

Un nuevo ataque de inyección de contexto criptográfico podría permitir a las páginas web robar datos de chat de Grok.

Adversa AI ha revelado una técnica de ataque que, según afirma, puede provocar que el chatbot Grok de xAI envíe el nombre del usuario, su ubicación aproximada, su nivel de suscripción y las indicaciones de la conversación en curso a un servidor controlado por el atacante después de que el usuario le pida que resuma una página web común

[ver artículo >>](#)

Scripts de explotación generados por IA atacan PLC Siemens S7 en infraestructura crítica de EE. UU.

El gobierno estadounidense advirtió el miércoles sobre una "amenaza activa" dirigida a organizaciones de infraestructura crítica en el país mediante scripts de explotación generados por inteligencia artificial (IA).

[ver artículo >>](#)

El propio controlador de Microsoft Defender puede utilizarse como arma para eliminar el software de seguridad al arrancar el sistema.

Check Point Research ha revelado una técnica que utiliza el controlador de corrección de arranque firmado legítimamente por Microsoft Defender para realizar operaciones arbitrarias de archivos y registro a nivel del kernel en sistemas Windows que van desde Windows 7 hasta Windows 11 25H2, sin explotar ninguna vulnerabilidad de software ni importar ningún controlador externo al equipo

[ver artículo >>](#)

INCIDENTES DE SISTEMAS



La vulnerabilidad CVE-2026-19478 de GitLab comienza a ser explotada activamente a los pocos días de su divulgación.

Según watchTowr, una vulnerabilidad de seguridad recientemente descubierta en GitLab ha sido objeto de explotación activa a los pocos días de su divulgación pública.

[ver artículo >>](#)



Microsoft corrige una grave vulnerabilidad de Entra ID (CVSS 10.0) que permitía la ejecución remota de código

Aunque el boletín de seguridad inicialmente marcó el campo "Explotado" en la tabla de Evaluación de Explotabilidad como "Sí", el 21 de agosto de 2026, Microsoft corrigió el estado de "Explotado" a "No" después de que The Hacker News contactara a la compañía para obtener comentarios. También señaló que "esta vulnerabilidad no fue explotada en la práctica"

[ver artículo >>](#)



RECOMENDACIONES DE LECTURA DE SEGURIDAD

Los atacantes de ransomware están centrando su atención en las empresas medianas.

Según Black Kite, las empresas medianas representaron el 73% de los incidentes de ransomware y extorsión de datos con ingresos conocidos que se hicieron públicos en Norteamérica y Europa entre enero de 2023 y junio de 2026.

[ver artículo >>](#)



Resumen semanal: Ataques a PLC con IA, ataques a GitLab, filtraciones de claves de Stripe y más.

Se instala un paquete. Se abre una ventana de inicio de sesión. El equipo queda conectado a internet. Hasta el momento, no se observa nada inusual.

[ver artículo >>](#)

El malware para automóviles Android se propaga a través de los actualizadores integrados para realizar fraude publicitario y crear una red de bots proxy.

Investigadores de ciberseguridad han detectado una nueva familia de malware diseñada específicamente para infectar el firmware de las unidades principales de vehículos basadas en Android, desarrollado por DoFun

[ver artículo >>](#)



NOTICIAS DE NUESTROS PARTNERS



Cuando los agentes de IA atacan: El caso de la detección de anomalías de comportamiento

Las recientes directrices del NCSC establecen los controles necesarios para implementar la IA con agentes de forma segura. Sin embargo, la aprobación es solo el punto de partida: el siguiente paso consiste en comprender cómo se comportan realmente los agentes una vez que operan en la empresa.

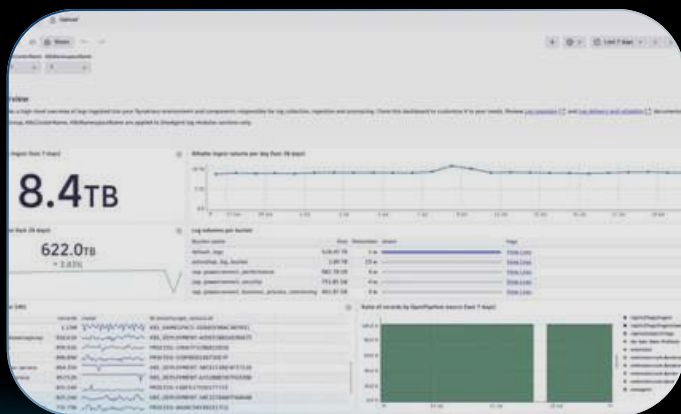
[ver artículo >>](#)



La gestión moderna de registros ahora es más sencilla: mejoras de resiliencia y autoservicio para la ingesta de registros.

Los registros son donde la observabilidad se vuelve real, y donde se complica. Los volúmenes aumentan repentinamente sin previo aviso.

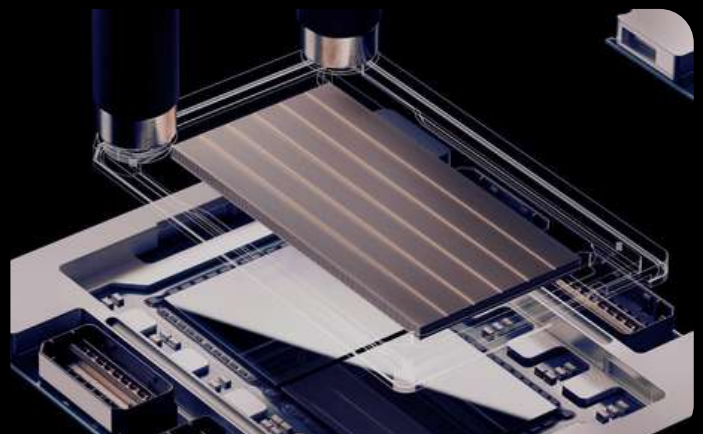
[ver artículo >>](#)



IBM presenta el procesador de arquitectura dual de próxima generación para IBM Z y LinuxONE.

Un diseño revolucionario permitirá llevar las aplicaciones nativas de Arm a los mainframes y servidores insignia de IBM, ampliando así las opciones de software para la informática empresarial.

[ver artículo >>](#)



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

 **BeyondTrust**

IBM
Gold Partner

[Más Información](#)

[Más Información](#)

[Más Información](#)