O que é Shadow AI, e quem dentro da minha organização está a criar o risco?

Resposta curta: Shadow AI refere-se a colaboradores que utilizam ferramentas de IA que o departamento de TI não aprovou ou desconhece. O risco não se limita ao pessoal de base — administradores privilegiados e contas comprometidas representam frequentemente a maior exposição.

Três fontes de exposição

- **Colaboradores** que utilizam ferramentas de IA não autorizadas para produtividade do dia a dia.
- **Administradores privilegiados**, cujo acesso de alto nível significa que tudo o que introduzem numa ferramenta de IA pode incluir dados corporativos altamente sensíveis.
- **Contas comprometidas**, em que um atacante com credenciais válidas utiliza ferramentas de IA como canal de exfiltração — tráfego que se assemelha a produtividade normal.

Isto já está a acontecer

A Cyber Crucible observou diretamente o acesso em massa a grandes volumes de dados de uma só vez, por colaboradores que utilizam ferramentas de IA para pesquisar e carregar informação. Este não é um risco futuro teórico a ser modelado; é um comportamento visível em implementações reais atualmente.

A terceira categoria merece atenção especial. Um atacante que utiliza ferramentas de IA para retirar dados é difícil de distinguir de um colaborador entusiasta — a menos que a aplicação de controlos ocorra ao nível do acesso aos dados, onde a intenção e a política podem ser avaliadas independentemente de quem está autenticado.

Revision #1
Created 2026-07-24 05:48:18 UTC by Dennis Underwood
Updated 2026-07-24 05:48:18 UTC by Dennis Underwood