# Model Context Protocol (MCP) Training

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

This training provides participants with a technical understanding of the Model Context Protocol (MCP) architecture and the skills needed to securely connect large language models (LLMs) with external systems, including APIs, file systems, databases, and Git.

During this one-day technical program, participants will explore the fundamental principles of MCP, its client-server architecture, tool-calling mechanisms, and the process of developing MCP servers. Through hands-on exercises, they will learn how to build a basic MCP server, connect MCP tools to Claude Code and Cursor, and retrieve information from external systems using these integrations.

The program also addresses essential security considerations, including permission boundaries, tool scoping, prompt injection vulnerabilities, output validation, and audit logging. By the end of the training, participants will have gained the technical knowledge and practical experience needed to design secure, manageable, and auditable MCP integrations that align with enterprise requirements.

## What You Will Learn

By the end of this training, participants will be able to:

- Understand the architecture and fundamental principles of Model Context Protocol (MCP).
- Explore MCP Client, MCP Server, and Tool Calling mechanisms.
- Define tools, create schemas, and validate input and output data.
- Develop and run a basic MCP server.
- Integrate MCP tools with Claude Code and Cursor.
- Connect MCP tools to file systems, Git, and external data sources.
- Manage access permissions, Tool Scoping, and Prompt Injection risks.
- Build secure, controlled, and auditable MCP integrations.

## Outline

### 1. Understanding MCP: Concepts and Theoretical Foundations

- Why large language models cannot directly access external systems
- Understanding the concept and functionality of tool calling
- The motivation and requirements behind the introduction of MCP
- Comparing MCP with conventional REST-based integrations

# Model Context Protocol (MCP) Training

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- How the context injection mechanism works
- Core components of the MCP Client–Server architecture

### 2. Developing an MCP Server (Hands-on)

- Defining MCP tools and creating their schemas
- Implementing input and output validation
- Developing handler functions
- Understanding the fundamentals of JSON-RPC
- Setting up and running an MCP server locally

### 3. Working with MCP in Claude Code

- Connecting MCP tools to the Claude Code environment
- Executing tool calls and handling their responses
- Combining a plan-first approach with tool calling
- Practical scenarios for data retrieval and analysis

### 4. Integrating MCP with Cursor

- Working with MCP tools in Agent Mode
- Invoking MCP tools during code generation
- Establishing file system and Git integrations

### 5. MCP Security and Enterprise Governance

- Defining tool access through tool scoping
- Managing permission boundaries and access restrictions
- Understanding prompt injection threats and security risks
- Validating outputs returned by MCP tools
- Implementing audit trails and logging mechanisms
- Designing an on-premises MCP server architecture

### 6. Final Project: Hands-on MCP Implementation

- Developing a functional basic MCP server
- Connecting the developed server to Claude Code

# Model Context Protocol (MCP) Training

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Retrieving external data through MCP tools
- Creating reports using the retrieved information
- Implementing a practical security scenario