AI Assisted Secure Software Development Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Bu yoğun **3 günlük eğitim**, yazılım geliştiricilerin modern yazılım geliştirme süreçlerinde yapay zekâdan verimli ve güvenli biçimde yararlanabilmeleri için tasarlanmıştır.

Eğitim boyunca katılımcılar **GitHub Copilot, Amazon Q ve Tabnine** gibi yapay zekâ destekli geliştirme araçlarını inceleyecek; prompt engineering yöntemlerini, yapay zekâ ile kod geliştirme süreçlerini ve bu teknolojilerin beraberinde getirdiği güvenlik risklerini uygulamalı olarak ele alacaktır.

Laboratuvar çalışmaları kapsamında katılımcılar foundation model'lerden yararlanan akıllı bir uygulama geliştirecek, makine öğrenmesi modellerini hem yerel hem de bulut ortamlarında çalıştırıp dağıtacak ve yapay zekâ sistemlerine yönelik yaygın saldırı yöntemlerini anlamak amacıyla red team tekniklerini uygulayacaktır.

Program; geliştirici üretkenliğini artırmanın yanı sıra yapay zekâ özelliklerine sahip uygulamalar geliştirmek ve AI teknolojilerini yazılım geliştirme ortamlarında sorumlu ve güvenli şekilde kullanmak için gerekli güncel becerileri kazandırmayı amaçlar.

Önkoşullar

Katılımcıların aşağıdaki bilgi ve deneyimlere sahip olması önerilir:

- Yazılım geliştirme prensipleri ve uygulamaları hakkında sağlam temel bilgi
- IDE ve sürüm kontrol sistemleriyle çalışma deneyimi
- Azure, AWS veya GCP gibi bulut ortamlarına aşinalık faydalıdır

Kimler Katılmalı

Bu eğitim özellikle aşağıdaki katılımcılar için uygundur:

- Yapay zekâyı geliştirme süreçlerine entegre etmek isteyen profesyonel yazılım geliştiriciler ve teknik liderler
- AI güvenlik risklerini ve savunma yöntemlerini öğrenmek isteyen DevOps ve güvenlik mühendisleri
- Yapay zekâ yardımıyla geliştirme verimliliğini artırmak ve akıllı uygulamalar oluşturmak isteyen yazılım ekipleri
- AI destekli iş akışlarını ve geliştirme araçlarını kullanmaya başlayan kurumlar

AI Assisted Secure Software Development Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Neler Öğreneceksiniz

Eğitimin sonunda katılımcılar:

- Temel yapay zekâ kavramlarını ve bunların yazılım geliştirmedeki önemini açıklayabilir.
- Dil modelleriyle daha etkili iletişim kurmak için prompt engineering tekniklerini uygulayabilir.
- AI destekli geliştirme araçlarıyla kodlama süreçlerini hızlandırabilir ve daha verimli hâle getirebilir.
- Mevcut veya yeni uygulamalara yapay zekâ tabanlı özellikler ve servisler ekleyebilir.
- Makine öğrenmesi modellerini yerel ve bulut ortamlarında eğitebilir ve dağıtabilir.
- Prompt injection ve model jailbreak gibi yaygın AI saldırı yöntemlerini tanıyabilir ve bunlara karşı önlemler geliştirebilir.
- Yapay zekâ teknolojilerini production ortamına yönelik güvenli yazılım geliştirme süreçlerinde kullanabilir.

Eğitim İçeriği

1. Gün – Yapay Zekâ Temelleri ve Geliştirici Verimlilik Araçları

Yazılım Geliştirmede Yapay Zekâ

- Yapay zekânın yazılım sektörüne etkisi ve gelişen trendler
- AI ile geliştirici üretkenliğinin artırılması
- Yapay zekâ destekli geliştirme iş akışlarına genel bakış

AI Geliştirme Araçları Ekosistemi

- GitHub Copilot: özellikler, kullanım senaryoları ve demolar
- Amazon Q Developer: kod oluşturma ve kod güvenliği
- Tabnine: gizlilik, ekip çalışması ve kodlama verimliliği
- Bulut tabanlı laboratuvar ortamının hazırlanması ve başlangıç uygulamaları

Prompt Engineering Temelleri

- Temel prompt teknikleri ve stratejileri
- Yapılandırılmış prompt geliştirmede SudoLang
- AI modellerinin sınırlamaları ve hallucination problemlerinin yönetimi
- Doğal dil ifadelerinin yapılandırılmış prompt'lara dönüştürülmesi

2. Gün – Yapay Zekâ Destekli Akıllı Uygulamalar Geliştirme

Copilot ile İleri Seviye Kodlama

- Otomatik kod tamamlama, unit test ve boilerplate kod üretimi
- Prompt engineering ile Copilot Chat'in birlikte kullanılması
- Bilinmeyen ortam ve framework'lerde gerçek dünya uygulamaları

AI Araçlarının Karşılaştırılması ve En İyi Uygulamalar

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- IDE ortamlarında ChatGPT kullanımı
- AI geliştirme araçlarının özellik ve performans açısından karşılaştırılması
- İhtiyaca uygun AI asistanının seçilmesi

AI Entegrasyonlu Uygulama Geliştirme

- Fresh Cart projesine genel bakış
- LLM tabanlı chatbot entegrasyonu
- Prompt routing ve orchestration
- Semantic search ve state mutation
- AI operasyonlarında logging ve self-correction yaklaşımları

Yapay Zekâ Sistemlerinde Güvenlik

- Prompt injection riskleri ve red team uygulamaları
- Model jailbreak saldırıları ve savunma yöntemleri
- Prompt extraction teknikleri
- ReBuff, Llama Guard ve Lakera kullanılarak savunma stratejileri

3. Gün – Modellerle Çalışma ve Deployment

Foundation Model'ler ve Inference

- Açık kaynak modeller: Llama 3 ve Stable Diffusion
- Modellerin yerel ortamda ve container içerisinde çalıştırılması
- Hugging Face: Transformers, Pipelines, AutoTrain ve Inference Endpoints

Bulut Ortamlarında AI Deployment

- Microsoft Azure: OpenAI Studio ve hosting
- Google Cloud: Vertex AI ve Model Garden
- Amazon AI: Bedrock ve makine öğrenmesi araçları
- Container tabanlı model deployment için Replicate ve Cog

Makine Öğrenmesinin Temelleri

- TensorFlow ve Keras iş akışları
- Model eğitimi, tuning ve deployment
- Docker kullanarak modellerin servis edilmesi

İleri Seviye Yapay Zekâ Konuları

- OpenAI, Vertex AI ve AWS üzerinde model fine-tuning
- Embedding teknikleri ve similarity search
- Retrieval Augmented Generation (RAG) uygulamaları
- Fresh Cart içerisinde araştırma araçları ve embedding akışları