Certified Offensive AI Security Professional (C|OASP) Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Overview

EC-Council tarafından geliştirilen **Certified Offensive AI Security Professional (C|OASP)**, yapay zekâ sistemlerinin güvenliğini test etmek, zafiyetleri tespit etmek ve savunma stratejileri geliştirmek isteyen siber güvenlik profesyonelleri için oluşturulmuş ileri seviye bir sertifika programıdır.
Bu eğitim, yapay zekâ ve makine öğrenimi sistemlerinin saldırı yüzeylerini anlamayı, AI modellerini manipüle eden teknikleri uygulamalı olarak deneyimlemeyi ve kurumların AI altyapılarını korumak için gelişmiş yöntemler geliştirmeyi öğretir.

Bu eğitimi başarıyla tamamlayan katılımcılar, **EC-Council Certified Offensive AI Security Professional (C|OASP)** sertifikasına hak kazanır.
Sertifika, AI güvenliği alanında **ofansif düşünme kabiliyeti** ve **savunma uzmanlığı** kazandırır.

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.

Who Should Attend

- Siber güvenlik uzmanları, Red/Blue Team profesyonelleri
- AI güvenliğiyle ilgilenen etik hacker'lar
- Makine öğrenimi mühendisleri ve veri bilimciler
- Güvenlik danışmanları, SOC analistleri

What You Will Learn

Eğitimin sonunda katılımcılar:

- AI sistemlerindeki saldırı vektörlerini tanımlamayı,
- Model manipülasyonu, veri zehirleme (data poisoning) ve adversarial saldırıları analiz etmeyi,
- AI Red Team operasyonlarını planlamayı ve yürütmeyi,
- AI tabanlı sistemlerin savunma katmanlarını güçlendirmeyi,
- Güvenli model yaşam döngüsü (Secure MLOps) prensiplerini uygulamayı,
- Etik hacking prensiplerini AI ortamlarına entegre etmeyi öğreneceklerdir.

Certified Offensive AI Security Professional (C|OASP) Eğitimi

Süre: **3 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Outline

1. Yapay Zekâ Güvenliğine Giriş

- AI güvenliği kavramları, riskleri ve tehdit modeli
- AI sistemlerinde saldırı yüzeyi analizi
- Model, veri ve API katmanlarının güvenlik zafiyetleri

2. Offensive AI (Red Team) Taktikleri

- Model Inversion Attack (Model Tersine Çevirme)
- Data Poisoning ve Model Poisoning teknikleri
- Adversarial örnek oluşturma ve bypass stratejileri
- Evasion, Extraction ve Backdoor saldırıları

3. Defensive AI (Blue Team) Yaklaşımları

- Güvenli veri eğitimi ve doğrulama
- AI model sertleştirme (Model Hardening)
- Anomali tespiti ve saldırı izleme sistemleri
- Adversarial savunma yöntemleri

4. AI Güvenlik Araçları ve Framework'leri

- AI Red Team toolkit'leri
- TensorFlow Security, PyTorch Defense mekanizmaları
- Explainable AI (XAI) ile güvenlik analizi
- Güvenlik test otomasyonu

5. Etik, Yasal ve Regülasyon Boyutu

- AI güvenliğinde etik hacking prensipleri
- Regülasyonlar: AB AI Act, ISO/IEC 23894, NIST AI RMF
- Kurumsal AI güvenlik politikaları ve yönetişim

6. Uygulamalı Laboratuvarlar

- Gerçek veri setleriyle saldırı simülasyonları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Model manipülasyon testleri
- Adversarial saldırı tespiti
- Kapsamlı Red Team operasyon senaryosu