

Agentic AI for Data Engineering & Data/AI Platform Engineering Eğitimi

Süre: 5 Gün

Açıklama

Eğitim Seviyesi: İleri Düzey Kurumsal veri platformlarında yapay zeka teknolojilerinin kullanımı, geleneksel veri işleme ve analiz uygulamalarının ötesine geçerek farklı sistemlerle etkileşime girebilen ve karmaşık veri mühendisliği süreçlerini destekleyen yapay zeka ajanlarına doğru gelişmektedir. Agentic AI mimarileri; büyük dil modellerini (LLM), kurumsal veri kaynaklarını, API servislerini, veri tabanlarını ve araçları bir araya getirerek veri keşfi, veri kalitesi kontrolü, metadata yönetimi, veri soy ağacı (data lineage) analizi ve operasyonel süreçlerin otomasyonunda yeni olanaklar sunmaktadır. Bu eğitim, katılımcıların kurumsal veri platformlarında kullanılabilecek yapay zeka ajanlarını tasarlama, geliştirme, orkestrasyon, entegrasyon, değerlendirme ve production ortamlarına taşıma süreçlerinde yetkinlik kazanmalarını hedefler. Program, bankacılık sektöründeki veri güvenliği, yetkilendirme, denetlenebilirlik ve operasyonel süreklilik gereksinimleri dikkate alınarak yapılandırılmıştır. Katılımcıların veri mühendisliği ve kurumsal Data/AI Platform Engineering süreçlerinde kullanılabilecek yapay zeka ajanlarını tasarlama, geliştirme, yönetme ve production ortamlarında güvenli şekilde çalıştırma becerilerini geliştirmektir. **Bu eğitimde neler öğreneceksiniz?**

- Agentic AI mimarilerini tasarlamak
- Tool Calling ve MCP entegrasyonları geliştirmek
- Tek ajanlı ve çok ajanlı sistemler oluşturmak
- RAG ve ajan hafızası mekanizmalarını entegre etmek
- Veri tabanları ve API servisleriyle etkileşime giren ajanlar geliştirmek
- Veri keşfi, veri kalitesi ve metadata yönetimi için ajan tabanlı çözümler tasarlamak
- Human-in-the-Loop kontrol mekanizmaları uygulamak
- Ajanların performansını değerlendirmek ve izlemek
- Kurumsal güvenlik, yetkilendirme ve veri erişim politikalarını uygulamak
- Agentic AI uygulamalarını production ortamlarına taşımak

Kimler Katılmalı?

- Data Engineer / Senior Data Engineer
- Data Platform Engineer
- AI Platform Engineer

- ML Engineer / MLOps Engineer
- Data Architect / Solution Architect
- AI Engineer / LLM Engineer
- Veri platformları ve yapay zeka altyapılarından sorumlu teknik ekipler

Eğitim İçeriği

1. Agentic AI Architecture & Foundations

- Agentic AI kavramı ve geleneksel LLM uygulamalarından farkları
- Agentic AI mimari bileşenleri
- Agent yaşam döngüsü
- Planning, Reasoning ve Acting yaklaşımları
- Tek ajanlı ve çok ajanlı mimarilerin karşılaştırılması
- Veri mühendisliği ve veri platformlarında Agentic AI kullanım senaryoları

2. Tool Calling / Function Calling

- LLM Tool Calling ve Function Calling mekanizmaları
- Tool tanımlama ve JSON Schema kullanımı
- Structured Outputs
- Tool execution ve sonuç yönetimi
- Tool Calling hata yönetimi
- Veri platformları için özel araçların geliştirilmesi
- Python tabanlı Tool Calling uygulamaları

3. Model Context Protocol (MCP)

- MCP mimarisi ve temel bileşenleri
- MCP Client ve MCP Server kavramları
- MCP Tools, Resources ve Prompts
- MCP Server geliştirme
- Kurumsal veri kaynaklarının MCP üzerinden erişilebilir hale getirilmesi
- MCP ile veri tabanı ve API entegrasyonları
- MCP güvenliği ve erişim kontrolleri
- Uygulama: Veri platformu için MCP Server geliştirme

4. Agent Orchestration

- Agent orkestrasyon mimarileri
- Workflow tabanlı ve dinamik ajan sistemleri
- State Management
- Agent execution lifecycle
- Retry, timeout ve hata yönetimi

- LangGraph ve benzeri orkestrasyon yaklaşımları
- Uzun süreli çalışan agent workflow'ları
- Uygulama: Veri mühendisliği iş akışının ajanlarla orkestrasyonu

5. Multi-Agent Architectures

- Multi-Agent sistemlerin mimarisi
- Supervisor ve Worker Agent modelleri
- Agent-to-Agent iletişim
- Görev dağılımı ve koordinasyon
- Uzmanlaşmış ajan tasarımı
- Çok ajanlı sistemlerde hata yönetimi
- Uygulama: Data Discovery, Data Quality ve Metadata ajanlarından oluşan sistem

6. RAG + Agents

- Retrieval-Augmented Generation (RAG) mimarisi
- Agentic RAG yaklaşımı
- Vector Database entegrasyonu
- Semantic Search ve Hybrid Search
- Retrieval stratejileri
- RAG sonuçlarının değerlendirilmesi
- Kurumsal doküman ve metadata kaynaklarıyla entegrasyon
- Uygulama: Kurumsal veri kataloğu üzerinde Agentic RAG

7. Agent Memory

- Agent Memory kavramı
- Short-Term ve Long-Term Memory
- Conversation Memory
- Persistent Memory
- Vector tabanlı hafıza
- Memory Management stratejileri
- Veri güvenliği ve hafıza yönetimi
- Uygulama: Bağlamı koruyan veri analizi ajanı

8. Agents Interacting with Databases & APIs

- Veri tabanlarıyla etkileşime giren ajan mimarileri
- Text-to-SQL yaklaşımları
- SQL sorgularının oluşturulması ve doğrulanması
- Veri tabanı erişim güvenliği
- API Calling ve servis entegrasyonları
- Authentication ve Authorization

- Hata yönetimi ve veri doğrulama
- Uygulama: SQL ve REST API kullanan veri asistanı

9. Data Discovery Agents

- Kurumsal veri keşfi süreçleri
- Veri kaynaklarının otomatik keşfi
- Veri şemalarının analiz edilmesi
- Veri profillemesi
- Veri kataloglarıyla entegrasyon
- Metadata üzerinden veri arama
- Veri varlıklarının sınıflandırılması
- Uygulama: Data Discovery Agent geliştirme

10. Data Quality Agents

- Veri kalitesi boyutları
- Veri kalitesi kurallarının oluşturulması
- Veri doğrulama ve tutarlılık kontrolleri
- Anomali tespiti
- Veri kalitesi problemlerinin sınıflandırılması
- Otomatik kalite raporları
- Veri kalitesi iyileştirme önerileri
- Uygulama: Data Quality Agent geliştirme

11. Metadata & Data Lineage Agents

- Metadata Management kavramları
- Technical ve Business Metadata
- Data Lineage kavramı
- Veri akışlarının ve bağımlılıkların analiz edilmesi
- Metadata kataloglarıyla entegrasyon
- Veri dönüşümlerinin izlenmesi
- Etki analizi (Impact Analysis)
- Uygulama: Metadata ve Lineage Analysis Agent

12. Human-in-the-Loop

- Human-in-the-Loop mimarileri
- İnsan onay mekanizmaları
- Kritik işlemlerde kontrol noktaları
- Approval Workflow tasarımı
- Agent execution pause/resume
- Manuel müdahale ve hata düzeltme

- Bankacılık sistemlerinde kontrollü ajan kullanımı
- Uygulama: İnsan onaylı veri güncelleme süreci

13. Agent Evaluation

- Agent Evaluation yaklaşımları
- Tool Calling doğruluğunun ölçülmesi
- Task Completion ve Success Rate
- RAG değerlendirme metrikleri
- Hallucination ve yanlış araç kullanımı analizi
- Test senaryoları ve benchmark oluşturma
- Regression Testing
- Uygulama: Agent Evaluation Pipeline

14. Observability

- Agent Observability kavramı
- Logging, Metrics ve Tracing
- Agent execution tracing
- Tool Calling izleme
- Token kullanımı ve maliyet analizi
- Latency ve performans ölçümü
- OpenTelemetry entegrasyonu
- Monitoring dashboard'ları
- Uygulama: Agent tracing ve monitoring

15. Security & Governance

- Agentic AI güvenlik riskleri
- Prompt Injection
- Tool misuse ve yetkisiz işlem riskleri
- Veri sızıntısı ve hassas veri yönetimi
- Agent güvenlik politikaları
- Audit Logging
- AI Governance prensipleri
- Kurumsal risk ve uyumluluk gereksinimleri

16. Permissions & Data Access

- Authentication ve Authorization
- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Least Privilege yaklaşımı
- Agent Identity

- Veri erişim politikalarının uygulanması
- Secret Management
- Veri tabanı ve API yetkilendirmeleri
- Bankacılık sistemleri için güvenli veri erişim senaryoları

17. Production Deployment & LLMOps

- Agentic AI uygulamalarının production mimarisi
- Containerization ve Docker
- Kubernetes üzerinde deployment yaklaşımları
- CI/CD süreçleri
- Agent Versioning
- Prompt ve model versiyonlama
- Configuration Management
- Monitoring ve Alerting
- Scalability ve High Availability
- LLMOps yaşam döngüsü
- Production hata yönetimi ve operasyonel süreçler

18. Uçtan Uca Uygulama: Enterprise Data Engineering Agent Platform

- Kurumsal veri platformu senaryosunun tanımlanması
- MCP tabanlı veri kaynaklarına erişim
- Data Discovery Agent geliştirme
- Data Quality Agent geliştirme
- Metadata / Lineage Agent geliştirme
- Multi-Agent orkestrasyon
- Human-in-the-Loop onay mekanizması
- Güvenlik ve yetkilendirme kontrolleri
- Agent Evaluation ve Observability entegrasyonu
- Production deployment mimarisinin oluşturulması

19. Önerilen 5 Günlük Dağılım

- 1. Gün: Agentic AI Architecture, Tool Calling, MCP
- 2. Gün: Agent Orchestration, Multi-Agent Architectures, RAG, Agent Memory
- 3. Gün: Database & API Agents, Data Discovery, Data Quality, Metadata & Lineage
- 4. Gün: Human-in-the-Loop, Agent Evaluation, Observability, Security & Governance, Permissions
- 5. Gün: Production Deployment, LLMOps, Uçtan Uca Uygulama
- Not: Derinlemesine uygulama ve production senaryolarına daha fazla zaman ayrılması istenirse eğitim süresi 6-7 güne genişletilebilir.

Ön Koşullar

- Python ile uygulama geliştirme deneyimi
- SQL ve ilişkisel veri tabanları hakkında bilgi
- REST API ve JSON veri formatlarına hakimiyet
- Veri mühendisliği ve ETL/ELT süreçleri hakkında temel bilgi
- LLM ve Generative AI kavramlarına aşinalık
- Docker, Git ve temel bulut/platform teknolojileri hakkında bilgi sahibi olunması önerilir