# L'intelligence artificielle et la cybersécurité

**Référence : WEB011**

**Durée : 1 jour / 7 heures** **Tarif : 500 €HT / 600 euros TTC**

## OBJECTIF DE LA FORMATION

À l'issue de la formation, les participants seront capables de :
Comprendre les principaux usages de l'IA en cybersécurité
Identifier les nouvelles menaces liées à l'intelligence artificielle
Évaluer les risques associés aux outils d'IA générative
Utiliser l'IA comme outil d'assistance à la détection et à l'analyse des incidents
Mettre en place des bonnes pratiques de sécurité
Sensibiliser les utilisateurs aux risques liés à l'IA

**PARTICIPANT :** Développeurs Web, développeurs Front-End ou Back-End, chefs de projet techniques et toute personne souhaitant utiliser l'intelligence artificielle pour accélérer le développement d'applications Web.

**PRÉ-REQUIS :** Responsables informatiques, responsables de la sécurité des systèmes d'information, techniciens, développeurs, chefs de projet et toute personne souhaitant comprendre les enjeux de l'intelligence artificielle appliquée à la cybersécurité.

**FORMATEURS :** Spécialiste en développement d'application avec l'IA

## MODALITÉS ET PÉDAGOGIE

- Questionnaire d'évaluation en début et en fin de formation
- Cas pratiques et études de cas, Quiz
- Horaires : 9h00 à 12h30 – 13h30 à 17h00
- Nombre maximum de stagiaires : 8
- Formation disponible à distance ou en présentiel
- Méthode interactive et intuitive
- Support de formation remis aux participants
- Assistance Technique et Pédagogique
- Attestation de fin de stage
- Questionnaire de fin de formation

## PROGRAMME

**1. Comprendre l'intelligence artificielle appliquée à la cybersécurité**
- Principes généraux de l'intelligence artificielle
- Différence entre IA classique et IA générative
- Place de l'IA dans les systèmes d'information
- Avantages, limites et risques

**2. Les usages de l'IA pour renforcer la sécurité**
- Détection d'anomalies et de comportements suspects
- Analyse des journaux et des événements de sécurité
- Identification des logiciels malveillants
- Détection du phishing et des contenus frauduleux
- Priorisation des alertes
- Assistance à l'analyse des incidents
- Automatisation de certaines tâches de sécurité

**3. Les nouvelles menaces liées à l'IA**
- Création de messages de phishing plus crédibles
- Génération de contenus frauduleux
- Usurpation d'identité et deepfakes
- Automatisation des attaques
- Recherche accélérée de vulnérabilités
- Manipulation des utilisateurs par ingénierie sociale
- Production de code malveillant

**4. Les risques liés à l'utilisation de l'IA générative**
- Divulgation de données confidentielles
- Utilisation de données sensibles dans les requêtes
- Réponses erronées ou trompeuses
- Dépendance excessive aux outils d'IA
- Fuite de propriété intellectuelle
- Utilisation de services non autorisés
- Risques liés aux extensions et aux outils connectés

**5. Sécuriser l'usage de l'IA dans l'entreprise**
- Définition d'une politique d'utilisation
- Classification des données
- Contrôle des accès
- Gestion des comptes et des droits
- Encadrement des outils autorisés
- Protection des données personnelles
- Traçabilité et journalisation
- Validation humaine des réponses produites

**6. Sécuriser les applications intégrant de l'IA**
- Protection des clés d'API
- Validation des données entrantes
- Prévention des injections de prompt
- Contrôle des réponses générées
- Sécurisation des appels à des outils externes
- Gestion des droits et des autorisations
- Surveillance des usages
- Gestion des incidents

**7. Bonnes pratiques et gouvernance**
- Mise en place de règles internes
- Sensibilisation des utilisateurs
- Évaluation des risques
- Supervision des outils d'IA
- Contrôle des fournisseurs
- Mise à jour des procédures de sécurité
- Intégration de l'IA dans le plan de réponse aux incidents
- Suivi de l'évolution des menaces

**DOLFI Formation**
91 rue Saint Lazare 75009 PARIS – RCS : B438093791 – Siret : 438 093 791 00046
Tel : 01 42 78 13 83 – Fax : 01 40 15 00 53 – : **formation@dolfi.fr**
Retrouver toutes les informations sur nos stages : **https://www.dolfi.fr**

Accès spécifique consulter notre page
**https://www.dolfi.fr/ressources**