

IA au service de la Cybersécurité

Référence : IA027

Durée : 2 jours (14 heures)

Certification : **Aucune**

CONNAISSANCES PRÉALABLE

- Maîtriser les fonctionnalités de base d'un ordinateur et des outils bureautiques
- Connaître les fondamentaux de la cybersécurité (gestion des risques, vulnérabilités, incidents, sécurité des systèmes d'information...).
- Aucune compétence en intelligence artificielle ou en développement informatique n'est requise

PROFIL DES STAGIAIRES

- Cette formation s'adresse aux professionnels de la cybersécurité souhaitant intégrer l'intelligence artificielle dans leurs activités afin d'améliorer la prévention, la détection, l'analyse et le traitement des risques de sécurité
- Elle concerne notamment : Responsables de la sécurité des systèmes d'information (RSSI) ; Responsables cybersécurité ; Consultants en cybersécurité ; Analystes SOC ; Analystes CERT/CSIRT ; Administrateurs systèmes et réseaux ; Architectes sécurité ; Ingénieurs cybersécurité ; Responsables conformité, risques ou gouvernance ; Chefs de projet cybersécurité ; Toute personne participant à la protection du système d'information

OBJECTIFS

- À l'issue de la formation, le participant sera capable de :
- Identifier les cas d'usage de l'intelligence artificielle applicables aux activités de cybersécurité
- Utiliser l'IA générative pour accélérer les activités d'analyse, de documentation, de veille et de gestion des risques
- Exploiter l'IA pour produire des livrables de cybersécurité (politiques, procédures, analyses de risques, rapports, supports de sensibilisation, etc.)
- Identifier les opportunités d'automatisation de certaines tâches récurrentes à l'aide d'outils d'IA et de solutions no-code
- Évaluer les risques liés à l'utilisation de l'intelligence artificielle dans un contexte de cybersécurité
- Mettre en œuvre les bonnes pratiques d'une utilisation sécurisée, responsable et conforme de l'IA

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique, de modèles de prompts, de modèles de livrables, d'études de cas et exercices pratiques, de ressources documentaires complémentaires,
- La formation est constituée d'apports théoriques, de démonstration réalisées à partir des principales plateformes d'IA générative du marché, d'études de cas inspirées de situations réelles, d'exercices pratiques individuels ou collectifs, d'atelier de production de livrables, d'analyse de scénarios d'incidents et de gestion des risques, d'échanges de pratiques entre les participants

FORMATEUR

- Consultant-formateur expert IA

MÉTHODES D'ÉVALUATION DES ACQUIS

- Évaluation diagnostique : en début de formation, un questionnaire de positionnement permet d'évaluer le niveau de connaissance des participants concernant les usages de l'intelligence artificielle dans le domaine de la cybersécurité
- Évaluations formatives Tout au long de la formation, les acquis sont validés au travers : d'exercices pratiques ; d'études de cas ; de quiz interactifs ; de la production de livrables de cybersécurité assistés par l'IA ; d'ateliers d'analyse de risques et de résolution de problématiques de sécurité. Le formateur apporte un retour individualisé sur les productions réalisées
- Évaluation des acquis : en fin de formation, les compétences sont évaluées au travers d'une mise en situation professionnelle consistant à traiter une problématique de cybersécurité en mobilisant les outils d'intelligence artificielle
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

ACCESSIBILITÉ DE LA FORMATION

- EduGroupe met en place un ensemble de dispositifs pour accueillir, accompagner et adapter ses formations aux personnes en situation de handicap (PSH).
- Notre référent(e) handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour tout besoin d'aménagement, afin de vous offrir la meilleure expérience possible.

CONTENU DU COURS

1. Panorama des usages IA en cybersécurité

- SOC
- Analyse
- Détection
- Veille
- Investigation

2. Renforcer les activités opérationnelles

- Analyse de logs
- IOC
- Vulnérabilités
- CVE
- Threat Intelligence

3. Améliorer la documentation

- Procédures
- Politiques
- Analyse de risques
- Sensibilisation
- Rapports

4. Automatiser les tâches

- Assistant SOC
- Agents IA
- Workflows
- Réponses aux incidents

5. Maîtriser les risques liés à l'IA

- Attaques sur les IA
- Prompt injection
- Fuite de données
- Shadow IA
- IA Act
- Gouvernance