# EC-Council Certified Threat Intelligence Analyst (CTIA)

| Price | Duration | Delivery Methods |
| --- | --- | --- |
| $2,097.00 | 3 Days | VILT, Private Group |

Do you possess an analytical mind? Is critical thinking a part of who you are? Then you've come to the right place. A Certified Threat Intelligence Analyst (CTIA) acts as a force multiplier for organizations looking to reinforce their cyber defense security measures. Threat intelligence is akin to what conventional intelligence agencies across the world engage in to perceive and neutralize threats before any harm can be done. As a certified threat intelligence analyst, you'll be at the vanguard of your organization's cybersecurity ecosystem, keeping a 360 degree vigil on existing and foreseen/unforeseen threats. The Certified Threat Intelligence Analyst (CTIA) program is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe. The aim is to help organizations hire qualified cyber intelligence trained professionals to identify and mitigate business risks by converting unknown internal and external threats into quantifiable threat entities and stop them in their tracks. Much like a 'hunter-killer' team, you'll be deployed as a 'Blue Team' operative, tasked with threat identification, and asked to employ the tools at hand to thwart active and potential cyberattacks.

## Who Should Attend

- Ethical Hackers
- Security Practitioners, Engineers, Analysts, Specialist, Architects, and 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 2 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 in the InfoSec domain.
- Importance of threat intelligence in risk management, SIEM, and incident response.
- Various cyber threats, threat actors, and their objectives for cyberattacks.
- Fundamentals of threat intelligence (including threat intelligence types, life cycle, strategy, capabilities, maturity model, frameworks, etc.)
- Cyber kill chain methodology, Advanced Persistent Threat (APT), Indicators of Compromise (IoCs), and the pyramid of pain.
- Threat intelligence program steps (Requirements, Planning, Direction, Review).
- 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).
- Data analysis types and techniques including Statistical Data Analysis, Structured Analysis of Competing Hypotheses (SACH), etc.
- Complete threat analysis process including threat modeling, fine-tuning, evaluation, runbook, and knowledge base creation.
- Different data analysis, threat modeling, and threat intelligence tools.
- Creating effective threat intelligence reports.
- Different threat intelligence sharing platforms, acts, and regulations for sharing strategic, tactical, operational, and technical intelligence.

## Agenda

### 1 - INTRODUCTION TO THREAT INTELLIGENCE

- Understanding Intelligence
- Understanding Cyber Threat Intelligence
- Overview of Threat Intelligence Lifecycle and Frameworks

### 2 - CYBER THREATS AND KILL CHAIN METHODOLOGY

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

### 3 - 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

## 4 - DATA COLLECTION AND PROCESSING

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

## 5 - 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

## 6 - 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