EC-Council Certified Incident Handler (ECIH)

ID ECIH **Price** on request **Duration** 3 days

Prerequisites

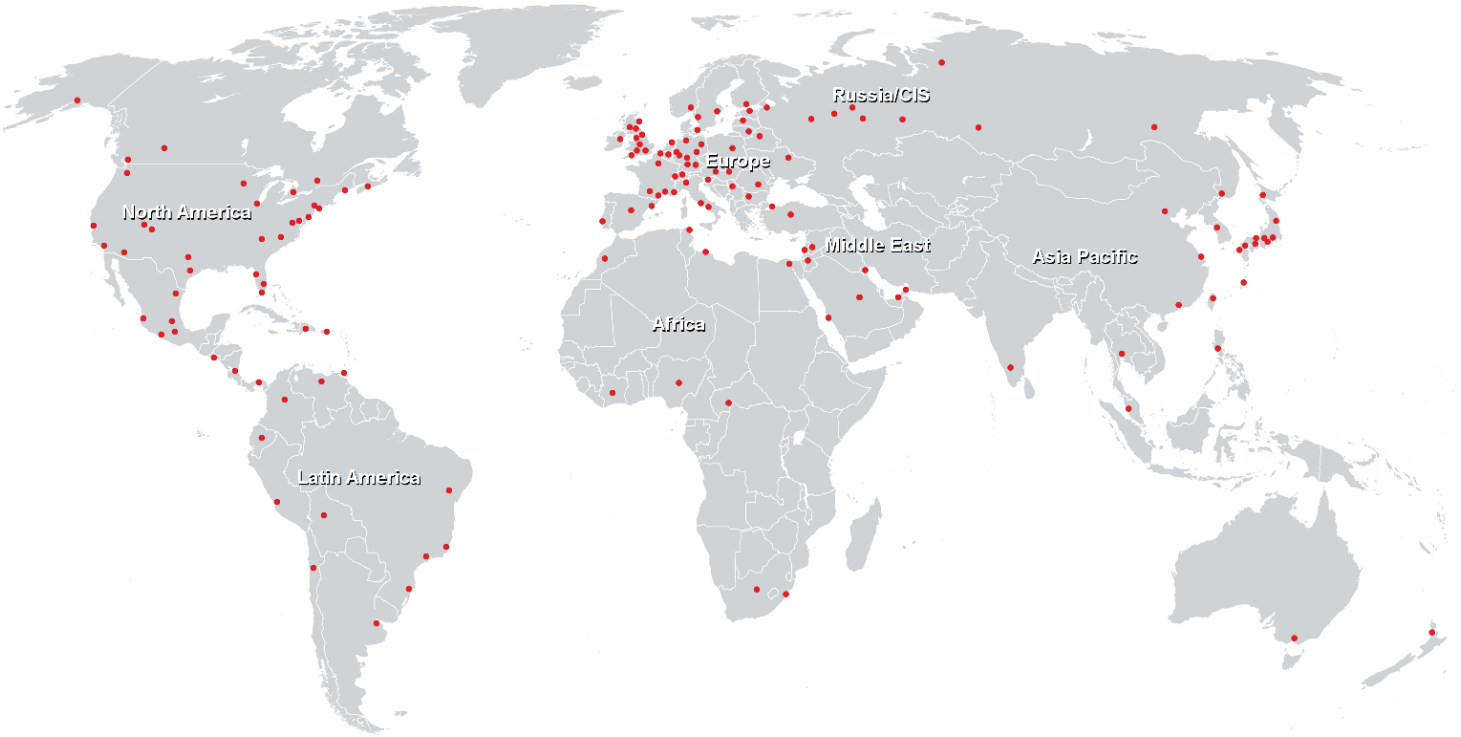
To qualify for the E|CIH program, one must have at least 3 years of experience working as a cyber security professional.

Course Objectives

- Key issues plaguing the information security world
- Various types of cybersecurity threats, attack vectors, threat actors, and their motives, goals, and objectives of cybersecurity attacks
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- Fundamentals of information security concepts (vulnerability assessment, risk management, cyber threat intelligence, threat modeling, and threat hunting)
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- Fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response, and incident response automation and orchestration)
- Different incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Various steps involved in planning incident handling and response program (planning, recording and assignment, triage, notification, containment, evidence gathering and forensic analysis, eradication, recovery, and post-incident activities)
- Importance of first response and first response procedure (evidence collection, documentation, preservation, packaging, and transportation)
- How to handle and respond to different types of cybersecurity incidents in a systemic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

EC-Council Certified Incident Handler (ECIH)

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