Formation Apport de l'IA dans la cybersécurité

Présentation

L'intelligence artificielle (IA) joue un rôle de plus en plus crucial dans la cybersécurité en permettant une détection avancée des menaces, une automatisation des réponses aux incidents et une réduction des faux positifs. Toutefois, cette intégration pose également des défis en termes de biais des algorithmes, de faux négatifs et de cyberattaques exploitant l'IA. Cette formation permettra aux participants de comprendre les principes fondamentaux de l'IA appliquée à la cybersécurité, d'explorer des cas concrets d'utilisation, et de mettre en pratique des outils et algorithmes d'apprentissage machine pour améliorer la sécurité des systèmes d'information.

Durée : 14,00 heures (2 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

À l'issue de cette formation, les participants seront capables de :

- Comprendre les enjeux et l'évolution de l'IA appliquée à la cybersécurité.
- Expliquer les concepts fondamentaux du Machine Learning et du Deep Learning.
- Découvrir les principales applications de l'IA dans la détection des menaces.
- Mettre en œuvre des techniques d'apprentissage automatique sur des scénarios réels de cybersécurité.
- Évaluer les limites, risques et implications éthiques de l'IA en cybersécurité.

Prérequis

Avoir un intérêt pour les technologies de l'intelligence artificielle et les enjeux de la cybersécurité.

Public

- Développeurs et ingénieurs logiciels
- Ceux qui veulent intégrer des techniques d'IA dans leurs projets de cybersécurité.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

DOCAPOSTE Institute

Programme de la formation

1/ Introduction à l'Intelligence Artificielle et à la Cybersécurité

1.1. Principes fondamentaux de l'intelligence artificielle

- Définition de l'IA et évolution historique.
- Différences entre Machine Learning, Deep Learning et IA symbolique.

1.2. Enjeux de l'IA en cybersécurité

- Pourquoi l'IA est essentielle pour améliorer la cybersécurité ?
- Opportunités et menaces liées à l'IA.

Démonstration :

- Visualisation d'attaques réelles sur un réseau et discussion sur le rôle de l'IA pour leur détection.

2/ Concepts de Base de l'Apprentissage Machine en Cybersécurité

2.1. Introduction au Machine Learning

- Apprentissage supervisé vs non supervisé.
- Fonction de coût, minimisation du risque empirique.
- Séparation entre ensemble d'entraînement et ensemble de test.

2.2. Principales méthodes de classification

- Régressions logistiques et linéaires.
- Classifieurs basés sur les arbres de décision (Random Forest, XGBoost).
- Méthodes probabilistes (Naïve Bayes, k-NN).

2.3. Introduction aux Réseaux de Neurones et Deep Learning

- Réseaux de neurones artificiels (ANN).
- Fonctionnement des couches convolutives et récurrentes.

Travaux Pratiques :

- Implémentation d'un modèle de classification des emails de phishing avec Scikit-Learn.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

DOCAPOSTE Institute

3/ Détection de Menaces avec l'IA

3.1. Applications de l'IA dans la détection des menaces

- Détection d'intrusions et d'activités suspectes.
- Analyse des malwares avec l'IA.
- Systèmes de détection d'anomalies pour la cybersécurité industrielle.

3.2. Exemples concrets de détection IA en cybersécurité

- Détection de fichiers malveillants avec des algorithmes de classification.
- Utilisation de l'IA pour la reconnaissance des comportements anormaux sur un réseau.

Travaux Pratiques :

- Lab 1 : Analyse d'un trafic réseau avec Wireshark et Zeek pour identifier des connexions suspectes.
- Lab 2 : Détection d'exécutables malveillants avec un modèle de Machine Learning (Random Forest).

4/ Attaques Basées sur l'IA et Contre-Mesures

4.1. Les risques liés à l'IA en cybersécurité

- Attaques adversariales sur les modèles IA.
- Falsification des résultats des modèles (data poisoning).
- Détection des faux positifs et faux négatifs.

4.2. Contre-mesures et solutions de sécurité

- Techniques pour améliorer la robustesse des modèles IA.
- Approches pour détecter et limiter les attaques sur les algorithmes IA.

Démonstration :

- Manipulation d'un modèle de classification pour le rendre vulnérable aux attaques adversariales.

5/ Perspectives et Éthique de l'IA en Cybersécurité

5.1. Réglementation et gouvernance de l'IA en cybersécurité

- Principes du RGPD et directives européennes sur l'IA.
- Normes et bonnes pratiques pour l'implémentation de l'IA en sécurité.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

5.2. IA et responsabilité éthique
- Impact des décisions algorithmiques en cybersécurité.
- Problématique des biais algorithmiques et des erreurs de classification.

5.3. L'avenir de l'IA en cybersécurité
- Évolution des cybermenaces exploitant l'IA.
- Recherche et innovations dans l'IA appliquée à la cybersécurité.

Travaux Pratiques :
- Atelier de réflexion : Étudier un cas d'usage réel où l'IA a échoué à détecter une menace et proposer des améliorations.

Organisation

Formateur
Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques
- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France