CTIA Certified Threat Intelligence Analyst

Duration: 3 days | **Presented in association with EC Council**

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.

Who Should Attend

- 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

Course Contents

- Introduction to Threat Intelligence
- Cyber Threats and Kill Chain Methodology
- Requirements, Planning, Direction, and Review
- Data Collection and Processing
- Data Analysis
- Intelligence Reporting and Dissemination

Exam Details

- 50 Multiple Choice Questions
- 2 Hours Duration
- Passing score of 70%
- Exam Title: Certified Threat Intelligence Analyst

Learning Objectives

- 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
- Creating effective threat intelligence reports
- 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