EC-Council Certified Incident Handler v3 (CIH) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bu **{*eğitim}**, siber güvenlik uzmanlarının olaylara etkin şekilde müdahale etmesi ve kurumların siber saldırılardan minimum hasarla kurtulması için geliştirilmiş, **dünya çapında tanınan bir uzmanlık programıdır**.
Program, alanında deneyimli profesyonellerle birlikte tasarlanmış olup,**sistematik olay yönetimi (Incident Handling & Response - IH&R)** yaklaşımını benimser.

Eğitim, **resmi EC-Council laboratuvarlarına erişim** ve **sertifika sınavını** içerir. Katılımcılar 50'den fazla laboratuvar, 800'den fazla araç ve 4 farklı işletim sistemi (Windows 10, Server 2016, Ubuntu, OSSIM) üzerinde uygulamalı deneyim kazanır.

Avantajlar

- NICE 2.0 ve CREST Framework uyumlu
- Uygulamalı laboratuvar ortamı (50+ Lab, 800+ araç)
- Resmi EC-Council sertifikası
- Gerçek senaryolara dayalı pratik eğitim
- Kurumsal risk ve itibar kaybını minimize etme

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

En az **1 yıllık siber güvenlik deneyimi**.

Who Should Attend

Bu eğitim şu roller için uygundur:

- **Olay Müdahale Uzmanları ve Güvenlik Operasyon Analistleri**
- **Sızma Test Uzmanları (Pentester'lar)**
- **Siber Adli Analiz Uzmanları**
- **Sistem Yöneticileri ve Güvenlik Mühendisleri**
- **Ağ ve BT Yöneticileri, Güvenlik Denetçileri**

EC-Council Certified Incident Handler v3 (CIH) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

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

- **Olay yönetimi** sürecinin aşamalarını kavrayacak
- Farklı türdeki **siber güvenlik olaylarını (malware, ağ, bulut, web, insider)** tanıyacak ve yönetecek
- **Zafiyet yönetimi** ve **risk analizi** uygulayabilecek
- **Olay önleme, kontrol altına alma, kurtarma** süreçlerini doğru şekilde uygulayacak
- **Adli analiz (forensic)** ve delil toplama süreçlerinde uzmanlaşacak
- **NICE 2.0** ve **CREST** standartlarına uygun olay müdahale süreçlerini uygulayabilecek

Outline

Modül 1 – Olay Yönetimi ve Müdahaleye Giriş

- Bilgi güvenliği tehditleri ve saldırı türleri
- Olay yönetimi döngüsü
- Risk ve zafiyet yönetimi
- Hukuki gereklilikler ve uyumluluk

Modül 2 – Olay Müdahale Süreci

- Hazırlık, kayıt, önceliklendirme
- Bildirim, sınırlama, delil toplama
- Adli analiz, giderme ve kurtarma

Modül 3 – Adli Hazırlık ve İlk Müdahale

- Dijital delil toplama prensipleri
- Delil güvenliği ve zinciri
- Anti-forensics teknikleri ve karşı önlemler

Modül 4 – Zararlı Yazılım (Malware) Olayları

- Malware tespiti, sınırlama ve giderme
- Önleme stratejileri ve araç kullanımı

EC-Council Certified Incident Handler v3 (CIH) Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Modül 5 – E-posta Güvenliği Olayları

- Kimlik avı (phishing) ve sosyal mühendislik tespiti
- Olay önleme ve kurtarma süreçleri

Modül 6 – Ağ Güvenliği Olayları

- Yetkisiz erişim, DoS/DDoS saldırıları
- Kablosuz ağ saldırılarını yönetme

Modül 7 – Web Uygulama Güvenliği Olayları

- OWASP Top 10 zafiyetleri ve çözüm teknikleri
- Web uygulamalarında adli inceleme yöntemleri

Modül 8 – Bulut Güvenliği Olayları

- Bulut tabanlı saldırılar ve karşı önlemler
- Veri kaybı sonrası kurtarma yöntemleri

Modül 9 – İç Tehditler (Insider Threats)

- İçeriden kaynaklanan saldırı türleri
- Davranışsal göstergeler ve önleme politikaları