+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 05/06/2024

S'inscrire

Formation GuardRails AI

1 jour (7 heures)

Présentation

Développez sereinement des applications IA en vous protégeant des risques inhérents comme les hallucinations, les biais, les fuites de données ou encore le langage toxique. Notre formation Guardrails AI vous permettra d'éviter ces dangers grâce à la plus grande library de validators personnalisés.

Nous vous enseignerons de manière exhaustive l'intégration de Guardrails AI sur vos systèmes à travers l'apprentissage des validators et des guards, nous vous présenterons, par ailleurs, les avantages et les limites de l'outil.

Sachez que cet outil est open-source et gratuit, nous vous apprendrons donc à l'installer et le configurer de la meilleure des manières. À l'issue de cette formation, vous maitriserez la syntaxe de l'API GuardRails et vous saurez déployer plusieurs guardrails dans un guard.

Inscrivez-vous à une de nos sessions pour devenir expert en développement IA sécurisé et éthique. Nous nous baserons sur la dernière version en date, Guardrails AI 0.4.

Objectifs

- Comprendre les dangers de l'intelligence artificielle
- Apprendre à utiliser les validators pour sécuriser les applications IA
- Savoir installer et configurer Guardrails
- Maîtriser la syntaxe et l'utilisation de l'API Guardrails

Public visé

- Data Scientist
- Big Data Engineer
- Machine Learning Engineer

- Lead Développeur
- Développeurs
- Ingénieurs IA

Pré-requis

- Maîtrise de Python
- Expérience en utilisation de LLM via API

Programme de notre formation Guardrails AI

Les dangers de l'intelligence artificielle

- Les hallucinations
- La sécurité
- Le langage inapproprié

Présentation de Guardrails

- L'utilisation des validators pour vos applications IA
- Guardrails Open Source vs Guardrails Hub
- La liste des validators
- Qu'est-ce qu'un Guard ?
- Les limites de Guardrails

Installation et configuration

- Installation de Guardrails
- Créer un guard
- Lancer plusieurs guardrails dans un guard
- Générer des données structurées à partir des LLMs

Guardrails API

- La syntaxe
- Les class
- Les arguments
- Utiliser Guardrails avec RAIL
- Troubleshooting

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.