Model Context Protocol (MCP) Training

Eğitim Açıklaması

LLM Integration and MCP Server Development – 1-Day Technical Program

The objective of this training is to enable participants to understand the Model Context Protocol (MCP) architecture and securely integrate LLM-based systems with external environments such as APIs, file systems, databases, and Git.

By the end of the training, participants will be able to understand the MCP architecture, build a simple MCP server, utilize MCP tools within Claude Code and Cursor environments, and design secure, enterprise-grade MCP architectures.

Training Outcomes

- Technical understanding of MCP architecture
- Ability to develop a basic MCP server
- Capability to integrate LLMs with external tools
- Ability to design enterprise MCP architectures
- Secure and auditable AI integration approach

Eğitim İçeriği Nedir?

1. What is MCP? (Theoretical Foundation)

- Why LLMs cannot directly connect to the external world
- Concept of tool calling
- Motivation behind the emergence of MCP

- MCP vs traditional REST integration
- Context injection mechanism
- MCP Client – MCP Server architecture

2. Building an MCP Server (Hands-on)

- Defining tools and creating schemas
- Input and output validation
- Writing handler functions
- JSON-RPC fundamentals
- Running a local MCP server

3. Using MCP with Claude Code

- Connecting MCP tools
- Calling tools and processing responses
- Plan-first + tool-calling approach
- Data retrieval and analysis scenarios

4. Cursor + MCP Integration

- Using tools in agent mode
- Calling MCP during code generation
- File system and Git integration

5. Security and Enterprise Controls

- Tool scoping
- Permission boundaries
- Prompt injection risks
- Output validation
- Audit and logging mechanisms
- Designing an on-prem MCP server

6. Final Hands-on Project

- Building a simple MCP server
- Integrating with Claude Code
- Fetching data via tools
- Generating reports
- Implementing a security scenario