Testing Generative AI Systems Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Testing Generative AI Systems eğitimi, üretken yapay zeka sistemlerini gerçek kullanım koşullarında test etmek, değerlendirmek ve yönetişim altına almak isteyen profesyonellere yönelik uygulamalı bir programdır.

Generative AI çözümleri, geleneksel yazılım sistemlerinden farklı olarak her zaman aynı girdiye aynı çıktıyı üretmez. Bu nedenle klasik ve tamamen deterministik test yaklaşımları, AI sistemlerinin kalite, güvenlik ve davranışlarını değerlendirmek için tek başına yeterli olmayabilir. Eğitim, katılımcıların bu farkı anlamasını ve olasılıksal, değişken ve zaman içinde evrilebilen AI davranışlarına uygun yeni test yöntemleri geliştirmesini amaçlar.

Program boyunca gerçekçi örnekler, yapılandırılmış test framework'leri, red-teaming çalışmaları ve uygulamalı değerlendirme aktiviteleri kullanılır. Katılımcılar üretken AI sistemlerinin neden başarısız olabildiğini, hallucination, bias, toxicity, privacy ve drift gibi risklerin nasıl ortaya çıktığını ve bu risklerin deployment sonrasında nasıl değişebildiğini inceler.

Eğitimin sonunda katılımcılar, yalnızca tek seferlik testler gerçekleştirmek yerine GenAI çözümlerinin ürün yaşam döngüsü boyunca kalite, güvenlik ve güvenilirlik açısından nasıl değerlendirilebileceğine ilişkin uygulanabilir bir yaklaşım geliştirir.

Eğitim Sonunda Katılımcıların Elde Edecekleri

Eğitim gününün sonunda katılımcılar:

- Gerçek bir generative AI kullanım senaryosu için uygulanabilir bir test stratejisi,
- GenAI sistemlerinde kalite, risk ve davranış değerlendirmesi için tekrar kullanılabilir bir framework,
- Red teaming ve non-deterministic testing konusunda uygulamalı deneyim,
- GenAI testlerinin product ve delivery lifecycle süreçlerine nasıl entegre edileceğine yönelik açık bir yaklaşım

geliştirmiş olur.

Önkoşullar

Katılımcıların:

- Dijital ürünler, AI veya software delivery konusunda temel düzeyde bilgiye,
- Kullanıcı, geliştirici veya stakeholder olarak AI destekli özellik veya sistemlerle bir miktar deneyime

sahip olmaları önerilir.

AI testing, data science veya machine learning konusunda önceden deneyim gerekli değildir.

Testing Generative AI Systems Eğitimi

Süre: **1 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Kimler Katılmalı

Bu eğitim özellikle:

- AI destekli sistemlerin kalitesinden sorumlu QA Engineer ve Test Lead'ler,
- Generative AI özelliklerini ürünlere dahil eden Product Manager ve Product Owner'lar,
- GenAI model veya servislerini geliştiren ya da entegre eden Developer ve AI Practitioner'lar,
- AI kullanımını yöneten Risk, Compliance ve Governance profesyonelleri,
- Trust, safety ve reliability konularına odaklanan UX, CX ve Innovation ekipleri

için tasarlanmıştır.

Neler Öğreneceksiniz

Eğitimi tamamlayan katılımcılar:

- Geleneksel test yöntemlerinin generative AI sistemlerinde neden yetersiz kalabildiğini açıklayabilir,
- Hallucination, bias, toxicity, privacy ve drift gibi temel GenAI risk kategorilerini belirleyebilir,
- Non-deterministic ve sürekli değişebilen çıktılar için uygun test stratejileri tasarlayabilir,
- GenAI kalitesini değerlendirmek için anlamlı benchmark ve evaluation criteria tanımlayabilir,
- Gizli ve adversarial hata senaryolarını ortaya çıkarmak için red-teaming tekniklerini uygulayabilir,
- AI testlerinde automation ile human judgement arasında uygun dengeyi kurabilir,
- GenAI testlerini continuous delivery ve governance süreçlerine entegre edebilir.

Eğitim İçeriği

Modül 1: Generative AI Neden Geleneksel Test Yaklaşımlarını Zorlar?

Bu bölümde klasik yazılım testleriyle üretken AI sistemlerinin test edilmesi arasındaki temel farklar ele alınır.

- Deterministic ve probabilistic sistemler arasındaki fark
- Aynı girdinin farklı çıktılar üretmesinin test süreçlerine etkisi
- Geleneksel pass/fail yaklaşımının sınırlamaları
- AI sistemlerinde değişken davranış ve belirsizlik
- GenAI için yeni test zihniyetinin oluşturulması

Modül 2: GenAI Risklerini ve Davranışlarını Anlamak

Katılımcılar üretken yapay zeka sistemlerinde ortaya çıkabilecek temel riskleri ve bu risklerin zaman içerisinde nasıl değişebileceğini inceler.

- Hallucination riskleri
- Bias ve fairness sorunları
- Toxic veya uygunsuz içerik üretimi
- Privacy ve hassas veri riskleri
- Model ve behaviour drift
- Risklerin deployment öncesi ve sonrası farklılaşması

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Kullanıcı davranışının risk profiline etkisi

Modül 3: Non-Deterministic Sistemler için Test Tasarlama

Bu bölüm, değişken çıktılar üreten sistemler için yapılandırılmış test yaklaşımı oluşturmaya odaklanır.

- Sabit sonuçlar yerine beklenen davranış aralıklarını tanımlama
- Test scenario ve test dataset oluşturma
- Tekrarlı testlerden yararlanma
- Output consistency ve variability değerlendirmesi
- Edge case'lerin belirlenmesi
- Human review gerektiren alanların tanımlanması

Modül 4: Benchmarking ve Evaluation Criteria

Katılımcılar GenAI performansını yalnızca teknik doğruluk üzerinden değil, farklı kalite boyutlarıyla değerlendirmeyi öğrenir.

- Kalite için uygun benchmark'lar oluşturma
- Evaluation criteria tanımlama
- Accuracy, relevance ve usefulness değerlendirmesi
- Safety ve reliability ölçütleri
- Human evaluation ile automated evaluation arasındaki ilişki
- Farklı kullanım senaryoları için kabul kriterleri oluşturma

Modül 5: Red Teaming ve Adversarial Testing

Bu bölümde sistemin beklenmeyen veya kötü niyetli girdiler karşısındaki davranışını değerlendirmeye yönelik yöntemler incelenir.

- Red teaming yaklaşımına giriş
- Adversarial prompt ve senaryolar oluşturma
- Hidden failure mode'ları ortaya çıkarma
- Güvenlik ve safety kontrollerini zorlayan testler
- Guardrail'lerin değerlendirilmesi
- Red-team bulgularının risk yönetimine aktarılması

Modül 6: Production Ortamında Test ve Governance

Son bölüm, GenAI testinin deployment sonrasında da devam eden bir faaliyet olarak ele alınmasına odaklanır.

- Production monitoring ile test yaklaşımını ilişkilendirme
- Live system behaviour değerlendirmesi
- Drift ve yeni risklerin izlenmesi
- Continuous evaluation süreçleri
- Test sonuçlarının governance ve risk management süreçlerine dahil edilmesi
- Product ve delivery lifecycle içerisine GenAI testing entegrasyonu
- Sürekli güven, güvenlik ve kalite geliştirme