EC-Council CTIA: Certified Threat Intelligence Analyst

Course Outline

1. Introduction to Threat Intelligence
- Understanding Intelligence
- Understanding Cyber Threat Intelligence
- Overview of Threat Intelligence Lifecycle and Frameworks

2. Cyber Threats and Kill Chain Methodology
- Understanding Cyber Threats
- Understanding Advanced Persistent Threats (APTs)
- Understanding Cyber Kill Chain
- Understanding Indicators of Compromise (IoCs)

3. 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

4. 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

5. 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

6. Dissemination and Reporting of Intelligence
- 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