AKADEMIA
FORMATION

PROGRAMME DE FORMATION

Agents IA avec Claude — SDK et Managed Agents

DURÉE	FORMAT	PUBLIC	CERTIFICATION
2 jours 14 heures	**Inter · Intra** Présentiel ou distanciel	**Tout collaborateur**	**Incluse**

À PROPOS DE LA FORMATION

Agents IA avec Claude — SDK et Managed Agents.

DURÉE	FORMAT	PÉDAGOGIE	CERTIFICATION
2 jours	**Inter · Intra**	**Active**	**Incluse**
14 heures	Présentiel ou distanciel	Petits groupes	Attestation délivrée

Objectifs pédagogiques

- Maîtriser l'Agent SDK (Python/TypeScript) : fonction query(), options, sessions et persistance de contexte
- Implémenter des boucles agentiques autonomes avec les outils built-in (Read, Edit, Bash, Glob, Grep, WebSearch)
- Configurer des guardrails programmatiques via les Hooks (PreToolUse, PostToolUse, Stop)
- Concevoir des architectures multi-agent avec subagents et orchestration
- Déployer des Managed Agents via l'API /v1/agents et /v1/sessions avec environnements sandbox
- Exploiter les fonctionnalités avancées : Memory Stores, Outcomes avec grader automatique, custom tools
- Sécuriser et monitorer des agents en production (permissions, tracing, rate limits, networking)

PROGRAMME

Huit modules progressifs pour monter en compétences.

MODULE

01.

1H45H

Introduction aux agents IA : concepts et positionnement

CONTENU PÉDAGOGIQUE

- Qu'est-ce qu'un agent IA ? De la conversation à l'action autonome
- Agent SDK vs Managed Agents : contrôle local vs infrastructure cloud managée
- Quand utiliser quoi : CI/CD et agents locaux vs tâches longues et sandbox cloud
- Multi-provider : Bedrock, Vertex AI, Azure AI Foundry — au-delà de l'API Anthropic
- Démonstration : un agent qui lit, analyse et corrige du code de manière autonome

MODULE

02.

1H45H

Agent SDK : query(), options et sessions

CONTENU PÉDAGOGIQUE

- Installation et authentification : pip install claude-agent-sdk, clé API, variables d'environnement
- La fonction query() : point d'entrée, streaming asynchrone, boucle d'outils automatique
- ClaudeAgentOptions : allowed_tools, permission_mode, hooks, agents, mcp_servers
- Sessions et persistance de contexte : capturer le session_id, reprendre avec resume
- Configuration filesystem : CLAUDE.md, Skills, Slash Commands, setting_sources

MODULE

03.

1H45H

Outils built-in et permissions granulaires

CONTENU PÉDAGOGIQUE

- Les 10 outils intégrés : Read, Write, Edit, Bash, Monitor, Glob, Grep, WebSearch, WebFetch, AskUserQuestion
- Contrôle des permissions : restreindre un agent en lecture seule (Read, Glob, Grep uniquement)
- Différence fondamentale : Client SDK classique (boucle manuelle) vs Agent SDK (boucle autonome)
- Compaction automatique du contexte et gestion des retries
- TP guidé : créer un agent de code review en lecture seule avec rapport structuré

MODULE

04.

1H45H

Hooks et Guardrails : sécuriser la boucle agent

CONTENU PÉDAGOGIQUE

- Architecture des Hooks : PreToolUse, PostToolUse, Stop, SessionStart, SessionEnd
- HookMatcher : filtrer par outil avec patterns ("Edit|Write"), bloquer ou valider
- Cas pratique : audit trail — logger toutes les modifications de fichiers
- Intégration MCP dans l'Agent SDK : connecter des serveurs MCP externes (Playwright, bases de données)
- TP guidé : implémenter des guardrails qui bloquent les écritures hors d'un répertoire autorisé

MODULE

05.

1H45H

Multi-Agent : subagents et orchestration

CONTENU PÉDAGOGIQUE

- Subagents dans l'Agent SDK : AgentDefinition, description, prompt, tools dédiés
- Pattern orchestrator-workers : l'agent principal délègue aux agents spécialisés
- parent_tool_use_id : tracer les messages provenant de chaque subagent
- Multi-agent dans Managed Agents : threads isolés, filesystem partagé, un seul niveau de délégation
- Cas d'usage : code review + génération de tests + recherche web en parallèle
- TP guidé : construire un système orchestrateur avec 2 subagents spécialisés

MODULE

06.

1H45H

Managed Agents API : agents cloud autonomes

CONTENU PÉDAGOGIQUE

- Créer un agent (POST /v1/agents) : modèle, system prompt, agent_toolset_20260401
- Environnements (POST /v1/environments) : packages pip/npm/apt, networking unrestricted/limited
- Sessions (POST /v1/sessions) : instancier un agent dans un environnement
- Streaming SSE : événements agent.message, agent.tool_use, session.status_idle
- Custom tools : définir des outils personnalisés, traiter agent.custom_tool_use
- Désactiver/activer des outils spécifiques : whitelist et blacklist dans l'agent_toolset

MODULE

07.

1H45H

Fonctionnalités avancées : Memory, Outcomes, Custom Tools

CONTENU PÉDAGOGIQUE

- Memory Stores : persistance cross-session, 6 outils automatiques (list, search, read, write, edit, delete)
- Écritures sécurisées : préconditions not_exists et content_sha256 (concurrence optimiste)
- Audit avec Memory Versions : traçabilité immutable, redaction RGPD pour supprimer les secrets
- Outcomes : définir des résultats attendus avec rubric, grader automatique, itérations (max 20)
- Files API : récupérer les livrables depuis /mnt/session/outputs/
- TP guidé : agent avec Memory Store qui apprend les préférences entre sessions

MODULE

08.

1H45H

Production : sécurité, monitoring et déploiement

CONTENU PÉDAGOGIQUE

- Rate limits : 60 req/min (création), 600 req/min (lecture), spend limits par organisation
- SDKs disponibles : Python, TypeScript, Java, Go, C#, Ruby, PHP + CLI ant
- Networking sécurisé : mode limited avec allowed_hosts, allow_mcp_servers, moindre privilège
- Événements de tracing : span.model_request_start/end, token counts, observabilité
- Événements session : status_running, status_idle, status_rescheduled, status_terminated
- TP final : déployer un agent Managed en production avec environnement sécurisé et monitoring

PASSONS À L'ACTION

Construisons ensemble votre session sur-mesure.

Dites-nous vos contraintes (format, lieu, dates, nombre de participants) et recevez une proposition personnalisée sous 24 heures ouvrées.

Akademia Formation

SERVICE ADMINISTRATION DES VENTES

adv@akademiaformation.com

www.akademiaformation.com

Devis personnalisé

RÉPONSE SOUS 24 H OUVRÉES

Format inter · intra

Présentiel ou distanciel

FIN DU PROGRAMME