen Technologien und Prozesse zur Erkennung und Behebung von Cyberangriffen vorgestellt. Das erworbene Wissen wird jeweils im Anschluss anhand der eigenen Bewältigung von simulierten Live-Angriffen trainiert. Hierzu wird eine Arena eingesetzt, in der die Teilnehmer gefahrlos verschiedene Taktiken zur Abwehr und Behebung trainieren können. Insbesondere wird auch die fachbereichsübergreifende Zusammenarbeit adressiert. Die Übungen beinhalten sowohl technische Elemente als auch Elemente des Managements von Vorfällen, Notfällen und Krisen.

Die Master Class wird von einem Moderator ("White Team Trainer") durchgeführt und von einem Angreifer ("Red Team Trainer") begleitet.

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

Über Fast Lane



Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.



Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center



Weltweit vertreten
mit High-End-Trainingszentren
rund um den Globus



Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft,
Cisco, Google, NetApp, VMware



Praxiserfahrene Experten
mit insgesamt mehr als
19.000 Zertifizierungen

Deutschland

Fast Lane Institute for Knowledge Transfer GmbH

Tel. +49 40 25334610

info@flane.de / www.flane.de

Österreich

ITLS GmbH

(ITLS ist ein Partner von Fast Lane)

Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Schweiz

Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Tel. +41 44 8325080

info@flane.ch / www.flane.ch