Mainsoft®

BOLETÍN INFORMATIVO

#220 | Mayo 2026

Cómo las alucinaciones provocadas por la IA están creando riesgos reales para la seguridad.

Las interpretaciones erróneas de la IA están introduciendo graves riesgos de seguridad en la toma de decisiones sobre infraestructuras críticas, al explotar la confianza humana mediante resultados altamente fiables pero incorrectos.

ver artículo >>

Cómo reducir la exposición al phishing antes de que se convierta en una interrupción del negocio.

Qué ocurre cuando un correo electrónico de phishing parece lo suficientemente limpio como para pasar los filtros de seguridad, pero es lo suficientemente peligroso como para exponer a la empresa con un solo clic?

ver artículo >>

La mayoría de los programas de remediación nunca confirman que la solución haya funcionado realmente.

Los equipos de seguridad nunca han tenido mejor visibilidad de sus entornos y nunca han sido peores a la hora de confirmar que lo que arreglan permanece arreglado.

ver artículo >>

Cuatro paquetes maliciosos de npm distribuyen malware de robo de información y ataques DDoS de bots fantasma.

Investigadores de ciberseguridad han descubierto cuatro nuevos paquetes npm que contienen malware para robar información, uno de los cuales es un clon del gusano Shai-Hulud, cuyo código fuente fue publicado por TeamPCP .

ver artículo >>

INCIDENTES DE SISTEMAS

La filtración del token de Grafana en GitHub provocó la descarga del código fuente y un intento de extorsión.

Grafana ha revelado que una "parte no autorizada" obtuvo un token que le otorgaba la capacidad de acceder al entorno GitHub de la empresa y descargar su código fuente.

ver artículo >>

Una vulnerabilidad en el módulo de reescritura de NGINX, con 18 años de antigüedad, permite la ejecución remota de código sin autenticación.

Investigadores de ciberseguridad han revelado múltiples vulnerabilidades de seguridad que afectan a NGINX Plus y NGINX Open, incluyendo un fallo crítico que permaneció sin detectar durante 18 años.

ver artículo >>

Una vulnerabilidad crítica del kernel de Linux, denominada 'ssh-keysign-pwn', expone claves SSH y contraseñas ocultas.

Una vulnerabilidad del kernel de Linux recientemente descubierta está generando gran preocupación en la comunidad de seguridad, ya que permite a los atacantes acceder a datos altamente confidenciales, incluidas claves privadas SSH y hashes de contraseñas, en los sistemas afectados.

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

La puerta trasera de IA que su pila de seguridad no está diseñada para ver

Las empresas que implementan sistemas de gestión de lógica de negocio (LLM) han dedicado los últimos dos años a desarrollar defensas basadas en una premisa razonable: el comportamiento malicioso deja rastro en los datos de entrada.

ver artículo >>

La economía del ransomware 3.0

Tácticas de triple extorsión y por qué el seguro cibernético ya no sustituye a una arquitectura madura de respuesta a incidentes.

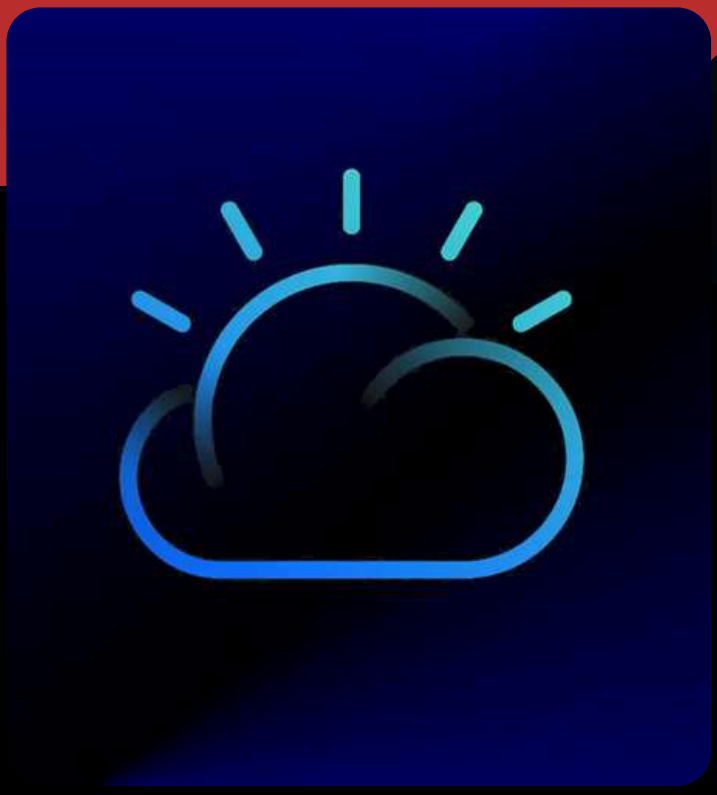
ver artículo >>

Resumen semanal: Vulnerabilidad de día cero en Exchange, gusano npm, repositorio de IA falso, exploit de Cisco y más.

El lunes comenzó con un problema de confianza. Se estaba utilizando activamente una vulnerabilidad en un servidor de correo. Un sistema de control de red fue atacado. Paquetes de confianza fueron infectados.

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS



Amenazas internas de la IA: Cómo la IA generativa está cambiando el riesgo interno

Este blog analiza cómo la IA ha transformado la manera de comprender y abordar las amenazas internas. Asimismo, explora un enfoque de defensa en profundidad y aborda las medidas que los CISO y los responsables del SOC pueden tomar para proteger a sus organizaciones de las amenazas internas derivadas de la IA.

ver artículo >>

IBM anuncia la integración de Red Hat AI Inference y Red Hat OpenShift Virtualization Service en IBM Cloud.

Anunció nuevos servicios gestionados: Red Hat AI Inference en IBM Cloud y Red Hat OpenShift Virtualization Service en IBM Cloud, para ayudar a las empresas a acelerar la adopción de la IA y ejecutar entornos de virtualización seguros, escalables y predecibles.

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

Más Información

BeyondTrust

Más Información

IBM Gold Partner

Más Información