EC-Council Certified Threat Intelligence Analyst (CTIA)

Category: Networking & Security | **Vendor:** EC-Council

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Certified Threat Intelligence Analyst (CTIA)
Related Exam:	CTIA

Course Overview

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.

About This Course

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.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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.

Detailed Course Outline

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

□□ Certification Path

Certified Threat Intelligence Analyst (CTIA)

Exam: CTIA

Frequently Asked Questions

Q: What delivery options are available for EC-Council Certified Threat Intelligence Analyst (CTIA)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The EC-Council Certified Threat Intelligence Analyst (CTIA) course helps prepare you for the Certified Threat Intelligence Analyst (CTIA) certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the CTIA official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 3-day EC-Council Certified Threat Intelligence Analyst (CTIA) course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the EC-Council Certified Threat Intelligence Analyst (CTIA) training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for EC-Council Certified Threat Intelligence Analyst (CTIA)?

Yes, we provide corporate training, dedicated training, and closed classes for EC-Council Certified Threat Intelligence Analyst (CTIA). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: Why choose Nexus Human for EC-Council Certified Threat Intelligence Analyst (CTIA)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your EC-Council Certified Threat Intelligence Analyst (CTIA) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)