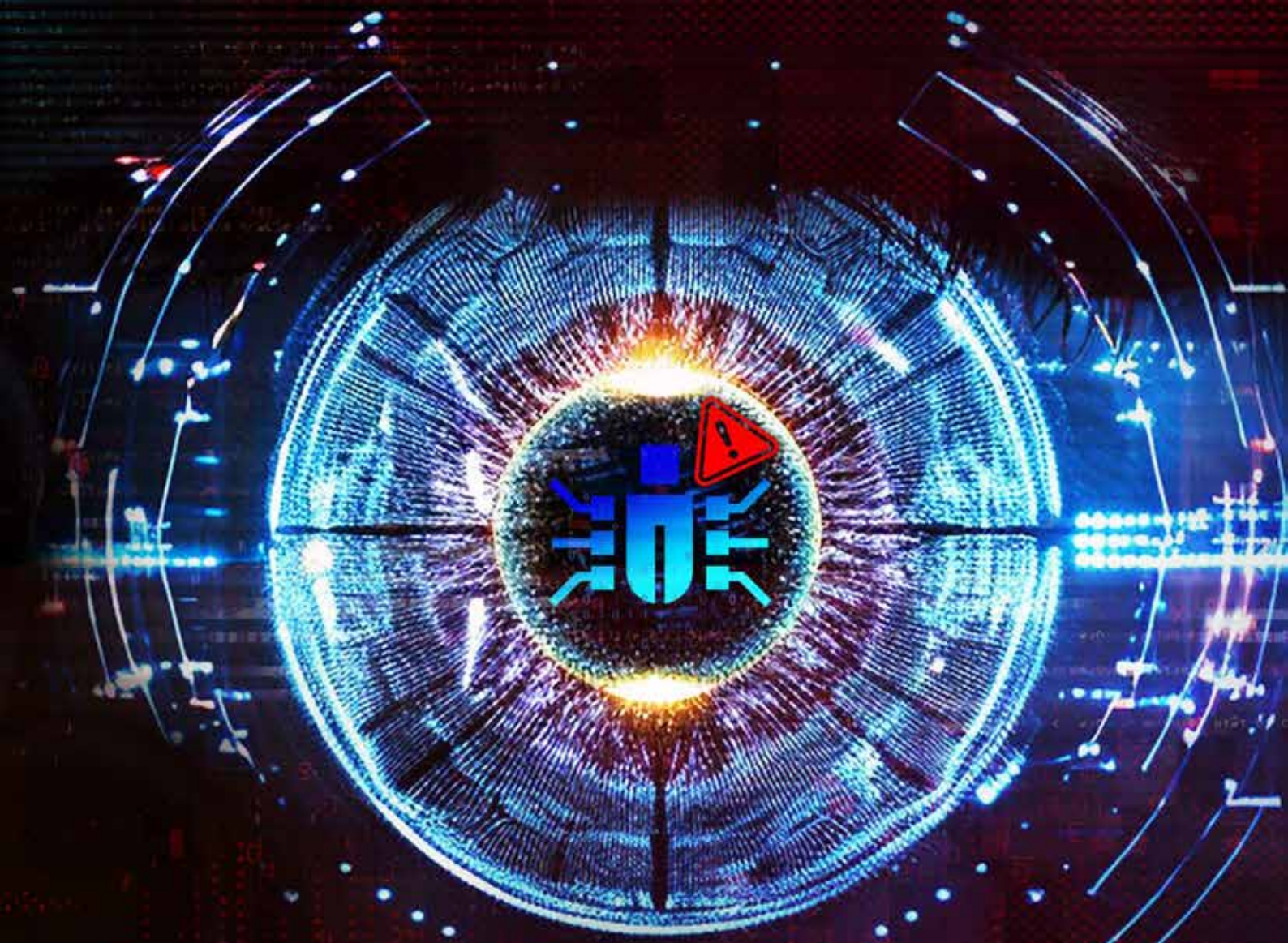
C|TIA
Certified | Threat Intelligence Analyst

ACCENTREX GLOBAL

EC-Council
Building A Culture Of Security



MASTER PREDICTIVE

THREAT INTELLIGENCE

FOR

PROACTIVE DEFENSE

Plan — Collect — Analyze — Disseminate

C|TIA: The Credential that Sets Gold Standard in Developing Global Threat Intelligence Skills, For Professionals Worldwide into the Ranks of the Elite.

Why is Threat Intelligence Crucial for Any Organization?

Problem enterprises face today:

Complex Cyberattacks:

As per BlackBerry® Cybersecurity solutions, threat actors deployed an average of **11.5 attacks per minute** between March and May 2023, including 1.7 novel malware samples per minute.

SonicWall reported that over 270,228 new malware variants were discovered in 2022.

Lack of skills:

According to the Vulcan Gartner Peer Insights Report, 73% of cybersecurity professionals indicated a "lack of skills" as their biggest threat intelligence challenge.

Solution enterprises need to stay secure:

- Identifying threats before they strike
- Adopting a proactive defense strategy
- Effectively detecting, responding, and mitigating focused and targeted threats

In short, organizations need cybersecurity professionals with appropriate threat intelligence skills to remediate attacks!

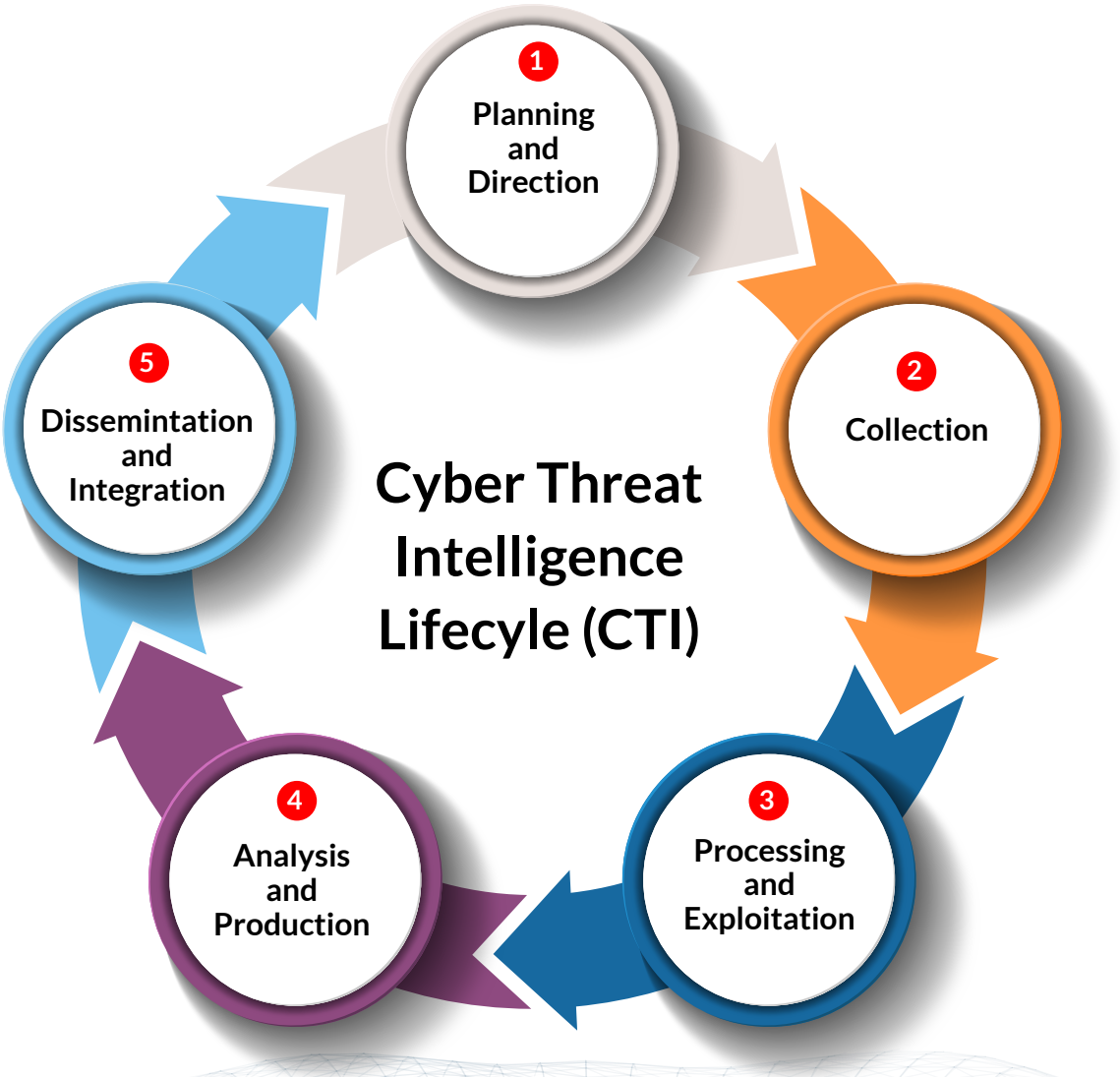
What is the Certified Threat Intelligence Analyst Program?

EC-Council's Certified Threat Intelligence Analyst (C|TIA) Certification is a comprehensive specialist-level professional program focused on the ever-evolving domain of threat intelligence. The program is designed for individuals involved in collecting, analyzing, and disseminating threat intelligence information.

C|TIA covers various topics, including the fundamentals of threat intelligence, the use of threat intelligence tools and techniques, and the development of a threat intelligence program. This course focuses on refining data and information into actionable intelligence that can be used to prevent, detect, and monitor cyber-attacks. It addresses all stages involved in the threat intelligence lifecycle, and this attention toward a realistic and futuristic approach makes it one of the most comprehensive threat intelligence certifications in the market today.

The program provides credible professional insights required for a successful threat intelligence career and enhances your overall skills, thus increasing your employability. It is desired by most cybersecurity engineers, analysts, and professionals globally and is respected by hiring authorities. Ideal for individuals working in information security, network security, incident response, and other related fields. Mastering skills and earning this certification can help enhance threat intelligence operations and investments for cybersecurity individuals and teams.

C|TIA Program: A Comprehensive and Structured Focus On Cyber Threat Intelligence Lifecycle (CTI)



C|TIA Course Modules:

1. **Introduction** to Threat Intelligence
2. **Cyber** Threats and Attack Frameworks
3. **Requirements,** Planning, Direction, and Review
4. **Data** Collection and Processing
5. **Data** Analysis
6. **Intelligence** Reporting and Dissemination
7. **Threat** Hunting and Detection
8. **Threat** Intelligence in SOC Operations, Incident Response, and Risk Management

What Will You Learn?

- Fundamentals of threat intelligence (Threat intelligence types, lifecycle, strategy, capabilities, maturity model, frameworks, platforms, etc.)
- Various cybersecurity 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
- 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

Key Features and Critical Components of C|TIA

01

Acquire a structured focus on the complete

Cyber Threat Intelligence (CTI) Lifecycle

1. Planning and Direction
2. Collection
3. Analysis and Production
4. Dissemination and Integration

02

Gain Skills in

4 Types of Threat Intelligence

1. Strategic 2. Operational
3. Tactical 4. Technical

03

800+

pages of the comprehensive student manual

04

350+

pages of lab manual covering detailed lab scenarios and instructions

05

200+

threa intelligence tools

06

27 hands-on labs

with real-life networks and platforms to emphasize the learning objectives

07

100%

compliance with **NICE Special Publication 800-181** Cybersecurity Workforce Framework and **CREST Certified Threat Intelligence Manager (CCTIM)** Frameworks

08

Structured

approach for performing data analysis

09

Lab intensive program:

40% of the training time is dedicated to labs

10

Threat intelligence

data collection and acquisition from various feeds and sources

11

Learn various

cybersecurity threats and attack frameworks (Advanced Persistent Threats, Cyber Kill Chain Methodology, MITRE ATT&CK Framework, Diamond Model of Intrusion Analysis, etc.)

Advantages of the CTIA Program

1. Gain skills for performing various types of threat intelligence
2. Learn various data collection techniques from multiple sources and feeds
3. Emphasis on collection, creation, and dissemination of Indicators of Compromise (IoCs) in various formats
4. Gain proficiency in developing a structured approach for performing threat analysis and threat intelligence evaluation
5. Learn various techniques for threat intelligence reporting and dissemination
6. Know the latest threat intelligence tools/platforms and frameworks
7. Know how to perform threat intelligence through Python Scripting
8. Gain skills in threat hunting and detection
9. Learn threat intelligence in SOC Operations, Incident Response, and Risk Management
10. Enhance your threat intelligence skills in the cloud environment
11. Based on a comprehensive industry-wide Job Task Analysis (JTA)

Training and Exam Details

Training Details:

iLearn (Self-Study)

This solution is an asynchronous, self-study environment in a video streaming format.

iWeek (Live Online)

This solution is a live, online, instructor-led training course.

Training Partner (In Person)

This solution offers "in-person" training so what you can benefit from collaborating with your peers and gaining real-world led by expert, certified instructors.

Exam Details:

Exam Code:	Number of Questions:	Duration:	Availability:	Test Format:
312-38	**50**	**2 hours**	**EC-Council Exam Portal**	**Multiple Choice**

Job Roles with C|TIA

- Cyber Threat Intelligence Analyst
- Cyber Threat Hunter
- Cyber Threat Intelligence Associate/Researcher/Consultant
- Cyber Security/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

Who Can Apply?

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

Salaries

The average threat intelligence analyst salary in the USA is $120,150

Why Do Top Cybersecurity Professionals Across the Globe Find C|TIA the Most Desirable Cyber Threat Intelligence Program

The C|TIA program is unique, and I could not find any other certification in the same area. I enjoyed the various insights into what threat intelligence is all about, how to gather the various sources of information and ways to correlate all this information to form a credible source regarding potential cyberattacks. C|TIA program, being a niche area on its own, is also very much related to many other cybersecurity practices.

23 Years Cybersecurity Trainer / Manager

Bachelor's Degree In Computer Science Diploma In Cyber Security

JOHN LIM
Singapore

14 years ago, I joined the United States Marine Corps as an All Source Intelligence Analyst. I now work for Clear Ridge Defense, a National Defense contractor alongside DoD and government agency in supporting missions and operations globally.

I appreciate three key aspects of this program. Firstly, its methodical approach allows us to address potential problems proactively, especially those stemming from unfamiliar methods. Secondly, the program's currency is commendable. The hard work invested in certifications is evident through the current and up-to-date problem sets and tools provided, fostering a forward-thinking mindset. Lastly, the lab environments are enjoyable. The simulation, combined with a relaxed setting, enables individuals to learn at their own pace, making it a valuable training ground when executed effectively – and C|TIA labs achieved just that.

WADE SPEAKS
USA
Senior Cyber Fusion Analyst
Clear Ridge Defense, a National Defense contractor

I have gained all the theoretical and practical knowledge for the cybersecurity domain, specifically in certain intelligence. I have taken a three-day training program from EC-Council, and the instructor's knowledge was up to the top. He had very good knowledge and helped me with all my queries in real-time. If you see the course content of the C|TIA program, it is set as per the industry standards, and it will help you in your career. The third thing I liked was its practical scenario. When you take the course and learn online with the instructor, you come across many practical components. The instructor helped me a lot and will surely help you if you take this course.

VARUL ARORA
UK

Security operation center engineer

Bachelor's Degree In Computer Science Diploma In Cyber Security

Organizations That Employ C|TIA Certified Members

About EC-Council

EC-Council invented the Certified Ethical Hacker (C|EH) Program. Founded in 2001 in response to 9/11, the EC-Council's mission is to provide the training and certifications that apprentice and experienced cybersecurity professionals need to keep corporations, government agencies, and others who employ them safe from cyber-attacks.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different training programs, certifications, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified over 350,000 professionals across the globe. EC-Council is the gold standard in cybersecurity education and certification, trusted by seven of the Fortune 10, half of the Fortune 100, and various agencies, public and private, across 140 nations.

A truly global organization with a driving belief in bringing diversity, equity, and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the US, the UK, India, Malaysia, Singapore, and Indonesia.

For more details, visit: www.eccouncil.org

EC-Council

Building A Culture Of Security

ACCENTREX GLOBAL