INTELLIGENCE ARTIFICIELLE ET CYBERSÉCURITÉ

FFCNCERCERXCS24 | PRIX : 1 910 € | DURÉE : 2 JOURS

Pauses et déjeuners offerts

AVANCÉ | ATELIER | FAISABLE À DISTANCE | RÉALISABLE EN ANGLAIS

PRÉSENTATION

L'intelligence artificielle et la cybersécurité jouent un rôle crucial dans le monde numérique. Une intégration efficace de l'IA permettra une détection et une réponse aux risques en temps réel, une réduction des faux positifs, une adaptation dynamique à de nouvelles menaces, etc.
Cette intersection entraîne aussi de nouveaux défis à cause des risques et des implications éthiques de l'IA dans la cybersécurité.

Cette formation présente les concepts fondamentaux des principes de l'intelligence artificielle ainsi que leurs mises en œuvre dans le cas de problématiques de cybersécurité.

OBJECTIFS

- Présenter les enjeux et les actualités de l'IA
- Expliquer les concepts de base de l'apprentissage statistique (Machine Learning)
- Présenter différentes techniques d'apprentissage statistique
- Explorer les applications de l'IA en cybersécurité
- Évaluer les risques associés à l'IA dans le domaine de la cybersécurité

PROGRAMME

Introduction

Les principes de l'intelligence artificielle et de l'apprentissage statistique
- Enjeux et actualités de l'intelligence artificielle
- Fondamentaux de l'apprentissage statistique
- Notions de la théorie de l'apprentissage statistique : Généralisation, fonction de coût, séparation entre ensemble de test et ensemble d'apprentissage, apprentissage supervisé et non supervisé, minimisation du risque empirique, etc.
- Les principales méthodes de classification supervisée : Classifieurs linéaires, méthodes à ensembles, plus proches voisins, etc.
- Réseaux de neurones et apprentissage profond (Deep Learning)
- Avantages et limites des approches à base d'apprentissage statistique
- Mises en œuvre de méthodes d'apprentissage statique
- Études de cas

Mise en œuvre et évaluation de méthodes d'apprentissage dans le cas de problématique de cybersécurité

Exemples de mise en œuvre de méthodes d'apprentissage en cybersécurité
- Détection d'exécutables malveillants
- Analyse de trafic réseau à la frontière d'un parc informatique
- Détection d'associations utilisateur-machine anormales
- Risques et scénarios d'attaques contre les IA et techniques de défense

Synthèse et conclusion

PUBLIC/PRÉREQUIS

Toute personne (ingénieur, technicien, scientifique) souhaitant comprendre les notions de base et mieux appréhender les enjeux de l'intelligence artificielle et notamment ces implications sur la cybersécurité.

RESPONSABLE(S)

Guillaume WISNIEWSKI
Enseignant-chercheur en informatique à Université Paris Cité. Il est diplômé de Télécom ParisTech (promo 2004) et de l'Université Pierre et Marie Curie (thèse en apprentissage statistique en 2007). Ses travaux de recherche portent sur la linguistique informatique et la compréhension automatique des langues. Depuis 2008, il enseigne la data science, le traitement des langues, l'apprentissage statistique, l'apprentissage profond et les giga-modèles de langue (LLMs).

MODALITÉS PÉDAGOGIQUES

Cours et travaux pratiques.