AYI NEDJIMI Consultants

Intégrer une API LLM en Fonction IA : Guide Tutoriel 2026

9 mai 2026 • Mis à jour le 17 mai 2026 • 27 min de lecture • 5564 mots • 89 vues •

> Tutoriel pas à pas pour intégrer une API LLM en tant que fonction IA : du function calling au protocole MCP, en passant par JSON Schema, la boucle ReAct multi-tour, la sécurité (Pydantic, sandbox, audit), les frameworks (OpenAI SDK, Anthropic SDK, LangChain, Pydantic AI) et les cas d'usage cybersécurité (SOC, threat intel, IR runbook).

Intégrer une **API LLM en tant que fonction IA** est devenu en 2026 le pivot architectural des applications intelligentes modernes : plutôt que de confiner un modèle de langage à la simple génération de texte, le **function calling** (ou *tool use* chez Anthropic, *tools* chez OpenAI) permet au LLM de déclencher des fonctions déterministes, d'interroger des API métier, d'exécute

SQL, de manipuler des fichiers ou d'orchestrer des workflows complexes. Cette mécanique transforme un assistant conversationnel passif en agent autonome capable d'agir sur le monde réel, et constitue le socle des architectures *agentic AI* qui dominent les déploiements d'entreprise en 2026. Pour un RSSI, un architecte logiciel ou un développeur senior, maîtriser le function calling n'est plus une option : c'est la compétence qui sépare un prototype de chatbot d'une application IA productive intégrée au SI. Ce tutoriel détaille pas à pas la conception d'une fonction IA, depuis la définition du schéma JSON Schema jusqu'à la boucle ReAct multi-tour, en passant par les pièges de sécurité, les patterns de tests automatisés, les frameworks (OpenAI SDK, Anthropic SDK, LangChain, Pydantic AI) et les cas d'usage cybersécurité (assistant SOC, enrichissement threat intel, automatisation IR runbook). L'objectif est d'acquérir une compréhension opérationnelle, du protocole sous-jacent à la mise en production sécurisée.

À RETENIR

Points clés à retenir

Le function calling est un protocole standardisé où le LLM ne fait pas l'appel lui-même : il émet un *tool_call* JSON structuré que le code applicatif intercepte, exécute, puis renvoie au modèle pour la génération finale.

JSON Schema est la lingua franca : OpenAI, Anthropic, Mistral, Cohere, Google et le Model Context Protocol (MCP) convergent tous sur ce format pour dé
signatures et paramètres des outils.

Réponse sous 24h

Devis gratuit →