Course Title

Enterprise AI Agents, MCP Servers, and Secure AI Development with ASP.NET and Azure AI Foundry (5 Days)

Prerequisites:

- Basic knowledge of **C#, ASP.NET Core, and REST APIs**.
- Familiarity with **Azure fundamentals and JSON** is recommended but not mandatory.

Day 1: Foundations of Agentic AI and Azure AI Foundry

Module 1: Introduction to Generative AI

- LLM fundamentals
- Tokens, context windows, embeddings
- AI application architectures
- Limitations and risks

Module 2: Agentic AI Fundamentals

- What are AI agents?
- Single-agent vs multi-agent systems
- Planning, reasoning, and memory
- Human-in-the-loop patterns
- Enterprise use cases

Module 3: Azure AI Foundry

- Creating projects
- Model deployments
- Agent creation
- Agent lifecycle
- Testing and debugging agents

Lab

- Create your first Foundry agent

- Connect it to an ASP.NET application

Day 2: Tools, Endpoints, and Enterprise Integrations

Module 4: Agent Tools

- Built-in tools
- File Search
- Code Interpreter
- Grounding concepts

Module 5: Custom Integrations

- Function tools
- OpenAPI tools
- REST endpoints
- When to use each approach

Module 6: Enterprise Design Patterns

- Tool orchestration
- Error handling
- API versioning
- Designing business capabilities as tools

Lab

- Connect external APIs
- Build custom tools for an agent

Day 3: MCP Servers with ASP.NET and Logic Apps

Module 7: Model Context Protocol (MCP)

- MCP architecture
- MCP vs REST APIs
- MCP vs OpenAPI tools
- Stateful vs stateless implementations

Module 8: Building MCP Servers in ASP.NET Core

- Tool registration

- Dependency Injection
- Logging
- Configuration
- Database integration

Module 9: Low-Code MCP with Logic Apps

- Creating Logic Apps
- Exposing business workflows
- Email and approval processes
- Connecting enterprise SaaS systems

Lab

- Weather MCP Server
- Employee Management MCP Server
- Logic App MCP integration

Day 4: Identity, Security, Governance, and Secrets

Module 10: Identity Management

- Microsoft Entra ID fundamentals
- RBAC
- Service principals
- Managed identities
- User-assigned vs system-assigned identities

Module 11: Securing Agents and MCP Servers

- Who can access agents?
- Who can invoke tools?
- OAuth and API keys
- Authentication patterns
- Enterprise authorization strategies

Module 12: Secrets and Configuration

- Azure Key Vault
- Secret rotation
- Certificates

- Access policies
- Using Managed Identity with ASP.NET

Module 13: Guardrails and Responsible AI

- Content filters
- Custom instructions
- Preventing sensitive data access
- Enterprise governance
- Compliance considerations

Lab

- Secure an MCP server using Entra ID
- Store secrets in Key Vault
- Configure guardrails

Day 5: Knowledge, Deployment, and Production Readiness

Module 14: Enterprise Knowledge Integration

You should definitely add this.

- File Search
- Vector stores
- Azure AI Search basics
- Retrieval-Augmented Generation (RAG)
- When to use RAG vs MCP

Module 15: Monitoring and Observability

- Logging
- Tracing
- Diagnostics
- Token usage monitoring
- Cost optimization

Module 16: Deployment Strategies

- Docker containers
- Azure Container Apps
- Azure App Service
- CI/CD with Azure DevOps
- Environment management