Certified Threat Intelligence Analyst

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. It is a highly interactive, comprehensive, standards-based, intensive 3-day training program that teaches information security professionals to build professional threat intelligence.

More than 40 percent of class time is dedicated to the learning of practical skills, and this is achieved through EC-Council labs. Theory to practice ratio for C|TIA program is 60:40, providing students with a hands-on experience of the latest threat intelligence tools, techniques, methodologies, frameworks, scripts, etc. C|TIA comes integrated with labs to emphasize the learning objectives.

The C|TIA lab environment consists of the latest operating systems including Windows 10 and Kali Linux for planning, collecting, analyzing, evaluating, and disseminating threat intelligence.

TARGET AUDIENCE

Any cyber security professional who needs to understand how to gather large amounts of relevant threat information from a multitude of intelligence sources which can then be analyzed to provide threat intelligence that accurately predicts the potential threats that an organization may encounter. These individuals may be fulfilling roles such as: Ethical Hackers, Threat Intelligence Analysts, Threat Hunters, SOC Professionals, Digital Forensic and Malware Analysts, Incident Response,

COURSE OBJECTIVES

After completing this course you should be able to understand:

1. Key issues plaguing the information security world
2. Importance of threat intelligence in risk management, SIEM, and incident response
3. Types of cyber threats, threat actors and their motives, goals, and objectives of cybersecurity attacks
4. Fundamentals of threat intelligence (including threat intelligence types, lifecycle, strategy, capabilities, maturity model, frameworks, etc.)
5. Cyber kill chain methodology, Advanced Persistent Threat (APT) lifecycle, Tactics, Techniques, and Procedures (TTPs), Indicators of Compromise (IoCs), and pyramid of pain
6. Various steps involved in planning a threat intelligence program (Requirements, Planning, Direction, and Review)
7. Different types of data feeds, sources, and data collection methods
8. Threat intelligence data collection and acquisition through Open Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Indicators of Compromise (IoCs), and malware analysis
9. Bulk data collection and management (data processing, structuring, normalization, sampling, storing, and visualization)
10. Different data analysis types and techniques including statistical Data Analysis, Analysis of Competing Hypotheses (ACH), Structured Analysis of Competing Hypotheses (SACH), etc.)
11. Complete threat analysis process which includes threat modeling, fine-tuning, evaluation, runbook, and knowledge base creation
12. Different data analysis, threat modeling, and threat intelligence tools
13. 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
14. Effective creation of threat intelligence reports
15. Different threat intelligence sharing platforms, acts, and regulations for sharing strategic, tactical, operational, and technical intelligence

COURSE CONTENT

Introduction to Threat Intelligence

1. Understanding Intelligence
2. Understanding Cyber Threat Intelligence

3. Overview of Threat Intelligence Lifecycle and Frameworks

Cyber Threats and Kill Chain Methodology

1. Understanding Cyber Threats
2. Understanding Advanced Persistent Threats (APTs)
3. Understanding Cyber Kill Chain
4. Understanding Indicators of Compromise (IoCs)

Requirements, Planning, Direction, and Review

1. Understanding Organization's Current Threat Landscape
2. Understanding Requirements Analysis
3. Planning Threat Intelligence Program
4. Establishing Management Support
5. Building a Threat Intelligence Team
6. Overview of Threat Intelligence Sharing
7. Reviewing Threat Intelligence Program

Data Collection and Processing

1. Overview of Threat Intelligence Data Collection
2. Overview of Threat Intelligence Collection Management
3. Overview of Threat Intelligence Feeds and Sources
4. Understanding Threat Intelligence Data Collection and Acquisition
5. Understanding Bulk Data Collection
6. Understanding Data Processing and Exploitation

Data Analysis

1. Overview of Data Analysis
2. Understanding Data Analysis Techniques
3. Overview of Threat Analysis
4. Understanding Threat Analysis Process
5. Overview of Fine-Tuning Threat Analysis
6. Understanding Threat Intelligence Evaluation
7. Creating Runbooks and Knowledge Base
8. Overview of Threat Intelligence Tools

Intelligence Reporting and Dissemination

1. Overview of Threat Intelligence Reports
2. Introduction to Dissemination

3. Participating in Sharing Relationships
4. Overview of Sharing Threat Intelligence
5. Overview of Delivery Mechanisms
6. Understanding Threat Intelligence Sharing Platforms
7. Overview of Intelligence Sharing Acts and Regulations
8. Overview of Threat Intelligence Integration

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

There are no hard set prerequisites for course attendance, however in order to apply to take the exam you must be able to show a minimum of 3 years working experience in information security or software design.

TEST CERTIFICATION

Recommended as preparation for the following exams:

312-85 - Certified Threat Intelligence Analyst

In order to achieve this certification you will need to prove course attendance through an accredited EC-Council Partner and be able to show a minimum of 3 years work experience in information security or software design.