ISO/IEC 27090:2026

Cybersécurité des systèmes d’intelligence artificielle

Menaces, impacts et points de vigilance : une lecture éditoriale pour les professionnels.

UNE LECTURE CYBERASTRE POUR LES PROFESSIONNELS

CYBERASTRE
#ReadyForward

01 / LE PÉRIMÈTRE ANNONCÉ PAR L'ISO

Une norme de cybersécurité dédiée aux systèmes d'IA.

ISO/IEC 27090:2026 fournit des orientations pour comprendre, détecter et atténuer les menaces et compromissions propres aux systèmes d'intelligence artificielle, tout au long de leur cycle de vie.

La présentation publique de l'ISO s'adresse aux organisations qui développent ou utilisent de l'IA. Elle met en relation les vulnérabilités, leur exploitation et leurs conséquences. Les pages suivantes proposent notre lecture opérationnelle de ces enjeux ; elles ne constituent pas une liste de contrôles exigés par la norme.

1 **DONNÉES**
apprentissage et usage

2 **MODÈLES**
comportement et propriété

3 **INTERACTIONS**
requêtes et sorties

4 **SERVICES**
interfaces et dépendances

L'ANGLE DÉCISIF

Pour une organisation, l'enjeu est de rendre visibles les dépendances entre données, modèle et usages. C'est sur cette chaîne que notre analyse de cybersécurité doit relier les menaces aux impacts métier.

La surface d’attaque suit la chaîne de l’IA.

Le risque ne s’arrête ni au serveur ni au modèle. Il suit les dépendances du système : acquisition des données, entraînement, mise à disposition du modèle, requêtes, sorties, services connectés, puis mises à jour.



Cette lecture par chaîne est importante : une attaque peut commencer sur une donnée apparemment secondaire et se manifester plus tard dans le comportement du modèle ou dans un service qui consomme ses réponses.

CONSÉQUENCE PRATIQUE

L’inventaire de cybersécurité doit rendre visibles les actifs IA et leurs dépendances, pas uniquement les machines qui les hébergent.

Quand la donnée est l’attaque elle-même.

L’empoisonnement des données consiste à altérer les exemples utilisés pour entraîner ou actualiser un système. L’effet n’est pas nécessairement visible au moment où la donnée entre dans le pipeline : il peut apparaître ensuite, dans une réponse ou un comportement ciblé.

SCÉNARIO DE RISQUE

Des données collectées en production sont réutilisées pour une mise à jour. Si une partie a été corrompue, elle peut contaminer la prochaine version du modèle.

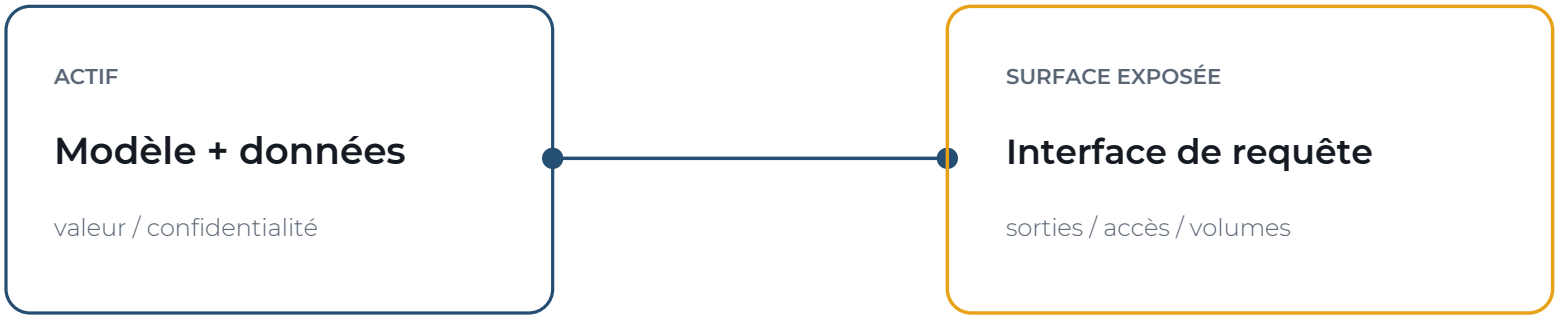
C’est pourquoi le cycle de vie compte : dans les systèmes mis à jour de façon continue ou itérative, les entrées opérationnelles peuvent devenir de futures données d’apprentissage. Le risque peut donc revenir après la mise en service, et pas seulement lors du premier entraînement.

LECTURE CYBERASTRE

Le point de contrôle se déplace aussi vers la collecte, la provenance et l’intégrité des données réutilisées. La question n’est pas seulement « le modèle est-il protégé ? », mais « quelles données façonneront sa prochaine version ? »

Un modèle peut être convoité sans intrusion classique.

Le vol de modèle figure parmi les menaces citées dans la présentation publique de l'ISO. Une interface peut aussi exposer la valeur d'un modèle : en observant de nombreuses réponses, un adversaire peut chercher à en imiter le comportement. La protection ne se limite donc pas au dépôt qui contient les fichiers du modèle.



Le second enjeu est la fuite : des données d'entraînement ou des informations fournies au système peuvent être exposées par son comportement. La confidentialité concerne alors autant le modèle et la propriété intellectuelle que les données confiées par les utilisateurs.

LECTURE CYBERASTRE

Traiter le modèle comme un actif sensible implique d'examiner qui peut l'interroger, quelles informations ses réponses révèlent et quels signaux permettraient de repérer une extraction progressive.

L’attaque peut se cacher dans une demande ordinaire.

L’injection d’instructions exploite la manière dont un système interprète un contenu fourni. La demande peut détourner la réponse attendue, révéler des informations ou influencer une action en aval. Dans un système relié à des outils ou à des services, l’impact ne s’arrête pas nécessairement au texte généré.



ENTRÉE

instruction malveillante

INTERPRÉTATION

comportement détourné

EFFET

sortie ou action

Le point d’analyse est le chemin complet entre entrée, décision et conséquence : quelles données sont accessibles au modèle ? Quelles capacités lui sont accordées ? Une sortie peut-elle déclencher une opération ou orienter une décision à fort impact ?

> **CE QUE LE RÉSUMÉ NE DOIT PAS MASQUER**
>
> Une sortie apparemment cohérente n’est pas une preuve d’intégrité. La réponse doit être évaluée selon les accès et les effets qu’elle peut produire dans le système réel.

Le risque évolue avec le système.

ISO/IEC 27090 traite les menaces sur le cycle de vie, du développement à l'exploitation. Cette continuité est particulièrement importante lorsque des données d'usage servent à mettre à jour ou réentraîner le modèle : un incident en production peut ainsi fragiliser une version future.



La norme complète les pratiques de cybersécurité établies, notamment celles d'ISO/IEC 27001 et 27002, en aidant à voir où les caractéristiques de l'IA créent des besoins supplémentaires pour les données, modèles et flux de travail.

À RETENIR

27090 est un guide de cybersécurité centré sur l'IA. Il ne remplace ni un système de management de la sécurité de l'information, ni la gouvernance plus large de l'IA.

Lire la norme.

En comprendre les enjeux.

Cyberastre propose cette lecture indépendante pour aider les organisations à relier la cybersécurité de l'IA à leurs actifs, à leurs usages et à leurs décisions métier.



Notre travail consiste à relier les menaces techniques aux actifs exposés, aux impacts métier et aux décisions de cybersécurité à prendre.

ÉCHANGEONS SUR VOS SYSTÈMES D'IA

Devenez Cyberastreur : travaillons ensemble sur les enjeux de vos systèmes d'intelligence artificielle.

PARLONS DE VOTRE BESOIN

cyberastre.com / Nous contacter

SOURCES Notice publique ISO · OWASP GenAI Security · Analyse Cyberastre

Publication indépendante de Cyberastre. Non affiliée à l'ISO ; ni publication officielle, ni reproduction du texte normatif.