Sécuriser les pipelines IAML : de l'entraînement à la production

Lien : https://innov-systems.com/formation/securiser-les-pipelines-iaml-de-lentrainement-a-la-production

DURÉE
5 jours (35h)

RÉFÉRENCE
BDI204

CATÉGORIE
Sécurité de l'Intelligence Artificielle

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les risques de sécurité propres aux pipelines IA/ML
- Concevoir des architectures Secure MLOps robustes
- Sécuriser les données d'entraînement et les modèles
- Protéger les environnements de développement et d'entraînement
- Mettre en œuvre des mécanismes de protection contre les attaques adversariales
- Sécuriser le déploiement des modèles en production
- Renforcer la sécurité de la supply chain IA
- Mettre en place un monitoring de sécurité des modèles
- Garantir la conformité réglementaire et la gouvernance de l'IA
- Déployer des pipelines IA sécurisés à l'échelle de l'entreprise
- Réduire les risques liés aux modèles et aux données
- Étudier des cas concrets de sécurisation de plateformes IA

POUR QUI ?

- Machine Learning Engineers
- MLOps Engineers
- AI Engineers
- Data Scientists
- Data Engineers
- DevSecOps Engineers
- Cloud Security Engineers
- Architectes IA et Cloud
- RSSI / CISO
- Consultants en cybersécurité
- Responsables gouvernance IA
- Toute personne impliquée dans le développement, le déploiement et la sécurisation de solutions d'intelligence artificielle

Innov Systems

Programme détaillé

1 / Fondamentaux de la sécurité des pipelines IA/ML

- Architecture d'un pipeline Machine Learning
- Menaces spécifiques aux systèmes d'IA
- Principes du MLOps sécurisé (Secure MLOps)

2 / Sécurisation des données d'entraînement

- Gouvernance et qualité des jeux de données
- Détection des données malveillantes (Data Poisoning)
- Protection des données sensibles et confidentialité

3 / Sécurité des environnements de développement

- Gestion sécurisée des notebooks et IDE
- Contrôle des dépendances et bibliothèques ML
- Gestion des secrets et des identifiants

4 / Sécurisation de l'entraînement des modèles

- Intégrité des modèles et reproductibilité
- Isolation des environnements d'entraînement
- Signature et vérification des artefacts ML

5 / Sécurité de la supply chain IA

- Gestion des modèles, datasets et artefacts
- Vérification des modèles préentraînés
- SBOM, provenance et signature des composants

Innov Systems

6 / Déploiement sécurisé des modèles

- Sécurisation des API d'inférence
- Conteneurisation et orchestration sécurisées
- Contrôle des accès et authentification

7 / Protection contre les attaques sur les modèles

- Attaques adversariales et évasion
- Model stealing et model extraction
- Défenses et techniques de robustesse

8 / Surveillance et sécurité en production

- Monitoring des modèles et détection de dérives
- Détection des comportements anormaux
- Journalisation, audit et réponse aux incidents

9 / Gouvernance, conformité et gestion des risques

- Gouvernance des modèles IA
- Conformité réglementaire et exigences sectorielles
- Gestion des risques et politiques de sécurité IA

10 / Cas pratiques et architecture Secure MLOps

- Sécurisation d'un pipeline ML de bout en bout
- Mise en œuvre d'une chaîne CI/CD sécurisée pour l'IA
- Bonnes pratiques de sécurisation des plateformes IA

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

23 au 27 Nov. 2026	Distanciel
18 au 22 Jan. 2027	Présentiel - Casablanca
15 au 19 Mars 2027	Présentiel - Casablanca
10 au 14 Mai 2027	Présentiel - Casablanca
05 au 09 Juil. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés