FORMATION EN ENTREPRISE · 2 JOURS · RSSI ET ÉQUIPES TECHNIQUES

Sécuriser les systèmes d'IA : OWASP Top 10 LLM

Injection de consignes, fuite de données, agents autonomes, chaîne d'approvisionnement des modèles : deux jours pour comprendre comment on attaque un système d'IA et comment on le protège, avec des exercices sur des maquettes.

DURÉE	FORMAT	ÉVALUATION	TARIF	RÉFÉRENCE
2 jours · 13 h 30	Dans vos locaux ou à distance	Quiz et attestation	Sur devis	C2IF-IA-05

EN BREF

- Les dix risques majeurs des applications à base de modèles de langage, expliqués et démontrés.
- Les mesures de sécurité : filtrage des entrées et des sorties, cloisonnement, moindre privilège, journalisation, tests.
- Les agents autonomes et leurs outils : où sont les nouveaux risques.
- Le lien avec votre SMSI et vos exigences clients.

Objectifs pédagogiques

- Décrire les dix risques OWASP des applications à base de modèles de langage
- Évaluer une application d'IA avec une grille structurée
- Choisir et mettre en œuvre les mesures de sécurité adaptées
- Tester un système d'IA avant sa mise en production
- Intégrer ces mesures dans le système de management existant

Public concerné

- RSSI et responsables sécurité
- Développeurs et architectes qui intègrent des modèles de langage
- Administrateurs systèmes et réseaux, équipes de supervision

Prérequis. Des bases en sécurité des systèmes d'information et en développement ou administration.

Programme détaillé

JOUR 1 · MATIN Comprendre les attaques

- Injection de consignes directe et indirecte
- Fuite de données sensibles
- Empoisonnement des données et des modèles
- Chaîne d'approvisionnement

JOUR 1 · APRÈS-MIDI Démonstrations et exercices

- Attaques sur une maquette d'application : ce qui marche, ce qui ne marche pas, ce que l'on observe dans les journaux.

JOUR 2 · MATIN Protéger

- Architecture, cloisonnement, moindre privilège, filtrage, validation humaine, journalisation, gestion des secrets.
- Les agents autonomes et leurs outils.

JOUR 2 · APRÈS-MIDI Évaluer et gouverner

- Grille d'évaluation
- Tests avant mise en production
- Exigences aux fournisseurs
- Intégration au SMSI et aux obligations de l'AI Act

Les plus de cette formation

- Construite sur vos outils, vos documents et vos cas
- Des exercices et une fiche réflexes, pas un exposé
- Un formateur qui pratique ce qu'il enseigne : audit, RSSI externalisé, gouvernance de l'IA
- Adaptable en durée et en format, dans vos locaux ou à distance

Évaluation des acquis

- Questionnaire de positionnement avant la séance
- Quiz de fin de formation, corrigé en séance
- Attestation de formation remise à chaque participant
- Questionnaire de satisfaction à chaud

Ce qui est compris

- Les supports et les maquettes d'exercice
- La grille d'évaluation d'une application d'IA
- Une liste de mesures de sécurité prête à adapter
- Une attestation de formation

Méthode et qualité

- Positionnement : questionnaire envoyé aux participants avant la séance, pour adapter les exemples et le niveau
- Pédagogie active : alternance d'apports courts, de démonstrations et d'exercices sur vos cas et vos outils ; supports remis
- Satisfaction : 94,5/100 de satisfaction globale des apprenants, plus de 360 professionnels formés depuis 2022
- Accessibilité : formation accessible aux personnes en situation de handicap ; contactez-nous pour adapter les modalités
- Délai d'accès : en général deux à quatre semaines après la validation du devis

Tarification et inscription

Dans votre entreprise, ou à distance : sur devis, pour un groupe (douze participants au plus par groupe). Le tarif dépend du format, de la durée retenue et du nombre de participants ; le devis précise le programme adapté à votre contexte.

Renseignements et devis : contact@c2if.com · 06 59 12 51 36 · c2if.com

Formation dispensée par C2IF, organisme de formation déclaré sous le numéro 75331474233. Cet enregistrement ne vaut pas agrément de l'État. Le financement dépend de votre OPCO et du montage retenu.

Formateur : Nicolas Mariage, auditeur de certification ISO/IEC 27001, formateur Platine PECB 2024, 2025 et 2026, certifié ISO/IEC 42001 Lead Implementer.