Cylian

Programme de formation

Sécurisation des IA en production

Code : EAI-SEC-100 Durée : 3 jours (21 heures)

Public visé

Ingénieurs IA/ML, Data Scientists en production, architectes DevSecOps, responsables sécurité, opérateurs de plateformes IA, auditeurs et consultants en sécurité des systèmes IA.

Prérequis

- Expérience pratique avec des frameworks IA (TensorFlow, PyTorch, Scikit-learn)
- Connaissances basiques en sécurité applicative et réseaux
- Familiarité avec CI/CD et DevOps

Objectifs pédagogiques

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

- Cartographier le cycle de vie d'un modèle IA selon MITRE ATLAS
- Implémenter des contrôles d'accès et la traçabilité dans les pipelines
- Détecter et atténuer les attaques adversariales
- Intégrer la surveillance continue avec des indicateurs IA
- Élaborer des plans de réponse aux incidents

Programme

Jour 1 - Matin : MITRE ATLAS et cartographie

- Introduction MITRE ATLAS
- Cartographie du pipeline IA
- Inventaire des actifs critiques

Jour 1 - Après-midi : Contrôles d'accès

- Contrôles d'accès IAM
- Séparation des environnements DEV/TRAIN/PROD
- Chiffrement des données et modèles
- Audit API

Jour 2 - Matin : Empoisonnement de données

- Techniques d'empoisonnement de données
- Détection d'anomalies statistiques

Jour 2 - Après-midi : Attaques adversariales

- Attaques d'évasion et inversion de modèle
- Défenses par distillation et randomisation

Jour 3 - Matin : Surveillance

- Surveillance IoCs-IA
- Dashboards et alertes (Grafana/Prometheus)

Jour 3 - Après-midi : Réponse aux incidents

- Plans de réponse aux incidents
- Rollback et réentraînement
- Simulation d'incident

Modalités d'évaluation des acquis

- En cours de formation, par des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation