

SÉCURITÉ ET CONFIDENTIALITÉ AVEC L'INTELLIGENCE ARTIFICIELLE

Pour utilisateur

Dans un environnement où les données personnelles et la protection de la vie privée sont des priorités, il est essentiel de comprendre les risques associés et de maîtriser les outils et protocoles pour les minimiser.



Cette formation est conçue pour former les professionnels aux meilleures pratiques en matière de sécurité et de confidentialité pour une utilisation responsable de l'intelligence artificielle dans le respect des réglementations et des normes en vigueur.

Objectifs

- Sensibiliser et comprendre les enjeux critiques liés à l'utilisation de l'IA .
- Analyser les risques liés à l'utilisation de l'IA.
- Appliquer les bonnes pratiques en matière de sécurité des données.

Contenu

1. Introduction à la sécurité et à la confidentialité en IA

- Comprendre les enjeux de la sécurité et de la confidentialité
- Identifier les vulnérabilités spécifiques aux systèmes d'IA
- Importance des pratiques éthiques et du respect de la vie privée

2. Principes fondamentaux de la sécurité des données

- Concepts de sécurité :
 - Intégrité, disponibilité, et confidentialité des données
- Défis spécifiques aux systèmes IA :
 - Manipulation des données
 - Biais et attaques adversaires
- Analyse de situations d'atteintes à la sécurité dans des systèmes IA

3. Gestion des données sensibles

- Catégorisation des données : données sensibles vs. non-sensibles
- Techniques de protection des données :
 - Chiffrement, anonymisation et pseudonymisation
- Rôle des politiques de sécurité et gestion des accès

4. Analyse des risques en IA

- Méthodologies d'évaluation des risques : identification, analyse et gestion des risques
- Cartographie des risques spécifiques liés à l'IA
- Outils et méthodologies de gestion des risques en entreprise

5. Conformité et réglementations

- Principaux cadres législatifs :
 - RGPD (Europe), CCPA (Californie), PIPEDA (Canada), etc.
- Processus de conformité pour les systèmes d'IA :
 - Collecte, traitement, et stockage des données
- Bonnes pratiques de conformité pour une utilisation éthique et responsable

6. Protocoles et outils de sécurité en IA

- Outils de détection et de prévention des intrusions spécifiques à l'IA
- Mise en place de pare-feu et de systèmes de sécurité IA
- Utilisation de plateformes sécurisées pour le développement et le déploiement de modèles IA

7. Gestion des incidents et réponse aux menaces

- Identification des signes de compromission dans les systèmes IA
- Plan de gestion des incidents :
 - Étapes et acteurs clés

8. Éthique et transparence dans l'IA

- Considérations éthiques liées à la confidentialité et à la sécurité des données
- Rôle de la transparence et de l'explicabilité dans les décisions IA
- Garantir une IA respectueuse des utilisateurs et minimiser les biais

9. Synthèse et bonnes pratiques

- Résumé des points clés :
 - Outils, méthodes et protocoles
- Adoption de bonnes pratiques pour la sécurité et la confidentialité
- Discussion sur les tendances futures en sécurité et confidentialité en IA