EC-Council Certified Incident Handler v3 (CIH) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The **{*training}** is a globally recognized, specialist-level certification program designed to equip cybersecurity professionals with the knowledge and skills to effectively handle and respond to security incidents.
Developed in collaboration with experienced practitioners worldwide, this hands-on program focuses on a **structured incident handling and response (IH&R) framework**, ensuring professionals can minimize damage and recover swiftly from cyberattacks.

This course includes full access to **EC-Council official labs** and an **exam voucher**. Participants gain practical exposure through 50+ labs, 800+ tools, and 4 OS environments (Windows 10, Server 2016, Ubuntu, OSSIM).

Benefits

- 100% Compliant with NICE 2.0 & CREST Framework
- Hands-on labs with real-world tools and frameworks
- Globally recognized EC-Council certification
- Focus on post-breach impact reduction and recovery
- Practical exposure with 800+ tools and 50+ labs

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

Prerequisites

At least **1 year** in the cybersecurity domain.

Who Should Attend

This course is ideal for:

- **Incident Handlers / Responders**
- **Penetration Testers**
- **Cyber Forensics Investigators**
- **System Administrators & Security Engineers**
- **Network Managers, IT Managers, Security Auditors**

EC-Council Certified Incident Handler v3 (CIH) Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

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

- Understand the fundamentals of **incident management** and the various stages of response
- Recognize and combat multiple forms of **cybersecurity incidents** including malware, network, web application, cloud, and insider threats
- Apply **risk and vulnerability management** methodologies
- Execute best practices for **incident containment, eradication, and recovery**
- Conduct **forensic readiness and evidence analysis**
- Implement the **NICE 2.0 and CREST-aligned** IH&R process effectively

Outline

Module 1: Introduction to Incident Handling and Response

- Information security concepts and threats
- Incident management lifecycle
- Risk, threat, and vulnerability management
- Legal and compliance considerations

Module 2: The Incident Handling and Response Process

- Preparation, Recording, Assignment
- Triage, Notification, Containment
- Evidence Gathering & Forensics
- Eradication, Recovery, and Post-Incident Activities

Module 3: Forensic Readiness and First Response

- Digital evidence principles
- Evidence collection and preservation
- Anti-forensics techniques and countermeasures

Module 4: Malware Incident Handling

- Detection, containment, eradication, and recovery

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Best practices for preventing malware incidents

Module 5: Email Security Incident Handling

- Identifying phishing and social engineering attacks
- Containment and mitigation strategies

Module 6: Network Security Incident Handling

- Unauthorized access and DoS/DDoS response
- Wireless and infrastructure attack mitigation

Module 7: Web Application Security Incident Handling

- OWASP Top 10 vulnerabilities and mitigation
- Forensic investigation of web attacks

Module 8: Cloud Security Incident Handling

- Cloud-based attacks and response strategies
- Incident containment and data recovery

Module 9: Insider Threats

- Identifying and mitigating insider risks
- Behavioral indicators and prevention policies