

CYBERSÉCURITÉ ET INTELLIGENCE ARTIFICIELLE POUR PROGRAMMEUR

Cette formation avancée en cybersécurité et intelligence artificielle pour programmeur est conçue pour les programmeurs souhaitant maîtriser les concepts essentiels de la cybersécurité et de l'intelligence artificielle (IA).



En combinant ces deux domaines cruciaux, cette formation offre des compétences pratiques et stratégiques pour créer des solutions sécurisées et innovantes adaptées à l'ère numérique. Grâce à une approche axée sur des projets réels et des exercices interactifs, vous serez prêt à relever les défis de la programmation sécurisée et de l'intégration d'algorithmes d'IA dans divers environnements.

OBJECTIFS

- Renforcer les connaissances des concepts fondamentaux de la cybersécurité, incluant les menaces, vulnérabilités et solutions.
- Maîtriser les techniques de programmation sécurisée pour réduire les risques liés aux cyberattaques.
- Intégrer des algorithmes d'intelligence artificielle pour détecter, analyser et prévenir les cybermenaces.
- Développer des outils et des applications sécurisées en utilisant des frameworks d'IA.
- Comprendre les normes et réglementations en matière de sécurité des données et d'éthique en IA.
- Appliquer des stratégies avancées pour sécuriser les réseaux et systèmes intelligents.

CONTENU

1. Introduction à la cybersécurité et à l'IA

- Concepts clés de la cybersécurité
 - Menaces, attaques et défenses
- Rôle et impact de l'intelligence artificielle en cybersécurité
- Études de cas réels
 - Cyberattaques majeures et solutions IA

2. Programmation sécurisée

- Identification des vulnérabilités dans le code source
- Techniques de codage sécurisé pour différents langages (Python, Java, C++)
- Validation des entrées, gestion des erreurs et contrôle des accès

3. Détection et prévention des menaces via l'IA

- Introduction aux algorithmes d'apprentissage machine et de *deep learning*
- Création de modèles d'IA pour identifier les anomalies et intrusions
- Développement d'outils d'analyse comportementale pour prévenir les menaces

4. Réseaux et systèmes sécurisés

- Principes de la sécurité des réseaux (pare-feu, cryptographie, VPN)
- Implémentation de systèmes d'authentification robustes (biométrie, MFA)
- Analyse des vulnérabilités des systèmes distribués intelligents

5. Développement d'applications sécurisées avec IA

- Utilisation de frameworks d'IA (TensorFlow, PyTorch) pour la cybersécurité
- Développement d'applications sécurisées intégrant des modèles IA
- Simulation et détection d'attaques dans un environnement contrôlé

6. Réglementations et éthique en cybersécurité et IA

- RGPD, normes ISO et autres réglementations
- Meilleures pratiques en matière d'éthique dans les systèmes IA
- Études d'impact
 - o IA, sécurité et vie privée