EC-Council Certified Threat Intelligence Analyst (CTIA)

ID CTIA **Prix** CHF 2 950,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

- Cyber Threat Intelligence Analyst
- Cyber Threat Hunter
- Cyber Threat Intelligence Associate/Researcher/Consultant
- Cybersecurity/Information Security Threat Intelligence Analyst
- Cyber Threat Intelligence Engineer/Specialist/Lead/Manager
- SOC Threat Intelligence Analyst
- Principal Cybercrime Threat Intelligence Analyst
- Threat Management Associate Director
- Project Manager/Director of Threat Intelligence

Pré-requis

- Any Mid-level to high-level cybersecurity professionals with a minimum of 3 years of experience.
- Individuals with EC-Council's recognized C|EH and C|ND certifications can enroll for this course.

Objectifs

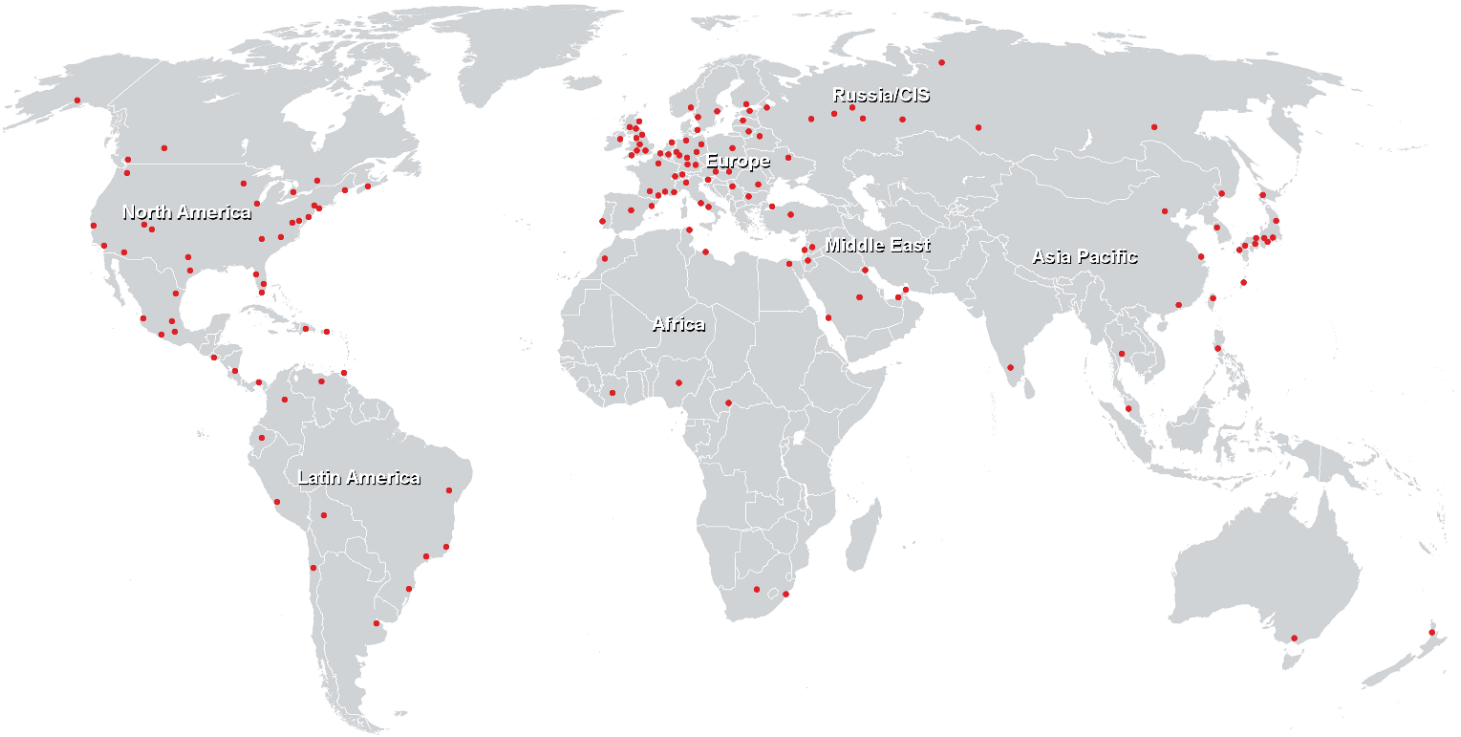
- Fundamentals of threat intelligence (Threat intelligence types, lifecycle, strategy, capabilities, maturity model, frameworks, platforms, etc.)
- Various cyber security threats and attack frameworks (Advanced Persistent Threats, Cyber Kill Chain Methodology, MITRE ATT&CK Framework, Diamond Model of Intrusion Analysis, etc.)
- Various steps involved in planning a threat intelligence program (Requirements, planning, direction, and review)
- Different types of threat intelligence feeds, sources, data collection methods
- Threat intelligence data collection and acquisition through Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Indicators of Compromise (IoCs), Malware Analysis, and Python Scripting
- Threat intelligence data processing and exploitation
- Threat data analysis techniques (Statistical Data Analysis, Analysis of Competing Hypotheses (ACH), Structured Analysis of Competing Hypotheses (SACH), etc.)
- Complete threat analysis process, which includes threat modeling, fine-tuning, evaluation, and runbook and knowledge base creation
- How to create and share threat intelligence reports
- Threat intelligence sharing and collaboration using Python scripting
- Different platforms, acts, and regulations for sharing intelligence
- How to perform threat intelligence in a cloud environment
- Fundamentals of threat hunting (Threat hunting types, process, loop, methodology, etc.)
- Threat-hunting automation using Python scripting
- Threat intelligence in SOC operations, incident response, and risk management

Contenu

- Module 01: Introduction to Threat Intelligence
- Module 02: Cyber Threats and Attack Frameworks
- Module 03: Requirements, Planning, Direction, and Review
- Module 04: Data Collection and Processing
- Module 05: Data Analysis
- Module 06: Intelligence Reporting and Dissemination
- Module 07: Threat Hunting and Detection
- Module 08: Threat Intelligence in SOC Operations, Incident Response, and Risk Management

EC-Council Certified Threat Intelligence Analyst (CTIA)

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