

MCP (Model Context Protocol)

Code : EAI-MCP-100

Durée : 1 jour (7 heures)

Public visé

Data Scientists, Data Analysts, ingénieurs Data, ingénieurs MLOps, développeurs, architectes Data, cadres dirigeants, managers, chefs de projets, Product Managers IA.

Prérequis

- Formation IA ou compétences équivalentes en IA
- Familiarité avec Python

Objectifs pédagogiques

À l'issue de cette formation, vous serez capable de :

- Concevoir des architectures composables à base de serveurs MCP
- Connecter des LLM à des outils et données exposés via le protocole MCP
- Implémenter des workflows d'IA utilisant le Model Context Protocol
- Identifier les meilleures pratiques d'authentification et sécurité en production

Programme

Matin : Introduction à MCP

Pourquoi MCP

- Intégrations, flexibilité, sécurité

Architecture

- Hôtes, clients, serveurs, sources locales, services distants

Serveurs disponibles

- Filesystem, PostgreSQL, Docker, Kubernetes, GitHub

Clients

- Fast-agent, Claude Desktop App, Copilot-MCP

Protocole

- Trois couches : protocole, transport, messages
- Cycle de vie des connexions

- Accès aux données via ressources
- SDK : Python, TypeScript, Java, Kotlin, C#

Après-midi : Notions avancées

Modèles de prompts et comportements agentiques

- Sampling et limitation du périmètre avec roots

Observabilité

- Logs et gestion des erreurs
- Inspection, tests et débogage
- Suivi de performance

Authentification et sécurité

- Données sensibles, contrôle d'accès, OAuth

Modalités d'évaluation des acquis

- En cours de formation, par des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation