L'intelligence artificielle et la sécurité opérationnelle
IA comme un champ des possibles pour des actes malveillants

Cours Synthèse de 1 jour - 7h
Réf : ICY - Prix 2024 : 950CHF HT

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 de comprendre l'importance de la sécurité opérationnelle.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

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...

LE PROGRAMME

dernière mise à jour : 06/2020

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.

Démonstration : 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.

PARTICIPANTS

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

PRÉREQUIS

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

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Possibilités et limites du ML et du DL dans l'identification des personnes.
- Utilisation détournée : faux positifs, faux négatifs, actes malveillants...

Démonstration : 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.

LES DATES

CLASSE À DISTANCE
2024 : 02 déc.