

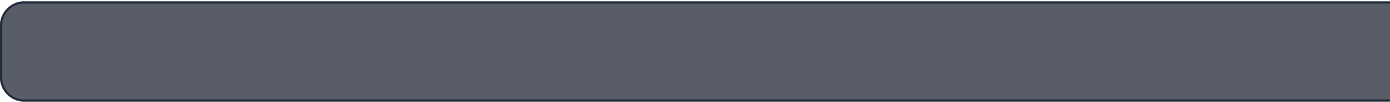


MLOps conforme ISO 27001 et NIS 2 — pipeline

16 mai 2026 • Mis à jour le 17 mai 2026 • 16 min de lecture • 3016 mots



Sécurisez vos pipelines MLOps en conformité ISO 27001 et NIS 2 : gouvernance ML, data lineage, CI/CD IA sécurisé, audit trail, gestion des secrets GPU. Guide pour les équipes.



À RETENIR

A retenir -- MLOps conforme ISO 27001 et NIS 2

La conformité MLOps aux référentiels ISO 27001 et NIS 2 est un sujet émergent. Les pipelines ML/IA sont désormais reconnus comme des actifs informationnels soumis aux mêmes exigences de sécurité que les systèmes IT traditionnels. Les spécialistes requièrent une approche adaptée : gouvernance des modèles ML (versioning, approbation), sécurité de la supply chain ML (intégrité des modèles et données), secrets GPU (clés API LLM, credentials de registres de modèles) et audit trail.

Un projet cybersécurité ?
Réponse sous 24h

Devis gratuit →

Réponse sous 24h

Devis
gratuit →