CYBERSÉCURITÉ ET IA
ENTRE MENACES ET BONNES PRATIQUES

Durée : 3 heures
Prérequis :
- Aucune connaissance préalable en cybersécurité requise.
- Avoir accès à un ordinateur avec une connexion Internet.

Moyens pédagogiques :
- Formation en ligne, en mode asynchrone
- Supports de formation inclus

Compétences acquises à l'issue de la formation :
- Comprendre le fonctionnement et les risques des outils d'IA générative
- Reconnaître les cyberattaques utilisant l'IA
- Utiliser et paramétrer les outils d'IA de façon sécuritaire

Attestation : oui

DESCRIPTION

L'intelligence artificielle (IA) offre des avantages considérables pour les organisations, mais elle est également exploitée par les cybercriminels. À travers cette formation, nous explorerons les méthodes actuelles d'utilisation de l'IA dans le cadre de la cybercriminalité et fournirons des recommandations pour utiliser l'IA de manière sécurisée dans nos activités professionnelles.

PROGRAMME :

Objectif général

Sensibiliser les participants aux risques de sécurité associés à l'IA. Former aux bonnes pratiques pour une utilisation sécurisée de l'IA en entreprise.

1. Introduction à l'intelligence artificielle et à ses applications pratiques — Évolution de l'IA dans le domaine technologique. Comprendre le fonctionnement général des modèles d'IA générative. Présentation des outils populaires (ChatGPT, Gemini, Copilot, Claude, etc.). Exemples d'utilisation de l'IA dans un contexte professionnel.

2. Tendances actuelles en cyberattaques utilisant l'IA — Exemples d'attaques utilisant l'IA (deepfakes, hameçonnage automatisé, création de contenus frauduleux, création de rançongiciels). Compréhension des deepfakes et des usurpations d'identité via l'IA. Outils de détection de deepfakes et de fraudes (machine learning, détection d'anomalies). Études de cas et simulations pour renforcer la prévention des attaques sophistiquées.

3. Fonctionnement des plateformes d'IA — Différencier les usages personnels des usages professionnels. Comprendre le traitement des données et les modèles d'apprentissage. Clarifier où sont hébergées les données et les implications en matière de protection des renseignements personnels.

4. Enjeux liés à la gestion des données — Considérations liées à la protection des renseignements personnels. Bonnes pratiques pour anonymiser l'information dans les requêtes (prompts). Enjeux liés à la propriété intellectuelle du contenu généré ou utilisé. Comprendre les limites des systèmes, incluant les hallucinations et les erreurs possibles. Sensibilisation aux biais dans les modèles IA (raciaux, sexistes) et leurs impacts.

5. Paramétrage et bonnes pratiques — Paramètres de confidentialité et gestion des historiques. Réutilisation possible des données pour l'entraînement des modèles. Exploration des IA « privées ». Recommandations pour une utilisation sécurisée des outils d'IA en organisation.

QUESTIONS/RÉPONSES