# EC Council Certified Threat Intelligence Analyst Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

Bu {*eğitim}, küresel siber güvenlik uzmanlarıyla birlikte geliştirilen,
**tehdit istihbaratı üretimi, analizi ve paylaşımı** üzerine odaklanan ileri düzey bir EC-Council sertifikasyon programıdır.

C|TIA, kurumların **bilinmeyen tehditleri tespit etmesini**, **bilinen tehditlere dönüştürmesini** ve proaktif savunma stratejileri geliştirmesini sağlar.

Bu program, **Threat Intelligence Life Cycle**'ın (İstihbarat Yaşam Döngüsü) tüm aşamalarını kapsayan metodolojik bir yaklaşımla, profesyonel istihbarat analizi becerilerini kazandırır.

Program **NICE 2.0** ve **CREST Threat Intelligence Manager (CC TIM)** standartlarına %100 uyumludur.

**C|TIA**, tehdit istihbaratı alanında derinlemesine bilgi edinmek ve siber tehditleri proaktif biçimde tespit etmek isteyen profesyoneller için tasarlanmış **en kapsamlı eğitimlerden biridir.**

Bu sertifika, analistlerin **veriden değerli istihbarat üretme**, **adversary davranışlarını analiz etme**, ve **organizasyonel savunmayı güçlendirme** yetkinliğini kanıtlar.

**Bilginç IT Academy**, **EC-Council'in Resmî Yetkili Eğitim Ortağı (Accredited Training Partner)** olarak, dünya genelinde EC-Council onaylı siber güvenlik eğitimlerini ve sertifikasyon programlarını sunmaktadır.

## Prerequisites

C|TIA sınavına girmek isteyen adaylar aşağıdaki koşullardan birini sağlamalıdır:

- Resmî bir **EC-Council C|TIA eğitimi** almış olmak
  veya
- En az **2 yıl bilgi güvenliği deneyimine** sahip olmak

Başvuru için USD 100 başvuru ücreti alınır (bazı eğitim ücretlerine dâhil olabilir).

# EC Council Certified Threat Intelligence Analyst Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Who Should Attend

- Siber Güvenlik Analistleri, Uzmanları ve Mühendisleri
- SOC (Security Operations Center) Ekip Üyeleri
- Threat Intelligence Analistleri, Danışmanlar ve Araştırmacılar
- Etik Hacker'lar
- Olay Müdahale (Incident Response) ve Dijital Adli Analiz Uzmanları
- Threat Hunters ve Malware Analistleri
- Siber Tehditleri önleme konusunda yetkinlik kazanmak isteyen tüm güvenlik profesyonelleri

## What You Will Learn

Bu {*eğitim} sonunda aşağıdaki konularda bilgi ve beceri kazanmış olacaksınız:

- **Stratejik, Operasyonel, Taktiksel ve Teknik Tehdit İstihbaratı** üretmeyi öğrenir.
- Farklı kaynaklardan (açık, kapalı, derin web vb.)**veri toplama tekniklerini** uygular.
- **IoC (Indicator of Compromise)** oluşturma, paylaşma ve korelasyon becerisi kazanır.
- **Kill Chain metodolojisi** ile siber saldırı sürecini analiz eder.
- Malware analiz teknikleriyle saldırı kökenini ve tehdit aktörünü belirler.
- Toplanan verilerden anlamlı **tehdit istihbaratı** çıkarma süreçlerini uygular.
- İstihbarat raporları hazırlayarak üst yönetime ve paydaşlara etkili sunum yapar.
- **C|TIA sertifikasyon sınavına** hazırlanır ve EC-Council üyelik avantajlarından yararlanır.

## Outline

### Modül 1 – Threat Intelligence'a Giriş

- Tehdit istihbaratının tanımı, kapsamı ve yaşam döngüsü
- Tehdit istihbaratı türleri (stratejik, operasyonel, taktiksel, teknik)
- Tehdit istihbaratı çerçeveleri: MITRE ATT&CK, Diamond Model, Cyber Kill Chain

### Modül 2 – Siber Tehditler ve Kill Chain Metodolojisi

- Siber tehdit aktörleri, motivasyonları ve saldırı taktikleri
- Kill Chain aşamaları ve istihbarat toplama sürecine entegrasyonu
- Adversary TTPs (Tactics, Techniques, Procedures) analizi

### Modül 3 – Gereksinimler, Planlama ve Yönlendirme

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Threat Intelligence projesi oluşturma
- İstihbarat gereksinimlerinin tanımlanması
- Proje hedefleri, kapsamı ve kaynak planlaması

### Modül 4 – Veri Toplama ve İşleme

- Açık kaynak (OSINT), kapalı ağ (Dark Web), sosyal medya, forumlardan veri toplama
- API, log, sensör, honeypot ve threat feed entegrasyonları
- Veri temizleme, etiketleme, korelasyon ve normalizasyon

### Modül 5 – Veri Analizi

- Toplanan verilerden anlamlı istihbarat çıkarma teknikleri
- Threat modeling ve saldırı trend analizi
- Adversary attribution (saldırgan tespiti)
- False positive ayıklama ve verinin güvenilirliğini ölçme

### Modül 6 – İstihbarat Raporlama ve Paylaşımı

- Etkili istihbarat raporları hazırlama
- Paylaşım protokolleri: STIX, TAXII, OpenIOC
- Paylaşım modelleri, güvenlik seviyeleri ve regülasyonlar
- En iyi uygulamalar ve paylaşım politikaları

## Uygulamalı Laboratuvarlar

- Eğitim süresinin %40'ı laboratuvar uygulamalarına ayrılmıştır.
- Kullanılan sistemler: **Windows 10 ve Kali Linux**
- Gerçek saldırı senaryoları, zararlı yazılım analizleri ve IoC üretimi
- Popüler istihbarat araçları: **MISP, Maltego, TheHive, Yeti, OpenCTI**
- Veri korelasyonu, reverse engineering ve MITRE ATT&CK haritalama