CompTIA SecAI+ Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

CompTIA SecAI+, BT ve **Siber Güvenlik** profesyonellerinin **Yapay Zeka Güvenliği** alanında ihtiyaç duyduğu bilgi ve becerileri kazanmasını sağlayan, eğitmen liderliğinde gerçekleştirilen 3 günlük kapsamlı bir eğitim programıdır. Bu üretici bağımsız (**vendor-neutral**) sertifikasyon, kuruluşların **Yapay Zeka Sistemleri** ile ilişkili güvenlik risklerini yönetmelerine ve AI teknolojilerini güvenli şekilde kullanmalarına yardımcı olur.

Eğitim boyunca katılımcılar, **Makine Öğrenmesi (Machine Learning)**, **Derin Öğrenme (Deep Learning)**, **Üretken Yapay Zeka (Generative AI)** ve modern güvenlik yaklaşımları hakkında bilgi edinirken; aynı zamanda **AI modelleri**, veri süreçleri ve dağıtım ortamlarının nasıl korunacağını öğrenirler. Ayrıca **Tehdit Tespiti**, **Olay Müdahalesi** ve **Güvenlik Operasyonları** için AI destekli araçların kullanımını deneyimleme fırsatı elde ederler.

Prerequisites

- En az **3-4 yıl BT deneyimi**
- Yaklaşık **2 yıl uygulamalı Siber Güvenlik deneyimi**
- **CompTIA Security+** veya eşdeğer seviyede bilgi sahibi olmak tavsiye edilir

Who Should Attend

Bu eğitim aşağıdaki profesyoneller için uygundur:

- **Siber Güvenlik Analistleri**
- **Güvenlik Mühendisleri**
- **SOC ve Güvenlik Operasyon Uzmanları**
- **Tehdit İstihbaratı Analistleri**
- **DevSecOps Uzmanları**
- Yazılım geliştiriciler
- **Güvenlik Mimarları**
- **Yapay Zeka Sistemleri** ile çalışan BT uzmanları

What You Will Learn

Eğitim sonunda katılımcılar:

- **Yapay Zeka** teknolojilerini güvenlik süreçlerine entegre edebilir.
- **AI Güvenlik Kontrolleri** uygulayabilir.
- **AI Tehditleri** ve güvenlik açıklarını belirleyebilir.
- **AI destekli Tehdit Tespiti** ve analiz araçlarını kullanabilir.
- **DevSecOps** süreçlerinde güvenli AI entegrasyonu gerçekleştirebilir.
- **Risk Yönetimi**, **Uyumluluk** ve **AI Yönetişimi** prensiplerini uygulayabilir.

CompTIA SecAI+ Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Modül 1: Siber Güvenlik İçin Yapay Zeka ve Veri Temelleri

- **Makine Öğrenmesi** ve **Derin Öğrenme** kavramları
- **Üretken Yapay Zeka (Generative AI)** teknolojileri
- Transformer mimarileri ve **Doğal Dil İşleme (NLP)**
- Model eğitimi yaklaşımları
- **Prompt Engineering** teknikleri
- Veri bütünlüğü ve veri güvenliği
- **Retrieval-Augmented Generation (RAG)** temelleri

Modül 2: Tehdit Modellemesi ve AI Sistemlerinin Güvenliği

- **Tehdit Modellemesi** metodolojileri
- AI sistemlerine yönelik saldırı senaryoları
- Güvenlik açıklarının tespit edilmesi
- **AI Güvenlik Kontrolleri**
- Güvenli yapılandırma ve guardrail uygulamaları
- Güvenlik doğrulama ve test süreçleri

Modül 3: Yapay Zeka Ortamlarında Erişim Kontrolleri

- **Erişim Kontrolü** modelleri
- API ve ağ güvenliği
- **Veri Koruma** ve şifreleme teknikleri
- İzleme ve log yönetimi
- Denetim ve uyumluluk süreçleri

Modül 4: AI Tehditleri ve Koruma Stratejileri

- **Adversarial AI** saldırıları
- **Model Poisoning** riskleri
- Model çalma ve model tersine mühendisliği
- **Etik Yapay Zeka** prensipleri
- Koruyucu güvenlik önlemleri
- Olay sonrası analiz çalışmaları

Modül 5: Güvenlik Operasyonlarında Yapay Zeka Kullanımı

- **AI destekli Tehdit Tespiti**
- Güvenlik analitiği
- Zafiyet yönetiminde AI kullanımı
- Güvenlik otomasyonu
- **Olay Müdahalesi** süreçleri
- **DevSecOps** entegrasyonu

Modül 6: AI Yönetişimi, Risk ve Uyumluluk

- **AI Yönetişimi** çerçeveleri
- Kurumsal roller ve sorumluluklar
- **Sorumlu Yapay Zeka** ilkeleri

CompTIA SecAI+ Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- **Risk Yönetimi** süreçleri
- Regülasyon ve **Uyumluluk** gereksinimleri
- Kurumsal politika ve raporlama mekanizmaları