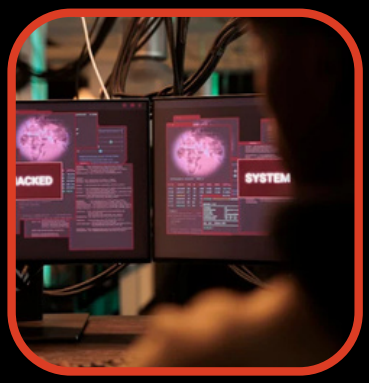
BOLETÍN INFORMATIVO N°212

DICIEMBRE 2025



Los marcos de seguridad tradicionales dejan a las organizaciones expuestas a vectores de ataque específicos de la IA

En diciembre de 2024, la popular biblioteca de IA Ultralytics se vio comprometida, instalando código malicioso que secuestró recursos del sistema para la minería de criptomonedas. En agosto de 2025 , paquetes Nx maliciosos filtraron 2349 credenciales de GitHub, la nube y la IA. A lo largo de 2024, las vulnerabilidades de ChatGPT permitieron la extracción no autorizada de datos de usuarios de la memoria de la IA.

MongoDB Vulnerability CVE-2025-14847 Under Active Exploitation Worldwide

Una vulnerabilidad de seguridad recientemente revelada en MongoDB ha sido explotada activamente, con más de 87.000 instancias potencialmente susceptibles identificadas en todo el mundo.

El nuevo ladrón de macOS MacSync usa una aplicación firmada para eludir el Gatekeeper de Apple

Investigadores de ciberseguridad han descubierto una nueva variante de un ladrón de información de macOS llamado MacSync que se distribuye a través de una aplicación Swift firmada digitalmente y notariada que se hace pasar por un instalador de aplicaciones de mensajería para eludir los controles Gatekeeper de Apple.

Una nueva falla de MongoDB permite a atacantes no autenticados leer memoria no inicializada

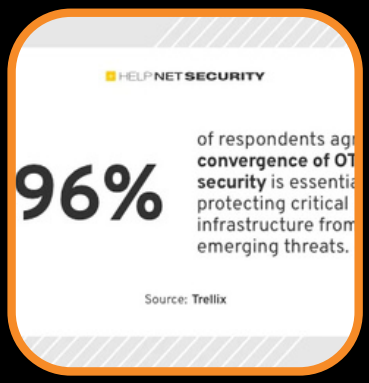
Se ha revelado una falla de seguridad de alta gravedad en MongoDB que podría permitir que usuarios no autenticados lean memoria de montón no inicializada.

Fortinet advierte sobre la explotación activa de la vulnerabilidad de omisión de 2FA en VPN SSL de FortiOS

Fortinet dijo el miércoles que observó un "abuso reciente" de una falla de seguridad de cinco años de antigüedad en FortiOS SSL VPN bajo ciertas configuraciones.

RECOMENDACIONES

LECTURA DE SEGURIDAD



La automatización obliga a reiniciar la estrategia de seguridad

Los equipos de seguridad empresarial trabajan bajo la premisa de que la disrupción es constante. Un estudio global de Trellix muestra que la resiliencia ha pasado de ser un objetivo a largo plazo a un requisito estructural para los CISO. El diseño de la infraestructura, la integración operativa y el uso de IA determinan cómo las organizaciones se preparan para la presión constante de las amenazas y la regulación.

Los LLM pueden ayudar con la puntuación de vulnerabilidad, pero el contexto aún importa

Cada nueva divulgación de vulnerabilidades supone un nuevo punto de decisión para los equipos de seguridad, que ya están sobrecargados. Un estudio reciente explora si los LLM pueden asumir parte de esa carga mediante la calificación de vulnerabilidades a gran escala. Si bien los resultados son prometedores en áreas específicas, las debilidades persistentes siguen frenando la calificación totalmente automatizada.

Resumen semanal: Ataques a MongoDB, filtraciones de billeteras, spyware para Android, delitos internos y más

Las noticias cibernéticas de la semana pasada en 2025 no se centraron en un gran incidente. Se centraron en muchas pequeñas grietas que se abrieron al mismo tiempo. Las herramientas en las que la gente confía a diario se comportaron de forma inesperada. Viejas fallas resurgieron. Se utilizaron nuevas casi de inmediato.

NOTICIAS DE

NUESTROS PARTNERS

Cómo proteger la IA en la empresa: un marco práctico para modelos, datos y agentes

La IA avanza a un ritmo superior al que la gobernanza puede seguir, ampliando las superficies de ataque y creando riesgos imprevistos. Desde datos y modelos hasta agentes e integraciones de IA, la seguridad empieza por saber qué proteger. Descubra cómo identificar los riesgos generados por la IA para establecer marcos de gobernanza y controles que aseguren la innovación sin exponer a la empresa a nuevas superficies de ataque.

Cuando su servicio no espera: Solución de problemas de EasyTrade con Dynatrace MCP y Gemini CLI

¿Conoces ese momento en el que todo debería funcionar, pero no es así? Tu implementación se desarrolló sin problemas, los pods están funcionando, pero aun así... errores. Muchos.

Encontrar a los olvidados: Por qué el descubrimiento de credenciales es esencial para proteger el acceso remoto privilegiado

La proliferación de credenciales es uno de los riesgos más ignorados en los entornos modernos de acceso remoto. Este blog explora por qué el descubrimiento de credenciales es esencial para proteger el acceso remoto privilegiado.

BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

HAZ CLICK

EVENTOS CERCANOS DE NUESTROS PARTNERS

DARKTRACE

Más Información

BeyondTrust

Más Información

IBM Gold Partner

Más Información