EC-Council Certified Threat Intelligence Analyst (CTIA) + Exam voucher

Duration: 3 Days **Course Code: CTIA** **Version: 2**

Overview:

EC-Council's Certified Threat Intelligence Analyst (C|TIA) certification is a comprehensive, specialist-level program focused on the rapidly evolving field of threat intelligence. The certification is designed for professionals involved in collecting, analyzing, and disseminating cyber threat intelligence within organizations.
The C|TIA program covers key areas such as threat intelligence fundamentals, threat intelligence tools and techniques, and the development and management of threat intelligence programs. The course emphasizes transforming raw data into actionable intelligence that can be used to prevent, detect, and monitor cyber-attacks effectively.
C|TIA addresses every stage of the threat intelligence lifecycle, providing learners with a practical and future-oriented approach to modern cybersecurity challenges. This makes it one of the most comprehensive threat intelligence certifications currently available in the market.
The certification equips professionals with the knowledge and practical insights required to build a successful career in threat intelligence while strengthening their analytical and operational cybersecurity skills. It is highly valued by cybersecurity professionals worldwide and recognized by employers across the industry.
C|TIA is particularly suitable for professionals working in information security, network security, incident response, cyber defense, and related domains. Earning this certification can help individuals and teams enhance their threat intelligence capabilities, improve cybersecurity operations, and support informed security decision-making.

Target Audience:

- Mid-level to senior-level cybersecurity professionals with a minimum of three years of experience in cybersecurity or related domains.
- Professionals holding Certified Ethical Hacker (C|EH) and Certified Network Defender (C|ND) certifications are also eligible to enroll in the program.

Objectives:

- **After completing this course you should be able to understand:**
- Fundamentals of threat intelligence, including threat intelligence types, lifecycle, strategy, capabilities, maturity models, frameworks, and platforms
- Various cybersecurity threats and attack frameworks, including Advanced Persistent Threats (APTs), Cyber Kill Chain Methodology, MITRE ATT&CK Framework, and Diamond Model of Intrusion Analysis
- Planning and managing a threat intelligence program, including requirements gathering, planning, direction, and review
- Different types of threat intelligence feeds, intelligence 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), malware analysis, and Python scripting
- Threat intelligence data processing and exploitation techniques
- Threat data analysis methodologies, including Statistical Data Analysis, Analysis of Competing Hypotheses (ACH), and Structured Analysis of Competing Hypotheses (SACH)
- Complete threat analysis processes, including threat modeling, fine-tuning, evaluation, and runbook and knowledge base creation
- Threat intelligence sharing and collaboration using Python scripting
- Different platforms, acts, and regulations related to threat intelligence sharing
- Performing threat intelligence activities in cloud environments
- Fundamentals of threat hunting, including threat hunting types, processes, loops, and methodologies
- Threat-hunting automation using Python scripting
- The role of threat intelligence in Security Operations Center (SOC) operations, incident response, and risk management

Prerequisites:

Attendees should meet the following prerequisites:

- Minimum of three years of cybersecurity industry experience
- C|EH or C|ND certification holders are eligible to enroll in the course

Testing and Certification

Recommended as preparation for the following exams:

- **312-85** - Certified Threat Intelligence Analyst

Exam Details:

- **Number of Questions:** 50
- **Duration:** 2 hours
- **Test Format:** Multiple Choice Questions (MCQs)
- **Availability:** EC-Council Exam Portal

Content:

Module 1: Introduction to Threat Intelligence

Module 2: Cyber Threats and Attack Frameworks

Module 3: Requirements, Planning, Direction, and Review

Module 4: Data Collection and Processing

Module 5: Data Analysis

Module 6: Intelligence Reporting and Dissemination

Module 7: Threat Hunting and Detection

Module 8: Threat Intelligence in SOC Operations, Incident Response, and Risk Management

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo