Plan de cours N° : 1365
Durée : 2 jours (14h)

Sécurité des systèmes IA & cybersécurité

PARTICIPANTS / PRE-REQUIS

RSSI, DSI, ingénieurs sécurité, développeurs IA, responsables conformité

Notions de cybersécurité et de systèmes informatiques

OBJECTIFS PEDAGOGIQUES

Comprendre les vulnérabilités spécifiques aux systèmes IA. Identifier les attaques adversariales, data poisoning et autres menaces IA. Appliquer les bonnes pratiques pour sécuriser les modèles et les données. Mettre en place une surveillance et un plan de réponse aux incidents IA.

MOYENS PEDAGOGIQUES

Tour de table au début de chaque formation pour définir les objectifs de chaque participant,
Alternance entre apports théoriques (en moyenne 30%) et exercices pratiques (en moyenne 70%),
Utilisation de cas concrets issus de l'expérience professionnelle de nos formateurs,
Remise d'un support de cours,
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS

Positionnement préalable oral ou écrit,
Evaluation des acquis tout au long de la formation par des exercices de synthèse,
Attestation de stage remise à chaque apprenant, avec son niveau d'acquisition pour chaque objectif pédagogique,
Feuille de présence signée par demi-journée,
Questionnaire de satisfaction pour évaluer la qualité de l'enseignement,
En option : passage certification possible selon les thématiques

MOYENS TECHNIQUES EN PRESENTIEL

Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc

MOYENS TECHNIQUES DES CLASSES A DISTANCE

Grâce à un logiciel comme Teams, suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
Nous vous conseillons très fortement l'utilisation de votre webcam et de disposer d'un double écran.
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 04.76.41.14.20..

ORGANISATION

Les cours ont lieu de 9h00-12h30 13h30-17h00 (adaptable à la demande).

PROFIL FORMATEUR

Nous recrutons méticuleusement nos formateurs selon 3 critères : expertise, pédagogie et agilité.

ACCESSIBILITE

Les personnes atteintes de handicap souhaitant suivre nos formations sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités d'organisation.

MISE A JOUR

10/06/2025

Plan de cours N° : 1365
Durée : 2 jours (14h)

Sécurité des systèmes IA & cybersécurité

Vulnérabilités et menaces IA

- Introduction aux risques spécifiques liés aux IA
- Attaques adversariales (exemples, impact, détection)
- Data poisoning et manipulation des données d'entraînement
- Problèmes de confidentialité et d'exfiltration de données

Sécurisation et gestion des incidents

- Architecture sécurisée des systèmes IA
- Gestion des accès, chiffrement, anonymisation
- Monitoring et détection d'anomalies IA
- Plans de réponse aux incidents et continuité opérationnelle