Información clave del informe

Las API basadas en IA son menos seguras que el resto.

La mayoría de las API basadas en inteligencia artificial (IA) son extremadamente accesibles y muchas utilizan mecanismos de autenticación inadecuados, una vulnerabilidad que se agrava con la creciente variedad de ataques con IA que las acechan.

La IA supone una ventaja técnica para los ciberdelincuentes.

Esto incluye avances como malware generado por IA, análisis de vulnerabilidades, ataques a sistemas integrados con IA y capacidades avanzadas de scraping web.

32 %

Porcentaje de crecimiento de los incidentes relacionados con los 10 principales riesgos de seguridad de API según OWASP

Los incidentes de seguridad de las API están aumentando y los 10 principales problemas de seguridad de las API según OWASP revelan fallos en la autenticación y autorización que dejan al descubierto funciones y datos confidenciales.

30 %

Aumento de las alertas relacionadas con el marco de seguridad MITRE

Los atacantes utilizan técnicas avanzadas, como la automatización y la IA, para explotar las API. El marco de trabajo MITRE puede ayudar a los defensores a identificar estos ataques de forma más rápida y precisa.

33 %

Porcentaje de aumento de los ataques web globales año tras año

El aumento de los ataques está directamente relacionado con la rápida adopción de servicios en la nube, microservicios y aplicaciones de IA, que amplían las superficies de ataque y presentan nuevos desafíos de seguridad.

230 000 millones+

Número de ataques web que afectan a las organizaciones comerciales,

lo que lo convierte en el sector más afectado, con casi el triple de ataques que el sector de la alta tecnología (el segundo más afectado).