Certified Threat Intelligence Analyst

Modality: Virtual Classroom

Duration: 3 Days

What's Included:

- *Official EC Council Invitation to the virtual class*
- *Official EC Council Print or e-courseware included*
- *Official EC Council ilabs subscription (6 months)*
- *EC Council Exam Voucher with included*

About this Course:

The Certified Threat Intelligence Analyst (CTIA) program is a specialist-level training and credentialing program developed in collaboration with cybersecurity and threat intelligence experts worldwide. It equips professionals with the knowledge and skills needed to identify and mitigate business risks by converting unknown threats into known threats. The program follows a structured approach to building effective threat intelligence and covers the entire Threat Intelligence Life Cycle, from project planning to report building and dissemination. By adopting a holistic method-driven approach, CTIA addresses the essential concepts required for effective threat intelligence, enabling professionals to protect organizations from future threats and enhancing their employability in the cybersecurity field.

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
- 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

Target Audience:

- Ethical Hackers, Security Practitioners, Engineers, Analysts, Specialists, Architects, and Managers in the cybersecurity field.
- Threat Intelligence Analysts, Associates, Researchers, and Consultants specializing in threat intelligence.
- Threat Hunters and SOC Professionals responsible for detecting and responding to cybersecurity threats.
- Digital Forensic and Malware Analysts involved in investigating and analyzing cyber incidents.
- Incident Response Team Members tasked with managing and mitigating cybersecurity incidents.
- Mid-level to high-level cybersecurity professionals with 3-5 years of experience.
- Information security professionals seeking to enhance their skills in cyber threat intelligence.Top of Form

Bottom of Form

Prerequisites:

A minimum of 3 years working experience in information security or software design

Course Outline:

- 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