+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 15/07/2025

S'inscrire

Formation Agent IA avec Model Context Protocol

4 jours (28 heures)

Présentation

Notre formation Agents IA avec Model Context Protocol vous permettra de comprendre le fonctionnement de MCP et de créer vos propres agents IA connectés. Vous apprendrez à déployer un client, à développer des serveurs MCP en Python, à orchestrer des appels d'outils multiples, et à intégrer ces agents dans des workflows data ou applicatifs.

Vous saurez concevoir des assistants qui résument des fichiers PDF, répondent à des questions métier via SQL, ou appellent des services externes, le tout sans écrire une ligne de code dans l'agent lui-même.

MCP permet une interaction sécurisée, modulaire et transparente entre LLM et vos systèmes internes, sans exposer vos données ou vos clés.

À l'issue de cette formation, vous serez en mesure de créer, connecter et superviser des agents IA interopérables dans vos environnements métiers. Comme toutes nos formations, celle-ci est conçue autour de la dernière spécification stable du protocole MCP, avec outils et SDK à jour.

Comme pour toutes nos formations, celle-ci vous sera présentée avec les toutes dernières avancées en matière d'Agents IA avec Model Context Protocol.

Objectifs

- Comprendre le rôle et l'architecture des agents IA connectés via MCP
- Déployer un client et connecter des serveurs MCP
- Créer vos propres outils accessibles via MCP (fichiers, bases, API)
- Orchestrer des workflows IA multi outils avec raisonnement autonome
- Intégrer un agent dans un pipeline data ou un poste de travail sécurisé

Public visé

- Data engineers
- Développeur IA / Pyhton
- Responsable Innovation ou IT
- Analystes techniques

Pré-requis

- Connaissance de base en Python et manipulation de fichiers/appels API
- Notions en IA générative ou utilisation de LLM recommandées
- Connaissance d'outils data (fichiers, SQL, JSON, REST) appréciée
- Aucun prérequis sur le protocole MCP : tout est introduit dans le cours

Programme de notre Formation Agent IA avec Model Context Protocol

Introduction aux agents IA modernes

- Qu'est-ce qu'un agent IA : définition, composants, capacités
- Évolution des assistants LLM vers des agents autonomes
- Limitations des LLM isolés vs connectés
- Modèle d'agent = LLM + outils + raisonnement + contexte
- Cas d'usage dans la donnée, l'entreprise, la recherche

Présentation du Model Context Protocol (MCP)

- Objectifs du protocole : standardiser l'accès aux outils
- Clients MCP (Claude, ChatGPT, etc.) vs serveurs MCP
- Fonctionnement technique : échange de messages structurés
- Architecture client/serveur + découverte dynamique
- Avantages sur les API propriétaires (interopérabilité, sécurité)

Installer et configurer son environnement MCP

- SDK et outils : mcp, cmcp, Claude Desktop, OpenAI + tools
- Structure d'un projet MCP (manifest, services, log)
- Lancement d'un client MCP local (agent IA + serveur)
- Connexion à Claude ou ChatGPT avec outils personnalisés
- Atelier : Lancer un agent IA local avec un serveur de fichiers en MCP pour résumer un PDF

Créer son premier serveur MCP

- Anatomie d'un serveur MCP
- Définir les méthodes exposées, le schéma d'entrée/sortie

- Configurer les permissions et la sécurité locale
- Journaliser les appels + structurer les réponses
- Exemples simples : lecture de fichier, transformation de texte

Exposer des données tabulaires et analytiques

- Connexion à une base SQLite ou PostgreSQL via MCP
- Création d'un serveur "query-db" en langage naturel
- Gestion des erreurs SQL + validation de requêtes
- Contrôle d'accès aux colonnes ou schémas
- Atelier : Créer un agent qui répond à des questions métier en interrogeant une base de données

Interaction avec des API externes

- Appel d'API REST à partir d'un serveur MCP
- Mapping paramètres / documentation API ? schema MCP
- Gestion des clés API en sécurité côté serveur
- Utiliser l'agent pour orchestrer des appels complexes
- Exemple : API météo, OpenAI, outil interne REST

Enrichir un agent multi-outils

- Enchaînement d'actions : raisonnement + appel MCP
- Planification pas à pas avec Claude ou ChatGPT
- Réutilisation des résultats intermédiaires
- Multiples serveurs MCP pour une tâche unique
- Atelier : Construire un agent qui lit un fichier PDF, extrait une info, puis interroge un second outil

Conception avancée : outils, chaînes et mémoire

- Structuration d'un "toolkit" d'entreprise
- Stockage temporaire des données de contexte
- Intégration mémoire conversationnelle + appels d'outils
- Exemple : "chaîne de brief client ? dashboard ? synthèse PDF"
- Gestion du formatage, des tokens et des résumés

Sécurité et gouvernance dans MCP

- Permissions serveur : scoping, fonctions autorisées
- Isolation des données locales vs cloud
- Journalisation des accès et auditabilité
- Cloisonnement par utilisateur ou service
- Modèle de confiance vs boîte noire LLM

Intégration dans un workflow data/IA

- Utiliser un agent MCP comme outil dans un pipeline
- Appels automatisés (cron, Airflow, Bash, FastAPI)
- Export des résultats (CSV, base, API, mail…)
- Atelier : Créer un mini-workflow automatisé orchestré par agent IA (lecture ? requête ? synthèse)

Comparaison avec LangChain et autres frameworks

- ReAct, OpenAI agents, LangChain : différences clés
- MCP vs outil + wrapper (plug-and-play vs orchestration)
- Forces : simplicité, interopérabilité, sécurité
- Limites actuelles de MCP (asynchrone, streaming, GPT-4o…)
- Choisir la bonne approche selon les cas d’usage

Déploiement, maintenance et perspectives

- Packager et redéployer un serveur MCP
- Hébergement local, cloud, container, ou serverless
- Mutualiser les outils dans un workspace d’équipe
- Roadmap du protocole MCP (authentification distante, marché d’outils)
- Agents full-autonomes + supervision

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.