EduGroupe
Accompagner pour réussir

Sécuriser les usages et applications IA en entreprises : risques, gouvernance et bonnes pratiques

Référence : **IA046** Durée : **3 jours (21 heures)** Certification : **Aucune**

CONNAISSANCES PRÉALABLE

- Connaissance générale des systèmes d'information
- Compréhension des principes fondamentaux de la cybersécurité
- Notions sur les architectures applicatives recommandées
- Une première sensibilisation à l'intelligence artificielle générative est un plus

PROFIL DES STAGIAIRES

- Responsables sécurité des systèmes d'information (RSSI)
- Architectes sécurité
- Architectes techniques
- Ingénieurs cybersécurité
- DevSecOps
- Responsables IT
- Consultants sécurité
- Chefs de projet impliqués dans des projets IA

OBJECTIFS

- Comprendre les risques spécifiques introduits par l'intelligence artificielle générative
- Identifier les vulnérabilités propres aux modèles LLM et applications IA
- Sécuriser les données exploitées par les solutions IA
- Évaluer les risques liés aux assistants IA et aux agents autonomes
- Définir des mesures de protection adaptées aux architectures IA modernes
- Intégrer la sécurité dans le cycle de développement des applications IA
- Mettre en place une gouvernance des usages IA en entreprise
- Prendre en compte les exigences réglementaires (RGPD, AI Act)

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Mise à dispositon d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique
- La formation est constituée d'apports théoriques illustrés par des cas réels, démonstration de vulnérabilité IA, étude de scénarios d'entreprise, exercices pratiques de sécurisation, construction progressive d'un référentiel de bonnes pratiques
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

- Consultant-formateur expert IA

MÉTHODES D'ÉVALUATION DES ACQUIS

- Quiz de validation - Exercices pratiques - Analyse de scénarios sécurité - Restitution de plan de sécurisation IA
- 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. Jour 1 – Comprendre et maîtriser les nouveaux risques liés à l'IA générative

2. Comprendre le fonctionnement des solutions IA modernes

- Principes des modèles de langage (LLM)
- Fonctionnement des assistants IA génératifs
- Applications IA, copilotes et agents autonomes
- Différence entre modèle, application et service IA
- Cycle de vie d'une solution IA

3. Identifier les nouvelles surfaces d'attaque

- Pourquoi l'IA modifie les modèles traditionnels de cybersécurité
- Nouvelles menaces liées aux modèles génératifs
- Risques liés aux données utilisées par l'IA
- Risques liés aux connecteurs et automatisations
- Panorama des référentiels sécurité IA

4. Comprendre les attaques spécifiques aux LLM

- Prompt injection
- Jailbreak
- Manipulation du comportement du modèle
- Extraction d'informations sensibles
- Contournement des règles internes
- Génération de contenus ou actions non désirées
- Hallucinations et impacts sécurité

5. Sécuriser les usages internes de l'IA

- Identifier les usages non maîtrisés (Shadow AI)
- Encadrer l'utilisation des assistants publics
- Définir les règles d'usage des données
- Sensibiliser les collaborateurs
- Choisir entre solutions publiques, privées ou souveraines
- Audit d'un environnement IA d'entreprise : identification des risques, classification des usages, définition des premières mesures de réduction du risque

6. Jour 2 – Protéger les applications IA, les données et les modèles

7. Sécuriser les données utilisées par l'IA

- Classification des données
- Protection des informations sensibles
- Gestion des prompts et historiques
- Cloisonnement des connaissances
- Gestion des accès utilisateurs
- Confidentialité dans les architectures RAG

8. Sécuriser une architecture RAG

- Fonctionnement d'un système RAG
- Risques liés aux bases documentaires
- Empoisonnement des connaissances
- Contrôle des sources
- Gestion des permissions documentaires
- Validation des réponses générées

9. Sécuriser les agents IA et automatisations

- Fonctionnement des agents autonomes
- Risques liés aux actions automatisées
- Gestion des droits accordés aux agents
- Validation humaine
- Journalisation et traçabilité

10. Intégrer la sécurité dans les développements IA

- Bonnes pratiques Secure by Design
- Sécurité des API IA
- Contrôle des entrées utilisateurs
- Validation des sorties générées
- Tests de robustesse
- Analyse des dépendances
- 💡 *Tests de sécurité sur une application IA : réalisation de scénarios d'attaque, identification des vulnérabilités, proposition de corrections*

11. Jour 3 – Gouverner et industrialiser la sécurité IA

12. Mettre en place une gouvernance IA sécurisée

- Définir une politique interne d'utilisation IA
- Identifier les rôles et responsabilités
- Mettre en place un processus de validation des usages
- Contrôler les nouveaux projets IA
- Définir les règles d'intégration dans le SI

13. Intégrer les exigences réglementaires

- Principes du RGPD appliqués à l'IA
- Comprendre les enjeux de l'AI Act
- Classification des risques IA
- Documentation et traçabilité
- Gestion des fournisseurs IA

14. Superviser et auditer les solutions IA

- Surveillance des usages
- Détection des comportements anormaux
- Gestion des incidents liés à l'IA
- Indicateurs de suivi
- Amélioration continue

15. Construire une feuille de route sécurité IA

- Évaluer la maturité de l'organisation
- Prioriser les actions
- Définir les contrôles indispensables
- Accompagner l'adoption des équipes

16. Atelier final - Construction d'un plan de sécurisation IA :

- 💡 *Cartographie des usages IA*
- 💡 *Analyse des risques*
- 💡 *Règles de gouvernance*
- 💡 *Mesures techniques*
- 💡 *Plan d'amélioration*