Certified Threat Intelligence Analyst

Duration: 4 Days

Course Description:

Certified Threat Intelligence Analyst (TIA) certification is a comprehensive specialist-level professional program focused on the ever-evolving domain of threat intelligence. The program is designed for individuals involved in collecting, analyzing, and disseminating threat intelligence information.

CTIA covers a wide range of topics, including the fundamentals of threat intelligence, the use of threat intelligence tools and techniques, and the development of a threat intelligence program. The cyber threat intelligence course focuses on refining data and information into actionable intelligence that can be used to prevent, detect, and monitor cyber-attacks. The program addresses all the stages involved in the threat intelligence lifecycle, and this attention toward a realistic and futuristic approach makes CTIA one of the most comprehensive threat intelligence certifications in the market today.

CTIA program provides credible professional knowledge required for a successful threat intelligence career. It enhances your skills as a threat intelligence analyst, thus increasing your employability. It is desired by most cybersecurity engineers, analysts, and professionals globally and is respected by hiring authorities. Ideal for individuals working in information security, network security, incident response, and other related fields, mastering in-demand skills and earning this certification will improve threat intelligence operations and investments for cybersecurity individuals and teams.

A CTIA professional will be proficient in specialized skills and knowledge to understand the methodology and mindset of modern attackers competently and deploy the threat intelligence accordingly.

Course Objectives:

- Fundamentals of threat intelligence (Threat intelligence types, lifecycle, strategy, capabilities, maturity model, frameworks, platforms, etc.)
- Various cybersecurity threats and attack frameworks (Advanced Persistent Threats, Cyber Kill Chain Methodology, MITRE ATT&CK Framework, Diamond Model of Intrusion Analysis, etc.)
- Various steps involved in planning a threat intelligence program (Requirements, planning, direction, and review)
- Different types of threat intelligence feeds, sources, data collection methods
- Threat intelligence data collection and acquisition through Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Indicators of Compromise (IoCs), Malware Analysis, and Python Scripting
- Threat intelligence data processing and exploitation
- Threat data analysis techniques (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, and runbook and knowledge base creation
- How to create and share threat intelligence reports
- Threat intelligence sharing and collaboration using Python scripting
- Different platforms, acts, and regulations for sharing intelligence
- How to perform threat intelligence in a cloud environment
- Fundamentals of threat hunting (Threat hunting types, process, loop, methodology, etc.)
- Threat-hunting automation using Python scripting.
- Threat intelligence in SOC operations, incident response, and risk management Creating effective threat intelligence reports.
- Different threat intelligence sharing platforms, acts, and regulations for sharing strategic, tactical, operational, and technical intelligence.
- Threat intelligence data collection and acquisition through Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Indicators of Compromise (IoCs), and malware analysis.
- Types of data feeds, sources, and data collection methods.

Target Audience:

- Ethical Hackers
- Security Practitioners, Engineers, Analysts, Specialist, Architects, and 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 oh 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.

Course Outlines:

- Module 01: Introduction to Threat Intelligence
- Module 02: Cyber Threats and Attack Frameworks
- Module 03: Requirements, Planning, Direction, and Review
- Module 04: Data Collection and Processing
- Module 05: Data Analysis
- Module 06: Intelligence Reporting and Dissemination
- Module 07: Threat Hunting and Detection
- Module 08: Threat Intelligence in SOC Operations, Incident Response, and Risk Management