

# Sécurisation des IA en production

3 jours (21 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

**2 625 € HT** par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 25/09/2026. Document téléchargé le 06/10/2026.

## Objectifs

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

- Cartographier le cycle de vie d'un modèle IA selon MITRE ATLAS et identifier les zones de risque
- Mettre en place des contrôles d'accès et de traçabilité pour chaque phase du pipeline (données, entraînement, inférence)
- Détecter et atténuer les attaques adversariales (empoisonnement, inversion de modèle, évasion) en production
- Intégrer des mécanismes de surveillance continue et d'alerte basés sur des indicateurs de compromission IA (IoCs-IA)
- Elaborer un plan de réponse aux incidents IA incluant rollback, réentraînement et communication aux parties prenantes.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

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

### Prérequis

Avoir une expérience pratique sur un framework IA (TensorFlow, PyTorch, Scikit-learn) et des connaissances de base en sécurité des applications et en réseau. Etre familier avec les concepts de CI / CD et DevOps.

# Programme

## 1 Pendant votre formation

### Sécurisation des IA en production

Jour 1 – Matin

#### Cartographie et contrôles d'accès

- Introduction MITRE ATLAS : tactiques et phases (reconnaissance, accès au pipeline, attaques sur le modèle)
- Cartographie d'un pipeline IA interne :
  - Flux de données
  - Artefacts de modèles
  - Points d'inférence

*Exemple de travaux pratiques (à titre indicatif)*

- Modéliser votre pipeline IA et inventorier les actifs critiques

Jour 1 – Après-midi

#### Cartographie et contrôles d'accès – Suite

- Contrôles d'accès et traçabilité : gestion des identités (IAM), séparation des environnements DEV/TRAIN/PROD
- Chiffrement des données et des modèles (au repos, en transit)

*Exemple de travaux pratiques (à titre indicatif)*

- Déployer un mécanisme d'audit sur les appels d'API d'inférence

Jour 2 – Matin

#### Attaques adversariales et atténuation

- Attaques par empoisonnement de données (Data Poisoning) et par falsification (Data Falsification)
- Détection des anomalies de données à l'entraînement (statistiques, ML-based)

*Exemple de travaux pratiques (à titre indicatif)*

- Injecter et détecter un cas simple d'empoisonnement de Dataset

Jour 2 – Après-midi

#### Attaques adversariales et atténuation – Suite

- Attaques d'évasion d'inférence (Evasion Attacks) et inversion de modèle (Model Extraction)
- Contre-mesures :
  - Défenses par distillation
  - Randomisation
  - Evaluation de robustesse (FGSM, PGD)

*Exemple de travaux pratiques (à titre indicatif)*

- Générer des exemples adversariaux et tester la robustesse du modèle en production

Jour 3 – Matin

### Surveillance continue et réponse

- Surveillance des indicateurs de compromission IA (IoCs-IA) : dérive de performance, patterns de requêtes anormales
- Mise en place de dashboards et alertes (logs d'inférence, métriques d'exactitude)

*Exemple de travaux pratiques (à titre indicatif)*

- Configurer un pipeline de monitoring dans Grafana / Prometheus pour un service IA

Jour 3 – Après-midi

### Surveillance continue et réponse – Suite

- Plan de réponse aux incidents IA :
  - Rollback de modèle
  - Réentraînement sécurisé
  - Communication
- Clôture et recommandations pour une gouvernance IA pérenne

*Exemple de travaux pratiques (à titre indicatif)*

- Exercice guidé : simulation d'un incident de compromission IA et exécution du plan de réponse

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

### Accessibilité aux personnes en situation de handicap

## Détails de la session

Du 2 novembre 2026 au 4 novembre 2026 (3 jours / 21 heures)

Le Havre

Du 2 novembre 2026 au 4 novembre 2026 **Le Havre**

- 2 novembre 2026 ..... 9h00 – 16h00
- 3 novembre 2026 ..... 9h00 – 16h00
- 4 novembre 2026 ..... 9h00 – 16h00