Certified Threat Intelligence Analyst (CTIA)

Introduction

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.

This program addresses all the stages involved in the Threat Intelligence Life Cycle. This attention to a realistic and futuristic approach makes C|TIA one of the most comprehensive threat intelligence certifications on the market today.

Key Outcomes

- Enable individuals and organizations with the ability to prepare and run a threat intelligence program that allows evidence-based knowledge and provides actionable advice about existing and unknown threats
- Ensure that organizations have predictive capabilities rather than just proactive measures beyond active defense mechanism
- Empower information security professionals with the skills to develop a professional, systematic, and repeatable real-life threat intelligence program
- Differentiate threat intelligence professionals from other information security professionals
- Provide an invaluable ability of structured threat intelligence to enhance skills and boost their employability

Course Outline

Module 01: Introduction to Threat Intelligence

- Understanding Intelligence
- Understanding Cyber Threat Intelligence
- Overview of Threat Intelligence Lifecycle and Frameworks

Module 02: Cyber Threats and Kill Chain Methodology

- Understanding Cyber Threats
- Understanding Advanced Persistent Threats (APTs)
- Understanding Cyber Kill Chain
- Understanding Indicators of Compromise (IoCs)

Module 03: 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

Module 04: 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

Module 05: 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

Module 06: 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
- Overview of Threat Intelligence Integration

Prerequisites

Basic Computer Knowledge.

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.

Duration

24 hours training course