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

ID CFR **Price** CHF 4,000.—(excl. VAT) **Duration** 5 days

Who should attend

This course is designed primarily for cybersecurity practitioners preparing for or who currently perform job functions related to protecting information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. It is ideal for those roles within federal contracting companies and private sector firms whose mission or strategic objectives require the execution of Defensive Cyber Operations (DCO) or DoD Information Network (DoDIN) operation and incident handling. This course focuses on the knowledge, ability, and skills necessary to provide for the defense of those information systems in a cybersecurity context, including protection, detection, analysis, investigation, and response processes.

In addition, the course ensures that all members of an IT team—regardless of size, rank, or budget—understand their role in the cyber defense, incident response, and incident handling process.

Prerequisites

To ensure your success in this course, you should meet the following requirements:

- At least two years (recommended) of experience or education in computer network security technology or a related field.
- The ability or curiosity to recognize information security vulnerabilities and threats in the context of risk management.
- Foundational knowledge of the concepts and operational framework of common assurance safeguards in network environments. Safeguards include, but are not limited to, firewalls, intrusion prevention systems, and VPNs.
- General knowledge of the concepts and operational framework of common assurance safeguards in computing environments. Safeguards include, but are not limited to, basic authentication and authorization, resource permissions, and anti-malware mechanisms.
- Foundation-level skills with some of the common operating systems for computing environments.
- Entry-level understanding of some of the common concepts for network environments, such as routing and switching.
- General or practical knowledge of major TCP/IP networking protocols, including, but not limited to, TCP, IP, UDP, DNS, HTTP, ARP, ICMP, and DHCP.

Course Objectives

In this course, you will identify, assess, respond to, and protect against security threats and operate a system and network security analysis platform. You will:

- Assess cybersecurity risks to the organization.
- Analyze the threat landscape.
- Analyze various reconnaissance threats to computing and network environments.
- Analyze various attacks on computing and network environments.
- Analyze various post-attack techniques.
- Assess the organization's security posture through auditing, vulnerability management, and penetration testing.
- Collect cybersecurity intelligence from various network-based and host-based sources.
- Analyze log data to reveal evidence of threats and incidents.
- Perform active asset and network analysis to detect incidents.
- Respond to cybersecurity incidents using containment, mitigation, and recovery tactics.
- Investigate cybersecurity incidents using forensic analysis techniques.

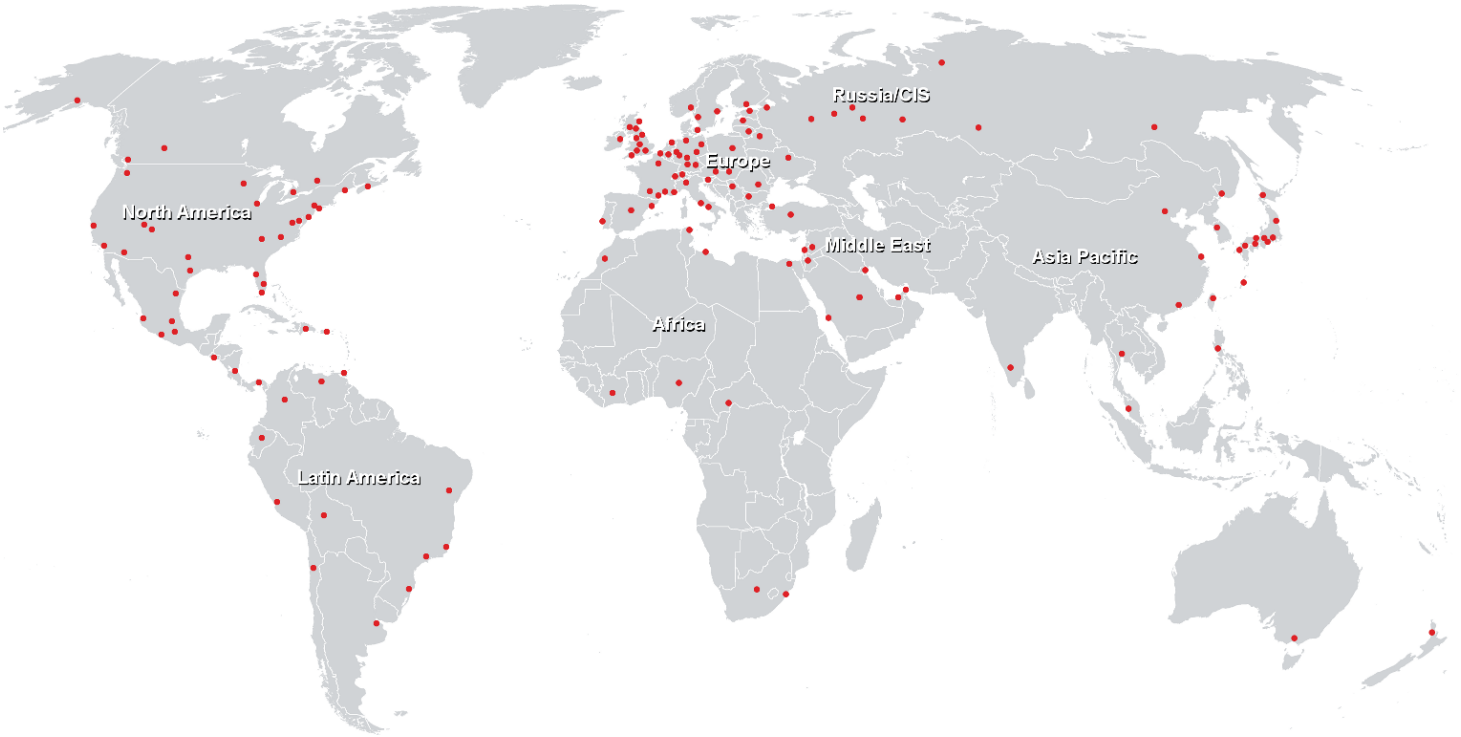
Course Content

- Assessing Cybersecurity Risk
- Analyzing the Threat Landscape
- Analyzing Reconnaissance Threats to Computing and Network Environments
- Analyzing Attacks on Computing and Network Environments

- Analyzing Post-Attack Techniques
- Assessing the Organization's Security Posture
- Collecting Cybersecurity Intelligence
- Analyzing Log Data
- Performing Active Asset and Network Analysis
- Responding to Cybersecurity Incidents
- Investigating Cybersecurity Incidents

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

Training Centres worldwide



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