Intelligence Artificielle et Cybersécurité : Opportunités, usages et risques

Durée : 1 jour (7 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'information.
- Connaissances de base en cybersécurité.
- Aucune compétence préalable en intelligence artificielle n'est requise..

PROFIL DES STAGIAIRES

- RSSI et responsables cybersécurité
- DSI et responsables informatiques
- Analystes SOC
- Équipes CERT / CSIRT
- Administrateurs systèmes et réseaux
- Responsables risques et conformité
- Consultants cybersécurité
- Toute personne souhaitant comprendre les apports et les risques de l'IA dans le domaine de la cybersécurité.

OBJECTIFS

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

- Comprendre les concepts fondamentaux de l'intelligence artificielle appliquée à la cybersécurité.
- Identifier les principaux cas d'usage de l'IA pour la défense des systèmes d'information.
- Comprendre comment les cybercriminels exploitent l'IA pour mener leurs attaques.
- Évaluer les bénéfices, limites et risques liés à l'utilisation de l'IA en cybersécurité.
- Intégrer des outils d'IA dans les activités de détection, d'analyse et de réponse aux incidents.
- Identifier les enjeux de gouvernance, d'éthique et de conformité associés.
- Construire une feuille de route d'adoption de l'IA dans les activités cyber..

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et de démonstrations.
- Analyse de cas d'usage réels issus du domaine de la cybersécurité.
- Ateliers collaboratifs d'identification des opportunités et risques.
- Démonstrations d'outils d'IA appliqués à la sécurité.
- Études de cas inspirées d'incidents récents.
- Réflexions collectives sur les enjeux éthiques et réglementaires.

FORMATEUR

- Consultant expert en cybersécurité et intelligence artificielle disposant d'une expérience significative dans l'utilisation des technologies d'IA appliquées à la détection des menaces, à l'analyse des incidents, à l'automatisation de la sécurité et à la gouvernance des systèmes d'intelligence artificielle.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Évaluation continue au travers des ateliers et études de cas.
- Quiz de validation des connaissances.
- Cas pratique de synthèse en fin de formation.
- Questionnaire d'évaluation des acquis.

CONTENU DU COURS

Module 1 : Comprendre l'intelligence artificielle appliquée à la cybersécurité (1h30)

Objectifs

- Comprendre les fondamentaux de l'IA et du Machine Learning.
- Identifier les principaux usages de l'IA dans le domaine cyber.

Contenu

- Définitions et concepts clés.
- Intelligence artificielle, Machine Learning et IA générative.
- Panorama des technologies disponibles.
- Évolution des usages de l'IA en cybersécurité.
- Tendances du marché et perspectives.

Mise en pratique

Brainstorming collectif :

- Identification des activités cybersécurité pouvant bénéficier de l'IA au sein de l'organisation.

Module 2 : Utiliser l'IA pour renforcer la cybersécurité (2h)

Objectifs

- Identifier les cas d'usage opérationnels de l'IA.
- Comprendre les bénéfices apportés par l'automatisation intelligente.

Contenu

- Détection des menaces assistée par IA.
- Analyse comportementale et détection d'anomalies.
- Priorisation des alertes de sécurité.
- Assistance aux analystes SOC.
- Threat Intelligence augmentée par IA.
- Réponse automatisée aux incidents.
- Génération et analyse de rapports de sécurité.

Mise en pratique

Étude de cas :

- Analyse d'un scénario SOC intégrant des outils d'IA pour la détection et l'investigation d'incidents.

Module 3 : L'IA comme arme des cyberattaquants (1h30)

Objectifs

- Comprendre les nouveaux risques induits par l'IA.
- Identifier les techniques offensives exploitant l'intelligence artificielle.

Contenu

- Phishing et ingénierie sociale assistés par IA.
- Génération automatisée de contenus frauduleux.
- Deepfakes et usurpation d'identité.
- Automatisation de la recherche de vulnérabilités.
- Création de malwares assistée par IA.
- Risques liés aux modèles génératifs publics.

Mise en pratique

Étude de cas :

- Analyse de scénarios d'attaques utilisant l'IA et identification des mesures de protection adaptées.

Module 4 : Gouvernance, risques et bonnes pratiques d'utilisation de l'IA (1h)

Objectifs

- Encadrer l'usage de l'IA dans les activités cyber.
- Identifier les risques liés aux modèles d'IA.

Contenu

- Gouvernance des systèmes d'IA.
- Confidentialité des données.
- Biais et erreurs des modèles.
- Hallucinations et fiabilité des résultats.
- IA Act européen.
- Bonnes pratiques d'utilisation des outils d'IA dans un contexte de sécurité.

Mise en pratique

Atelier :

- Élaboration d'une charte d'utilisation de l'IA pour les équipes cybersécurité.

Module 5 : Cas pratique de synthèse – Construire une stratégie IA pour la cybersécurité (1h)

Objectifs

- Identifier les opportunités d'intégration de l'IA.
- Formaliser une démarche cohérente d'adoption.

Mise en pratique

Exercice fil rouge :

À partir d'une organisation fictive :

- Identification des besoins cyber.
- Sélection des cas d'usage IA à forte valeur ajoutée.
- Analyse des risques associés.
- Définition des mesures de gouvernance.
- Élaboration d'une feuille de route d'intégration de l'IA dans les activités de cybersécurité.
- Présentation des recommandations au groupe.

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