

EC-Council Certified Threat Intelligence Analyst (CTIA)

ID CTIA Price on request Duration 3 days

Who should attend

- Ethical Hackers
- Security Practitioners, Engineers, Analysts, Specialist, Architects, Managers
- Threat Intelligence Analysts, Associates, Researchers, Consultants
- Threat Hunters
- SOC Professionals
- Digital Forensic and Malware Analysts
- Incident Response Team Members
- Any mid-level to high-level cybersecurity professionals with a minimum of 3-5 years of experience.
- Individuals from the information security profession and who want to enrich their skills and knowledge in the field of cyber threat intelligence.
- Individuals interested in preventing cyber threats.

Course Objectives

- Key issues plaguing the information security world
- Importance of threat intelligence in risk management, SIEM, and incident response
- Various types of cyber threats, threat actors and their motives, goals, and objectives of cybersecurity attacks
- Fundamentals of threat intelligence (including threat intelligence types, lifecycle, strategy, capabilities, maturity model, frameworks, etc.)
- Cyber kill chain methodology, Advanced Persistent Threat (APT) lifecycle, Tactics, Techniques, and Procedures (TTPs), Indicators of Compromise (IoCs), and pyramid of pain
- Various steps involved in planning a threat intelligence program (Requirements, Planning, Direction, and Review)
- Different types of data feeds, sources, and data collection methods
- Threat intelligence data collection and acquisition through Open Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Indicators of Compromise (IoCs), and malware analysis
- Bulk data collection and management (data processing, structuring, normalization, sampling, storing, and visualization)
- Different data analysis types and techniques including 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, runbook, and knowledge base creation
- Different data analysis, threat modeling, and threat intelligence tools
- Threat intelligence dissemination and sharing protocol including dissemination preferences, intelligence collaboration, sharing rules and models, TI exchange types and architectures, participating in sharing relationships, standards, and formats for sharing threat intelligence
- Creating effective threat intelligence reports
- Different threat intelligence sharing platforms, acts, and regulations for sharing strategic, tactical, operational, and technical intelligence

Course Content

Introduction to Threat Intelligence

- Understanding Intelligence
- Understanding Cyber Threat Intelligence
- What Organizations and Analysts Expect?
- Overview of Threat Intelligence Lifecycle and Frameworks

Cyber Threats and Kill Chain Methodology

- Understanding Cyber Threats
- Understanding Advanced Persistent Threats (APTs)
- Understanding Cyber Kill Chain
- Understanding Indicators of Compromise (IoCs)

Requirements, Planning, Direction, and Review

- Understanding Organization's Current Threat Landscape
- Understanding Requirements Analysis
- Planning Threat Intelligence Program
- Establishing Management Support
- Building a Threat Intelligence Team
- Overview of Threat Intelligence Sharing
- Reviewing Threat Intelligence Program

Data Collection and Processing

- Overview of Threat Intelligence Data Collection
- Overview of Threat Intelligence Collection Management

EC-Council Certified Threat Intelligence Analyst (CTIA)

- Overview of Threat Intelligence Feeds and Sources
- Understanding Threat Intelligence Data Collection and Acquisition
- Understanding Bulk Data Collection
- Understanding Data Processing and Exploitation

Data Analysis

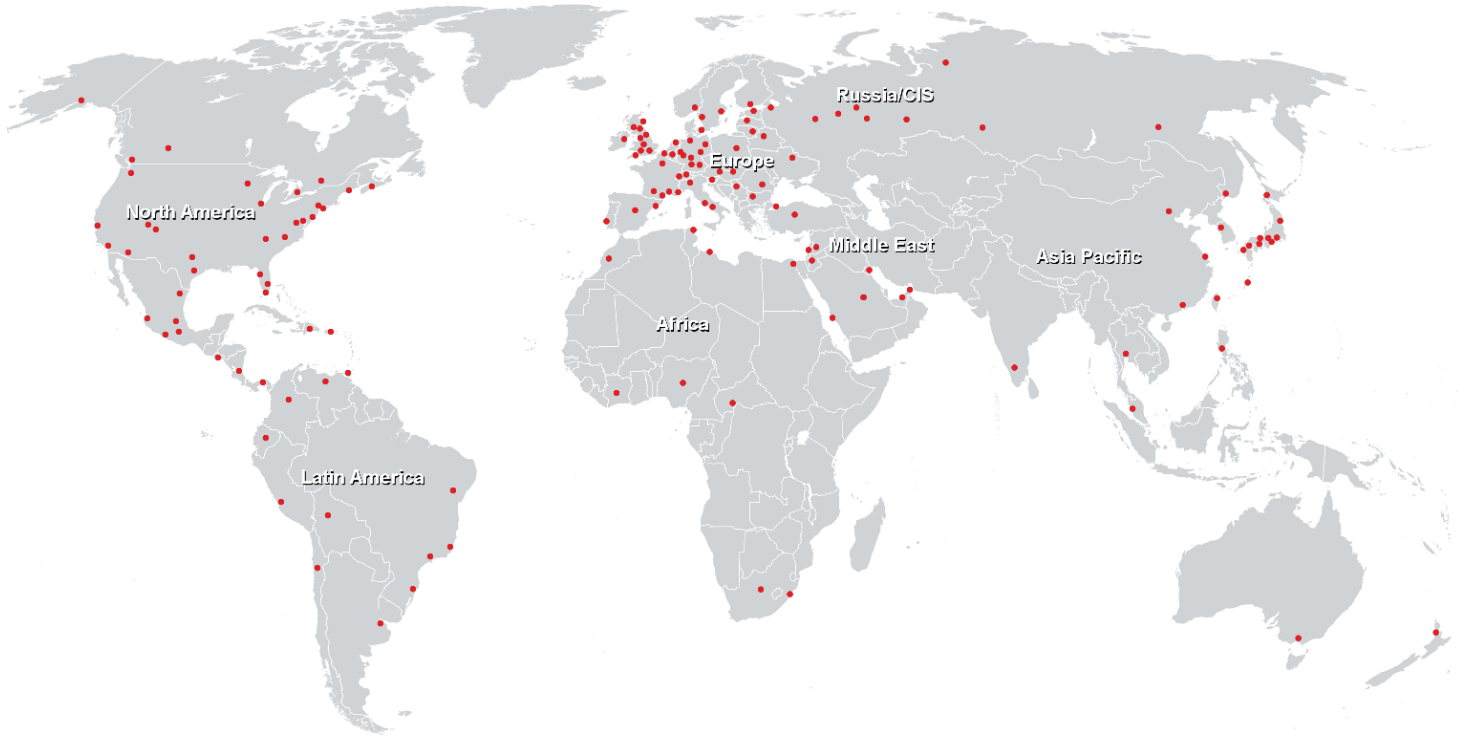
- Overview of Data Analysis
- Understanding Data Analysis Techniques
- Overview of Threat Analysis
- Understanding Threat Analysis Process
- Overview of Fine-Tuning Threat Analysis
- Understanding Threat Intelligence Evaluation
- Creating Runbooks and Knowledge Base
- Overview of Threat Intelligence Tools

Intelligence Reporting and Dissemination

- Overview of Threat Intelligence Reports
- Introduction to Dissemination
- Participating in Sharing Relationships
- Overview of Sharing Threat Intelligence
- Overview of Delivery Mechanisms
- Understanding Threat Intelligence Sharing Platforms
- Overview of Intelligence Sharing Acts and Regulations
- Overview of Threat Intelligence Integration

EC-Council Certified Threat Intelligence Analyst (CTIA)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>