EduGroupe
Accompagner pour réussir

L'intelligence artificielle et la sécurité opérationnelle

Référence : **SECIA100** Durée : **1 jour (7 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissance préalable d'un langage de l'outil informatique et d'un langage de programmation

Profil des stagiaires

- Décideur, chef de projet, ingénieur, développeur, chercheurs

Objectifs

- Comprendre en quoi l'intelligence artificielle peut être utile à la cybersécurité
- Appréhender les problèmes de sécurité liés aux objets connectés
- Découvrir les outils et moyens de détection contre les attaques d'Ingénierie sociale, biométrique, usurpation...

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur·rice

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Définir les enjeux entre : IA, robotique et cybersécurité

- Définition et concepts
- Enjeux pour les états, les armées et toute organisation liée à l'informatique
- Possibilités et limites de la cybersécurité liées à l'IA
- Menaces logicielles. Outils de détection de logiciels malveillants
- Problèmes de sécurités liés à l'Internet des Objets (IoT)
- Possibilités et limites de l'IoT dans un contexte de cybersécurité
- Objets connectés malveillants vs moyens de détections
- Démonstrations : logiciels polymorphiques, algorithmes génétiques utiles à la génération de codes polymorphes, matériels électroniques et robotiques

2. Ingénierie sociale et intelligence artificielle

- Qu'est ce qu'une attaque d'ingénierie sociale ? Quelles en sont les conséquences ?
- Principes des « deepfakes » (fausses identités, images, voix et vidéos)
- Possibilités et limites d'un réseau GAN (Generative Adversarial Networks)
- De nouveaux outils comme moyens de détections
- Démonstration : Mise en œuvre d'un réseau GAN pour produire des images aux styles factices

3. L'IA comme outil de détection, protection, surveillance, identification...

- Des systèmes à la « complexité » toujours plus croissante
- Des indicateurs statistiques « classiques » insuffisants pour surveiller un système complexe
- Machine Learning (ML) et Deep Learning (DP) pour la détection et la prévention des anomalies
- IA, outil de surveillance. Utilisation du ML et DL par les systèmes biométriques
- Possibilités et limites du ML et du DL dans l'identification des personnes
- Utilisation détournée : faux positifs, faux négatifs, actes malveillants...
- Démonstrations : Modèle de détection. Typologie des caméras (360, HD, 3D-RGBd...). Démonstrations des limites, des « biais » liés à l'IA et des cas où l'IA est plus efficace que l'œil humain

4. Une écoute boostée à l'IA

- Contexte d'écoutes « boostées » à l'intelligence artificielle
- Outils et moyens pour écouter une conversation, déceler un code secret, reconstituer un mail...
- Des projets menés à bien accessible à tous
- Comment préserver la confidentialité de nos échanges ?
- Possibilités et limites entre « frappologie » et IA. Comment s'en protéger ?
- Démonstration : Outils et recherches utiles pour reconstruire, prédire des signaux indirects dans un environnement bruité

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.