EC-Council

CTIA
Certified Threat Intelligence Analyst

# CERTIFIED THREAT INTELLIGENCE ANALYST

**PROGRAM BROCHURE**

# Predictive Capabilities for Proactive Defense!

Cyber threat incidents have taken a drastic upsurge in recent times. Today, most organizations are concerned about the loss of personally identifiable information to targeted cyber-attack, malware campaign, zero-day vulnerabilities, and ransomware attacks. WannaCry and Petya/NotPetya ransomware attacks in 2017 reminded the entire global cybersecurity community that cyber threats can surprise organizations at any moment from any unexpected sources .

## Threat Intelligence


"Threat intelligence" (TI) is evidence-based knowledge - including context, mechanisms, indicators, implications, and actionable advice — about an existing or emerging menace or hazard to IT or information assets. It can be used to inform decisions regarding the subject's response to that menace or hazard. - Gartner

**As described by the 'National Cyber Security Center' of United Kingdom**

Some organizations have the resources and skills to protect their IT infrastructure against such threats; however, there are still many organizations that do not have the capacity to do so. It does not matter if an organization installs a state-of-the-art security software solution or if it spends thousands of dollars on security tools, the fact remains that no organization is completely secure. An organization must be aware of attack trends in order to know the threats they are likely to face, and this is where threat intelligence comes into play.

Certified Threat Intelligence Analyst (C|TIA) allows students to enhance their skills in building effective organizational cyber threat intelligence.

Cyber threat intelligence includes reliable data collection from numerous sources, context relevant analysis, production of useful intelligence, and distributing the relevant information to stakeholders. Organizations can upgrade their defenses and create countermeasures by acquiring intelligence related to the Tactics, Techniques, and Procedures (TTPs) of potential threat actors. A threat intelligence analyst should have specialized skills and knowledge to competently understand the methodology and mindset of modern attackers deploy the threat intelligence accordingly.

# Course Description

Certified Threat Intelligence Analyst (C|TIA) is a training and credentialing program designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive specialist-level program that teaches a structured approach for building effective threat intelligence.

The program was based on a rigorous Job Task Analysis (JTA) of the job roles involved in the field of threat intelligence. This program differentiates threat intelligence professionals from other information security professionals. It is a highly interactive, comprehensive, standards-based, intensive 3-day training program that teaches information security professionals to build professional threat intelligence.

In the ever-changing threat landscape, C|TIA is an highly essential program for those who deal with cyber threats on a daily basis. Organizations today demand a professional level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional level programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

C|TIA is a method-driven program that uses a holistic approach, covering concepts from planning the threat intelligence project to building a report to disseminating threat intelligence. These concepts are highly essential while building effective threat intelligence and, when used properly, can secure organizations from future threats or attacks.

This program addresses all the stages involved in the Threat Intelligence Life Cycle, with This attention to a realistic and futuristic approach makes C|TIA one of the most comprehensive threat intelligence certifications on the market today. This program provides the solid, professional knowledge that is required for a career in threat intelligence, and enhances your skills as a Threat Intelligence Analyst, increasing your employability. It is desired by most cybersecurity engineers, analysts, and professions from around the world and is respected by hiring authorities.

# Why Organizations Need A Threat Intelligence Team

Only 1 in 10 organizations say that they are likely to detect an attack.

Traditional approaches to malicious attacks are slowly dying out, with new malware formed every four seconds. However, many organizations today still follow the basic, traditional methods to address these evolving techniques.

Reacting to threats is extremely important but reacting also signifies that the damage is already done. Having a threat intelligence analyst will give organizations the chance to fight the unforeseen battles that are constantly arising in the cyber world.

A skilled threat intelligence analyst will be able to gather large amounts of relevant threat information from a multitude of intelligence sources which will then be analyzed to provide threat intelligence that accurately predicts the potential threats that an organization may encounter.

The modern-day security scenario calls for the implementation of cyber threat intelligence as it helps organizations keep up with evolving threats and malware to defend rather than reconstruct!

# Who is it for?

## Target Audience

- 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 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.

## Suggested Duration

| | |
|---|---|
| 3 Days (9:00 AM to 5:00 PM) | 24 hours |

## Certification:

The C|TIA exam can be challenged after the completion of the complete, official C|TIA training program. Candidates that successfully pass the exam will receive their C|TIA certificate and membership privileges. Members are required to adhere to the policies of EC-Council's Continuing Education Policy.

## Exam Details

| | |
|---|---|
| **Exam Title**<br>Certified Threat Intelligence Analyst | **Exam Code**<br>312-85 |
| **Number of Questions**<br>50 | **Duration**<br>2 hours |
| **Availability**<br>EC-Council Exam Portal | **Test Format**<br>Multiple Choice |
| **Passing Score**<br>70% | |

## Eligibility Criteria

To be eligible to challenge the C|TIA Exam, the candidate must either:

- Attend official EC-Council C|TIA training through an accredited EC-Council Partner (Accredited Training Center, iWeek, iLearn) (All candidates are required to pay the USD100 application fee unless your training fee already includes this) or
- Submit an application showing a minimum of 2 years working experience in information security (All candidates are required to pay USD 100 as a non-refundable application fee)

# Top 10 Critical Components of C|TIA

1. **100% compliance to NICE 2.0 and CREST frameworks**

   C|TIA maps 100 percent to the National Initiative for Cybersecurity Education (NICE) in the category "Analyze" and specialty area "Threat/Warning Analyst (TWA)", as well as the "CREST Certified Threat Intelligence Manager (CC TIM)."

2. **Focus on developing skills for performing various types of threat intelligence**

   It focuses on developing the skills to perform different types of threat intelligence including strategic, operational, tactical, and technical threat intelligence for a particular organization.

3. **Emphasis on various data collection techniques from multiple sources and feeds**

   It emphasizes various data collection techniques from various sources and feeds. It allows students to employ different data collection strategies to collect relevant threat information.

4. **Emphasis on collection, creation, and dissemination of Indicators of Compromise (IoCs) in various formats**

   C|TIA discusses Indicators of Compromise (IoCs) indetail, including internal and external IoCs. It illustrates how to acquire these IoCs from various sources. IoCs are a good source of information about cyber threats and an organization can easily detect cyber-attacks and respond in time by monitoring IoCs. C|TIA elaborately explains how to create and disseminate these IoCs.

5. **Focus on intense malware analysis to collect adversary data and pivot off of it**

   It explains in detail how to reverse engineer malware and pivot off of it in order to determine the origin, functionality, and potential impact of malware as well as determine the threat actor. This is a crucial skill required for threat intelligence analyst.

6. **Focus on a structured approach for performing threat analysis and threat intelligence evaluation**

Analyzing the collected threat data and evaluating the required threat intelligence from the analysis process is one of the crucial steps for extracting threat intelligence. C|TIA discusses a structured approach that can be employed by an analyst for performing threat analysis and also threat modeling. This program also illustrates how to fine-tune the analysis process in order to filter out unnecessary information and extract effective intelligence. C|TIA also discuss different types of threat intelligence evaluation techniques for acquiring desired intelligence.

7. **Focus on various techniques for threat intelligence reporting and dissemination**

   C|TIA emphasizes the creation of efficient threat intelligence reports. It describes building blocks for threat intelligence sharing along with different sharing rules and models. It explains the best practices for sharing TI and also discuss different intelligence sharing acts and regulations.

8. **Hands-on program**

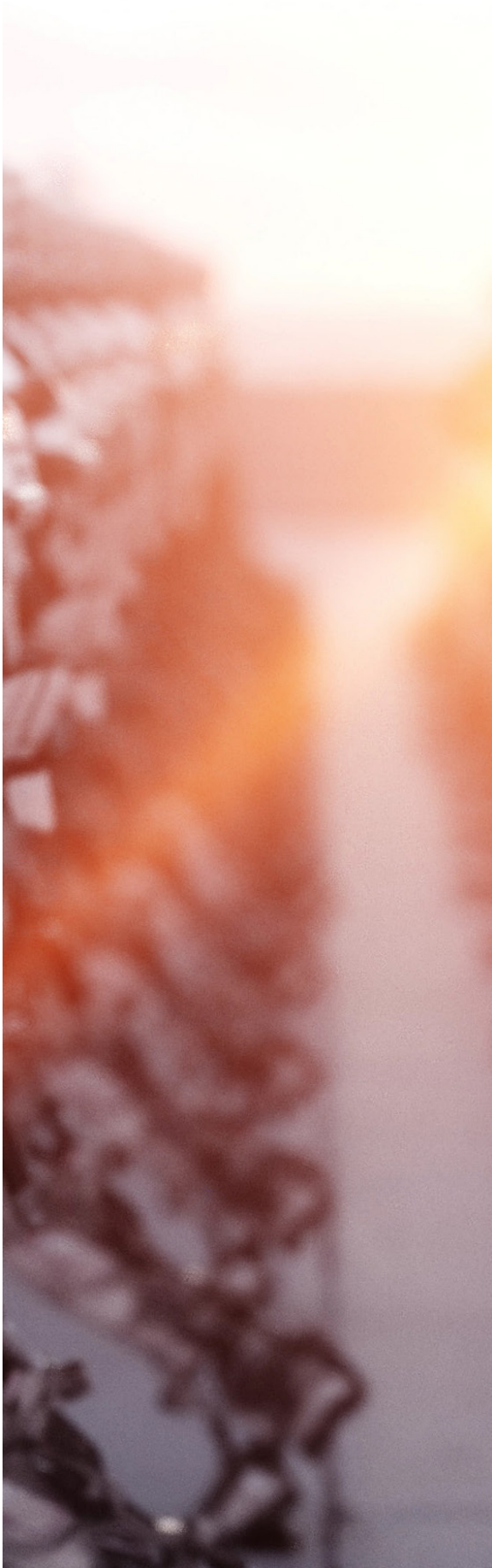
   More than 40 percent of class time is dedicated to the learning of practical skills, and this is achieved through EC-Council labs. Theory to practice ratio for C|TIA program is 60:40, providing students with a hands-on experience of the latest threat intelligence tools, techniques, methodologies, frameworks, scripts, etc. C|TIA comes integrated with labs to emphasize the learning objectives.

9. **Lab environment simulates a real-time environment**

   The C|TIA lab environment consists of the latest operating systems including Windows 10 and Kali Linux for planning, collecting, analyzing, evaluating, and disseminating threat intelligence.

10. **Covers latest threat intelligence tools, platforms, and frameworks**

    The C|TIA course includes a library of tools, platforms, and frameworks across different operation platforms that are required by security professionals to extract effective organizational threat intelligence. This provides a wider option to students than any other program on the market.



## Course Outline

| | |
|---|---|
| 01 | Introduction to Threat Intelligence |
| 02 | Cyber Threats and Kill Chain Methodology |
| 03 | Requirements, Planning, Direction, and Review |
| 04 | Data Collection and Processing |
| 05 | Data Analysis |
| 06 | Intelligence Reporting and Dissemination |

# Learning Objectives of C|TIA Program

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

EC-Council

www.eccouncil.org