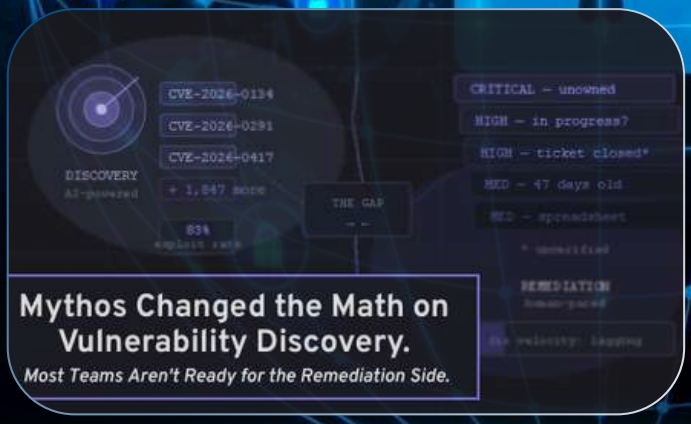
BOLETÍN INFORMATIVO

#217 | Abril 2026

Mythos cambió las matemáticas del descubrimiento de vulnerabilidades. La mayoría de los equipos no están preparados para la parte de remediación.



Investigadores de ciberseguridad han detectado un nuevo programa malicioso llamado ZionSiphon que parece estar diseñado específicamente para atacar los sistemas israelíes de tratamieLa versión preliminar de Claude Mythos de Anthropic ha dominado los debates sobre seguridad desde su anuncio el 7 de abril.

ver artículo >>

PhantomCore explota las vulnerabilidades de TrueConf para infiltrarse en redes rusas.

Se ha atribuido a un grupo de hacktivistas proucranianos llamado PhantomCore los ataques dirigidos activamente contra servidores que ejecutan el software de videoconferencia TrueConf en Rusia desde septiembre de 2025.

ver artículo >>

La interfaz de línea de comandos de Bitwarden se ve comprometida en la campaña en curso de la cadena de suministro de Checkmarx.

Según los hallazgos de JFrog y Socket, Bitwarden CLI , la interfaz de línea de comandos del gestor de contraseñas Bitwarden, ha sido comprometida como parte de una campaña de la cadena de suministro de Checkmarx recientemente descubierta y en curso.

ver artículo >>

Investigadores advierten que textutil y KeePassXC de macOS pueden convertirse en herramientas de ataque en la automatización.

Investigadores de seguridad han alertado sobre dos herramientas muy fiables, macOS textutil y KeePassXC, demostrando que ambas pueden volverse peligrosas cuando se integran en sistemas automatizados que procesan datos de entrada controlados por atacantes.

ver artículo >>

INCIDENTES DE SISTEMAS

Una vulnerabilidad crítica en la interfaz de línea de comandos de Gemini permite ataques de ejecución remota de código.

Google ha corregido una vulnerabilidad de seguridad crítica en la interfaz de línea de comandos de Gemini que podría permitir a los atacantes ejecutar código remoto en determinados flujos de trabajo automatizados.

ver artículo >>

Vercel confirma una brecha de seguridad: se han visto comprometidas varias cuentas de clientes.

La plataforma de infraestructura web Vercel ha revelado un importante incidente de seguridad relacionado con el acceso no autorizado a sistemas internos, y ha rastreado la cadena de ataque hasta una vulneración de Context.ai, una herramienta de productividad de IA de terceros utilizada por uno de sus empleados

ver artículo >>

RECOMENDACIONES DE LECTURA DE SEGURIDAD

El "gestor de agentes": cómo la IA transforma el rol del analista del SOC.

La IA no está tomando el control del SOC; está convirtiendo a los analistas en "gestores de agentes" que supervisan las investigaciones automatizadas en lugar de quedar sepultados en la clasificación repetitiva de alertas.

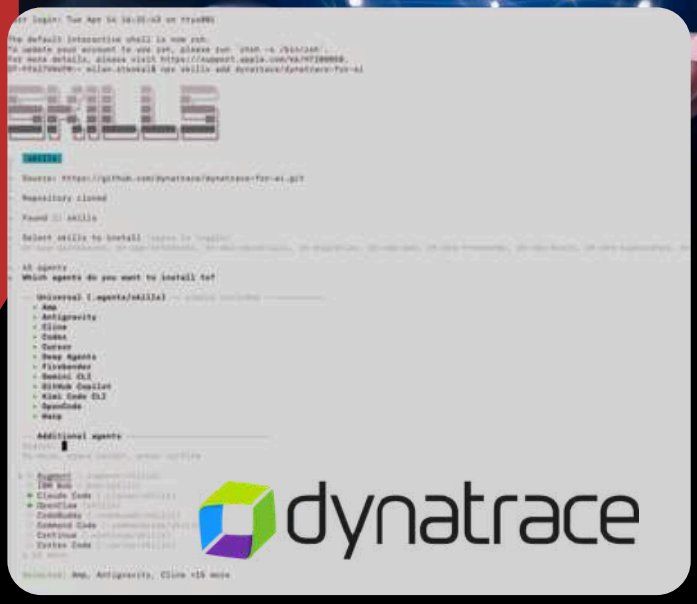
ver artículo >>

Las principales técnicas que utilizan los atacantes para infiltrarse en sus sistemas hoy en día

El abuso de herramientas populares, ClickFix y los ataques basados en la identidad se encuentran entre las técnicas más comunes que los ciberdelincuentes utilizan actualmente para infiltrarse en las redes empresariales.

ver artículo >>

NOTICIAS DE NUESTROS PARTNERS



Dynatrace para IA: Enseña a tu agente de codificación de IA a usar Dynatrace.

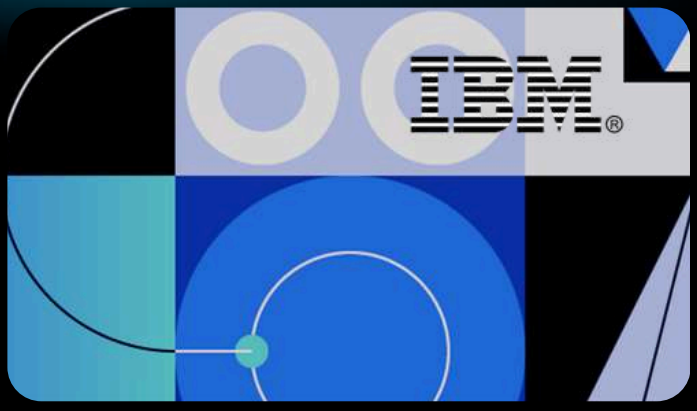
Presentamos Dynatrace para IA, una colección de código abierto de habilidades y sugerencias para agentes que proporciona a cualquier asistente de codificación de IA compatible con habilidades la experiencia en el dominio que necesita para trabajar de forma productiva y precisa con Dynatrace.

ver artículo >>

Riesgo cibernético transmitido por correo electrónico: un desafío fundamental para el CISO en la era del volumen y la sofisticación.

Un antiguo CISO comparte su perspectiva sobre el reto de proteger la capa humana, las deficiencias de la formación actual en concienciación sobre seguridad y cómo se puede mejorar para prepararse mejor para las amenazas de gran volumen, alto impacto y centradas en el ser humano.

ver artículo >>



IBM colabora con Google Cloud para acelerar la modernización de la IA empresarial y la nube híbrida.

En todos los sectores, recibimos un mensaje constante de las grandes empresas: necesitan modernizar sus sistemas centrales, poner en marcha la IA y ejecutar cargas de trabajo en múltiples nubes sin añadir complejidad. Muchas buscan flexibilidad híbrida, operaciones predecibles e IA fiable, pero la integración de plataformas, modelos y herramientas entre proveedores de nube sigue siendo un reto importante.

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