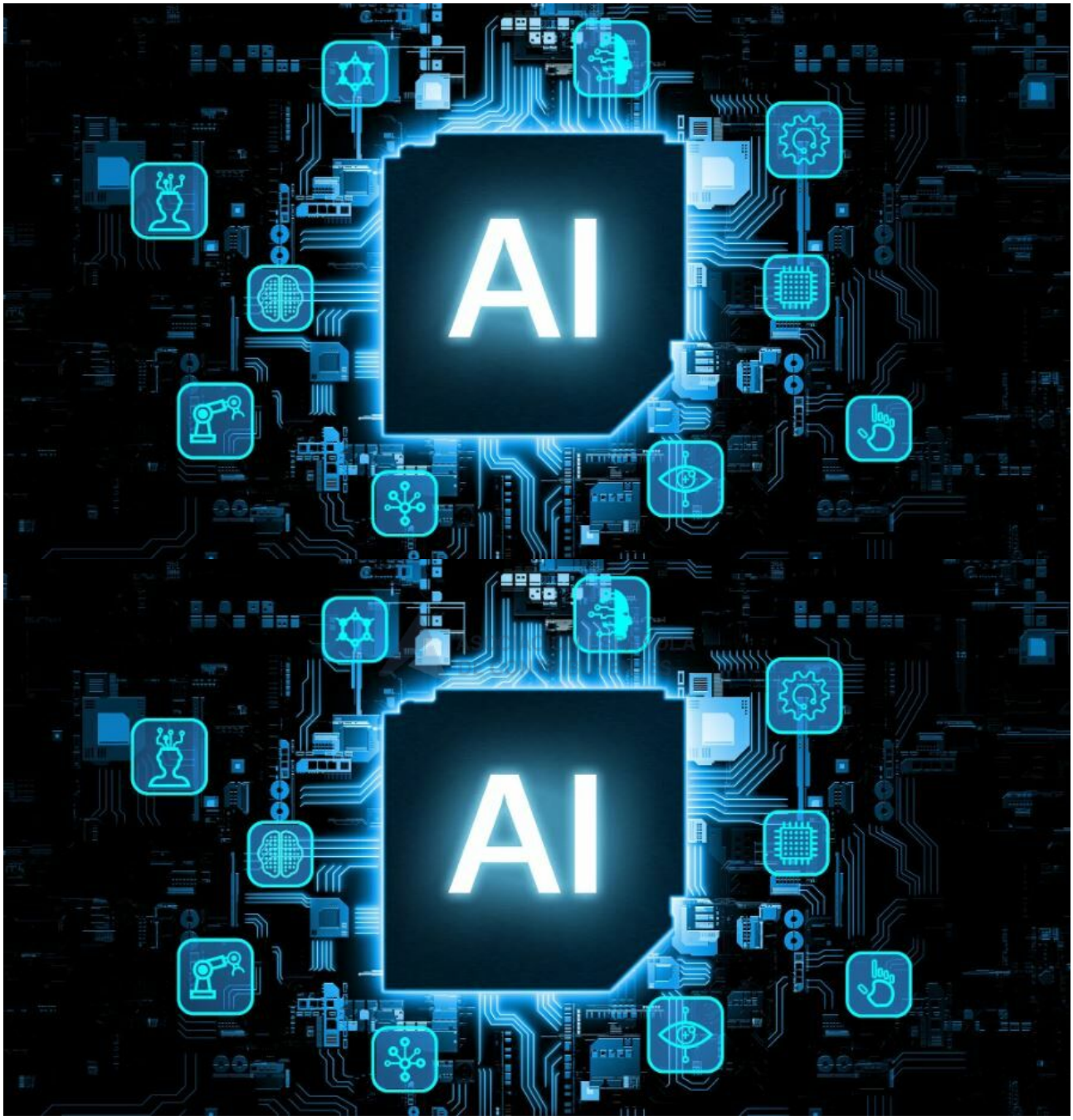
La IA ya multiplica por cuatro la velocidad de los ciberataques a las empresas

Estrategias de Inversión
21/02/2026



El último Informe Global de Respuesta a Incidentes 2026 de Unit 42, la división de inteligencia de amenazas de Palo Alto Networks, dibuja un escenario inquietante: **los atacantes están utilizando inteligencia artificial de forma sistemática y han conseguido acelerar el ciclo**

completo de intrusión hasta cuatro veces en apenas un año.

El dato más alarmante es el tiempo que tardan algunos grupos en pasar del acceso inicial a la exfiltración de datos. En los casos más rápidos analizados, ese proceso se ha reducido a solo 72 minutos.

Es decir, una empresa puede ser vulnerada, explorada y saqueada en poco más de una hora si no cuenta con mecanismos de detección automatizados.

El estudio se basa en el análisis de más de 750 incidentes críticos gestionados durante el último ejercicio. La conclusión es clara: **la IA ya forma parte estructural del arsenal ofensivo y está siendo empleada a lo largo de todo el ciclo de vida del ataque,** desde la fase de reconocimiento hasta la evasión de controles y la automatización del movimiento lateral dentro de las redes corporativas.

Identidades en el punto de mira

Uno de los cambios más significativos detectados en el informe es el protagonismo de las técnicas basadas en identidad. **El 65% de los accesos iniciales se producen mediante el abuso de credenciales, ingeniería social o explotación de fallos en la gestión de identidades humanas y de máquina**. Las vulnerabilidades técnicas tradicionales representan un porcentaje menor del punto de entrada.

Los atacantes ya no necesitan explotar únicamente un servidor mal configurado. Les basta con comprometer una cuenta válida, un token OAuth o una clave API para moverse por entornos corporativos complejos.

La identidad se ha convertido en la nueva superficie crítica y, al mismo tiempo, en uno de los eslabones más débiles de la cadena de defensa.

Ataques multicanal y más difíciles de contener

El informe revela que el 87% de los incidentes analizados implican dos o más superficies de ataque. No se trata de intrusiones lineales, sino de operaciones coordinadas que combinan acciones en endpoints, plataformas cloud, sistemas de identidad y aplicaciones de terceros. En

algunos casos se ha observado actividad simultánea en hasta diez frentes distintos.

El navegador corporativo también emerge como un campo de batalla clave. Casi la mitad de los ataques estudiados incluyen algún tipo de manipulación de sesiones web, robo de credenciales a través de páginas aparentemente legítimas o abuso de extensiones. Lo que antes era una simple herramienta de trabajo se ha convertido en un vector estratégico.

Además, los ataques vinculados a la cadena de suministro SaaS se han disparado. **Desde 2022 se han multiplicado por casi cuatro y ya representan una parte relevante del total de incidentes.**

La explotación de integraciones entre aplicaciones y el uso indebido de permisos concedidos a terceros permiten a los atacantes moverse lateralmente sin levantar sospechas inmediatas.

Brechas que nacen de la complejidad

Unit 42 vincula el 90% de las brechas de datos a configuraciones incorrectas o fallos de seguridad derivados de la complejidad. **La falta de visibilidad unificada, la fragmentación de herramientas y el exceso de confianza** implícita facilitan el éxito de los adversarios.

Cuando los equipos de seguridad dependen de soluciones aisladas que no comparten información en tiempo real, la capacidad de respuesta se ralentiza. En un entorno donde los atacantes operan en minutos, **cualquier demora puede marcar la diferencia entre contener un incidente o sufrir una fuga masiva de información sensible.**

La adopción de **agentes autónomos basados en IA** por parte de los ciberdelincuentes añade una capa adicional de riesgo. Estos sistemas pueden correlacionar credenciales humanas y de máquina, escalar privilegios y ejecutar acciones sin intervención constante, reduciendo drásticamente los tiempos tradicionales de ataque.

Hacia una defensa a velocidad de máquina

El informe plantea la necesidad de evolucionar hacia modelos de seguridad integrados capaces de operar con automatización avanzada. Las organizaciones deben reforzar sus centros de operaciones con **herramientas que detecten anomalías en segundos y apliquen medidas de contención sin intervención manual prolongada.**

También resulta esencial integrar la seguridad en el ciclo de desarrollo de software y de inteligencia artificial, evitando que vulnerabilidades lleguen a entornos productivos.