CyberSec First Responder (CFR): Threat Detection & Response (CFR)

ID CFR **Preis** CHF 4'000.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

Dieser Kurs richtet sich in erster Linie an Fachleute für Cybersicherheit, die sich auf eine Tätigkeit zum Schutz von Informationssystemen vorbereiten oder diese derzeit ausüben, indem sie deren Verfügbarkeit, Integrität, Authentifizierung, Vertraulichkeit und Nichtabstreitbarkeit sicherstellen. Er eignet sich ideal für jene Funktionen innerhalb von bundesstaatlichen Vertragsunternehmen und Firmen des privaten Sektors, deren Auftrag oder strategische Ziele die Durchführung von Defensive Cyber Operations (DCO) oder DoD Information Network (DoDIN) und die Bearbeitung von Vorfällen erfordern. Dieser Kurs konzentriert sich auf das Wissen, die Fähigkeiten und die Fertigkeiten, die für die Verteidigung dieser Informationssysteme in einem Cybersicherheitskontext erforderlich sind, einschliesslich Schutz, Erkennung, Analyse, Untersuchung und Reaktionsprozesse.

Darüber hinaus stellt der Kurs sicher, dass alle Mitglieder eines IT-Teams - unabhängig von Grösse, Rang oder Budget - ihre Rolle bei der Cyberabwehr, der Reaktion auf Vorfälle und der Bearbeitung von Vorfällen verstehen.

Voraussetzungen

Damit Sie diesen Kurs erfolgreich absolvieren können, sollten Sie die folgenden Voraussetzungen erfüllen:

- Mindestens zwei Jahre (empfohlen) Erfahrung oder Ausbildung in der Computer-Netzwerksicherheitstechnologie oder einem verwandten Bereich.
- Die Fähigkeit oder Neugierde, Schwachstellen und Bedrohungen der Informationssicherheit im Rahmen des Risikomanagements zu erkennen.
- Grundlegende Kenntnisse der Konzepte und des betrieblichen Rahmens allgemeiner Sicherheitsvorkehrungen in Netzumgebungen. Zu den Schutzmassnahmen gehören unter anderem Firewalls, Intrusion Prevention Systeme und VPNs.
- Allgemeine Kenntnis der Konzepte und des operativen Rahmens allgemeiner Sicherheitsvorkehrungen in Computerumgebungen. Zu den Schutzmassnahmen gehören u. a. die grundlegende Authentifizierung und Autorisierung, Ressourcenberechtigungen und Anti-Malware-Mechanismen.
- Grundlegende Kenntnisse über einige der gängigen Betriebssysteme für Computerumgebungen.
- Grundlegende Kenntnisse einiger gängiger Konzepte für Netzwerkumgebungen, z. B. Routing und Switching.
- Allgemeine oder praktische Kenntnisse der wichtigsten TCP/IP-Netzwerkprotokolle, einschliesslich, aber nicht beschränkt auf TCP, IP, UDP, DNS, HTTP, ARP, ICMP und DHCP.

Kursziele

In diesem Kurs werden Sie Sicherheitsbedrohungen erkennen, bewerten, auf sie reagieren und sich vor ihnen schützen und eine System- und Netzwerksicherheitsanalyseplattform betreiben. Sie werden:

- Bewertung der Cybersicherheitsrisiken für das Unternehmen.
- Analysieren Sie die Bedrohungslandschaft.
- Analyse der verschiedenen Aufklärungsbedrohungen für Computer- und Netzwerkumgebungen.
- Analysieren verschiedener Angriffe auf Computer- und Netzumgebungen.
- Analysieren Sie verschiedene Techniken zur Nachbereitung von Angriffen.
- Bewertung der Sicherheitslage des Unternehmens durch Audits, Schwachstellenmanagement und Penetrationstests.
- Sammeln von Informationen zur Cybersicherheit aus verschiedenen netz- und hostbasierten Quellen.
- Analysieren Sie Protokolldaten, um Hinweise auf Bedrohungen und Vorfälle zu finden.
- Aktive Bestands- und Netzwerkanalyse zur Erkennung von Vorfällen.
- Reagieren Sie auf Cybersicherheitsvorfälle mit Eindämmungs-, Abschwächungs- und Wiederherstellungstaktiken.
- Untersuchung von Cybersicherheitsvorfällen mithilfe

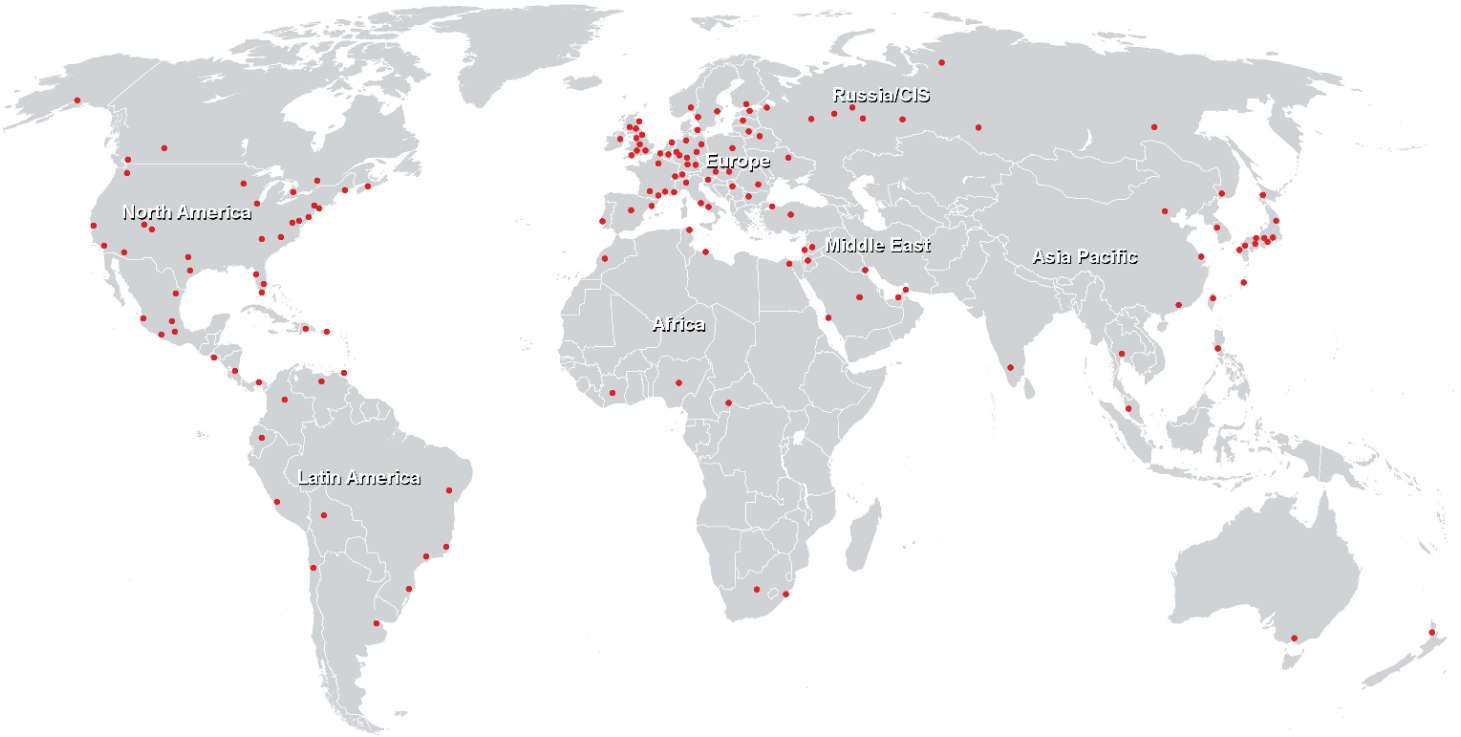
forensischer Analysetechniken.

Kursinhalt

- Bewertung des Cybersecurity-Risikos
- Analysieren der Bedrohungslandschaft
- Analyse von Aufklärungsbedrohungen für Computer- und Netzwerkumgebungen
- Analyse von Angriffen auf Computer- und Netzwerkumgebungen
- Analyse von Techniken nach Angriffen
- Bewertung der Sicherheitsposition der Organisation
- Sammeln von Cybersecurity Intelligence
- Analysieren von Protokolldaten
- Aktive Bestands- und Netzwerkanalyse durchführen
- Reaktion auf Cybersecurity-Vorfälle
- Untersuchung von Cybersecurity-Vorfällen

CyberSec First Responder (CFR): Threat Detection & Response (CFR)

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