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

ID CFR **Prix** CHF 4 000,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

Ideal for those with 2+ years of experience in IT or information security, CFR prepares cybersecurity professionals for performing numerous tasks within an organization. From developing secure networks to identifying breaches in real time, CFR equips professionals with the skills they need to keep the hackers out.

This course is also designed to assist students in preparing for the *CyberSec First Responder: Threat Detection and Response (Exam CFR-210)* certification examination. What you learn and practice in this course can be a significant part of your preparation.

In addition, this course can help students who are looking to fulfill DoD directive 8570.01 for information assurance (IA) training. This program is designed for personnel performing IA functions, establishing IA policies and implementing security measures and procedures for the Department of Defense and affiliated information systems and networks.

Pré-requis

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

- At least two years (recommended) of experience in computer network security technology or a related field.
- Recognize information security vulnerabilities and threats in the context of risk management.
- Operate at a foundational level some of the common operating systems for computing environments.
- Foundational 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.
- Operate at a foundational level some of the common concepts for network environments, such as routing and switching.
- 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 virtual private networks (VPNs).

You can obtain this level of skills and knowledge by taking the following courses or by passing the relevant exams:

- CompTIA® A+®: A Comprehensive Approach (Exams 200-801 and 220-802)
- CompTIA® Network+® (Exam N10-005)
- CompTIA® Security+® (Exam SY0-401)

Objectifs

In this course, you will develop, operate, manage, and enforce security capabilities for systems and networks. You will:

- Assess information security risk in computing and network environments.
- Create an information assurance lifecycle process.
- Analyze threats to computing and network environments.
- Design secure computing and network environments.
- Operate secure computing and network environments.
- Assess the security posture within a risk management framework.
- Collect cybersecurity intelligence information.
- Analyze collected intelligence to define actionable response.
- Respond to cybersecurity incidents.
- Investigate cybersecurity incidents.
- Audit secure computing and network environments.

Contenu

Lesson 1: Assessing Information Security Risk

- Identify the Importance of Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

Lesson 2: Analyzing the Threat Landscape

- Classify Threats and Threat Profiles
- Perform Ongoing Threat Research

Lesson 3: Analyzing Reconnaissance Threats to Computing and Network Environments

- Implement Threat Modeling
- Assess the Impact of Reconnaissance Incidents
- Assess the Impact of Social Engineering

Lesson 4: Analyzing Attacks on Computing and Network Environments

- Assess the Impact of System Hacking Attacks
- Assess the Impact of Web-Based Attacks
- Assess the Impact of Malware
- Assess the Impact of Hijacking and Impersonation Attacks
- Assess the Impact of DoS Incidents
- Assess the Impact of Threats to Mobile Security
- Assess the Impact of Threats to Cloud Security

Lesson 5: Analyzing Post-Attack Techniques

- Assess Command and Control Techniques
- Assess Persistence Techniques
- Assess Lateral Movement and Pivoting Techniques
- Assess Data Exfiltration Techniques
- Assess Anti-Forensics Techniques

Lesson 6: Evaluating the Organization's Security Posture

- Conduct Vulnerability Assessments
- Conduct Penetration Tests on Network Assets
- Follow Up on Penetration Testing

Lesson 7: Collecting Cybersecurity Intelligence

- Deploy a Security Intelligence Collection and Analysis Platform
- Collect Data from Network-Based Intelligence Sources
- Collect Data from Host-Based Intelligence Sources

Lesson 8: Analyzing Log Data

- Use Common Tools to Analyze Logs
- Use SIEM Tools for Analysis
- Parse Log Files with Regular Expressions

Lesson 9: Performing Active Asset and Network Analysis

- Analyze Incidents with Windows-Based Tools
- Analyze Incidents with Linux-Based Tools
- Analyze Malware
- Analyze Indicators of Compromise

Lesson 10: Responding to Cybersecurity Incidents

- Deploy an Incident Handling and Response Architecture
- Mitigate Incidents
- Prepare for Forensic Investigation as a CSIRT

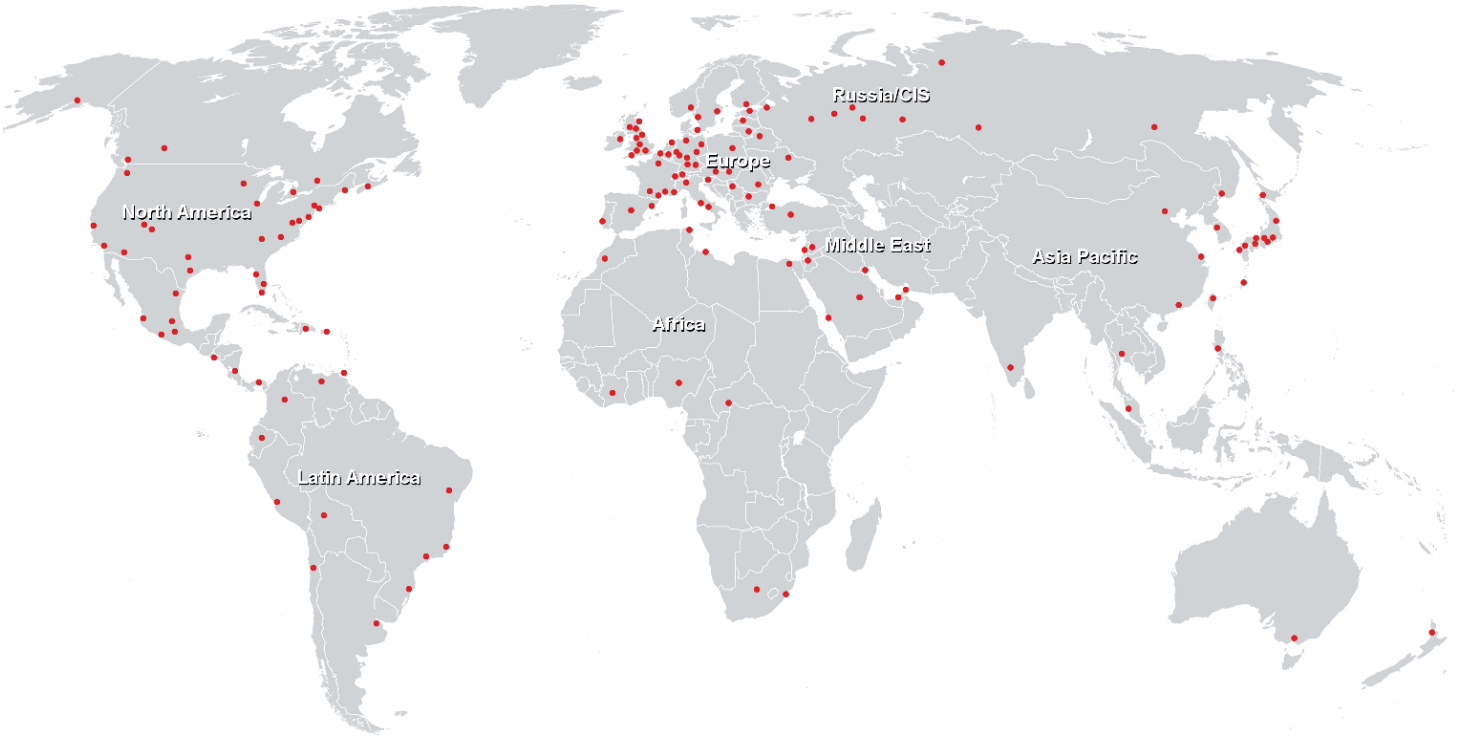
Lesson 11: Investigating Cybersecurity Incidents

- Apply a Forensic Investigation Plan
- Securely Collect and Analyze Electronic Evidence
- Follow Up on the Results of an Investigation

- Appendix A: Mapping Course Content to CyberSec First Responder (Exam CFR-210)
- Appendix B: List of Security Resources

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

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, https://www.flane.ch