Ageris group

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

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 au +33 3 87 62 06 00, par mail, par le formulaire 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

- SSI IASECU

TARIF

- 890 € HT

DUREE DE LA FORMATION

- 1 jour – 7 heures

DATES DES SESSIONS

- Paris : voir site web
- Distanciel : voir site web

FINANCEMENT

- OPCO

FORMULE INTRA-ENTREPRISE

Formulaire : Soumettez votre projet

RESSOURCES PEDAGOGIQUES

- Cours théorique
- Etude de cas pratique
- Support de cours remis au stagiaire en fin de formation
- Outil distanciel : Teams

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, ce **stage pratique** 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

Fonction RSSI obligatoire, connaissance du réseau et de son fonctionnement. Être équipé d'un PC avec accès à internet.

PROGRAMME

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 ?

2. Cas d'usage de l'IA en cybersécurité
Utilisation de l'outil Wazuh (outil open source IA)

- 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)

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

POUR ALLER PLUS LOIN:

- Devenir RSSI - 7 j
- Etat de l'art de la SSI – 3 j
- Cybercriminalité – 2j

PLUS D'INFOS

- Contactez-nous par téléphone au +33 3 87 62 06 00, par mail, par le formulaire de contact.

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

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

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

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

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

9. Conclusions

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

MODALITES D'EVALUATION

Validation des connaissances et compétences par des cas pratiques et la prise en mains d'outils IA.