

CYBERSÉCURITÉ POUR INTELLIGENCE ARTIFICIELLE POUR PROGRAMMEUR

Cette formation est spécialement conçue pour les programmeurs souhaitant développer des solutions basées sur l'intelligence artificielle (IA) tout en intégrant des pratiques avancées de cybersécurité.



Avec des menaces en constante évolution et des systèmes d'IA devenant des cibles privilégiées, il est essentiel d'apprendre à sécuriser les données, modèles et infrastructures pour une mise en œuvre réussie et sécurisée de vos projets IA.

À la fin de cette formation, le participant comprendra les risques spécifiques liés à l'IA. Il saura sécuriser les données sensibles, prévenir les vulnérabilités dans le code, protéger les modèles d'IA, respecter les réglementations et normes, améliorer la confiance dans les systèmes d'IA, anticiper les menaces futures, collaborer avec des experts en sécurité, éviter les coûts liés aux failles de sécurité, et il développera des compétences transversales

OBJECTIFS

- Maîtriser les principes fondamentaux de la cyber sécurité dans le contexte de l'IA.
- Identifier et atténuer les vulnérabilités dans les pipelines de données et modèles d'IA.
- Implémenter des protocoles de sécurité pour protéger les algorithmes et infrastructures IA.
- Garantir la confidentialité, l'intégrité et la disponibilité des systèmes IA face aux cybermenaces.
- Comprendre les normes de sécurité applicables à l'IA (RGPD, ISO, etc.).

CONTENU

1. Introduction à la Cyber Sécurité et l'IA

- Définitions clés : Cyber sécurité, IA, et leurs intersections
- Aperçu des menaces spécifiques aux systèmes IA

2. Principes fondamentaux de la cyber sécurité

- Les trois piliers : Confidentialité, intégrité, disponibilité
- Authentification, autorisation et gestion des accès
- Sécurisation des infrastructures et réseaux

3. Sécurité des données dans l'IA

- Chiffrement des données sensibles et anonymisation
- Gestion des pipelines de données et contrôle des accès
- Prévention des attaques adversariales sur les données d'entraînement

4. Protection des modèles d'IA

- Défense contre les attaques adversariales sur les modèles
- Gestion des mises à jour des modèles et suivi des versions
- Surveillance et détection des anomalies dans les systèmes en production

5. Sécurisation des systèmes et des infrastructures IA

- Meilleures pratiques pour déployer des modèles sur le cloud ou en local
- Gestion des clés et des certificats pour les API et microservices IA
- Audit et suivi de la conformité

6. Études de cas et exercices pratiques

- Analyse d'attaques réelles sur des systèmes IA et leurs solutions
- Mise en place d'un environnement sécurisé pour un modèle IA
- Simulation d'une réponse à une cyberattaque ciblant un pipeline IA