

Agents IA – Etat de l'art et mise en oeuvre

2 jours (14 heures)

Initiation

Présentiel ou classe à distance

à partir de

1750 € HT par personne (TVA en vigueur)

Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

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

- Décrire l'état de l'art des agents d'Intelligence Artificielle (IA) (concepts, tendances et écosystème outils / cadres)
- Concevoir l'architecture d'un agent IA (LLM, RAG, outils, mémoire et protocoles de communication)
- Mettre en oeuvre des agents IA simples puis multi-agents avec au moins un framework moderne (LangGraph, CrewAI, AutoGen...)
- Intégrer des agents IA dans un SI existant via des API, outils métiers et protocoles (MCP, A2A)
- Appliquer les bonnes pratiques de sécurité, de guardrails et de gouvernance pour des agents en production
- Mettre en place l'observabilité, l'évaluation et le pipeline de déploiement (CI/CD) pour des agents IA en environnement professionnel.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Développeurs logiciels (backend / full-stack) travaillant sur des projets d'Intelligence Artificielle (IA) ou d'intégration de LLM, architectes techniques / software architects impliqués dans la conception de solutions IA, Tech Leads et engineering managers responsables de projets d'agents IA ou de plateformes IA internes, data engineers / MLOps / DevOps devant intégrer, déployer et superviser des agents IA et consultants IT engagés dans des projets de transformation numérique incluant de l'IA Générative.

Prérequis

Avoir une maîtrise d'un langage de programmation (idéalement Python) pour suivre et adapter les exemples de code ainsi que des connaissances de base sur les LLM (prompts, température, context window...). Avoir des notions d'API REST et de consommation d'API (authentification, JSON et HTTP) et une connaissance générale des architectures applicatives modernes (services, microservices, queues...). Etre à l'aise avec la ligne de commande et les outils de développement modernes (Git, environnements virtuels et Docker) est un plus.

Programme

1 Pendant votre formation

Agents IA – Etat de l'art et mise en oeuvre

Jour 1 – Matin

Introduction aux agents d'Intelligence Artificielle (IA)

- Définition d'un agent IA, chatbot et assistant IA
- Du LLM passif à l'agent autonome : historique et évolution
- Les capacités fondamentales :
 - Planification
 - Raisonnement
 - Utilisation d'outils
 - Mémoire
- Taxonomie des agents :
 - Réactifs
 - Délibératifs
 - Hybrides
- Panorama du marché et tendances :
 - Agents collaboratifs
 - Agents personnels
 - IA agentique en entreprise
- L'IA agentique en chiffres :
 - Adoption
 - ROI
 - Perspectives (McKinsey, Gartner et PwC)

Modèles de langage et capacités agentiques

- Modèles de raisonnement (chain-of-thought et inference-time compute)
- Modèles petits vs grands : orchestrateurs et agents spécialisés
- Fenêtres de contexte étendues et leur impact sur les agents
- Function calling / Tool calling :
 - Principe
 - Schémas types
 - Parallel tool calling
- Structured outputs et extraction de données

Exemples de travaux pratiques (à titre indicatif)

- Implémenter un function calling avec une API de LLM Cloud type ChatGPT
- Définir des outils typés et traiter les appels de fonctions dans une boucle agentique

Jour 1 – Après-midi

RAG et RAG agentique

- Rappels sur le RAG classique :
 - Embeddings
 - Vector stores
 - Retrieval
 - Generation
- Limites du RAG statique
- RAG agentique :
 - Boucle plan
 - Retrieve
 - Act
 - Reflect
 - Answer
- Stratégies de chunking, reranking et hybrid search
- Gestion de la fenêtre de contexte et context management

Exemples de travaux pratiques (à titre indicatif)

- Construire un pipeline RAG agentique : l'agent décide quand et quoi rechercher, reformule ses requêtes et vérifie ses réponses

Protocoles de communication : MCP et A2A

- Model Context Protocol (MCP)
 - Architecture client-serveur
 - MCP Servers et MCP Clients
 - Interopérabilité multi modèles

- Ecosystème : Smithery, Glama et marketplaces de serveurs MCP
- Agent-to-Agent Protocol (A2A)
 - Architecture peer-to-peer
 - Agent Cards et découverte de capacités
 - Coordination horizontale entre agents
- MCP vs A2A :
 - Intégration verticale vs coordination horizontale
- Utiliser MCP et A2A ensemble :
 - Routing d'agents et exécution d'outils

Exemples de travaux pratiques (à titre indicatif)

- Configurer un serveur MCP, connecter un agent client, puis exposer un agent via A2A avec une Agent Card

Jour 2 – Matin

Frameworks d'agents IA

- LangChain / LangGraph :
 - Ecosystème complet
 - Workflows stateful en graphe
 - Intégrations massives
- CrewAI :
 - Orchestration par rôles
 - Délégation de tâches
 - Collaboration multi-agents
- Microsoft AutoGen :
 - Conversations multi-agents
 - Exécution de code sandboxée
- OpenAI Agents SDK :
 - Handoffs
 - Guardrails intégrés
 - Computer Use Agent
- Google ADK (Agent Development Kit) :
 - Orchestration flexible
 - Architectures hiérarchiques
- Autres :
 - LlamaIndex
 - Semantic Kernel

- AgentGPT

Exemples de travaux pratiques (à titre indicatif)

- Construire un agent avec LangGraph (workflow en graphe avec état), puis le même scénario avec CrewAI (équipe de rôles)
- Comparer les approches

Systèmes multi-agents

- Architectures :
 - Orchestrateur central
 - Peer-to-peer
 - Hiérarchique
- Patterns de conception :
 - Superviseur
 - Chaîne séquentielle
 - Routage dynamique
 - Agents imbriqués
- Communication inter-agents :
 - Handoffs
 - Mémoire partagée
 - Message bus
- Equipes d'agents collaboratifs :
 - Spécialisation
 - Délégation
 - Consensus
- Gestion de l'état et de la mémoire dans les systèmes multi-agents

Exemples de travaux pratiques (à titre indicatif)

- Créer un système multi-agents (3 agents spécialisés et 1 orchestrateur) pour un cas métier :
 - Analyse de données
 - Rédaction de rapport
 - Validation qualité

Jour 2 – Après-midi

Sécurité, guardrails et gouvernance

- Risques agentiques :
 - Prompt injection
 - Tool use toxique
 - Escalade de privilèges

- Framework de guardrails :
 - Validation d'entrée
 - Filtrage de sortie
 - Contraintes comportementales
- Les 3 piliers :
 - Guardrails
 - Permissions
 - Auditabilité
- La défense en couches
- La sécurité des identités agents
- Sandboxing des outils et isolation d'exécution
- Conformité et régulation : EU AI Act, NIST AI RMF...
- Shadow agents et gouvernance d'entreprise

Exemples de travaux pratiques (à titre indicatif)

- Implémenter des guardrails sur un agent existant avec validation d'input, filtrage d'output, restrictions d'outils et logging d'audit

Observabilité, évaluation et déploiement en production

- Observabilité :
 - Tracing distribué des agents : LangSmith, Maxim, OpenTelemetry...
 - Visualisation des traces : chaque étape, appel d'outil et réponse LLM
 - Métriques clés : coût, latence, qualité des réponses et taux d'erreur
 - Détection automatique de patterns et clustering de conversations
- Evaluation :
 - Métriques custom et évaluateurs LLM (LLM-as-a-judge)
 - Datasets d'évaluation à partir des traces
 - Tests automatisés : unitaires, intégration, performance et sécurité
- Déploiement :
 - Pipeline CI/CD pour agents IA
 - Environnements staging / production
 - Rollout progressif, A/B testing et canary deployments
 - Scaling horizontal et gestion de charge
 - Human-in-the-loop : escalade, timeouts et boucles de feedback
 - Checklist de mise en production

Exemples de travaux pratiques (à titre indicatif)

- Instrumenter un agent avec LangSmith (tracing)
- Définir des métriques d'évaluation custom

- *Simuler un déploiement avec rollback*

Cas d'usage en entreprise et perspectives

- Cas d'usage à forte valeur ajoutée
 - Service client autonome
 - Automatisation financière (traitement de factures, détection de fraude...)
 - Maintenance prédictive industrielle
 - Assistants RH et onboarding
 - Chaîne logistique et gestion des risques fournisseurs
- Retours d'expérience
- Tendances :
 - Agents continus
 - Apprentissage continu
 - IA spatiale...
- Recommandations pour démarrer un projet agent IA en entreprise

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)

- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 3 décembre 2026 au 4 décembre 2026 (2 jours / 14 heures)

Mulhouse

Du 3 décembre 2026 au 4 décembre 2026 Mulhouse

- 3 décembre 2026 9h00 – 16h30
- 4 décembre 2026 9h00 – 16h30