[TECH10]

- **Objectifs**
  - **Comprendre les enjeux de sécurité liés à l'IA générative**
  - **Identifier les risques cyber spécifiques à la conception et à l'utilisation** de l'IA générative
  - **Mettre en place des mesures pour intégrer la sécurité dès la phase de développement**
  - **Favoriser une démarche proactive de gestion des risques cyber** dans les projets d'IA générative

- **Public visé**
  - Profils techniques : développeurs, architectes, etc…
  - Chefs de projets souhaitant acquérir les connaissances pour sécuriser la conception d'IA générative

- **Prérequis**
  - Connaissances de bases en IA et machine learning
  - Notions en cybersécurité et en règlementations sur la protection des données

- **Accessibilité aux personnes en situation de handicap**
  - Si l'un des participants est en situation de handicap et souhaite nous en faire part, n'hésitez pas à prendre contact avec notre Référente Handicap clients par mail à l'adresse trainingcenter.ocd@orange.com

Cyberdefense

Intégrer les risques cyber dans la conception d'IA générative

Programme de formation

- **Introduction à l'IA générative et ses enjeux**
  - Présentation de l'IA générative : concepts, applications, et enjeux
  - Panorama des risques liés à l'IA générative
  - Impact potentiel sur la sécurité et la confidentialité

- **Risques cyber spécifiques à l'IA générative**
  - Vulnérabilités des modèles d'IA (exploitation, manipulation, injection de données malveillantes)
  - Risques liés à la confidentialité et à la fuite de données
  - Risques de génération de contenus malveillants ou trompeurs
  - Attaques adversariales et leur impact

- **Approches pour intégrer la sécurité dès la conception**
  - Principes de sécurité dès la conception (Security by Design)
  - Analyse de risques et évaluation de la vulnérabilité
  - Techniques de sécurisation des données d'entraînement
  - Validation et vérification des modèles

- **Mesures de mitigation et bonnes pratiques**
  - Mise en place de contrôles et de tests de sécurité
  - Surveillance continue et détection d'anomalies
  - Gestion des incidents et plan de réponse
  - Respect des réglementations et normes en cybersécurité

[TECH10] Intégrer les risques cyber dans la conception d'IA générative

Méthodes pédagogiques

- Alternance de théorie et de pratique, études de cas
- Retour d'expérience, échange de bonnes pratiques et écueils à éviter
- Remise d'un support pédagogique favorisant la transférabilité des acquis

Méthodes d'évaluation de l'atteinte des objectifs

- Évaluation continue lors des exercices et des mises en situation pratique
- QCM en fin de formation

Durée	1 jour (7 heures)
Groupe de formation	De 3 à 10 participants
Langue	Français / Anglais

Mode de déploiement	Présentiel	Distanciel	E-learning
Modalités	Intra	Inter	Sur-mesure
Tarif	Sur devis	Non concerné	Sur devis

Demande de devis – Modalités et délais d'accès

- **Pour toute demande intra**, contacter le Training Center à l'adresse **trainingcenter.ocd@orange.com** ou **au 06 87 05 79 34.** Le délai moyen de mise en œuvre est d'**environ 2 mois** (hors demande urgente).