¿Qué es la Shadow AI y quién dentro de mi organización está generando el riesgo?

Respuesta breve: Shadow AI se refiere a empleados que utilizan herramientas de IA que TI no ha aprobado o de las que no tiene conocimiento. El riesgo no se limita al personal de base: los administradores con privilegios y las cuentas comprometidas suelen representar la mayor exposición.

Tres fuentes de exposición

- **Empleados** que utilizan herramientas de IA no autorizadas para la productividad cotidiana.
- **Administradores con privilegios**, cuyo acceso de alto nivel implica que cualquier información que introduzcan en una herramienta de IA puede incluir datos corporativos altamente sensibles.
- **Cuentas comprometidas**, en las que un atacante con credenciales válidas utiliza herramientas de IA como canal de exfiltración, generando un tráfico que parece productividad habitual.

Esto ya está ocurriendo

Cyber Crucible ha observado directamente accesos masivos a grandes volúmenes de datos a la vez por parte de empleados que utilizan herramientas de IA para buscar y cargar información. No se trata de un riesgo futuro teórico que se esté modelando; es un comportamiento visible en implementaciones reales actualmente.

La tercera categoría merece especial atención. Un atacante que utiliza herramientas de IA para extraer datos es difícil de distinguir de un empleado entusiasta, a menos que la aplicación de controles se realice en la capa de acceso a los datos, donde la intención y la política pueden evaluarse independientemente de quién haya iniciado sesión.

Revision #1
Created 2026-07-24 01:49:59 UTC by Dennis Underwood
Updated 2026-07-24 01:50:00 UTC by Dennis Underwood