BOLETÍN INFORMATIVO N°199

SEPTIEMBRE 2025

HybridPetya: un imitador del ransomware Petya/NotPetya que anula UEFI Secure Boot

Análisis de este imitador UEFI de Petya/NotPetya que explota CVE-2024-7344, descubierto por VirusTotal.

HiddenGhost, Winos y kkRAT explotan páginas SEO y de GitHub en ataques de malware chinos

Los usuarios de habla china son el objetivo de una campaña de envenenamiento de optimización de motores de búsqueda (SEO) que utiliza sitios de software falsos para distribuir malware.

Una falla en el editor de código de Cursor AI permite la ejecución silenciosa de código a través de repositorios maliciosos

Se ha revelado una debilidad de seguridad en el editor de código Cursor , impulsado por inteligencia artificial (IA) , que podría desencadenar la ejecución de código cuando se abre un repositorio creado con fines malintencionados utilizando el programa.

Senador estadounidense insta a la FTC a investigar a Microsoft por "negligencia grave en ciberseguridad"

El senador estadounidense Ron Wyden solicitó el miércoles a la Comisión Federal de Comercio (FTC) "investigar y responsabilizar a Microsoft" por su papel en una serie de incidentes de ciberseguridad de alto perfil en los últimos años, diciendo que el enfoque de la compañía hacia la seguridad "continúa amenazando la seguridad nacional de Estados Unidos".

IBM QRadar SIEM Vulnerability Let Attackers Perform Unauthorized Actions

A critical permission misconfiguration in the IBM QRadar Security Information and Event Management (SIEM) platform could allow local privileged users to manipulate configuration files without authorization.

Vulnerabilidad del agente de credenciales de identificación de usuario de Palo Alto Networks expone contraseñas en texto sin cifrar

Una vulnerabilidad recientemente revelada en el agente de credenciales de identificación de usuario de Palo Alto Networks para Windows, identificada como CVE-2025-4235, podría exponer la contraseña de una cuenta de servicio en texto sin formato bajo ciertas configuraciones no estándar.

RECOMENDACIONES

LECTURA DE SEGURIDAD

¿Cómo podría ser una red 6G segura?

Los estándares oficiales para 6G se anunciarán a fines de 2029. Si bien la industria avanza hacia un consenso sobre cómo se construirá la red 6G, también necesita anticipar cómo se verá comprometida y asegurarse de construirla con un enfoque de seguridad por diseño.

Seguridad OT: Por qué vale la pena considerar el código abierto

Las soluciones comerciales de seguridad OT pueden ser muy costosas. Aquí hay algunas alternativas.

6 ataques basados en navegador para los que los equipos de seguridad deben prepararse ahora mismo

Los ataques dirigidos a los usuarios a través de sus navegadores web han experimentado un aumento sin precedentes en los últimos años. En este artículo, exploraremos qué es un "ataque basado en navegador" y por qué está demostrando ser tan efectivo.

NOTICIAS DE

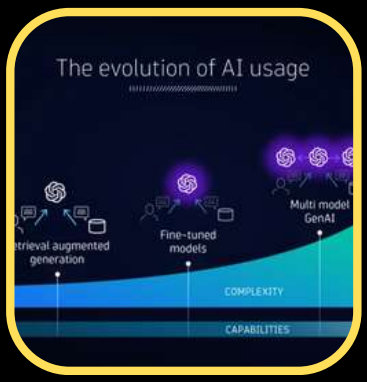
NUESTROS PARTNERS

Los beneficios de integrar la seguridad de la red y el correo electrónico

Unificar la seguridad de la red y el correo electrónico cierra brechas críticas en sus defensas, lo que permite una detección, investigación y respuesta más rápidas. Descubra cómo un enfoque integrado basado en IA refuerza la protección durante todo el ciclo de vida de los ataques.

Garantizar la fiabilidad de la IA: por qué es fundamental la observabilidad de la IA

A medida que se acelera la inversión en IA, está surgiendo una brecha entre la ambición y la ejecución. IDC prevé1 que, para 2028, el gasto en IA representará el 16,4 % del gasto total en TI. Sin embargo, Gartner, Inc.2 predice que más del 40 % de los proyectos de IA agencial se cancelarán a finales de 2027.



BeyondTrust Privileged Remote Access 25.2: Innovación que impulsa la seguridad

BeyondTrust Privileged Remote Access 25.2 presenta nuevas capacidades y mejoras que fortalecen el acceso seguro, agilizan la gestión de credenciales y amplían la automatización, lo que ayuda a los equipos de TI y OT a moverse más rápido sin sacrificar el control.

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