Certified Threat Intelligence Analyst (CTIA)

Course Duration: 3 Days
Course overview

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.
In the ever-changing threat landscape**, C|TIA** is a 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.

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.

What you will learn

- 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
- Creating effective threat intelligence reports
- Different threat intelligence sharing platforms, acts, and regulations for sharing strategic, tactical, operational, and technical intelligence

Top 10 Critical Components of CTIA

1. 100% compliance to NICE 2.0 and CREST frameworks
2. Focus on developing skills for performing various types of threat intelligence
3. Emphasis on various data collection techniques from multiple sources and feeds
4. Emphasis on collection, creation, and dissemination of Indicators of Compromise (IoCs) in various formats
5. Focus on intense malware analysis to collect adversary data and pivot off of it
6. Focus on a structured approach for performing threat analysis and threat intelligence evaluation
7. Focus on various techniques for threat intelligence reporting and dissemination
8. Hands-on program

9. Lab environment simulates a real-time environment
10. Covers latest threat intelligence tools, platforms, and frameworks

Course Outlines

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

Exam Details:

Exam Details	(CTIA Exam)
Number of Questions	**50**
Test Duration	**2 Hours**
Test Format	**Multiple Choice**
Test Delivery	**ECC Exam Portal**
Passing Score	**Score should be at least 70%**