

IA & Cybersécurité

Journée d'immersion - Programme complet

Une journée d'immersion pour les profils IT et Cyber : consolider les fondamentaux, automatiser des usages concrets et construire des agents IA adaptés à leur réalité professionnelle.



CADRE DE LA JOURNÉE

Une immersion IA appliquée aux métiers IT & Cyber

Public cible

- DSI, RSSI, CTO, DAF, Analyste SOC, Expert en conformité
- Administrateur Systèmes et Réseaux, Ingénieur cloud
- Acteur MSP et ESN, Ingénieur Data, etc.

Prérequis

- Utilisation des IA génératives au quotidien dans le cadre professionnel.
- Savoir écrire un prompt simple.
- Avoir configuré son IA selon les process de son entreprise : contexte, rôle, tâches, missions et objectifs.

Objectifs de l'immersion

- Passer du prompt manuel à l'exécution automatisée de l'IA.
- Construire des workflows transposables dans un environnement professionnel.
- Créer et tester un agent IA avec des règles de sécurité et des guardrails adaptés aux enjeux cyber.

Format pédagogique

Apports théoriques

Ateliers en groupes

Retours d'expérience

DURÉE

1 journée d'immersion

EFFECTIF

Jusqu'à 30 personnes

LIEU

Centre Novamind, Paris 03

FORMAT

Présentiel

TARIF

Sur mesure

FINANCEMENT

OPCO possible

DATES

Nous consulter pour les dates de formation

- **8h30** Accueil
- **9h** Masterclass IA
- **11h15** Workflows
- **12h30** Déjeuner
- **14h** Agents IA
- **18h** Débrief
- **18h45** Retex
- **19h15** Cocktail

Déroulé de la journée

De la compréhension des mécanismes à la construction d'un agent IA opérationnel

8h30 - 12h30 | MATIN - MASTERCLASS & AUTOMATISATION

8h30 - 9h00 Accueil Petit-déjeuner d'accueil : viennoiseries, fruits frais, café et thé.

9h00 - 11h00 | Masterclass IA générative

- LLM : architecture Transformer, tokenisation, prédiction du prochain mot, cycle d'apprentissage et limites intrinsèques.
- No-code : introduction, architecture, « Stack » No-Code, cartographie et choix de l'écosystème.
- Prompt engineering avancé : frameworks de raisonnement complexe, formats de sorties stricts, structuration des requêtes et injection dynamique.
- Protection contre la Prompt Injection et les fuites de prompt système ; réduction des hallucinations par l'ancrage factuel.
- Prompt Compression : réduction du coût en tokens sans perte de performance.
- Automatisation des Workflows et intégration d'API.

11h00 - 11h15 PAUSE

11h15 - 12h30 | Prompt avancé & automatisation workflows

- Atelier opérationnel sur une automatisation dans l'IA générative.
- Concevoir ses premiers flux d'IA automatisés et repartir avec une IA clé en main adaptée à sa réalité professionnelle.

12h30 - 14h00 Déjeuner Servi à table pour favoriser les échanges entre pairs.

14h00 - 18h00 | APRÈS-MIDI - ATELIER AGENTS IA

Cas d'usage Cyber

- Agent d'analyse de logs / SIEM : lecture de logs, détection d'anomalies (force brute, IP suspectes) et rapport de synthèse.
- Assistant d'investigation rapide : analyse d'un e-mail de phishing, extraction des liens, pièces jointes et réputations de domaine.
- Contrôleur de conformité / durcissement : analyse d'un fichier de configuration et remontée des failles selon les référentiels.

Construire son agent - étape par étape

- Fondamentaux : comprendre l'agent IA et ses interactions avec prompts, mémoire et outils.
- Configuration pas à pas : rôle, consignes de sécurité, rédaction du prompt et caractéristiques de l'agent.
- Configuration du flux : connexion des outils et création du circuit automatique.
- Test & Guardrails : fausses alertes, correction des hallucinations et blocage des tentatives de prompt injection.
- Connexion à leur système : automatisations, logiciels et mise en forme de l'alerte à l'équipe IT.

CLÔTURE DE LA JOURNÉE

18h - 18h30
Débriefing

18h45
Retex éditeur

19h15
Cocktail de clôture