Savez-vous quelles IA vos équipes utilisent ?

Votre entreprise a peut-être choisi une IA. Vos équipes en utilisent souvent d'autres, et y collent des données sensibles. Le plus souvent, personne ne le voit : c'est le **Shadow IA**.

VOUS VOUS RECONNAISSEZ ?

ESN ET INFOGÉRANCE — compte personnel

« Un chef de projet colle le cahier des charges d'un client dans son IA personnelle. »

Le cahier des charges de votre client est sorti de l'entreprise.

COLLECTIVITÉ — IA gratuite

« Un agent colle le dossier d'un administré dans une IA gratuite trouvée la veille. »

Son identité, son adresse et sa situation sont parties chez un tiers.

SANTÉ ET PHARMACIE — extension de navigateur

« Un chercheur fait résumer des résultats d'essais par une extension. »

Des données de santé ont quitté l'établissement.

ÉQUIPE INFORMATIQUE — assistant de code

« Un développeur confie son code à l'assistant de son éditeur, avec la clé d'accès en clair. »

La clé est partie : quelqu'un peut l'utiliser, à vos frais.

L'IA, une porte d'entrée souvent sans gardien.

Messagerie	Site web	Réseau	Postes	NOUVEAU IA
antispam	pare-feu web	pare-feu	antivirus	peu d'outils la voient

CE QUI SORT

La fuite de données

Une fois envoyée à une IA externe, une donnée est sortie de chez vous. Vous ne pouvez plus la rappeler.

2023 · SAMSUNG · CHATGPT
Des employés collent du code source confidentiel pour le faire corriger. Le code sort de l'entreprise.

CE QUI ENTRE

La manipulation de l'IA

Un document ou un e-mail piégé porte une consigne cachée. Si l'IA est branchée sur vos outils, la consigne peut devenir une action.

2025 · ECHOLEAK · MICROSOFT 365 COPILOT
Un e-mail piégé contient des consignes cachées. L'assistant les suit, sans que l'utilisateur clique.

Interdire ne suffit pas. Rendez le Shadow IA visible, sans envoyer vos données ailleurs.

VOIR AU VERSO

ATLAS vous rend la main.

Sur chaque poste, ATLAS applique votre charte IA. Il regarde ce qui part vers les IA en ligne, et ce qui en revient. Votre équipe informatique fixe les règles et garde le dernier mot. Chaque décision est conservée : de quoi vous aider à répondre à NIS2, ISO 27001 et RGPD.



CHEZ VOUS

L'IA qui détecte est installée chez vous.

Les modèles de détection d'ATLAS tournent sur votre infrastructure. **Installé, rien ne part chez un tiers pour être analysé.**

Pendant la bêta, des données de test remontent chez Kodetis, selon un périmètre fixé avec vous.

96 %
de détection sur 3 810 requêtes

3 s
au plus pour une analyse

Test interne Kodetis.

FEUILLE DE ROUTE

Ce qui tourne en bêta, et ce que nous construisons avec vous.

DÉJÀ EN BÊTA

- **La détection**, installée sur vos serveurs.
- **Un agent pour les développeurs**, branché sur leur assistant de code.
- **La console** : alertes et historique.

EN COURS

- **L'agent sur chaque poste**, déployé par votre outil de gestion de parc.
- **L'inventaire Shadow IA** : quelles IA sont utilisées, poste par poste.
- **Les fichiers joints**, contrôlés avant de partir vers l'IA.
- **Les assistants IA de bureau**, en commençant par Claude Desktop.

Ensuite, à l'étude : les IA consultées dans le navigateur, et les postes Windows.

Vous vous êtes reconnu ? Construisez ATLAS avec nous.

Nous cherchons des bêta-testeurs parmi les entités soumises à NIS2. Vous essayez ATLAS sur vos usages réels de l'IA, nous l'améliorons avec vous.

VOTRE CONTACT

Thibaut Fontaine
Fondateur de Kodetis
contact@kodetis.com

atlas.kodetis.com