EC Council Certified Threat Intelligence Analyst Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

The {*training} is a globally respected EC-Council credential
that trains cybersecurity professionals to transform unknown threats into actionable intelligence.

Developed in collaboration with global cybersecurity experts, C|TIA provides a**structured, method-driven approach**
to building and managing effective cyber threat intelligence programs.

Fully compliant with **NICE 2.0** and **CREST Threat Intelligence Manager (CC TIM)** frameworks,
C|TIA covers the entire **Threat Intelligence Life Cycle** — from planning and collection to analysis and dissemination.

This intensive 3-day program emphasizes both theoretical frameworks and practical, lab-based exercises,
making it ideal for mid- to senior-level cybersecurity professionals.

The **C|TIA** certification distinguishes professionals who can transform raw cyber data
into actionable intelligence that enhances organizational resilience.

Graduates of this program demonstrate mastery in**collecting, analyzing, and operationalizing threat intelligence**,
preparing them for roles such as **Threat Intelligence Analyst, SOC Specialist, or Cyber Threat Hunter**.

With C|TIA, you'll gain the expertise to **predict, prevent, and respond** to evolving cyber threats proactively.

Bilginç IT Academy is an **Official Accredited Training Partner of EC-Council**, delivering EC-Council-authorized cybersecurity trainings and certification programs globally.

Prerequisites

Candidates must meet one of the following:

- Attend official **EC-Council C|TIA training** via an Accredited Partner, or
- Have **a minimum of 2 years of professional experience** in information security.

All applicants are required to pay a**USD 100 non-refundable application fee** (often included in training cost).

EC Council Certified Threat Intelligence Analyst Training

Duration: **3 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

- Security Analysts, Engineers, and Practitioners
- Threat Intelligence Analysts and Researchers
- SOC Analysts and Incident Responders
- Ethical Hackers and Threat Hunters
- Digital Forensics and Malware Analysts
- Cybersecurity Managers and Architects
- Professionals seeking to specialize in **Threat Intelligence**

What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- Perform strategic, operational, tactical, and technical threat intelligence.
- Collect and analyze data from multiple sources (open, deep, and dark web).
- Create and disseminate **Indicators of Compromise (IoCs)** in STIX/TAXII formats.
- Reverse-engineer malware to extract adversary tactics and origin.
- Conduct structured threat modeling and intelligence evaluation.
- Generate professional threat intelligence reports and share securely.
- Leverage frameworks such as **MITRE ATT&CK** and **Cyber Kill Chain**.
- Apply NICE-compliant methodologies to real-world investigations.

Training Outline

Module 1 – Introduction to Threat Intelligence

- Overview of threat intelligence types and value
- The Threat Intelligence Life Cycle
- Frameworks: MITRE ATT&CK, Diamond Model, Cyber Kill Chain

Module 2 – Cyber Threats and Kill Chain Methodology

- Understanding threat actors and motivations
- Kill Chain stages and attack mapping
- Adversary TTPs (Tactics, Techniques, and Procedures)

Module 3 – Requirements, Planning, and Direction

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Developing a threat intelligence strategy
- Defining project goals and intelligence requirements
- Establishing scope and direction

Module 4 – Data Collection and Processing

- Data acquisition from OSINT, dark web, social media, APIs, and feeds
- Data normalization, tagging, and correlation
- Toolsets for large-scale intelligence processing

Module 5 – Data Analysis

- Filtering noise, performing threat modeling, and data validation
- Attribution and clustering techniques
- Malware reverse engineering for adversary profiling

Module 6 – Intelligence Reporting and Dissemination

- Creating impactful threat intelligence reports
- Sharing models, protocols, and data standards (STIX, TAXII, OpenIOC)
- Regulatory compliance and ethical considerations

Hands-On Labs

- 40% of course time dedicated to practical exercises
- Live lab environments using **Windows 10 and Kali Linux**
- Tools: **MISP, Maltego, TheHive, Yeti, OpenCTI**
- Real-world data correlation and malware analysis
- Reverse engineering and adversary tracking challenges