

Mis à jour le 26/02/2026

S'inscrire

Formation Open WebUI : Déployer des LLM Sécurisés

2 jours (14 heures)

Présentation

Open WebUI est une plateforme open source permettant de déployer et d'exploiter des LLM en environnement local ou serveur, avec une approche self-hosted orientée sécurité et gouvernance.

Notre formation vous permettra d'installer, configurer et sécuriser une plateforme IA interne adaptée aux exigences professionnelles.

Vous apprendrez à connecter différents modèles (locaux et API compatibles), optimiser les performances, structurer des prompts métier et mettre en place un contrôle des usages.

À l'issue de cette formation, vous serez capable d'industrialiser l'usage des LLM dans votre organisation tout en garantissant sécurité, traçabilité et conformité.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre l'architecture des LLM.
- Déployer et configurer Open WebUI.
- Gérer plusieurs modèles IA en environnement sécurisé.
- Structurer des prompts professionnels et partagés.
- Industrialiser l'usage des LLM en entreprise.

Public visé

- Administrateurs systèmes
- DevOps
- Ingénieurs Cloud
- Responsables innovation / IA
- Développeurs backend

Pré-requis

- Notions d'administration système
- Connaissance Docker
- Compréhension des concepts cloud

Open WebUI : Déployer des LLM Sécurisés

[Jour 1 - Matin]

Architecture des LLM et rôle d'Open WebUI

- Comprendre le fonctionnement des LLM
- Différence entre API cloud et modèles locaux
- Positionnement d'Open WebUI dans un écosystème IA
- Architecture technique globale
- Intégration avec Ollama et API compatibles
- Atelier pratique : Installation d'Open WebUI et connexion à un modèle local sécurisé.

[Jour 1 - Après-midi]

Déploiement et configuration sécurisée

- Déploiement via Docker et bonnes pratiques de runtime
- Paramétrage des variables d'environnement et persistance
- Gestion des utilisateurs et authentification
- Configuration réseau et exposition sécurisée (HTTPS, reverse proxy)
- Isolation et contrôle d'accès
- Atelier pratique : Mise en place d'une instance sécurisée multi-utilisateurs.

Gestion des modèles et optimisation

- Téléchargement et gestion des modèles Ollama
- Connexion à des API externes (OpenAI et autres LLM)
- Paramétrage : contexte, température, tokens
- Optimisation des performances serveur
- Gestion des ressources et limitations

- Atelier pratique : Configuration multi-modèles avec tests de performance.

[Jour 2 - Matin]

Prompts, templates et contrôle des usages

- Structuration des prompts professionnels
- Création de templates réutilisables
- Gestion des historiques et logs
- Modération et contrôle des interactions
- Gouvernance des usages IA
- Atelier pratique : Création d'un template métier sécurisé et partagé.

[Jour 2 - Après-midi]

Intégration en environnement entreprise

- Déploiement en environnement cloud ou hybride
- Intégration avec outils internes et pratiques d'industrialisation
- Gestion des droits et rôles
- Cas d'usage métier (support, documentation, assistant interne)
- Stratégie de déploiement par périmètre

Supervision, conformité et stratégie LLM

- Monitoring de l'usage et alerting
- Sécurité des données sensibles et cloisonnement
- Conformité et traçabilité
- Limites des LLM et garde-fous
- Stratégie d'adoption et plan de montée en charge
- Atelier pratique : Élaboration d'un plan de déploiement sécurisé en organisation.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs

personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.