

Formation Développeur augmenté par l'IA – Avancé : orchestrer des agents et sécuriser le code produit

Réf. SF34751

Passez d'un agent à une équipe d'agents coordonnés, en maîtrisant le contexte qu'ils partagent ainsi que la qualité et la sécurité du code qu'ils livrent.

1 j
Durée

800 € HT
Inter / participant

0
Sessions à venir

Objectifs pédagogiques

- ✓ Architecturer le contexte d'un projet (instructions, skills, spécifications) pour le rendre exploitable par plusieurs agents
- ✓ Concevoir et orchestrer un workflow multi-agents, du ticket à la pull request, avec des points de supervision humaine
- ✓ Implémenter des contrôles automatiques de qualité sur le code produit par les agents
- ✓ Configurer la sécurité du code produit et de l'exécution des agents : scans, moindre privilège, isolation, défense contre l'injection de prompt

Public visé & prérequis

Public visé Architectes logiciels, Développeurs

Prérequis- Avoir suivi la formation Développeur augmenté par l'IA, ou pratiquer un agent de code au quotidien (fichier d'instructions, mode plan, revue de diff) - Maîtriser Git (branches, pull requests) et savoir lire un pipeline d'intégration continue

Programme détaillé

Ingénierie de contexte : architecturer ce que voient les agents

- Contexte de session et contexte persistant : ce qui reste éphémère, ce qui doit être capturé, versionné et partagé
- Architecture des fichiers d'instructions : niveaux global, projet et dossier, sans dérive ni contradiction
- Chargement à la demande : skills et documentation référencée plutôt qu'un fichier principal surchargé
- Budget de contexte : signes de saturation, compaction, isolation d'une tâche dans un sous-agent
- Spécifications comme contexte (spec-driven development) : de la spec au plan puis aux tâches, avec des outils comme Spec-Kit ou les modes spec intégrés aux agents
- Cohérence spec / code dans la durée : mettre à jour la spec plutôt que corriger le code à la main
- Document d'état : la mémoire de travail qui permet de reprendre une tâche longue ou de la transmettre à un autre agent

Activités pratiques :

- Audit et restructuration du contexte du dépôt fil rouge : ce qui reste en session, ce qui devient un asset partagé
- Rédaction d'une spécification exploitable par un agent et dérivation du plan de tâches
- Conception d'un skill qui encapsule une procédure récurrente du projet

Orchestrer plusieurs agents

- Limites de l'agent unique : contexte saturé, auto-validation, tâches trop larges
- Rôles spécialisés : planification, implémentation, tests, revue contradictoire, préparation de la pull request
- Patterns d'orchestration : séquentiel, parallèle, supervisé par un agent orchestrateur
- Agents en parallèle : branches ou worktrees isolés, répartition du travail, fusion des résultats
- Passage de relais : document d'état partagé, critères de fin de tâche, points de validation humaine
- Reprise sur erreur : détecter une dérive, relancer une étape, reprendre la main
- Choix du modèle et de l'effort de raisonnement par rôle : équilibre entre qualité, délai et coût

Activités pratiques :

- Workflow à deux agents (plan puis implémentation) sur un ticket du dépôt fil rouge
- Enrichissement du workflow avec un agent de revue et un agent de préparation de PR
- Deux agents travaillant en parallèle sur des worktrees séparés, puis fusion

Garantir la qualité du code produit

- Contrôles déterministes plutôt que consignes : hooks bloquants pour les tests, le lint et le typage
- Agent de revue contradicteur : critères explicites, désaccords tracés, arbitrage humain
- Validation multi-critères : maintenabilité, performance et sécurité vérifiées à chaque itération
- Revue humaine proportionnée au risque : où concentrer l'attention selon la nature du changement
- Revue automatique des pull requests en intégration continue : configuration, périmètre et limites
- Suivre la qualité dans le temps : régressions, dette, taux de reprise des PR produites par des agents

Activités pratiques :

- Pipeline de validation automatique multi-critères appliqué au workflow multi-agents
- Mise en place de hooks bloquants et d'une revue automatique des PR sur le dépôt fil rouge

Sécuriser le code et les agents

- Scans dans la boucle : analyse statique, dépendances et secrets vérifiés par l'agent et en intégration continue
- Dépendances inventées ou typosquattées : contrôle avant installation, listes autorisées
- Moindre privilège : permissions par rôle d'agent, commandes autorisées, accès réseau et fichiers restreints
- Exécution isolée : conteneur ou sandbox pour les agents qui travaillent en autonomie
- Injection de prompt : instructions malveillantes cachées dans une issue, une page web, un fichier ou une réponse d'outil
- Confiance dans les extensions tierces : serveurs MCP, skills et plugins à évaluer avant adoption
- Traçabilité : journaliser les actions des agents pour pouvoir auditer et expliquer un changement

Activités pratiques :

- Ajout d'un scan de secrets et de dépendances au workflow du dépôt fil rouge
- Configuration des permissions de chaque agent du workflow selon son rôle
- Démonstration d'une injection de prompt via une issue piégée, puis mise en place de la parade

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 165 avis

Selim B. — Très bonne formation, très instructif même après quelques années de Python dans les bras. Une très petite équipe de stagiaires qui facilite les échanges. Je redoutais le mode...

Alexis C. — Anthony explique bien les concepts attendus et prend le temps de répondre aux questions et aux différents problèmes rencontrés. Le support présenté créé par lui-même est différent des...

Ils nous font confiance

Cette année notre filière Développement et Ingénierie de Logiciels a accompagné plus de 459 entreprises dont :

SOPRA STERIA RENAULT SAS ORANGE CAMPUS TECH ORANGE INNOVATION SCHOOL STMICROELECTRONICS ARPEGE GRANT THORNTON FRANCE ORANGE BUSINESS RTE SII ILE DE FRANCE +449 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com