Model Context Protocol (MCP) Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bu eğitim, katılımcıların Model Context Protocol (MCP) mimarisini teknik açıdan kavramalarını ve büyük dil modellerini (LLM) API'ler, dosya sistemleri, veritabanları ve Git gibi harici sistemlerle güvenli biçimde entegre edebilmelerini sağlamak amacıyla hazırlanmıştır.

Bir günlük teknik program kapsamında MCP'nin çalışma prensipleri, istemci-sunucu mimarisi, araç çağırma (tool calling) mekanizmaları ve MCP sunucu geliştirme süreçleri ele alınacaktır. Katılımcılar, uygulamalı çalışmalarla temel bir MCP sunucusu oluşturmayı, Claude Code ve Cursor ortamlarında MCP araçlarını kullanmayı ve bu araçlar üzerinden harici sistemlerden veri almayı öğreneceklerdir.

Eğitimde ayrıca erişim izinleri, araç kapsamının sınırlandırılması, prompt injection riskleri, çıktı doğrulama ve denetim kayıtları gibi güvenlik konuları incelenecektir. Program sonunda katılımcıların, kurumsal gereksinimlere uygun, güvenli, kontrol edilebilir ve denetlenebilir MCP entegrasyonları tasarlayabilecek teknik bilgi ve becerileri kazanmaları hedeflenmektedir.

What You Will Learn

Bu eğitim sonunda katılımcılar;

- Model Context Protocol (MCP) mimarisini ve temel çalışma prensiplerini anlayabilecek,
- MCP Client, MCP Server ve Tool Calling mekanizmalarını öğrenebilecek,
- Araç tanımlama, şema oluşturma ve veri doğrulama işlemlerini gerçekleştirebilecek,
- Temel bir MCP sunucusu geliştirip çalıştırabilecek,
- Claude Code ve Cursor ortamlarında MCP entegrasyonları oluşturabilecek,
- Dosya sistemi, Git ve harici veri kaynaklarıyla bağlantılar kurabilecek,
- Erişim izinleri, Tool Scoping ve Prompt Injection risklerini yönetebilecek,
- Güvenli, kontrol edilebilir ve denetlenebilir MCP entegrasyonları geliştirebileceklerdir.

Outline

1. MCP Nedir? Temel Kavramlar ve Teorik Altyapı

- Büyük dil modellerinin harici sistemlere neden doğrudan erişemediği
- Tool Calling (araç çağırma) kavramı ve çalışma mantığı
- MCP'nin ortaya çıkış nedenleri ve çözmeyi hedeflediği ihtiyaçlar
- MCP ile geleneksel REST entegrasyonlarının karşılaştırılması

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Context Injection (bağlam ekleme) mekanizması
- MCP Client ve MCP Server mimarisinin temel bileşenleri

2. MCP Sunucusu Geliştirme (Uygulamalı)

- MCP araçlarının tanımlanması ve şema oluşturma
- Girdi ve çıktı doğrulama süreçleri
- Handler fonksiyonlarının geliştirilmesi
- JSON-RPC protokolünün temel prensipleri
- Yerel ortamda MCP sunucusunun çalıştırılması

3. Claude Code ile MCP Kullanımı

- MCP araçlarının Claude Code ortamına bağlanması
- Araç çağrılarının gerçekleştirilmesi ve yanıtların işlenmesi
- Plan-first yaklaşımı ile Tool Calling kullanımının birleştirilmesi
- Araçlar üzerinden veri toplama ve analiz senaryoları

4. Cursor ve MCP Entegrasyonu

- Agent Mode içerisinde MCP araçlarının kullanılması
- Kod üretimi sırasında MCP araçlarının çağrılması
- Dosya sistemi ve Git entegrasyonlarının gerçekleştirilmesi

5. MCP Güvenliği ve Kurumsal Kontrol Mekanizmaları

- Tool Scoping ile araçların erişim kapsamının belirlenmesi
- Yetki sınırlarının ve erişim izinlerinin yönetilmesi
- Prompt Injection saldırıları ve olası güvenlik riskleri
- Araç çıktılarının doğrulanması
- Audit ve Logging mekanizmalarının oluşturulması
- Kurum içi (On-Premises) MCP sunucu mimarisinin tasarlanması

6. Final Projesi: Uygulamalı MCP Geliştirme

- Temel bir MCP sunucusunun geliştirilmesi
- Geliştirilen sunucunun Claude Code ile entegre edilmesi

Model Context Protocol (MCP) Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- MCP araçları aracılığıyla veri çekme işlemleri
- Elde edilen verilerle rapor oluşturulması
- Örnek bir güvenlik senaryosunun uygulanması