Formation SSI : Utiliser l'IA au service de la cybersécurité

PLUS D'INFOS

- Contactez-nous

CONTACT REFERENT

- Commercial@ageris-group.com
- +33 3 87 62 06 00

MODALITES D'ACCES

- Inscription en réservant votre place sur une session disponible ou par téléphone, par mail, par demande de contact. Vous recevrez un devis à nous retourner avec votre accord pour confirmer votre inscription.

DELAI D'ACCES

- La durée estimée entre la demande du stagiaire et le début de la formation est de 7 jours (peut être raccourci pour le mode distanciel)

ACCESSIBILITE AUX PERSONNES EN SITUATION D'HANDICAP

- Accessible à distance pour les personnes à mobilité réduite
- Pour connaître l'accessibilité aux salles de formation, vous pouvez nous joindre au +33 3 87 62 06 00

REFERENCE

- SSIIASECU

TARIF

- 890€ HT

DUREE DE LA FORMATION

- 1 jour – 7 heures

DATES DES SESSIONS

- Voir site internet

FINANCEMENT

- OPCO

FORMULE INTRA-ENTREPRISE

- Formulaire : soumettez votre projet

RESSOURCES PEDAGOGIQUES

- Cours théorique
- Exemples concrets
- Evaluation des compétences par un quizz en cours et en fin de formation

PRESENTATION DE LA FORMATION

Exploiter l'IA dans le domaine de la cybersécurité peut permettre aux RSSI de gérer davantage de menaces de manière efficace et pratique. Les modèles de sécurité basés sur l'IA peuvent analyser de grands volumes de données en peu de temps, repérer des modèles d'attaques et toute activité qui s'écarte de la norme. En outre, l'IA peut également être utilisée pour analyser l'ensemble du réseau à la recherche de vulnérabilités.
Cependant, l'ajout d'un système d'IA au portefeuille existant de logiciels de cybersécurité comporte également des risques à ne pas négliger.

A travers de multiples exemples et retours d'expériences, cette formation permettra aux RSSI participants de renforcer leurs connaissances initiales sur les solutions apportées par l'IA pour amorcer efficacement une mise en œuvre de solution d'Intelligence Artificielle adaptée à leur activité.

OBJECTIFS DE CETTE FORMATION

A l'issue de cette formation, le stagiaire aura les compétences pour :

- Choisir les solutions, outils et technologies IA disponibles
- Utiliser l'IA au service de la cybersécurité
- Appréhender les risques liés à l'usage de l'IA
- intégrer l'IA dans un programme de cybersécurité à long terme

PUBLIC

DSI, RSSI, développeurs.

PREREQUIS

Aucun prérequis n'est nécessaire.

PROGRAMME DETAILLE

Chapitre 1 : Introduction à l'Intelligence Artificielle et à la cybersécurité

- Définition et panorama de l'IA (types d'IA, machine learning, deep learning)
- Enjeux actuels de la cybersécurité dans un environnement numérique en constante évolution
- La convergence entre IA et cybersécurité : Pourquoi l'IA est-elle cruciale pour la cybersécurité actuelle ?

Chapitre 2 : Cas d'usage de l'IA en cybersécurité

- Détection d'anomalies dans les réseaux grâce à l'apprentissage automatique
- Analyse comportementale des utilisateurs et systèmes (User & Entity Behavior Analytics - UEBA)
- Automatisation des réponses aux incidents (SOAR)
- Intelligence artificielle et prévention des menaces avancées persistantes (APT)

Chapitre 3 : Outils et technologies basés sur l'IA pour la cybersécurité

- Présentation des technologies : plateformes de SIEM avec IA, solutions de détection et de réponse aux menaces basées sur l'IA (EDR, NDR)
- Étude de cas : Utilisation concrète d'un outil de cybersécurité basé sur l'IA

Formation SSI : Utiliser l'IA au service de la cybersécurité

- Support de cours remis au stagiaire par mail en fin de formation
- Outil distanciel : Teams

POUR ALLER PLUS LOIN

- RGPD – Le rôle de la DSI dans la mise en conformité au RGPD
- RGPD – La démarche AIPD / PIA : Analyse d'Impact relative à la Protection des Données

PLUS D'INFOS

- Contactez-nous

Chapitre 4 : IA et attaques sophistiquées : les risques

- Comment les attaquants utilisent l'IA pour contourner les systèmes de sécurité (exemple : DeepFakes, phishing automatisé, attaques par force brute améliorées)
- Les limites et défis de l'IA dans la défense contre les cybermenaces
- Discussion sur les menaces futures possibles alimentées par l'IA

Chapitre 5 : Implémenter l'IA dans les processus de cybersécurité d'entreprise

- Comment intégrer l'IA dans une stratégie globale de cybersécurité
- Exemples d'implémentations réussies dans différents secteurs
- Défis d'adoption : gestion des coûts, impact sur les processus existants, besoins en compétences

Chapitre 6 : Prise en main pratique d'outils IA pour la cybersécurité

- Atelier pratique : Démonstration d'un outil d'analyse de log basé sur l'IA
- Identification d'anomalies en temps réel et réponses automatisées

Chapitre 7 : Les enjeux éthiques et réglementaires de l'IA en cybersécurité

- Questions éthiques autour de l'IA dans la surveillance et la protection des données
- Impact des réglementations (RGPD, NIS2) sur l'utilisation de l'IA en cybersécurité
- Discussion sur la transparence des algorithmes et la responsabilité

Chapitre 8 : Élaboration d'une feuille de route pour l'IA en cybersécurité

- Planification stratégique pour intégrer l'IA dans un programme de cybersécurité à long terme
- Évaluer les priorités et mesurer le retour sur investissement (ROI)
- Implication des équipes et montée en compétences en IA

Chapitre 9 : Conclusions

- Retour sur les principaux éléments IA/Cybersésurité
- Questions-réponses finales et perspectives

MODALITES D'EVALUATION

- Au début de la formation, les stagiaires s'expriment lors d'un tour de table sur ce qu'ils attendent de la formation en termes d'enjeux, de contenus, d'apports. En fin d'action, ces mêmes stagiaires vont pouvoir évaluer l'atteinte de leurs objectifs individuels.
- L'évaluation des acquis/des apprentissages portera sur les connaissances assimilées par le stagiaire tout au long de la formation. Le formateur s'assure de l'assimilation des connaissances à travers des quizz, exercices, études de cas et mises en situation.
- L'évaluation de la satisfaction à chaud est mise place par l'équipe pédagogique en fin de formation et permettra de mesurer la satisfaction des bénéficiaires quant à la qualité des apports pédagogiques et de s'assurer que la formation a bien répondu aux attentes de départ.