800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Certified Threat Intelligence Analyst (CTIA) Training

EC-Council Authorized Training · Applied Technology Academy

EC-Council's Certified Threat Intelligence Analyst (CTIA) 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. CTIA covers a wide range of topics, including the fundamentals of threat intelligence, the use of threat intelligence tools and techniques, and the development of a threat intelligence program. The cyber threat intelligence course focuses on refining data and information into actionable intelligence that can be used to prevent, detect, and monitor cyber-attacks. The program addresses all the stages involved in the threat intelligence lifecycle, and this attention toward a realistic and futuristic approach makes CTIA one of the most comprehensive threat intelligence certifications in the market today.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**3 Days**	**3 years: CEH**	**$72,000**	**Yes**

Course Overview

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

Acquired Skills:

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
- How to create and share threat intelligence reports
- 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

Course Outline

- **Module 01: Introduction to Threat Intelligence**
- **Module 02: Cyber Threats and Attack Frameworks**
- **Module 03: Requirements, Planning, Direction, and Review**
- **Module 04: Data Collection and Processing**
- **Module 05: Data Analysis**
- **Module 06: Intelligence Reporting and Dissemination**
- **Module 07: Threat Hunting and Detection**
- **Module 08: Threat Intelligence in SOC Operations, Incident Response, and Risk Management**

Intended Audience

- 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

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Prerequisites

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

Follow-On Courses

To gain specific knowledge and abilities in SOC, threat intelligence, digital forensics, and incident response, you can seek all Blue Team certificates and the CTIA, including the CND, ECIH, CSA, and CHFI. Also, CND can be an ideal place to start for any red team certification, CEH for ethical hacking, and CPENT for pen testing since network security skills are fundamental to the work of any cybersecurity professional.

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.