Certified Threat Intelligence Analyst (C|TIA)

Duration 3 days

COURSE DESCRIPTION

The Certified Threat Intelligence Analyst (CTIA) course is a specialized training program designed for individuals seeking to enhance their skills in identifying and mitigating cyber threats. It covers the foundational aspects of threat intelligence, including understanding intelligence, cyber threats, the kill chain methodology, and the lifecycle of threat intelligence. The course provides a detailed exploration of how to collect, process, analyze, and disseminate threat data, ensuring learners can effectively support their organizations' security posture. Through Certified Threat Intelligence Analyst training, participants will grasp the intricacies of cyber threat intelligence (CTI), learn to plan and direct CTI programs, and understand the significance of threat intelligence sharing. This Threat Intelligence Training is crucial for security professionals as it equips them with the knowledge to preemptively combat cyber threats, making it an invaluable asset for any cybersecurity defense strategy.

COURSE 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
- Creating effective threat intelligence reports
- 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

COURSE OUTLINE

- Introduction to Threat Intelligence
- Cyber Threats and Attack Frameworks
- Requirements, Planning, Direction, and Review
- Data Collection and Processing
- Data Analysis
- Intelligence Reporting and Dissemination
- Threat Hunting and Detection
- Threat Intelligence in SOC Operations, Incident Response, and Risk Management

PREREQUISITES

To successfully undertake the Certified Threat Intelligence Analyst (CTIA) course, students should meet the following minimum prerequisites:

- Basic understanding of cybersecurity concepts and terminology
- Familiarity with information security principles and frameworks
- Knowledge of network operations, including common network devices and protocols
- Awareness of common cyber threats and attack vectors
- Basic proficiency in using computers and internet research
- Ability to comprehend technical reports and documents
- Some experience with incident response or security operations is beneficial but not mandatory

These prerequisites are intended to ensure that participants have a foundational understanding that will allow them to fully benefit from the course content. No advanced technical skills are required, and the course is designed to be accessible to individuals with a general interest in cybersecurity and threat intelligence.

WHO SHOULD ATTEND

Certified Threat Intelligence Analyst (CTIA) course equips professionals with skills to identify and mitigate cyber threats effectively.

- Cybersecurity Analysts / Threat Intelligence Analysts
- Security Operations Center (SOC) Staff
- Incident Response Team Members
- Information Security Managers
- IT Managers / Risk Management Professionals
- Network & System Administrators
- Law Enforcement Personnel and Cybercrime Investigators
- Security Consultants
- Military and Defense Intelligence Staff
- Cybersecurity Enthusiasts and Students pursuing a career in cybersecurity

CERTIFICATION

C|TIA allows cybersecurity professionals to demonstrate their mastery of the knowledge and skills required for threat intelligence:

- Number of Questions: 50
- Duration: 2 hours
- Availability: EC-Council Exam Portal
- Test Format: Multiple Choice
- Passing Score: 70%

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th