Qu'est-ce que le Shadow AI, et qui, au sein de mon organisation, crée le risque ?

Réponse courte : Le Shadow AI désigne les employés qui utilisent des outils d'IA que le service informatique n'a pas approuvés ou dont il ignore l'existence. Le risque ne se limite pas au personnel non hiérarchique — les administrateurs privilégiés et les comptes compromis constituent souvent une exposition plus importante.

Trois sources d'exposition

- **Les employés** utilisant des outils d'IA non autorisés pour leur productivité quotidienne.
- **Les administrateurs privilégiés**, dont l'accès de haut niveau signifie que tout ce qu'ils transmettent à un outil d'IA peut inclure des données d'entreprise hautement sensibles.
- **Les comptes compromis**, où un attaquant disposant d'identifiants valides utilise les outils d'IA comme canal d'exfiltration — un trafic qui ressemble à une activité de productivité ordinaire.

Cela se produit déjà

Cyber Crucible a directement observé des accès massifs à de gros volumes de données en une seule fois, par des employés utilisant des outils d'IA pour rechercher et téléverser des informations. Il ne s'agit pas d'un risque futur théorique en cours de modélisation ; c'est un comportement visible dans des déploiements réels dès aujourd'hui.

La troisième catégorie mérite une attention particulière. Un attaquant utilisant des outils d'IA pour exfiltrer des données est difficile à distinguer d'un employé enthousiaste — à moins que l'application des règles n'intervienne au niveau de l'accès aux données, où l'intention et la politique peuvent être évaluées indépendamment de l'identité de la personne connectée.

Revision #1
Created 2026-07-24 06:58:58 UTC by Dennis Underwood
Updated 2026-07-24 06:58:58 UTC by Dennis Underwood