L'INTELLIGENCE ARTIFICIELLE ET LA SÉCURITÉ OPÉRATIONNELLE

500 € HT (tarif inter) | REF : INT20
TARIF SPÉCIAL : particuliers et demandeurs d'emploi

Cette formation permet de comprendre ce qu'est l'Intelligence Artificielle (IA), comment la définir dans le contexte de la cybersécurité et aussi de mesurer l'importance de sécuriser nos objets connectés, nos identités, nos données personnelles, etc. et d

5 JOURS | **35** HEURES

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..

PUBLIC | PRÉREQUIS

PUBLIC : Décideur, chef de projet, ingénieur, développeur, chercheurs.
PRÉREQUIS : Connaissance préalable d'un langage de l'outil informatique et d'un langage de programmation.

PROGRAMME

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.

Travaux pratiques : Démonstrations : logiciels polymorphiques, algorithmes génétiques utiles à la génération de codes polymorphes, matériels électroniques et robotiques.

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 co.

Travaux pratiques : Mise en œuvre d'un réseau GAN pour produire des images aux styles factices.

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, o.

Travaux pratiques : 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.

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 échan.

Travaux pratiques : Outils et recherches utiles pour reconstruire, prédire des signaux indirects dans un environnement bruité.

INFOS PRATIQUES

Méthodes pédagogiques
Alternance équilibrée de présentations, d'ateliers sur simulateur et de mises en situation dans des conditions similaires à celles de l'examen.

Modalités de l'évaluation initiale
Test de positionnement en amont de la session de formation.

Modalités d'évaluation finale
Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques.

Accessibilité aux personnes handicapés
Dans votre espace candidat, une rubrique dédiée au handicap vous permettra d'exprimer vos besoins d'adaptation afin que vous puissiez suivre votre formation dans les meilleures conditions.

Modalités et délais d'accès
L'inscription doit être finalisée 72 heures avant le début de la formation.

STATISTIQUES

Taux de satisfaction : 100%
Taux d'abandon : 0%

DATES ET LIEUX

Nous consulter