

FEBRERO 2025

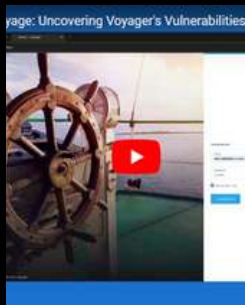


Los piratas informáticos abusan de AWS y Microsoft Azure para lanzar ciberataques a gran escala

Los piratas informáticos aprovechan cada vez más plataformas en la nube como Amazon Web Services (AWS) y Microsoft Azure para orquestar ataques cibernéticos a gran escala.

Una estafa de publicidad maliciosa utiliza anuncios falsos de Google para secuestrar cuentas de publicidad de Microsoft

Investigadores de ciberseguridad han descubierto una campaña de publicidad maliciosa que se dirige a los anunciantes de Microsoft con anuncios falsos de Google que pretenden llevarlos a páginas de phishing capaces de recopilar sus credenciales.



Los fallos de PHP Voyager sin parchear dejan los servidores expuestos a ataques RCE con un solo clic

Se han revelado tres fallas de seguridad en el paquete PHP de código abierto Voyager que podrían ser explotadas por un atacante para lograr la ejecución remota de código con un solo clic en las instancias afectadas.

Broadcom corrige los fallos de VMware Aria: los exploits pueden provocar el robo de credenciales

Broadcom ha lanzado actualizaciones de seguridad para corregir cinco fallas de seguridad que afectan a VMware Aria Operations y Aria Operations for Logs, advirtiendo a los clientes que los atacantes podrían explotadas para obtener acceso elevado u obtener información confidencial.





El ransomware WantToCry aprovecha las vulnerabilidades de SMB para cifrar de forma remota las unidades NAS

El conocido grupo de ransomware WantToCry aprovecha servicios de bloque de mensajes de servidor (SMB) mal configurados para infiltrarse en redes y lanzar ataques generalizados.

INCIDENTES DE SISTEMAS



Se descubren nuevos vectores de ataque de vaciado de procesos en Windows 11 (24H2).

El reciente lanzamiento de la versión 24H2 de Windows 11 ha introducido una gama de nuevas características y actualizaciones, pero también ha suscitado importantes preocupaciones en materia de ciberseguridad.

Vulnerabilidad en el controlador de pantalla de la GPU NVIDIA permite a los atacantes robar archivos de forma remota

NVIDIA ha lanzado una actualización de seguridad de software crítica para abordar múltiples vulnerabilidades que afectan a su controlador de pantalla de GPU y al software de GPU virtual (vGPU).

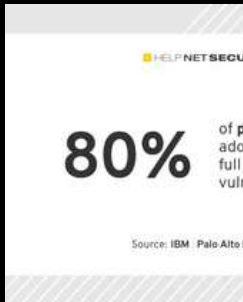


Vulneración de seguridad de día cero en BeyondTrust: la clave API de 17 clientes de SaaS está comprometida

BeyondTrust, una empresa líder en gestión de identidad y acceso, reveló una violación de seguridad crítica que afectó a 17 clientes de su plataforma SaaS de soporte remoto .

RECOMENDACIONES

LECTURA DE SEGURIDAD



La plataformización es clave para reducir la complejidad de la ciberseguridad

Según un informe de IBM y Palo Alto Networks, las organizaciones se enfrentan a desafíos de complejidad en materia de seguridad al combinar un promedio de 83 soluciones de seguridad diferentes de 29 proveedores. También muestra que 7 de cada 10 empresas encuestadas con un alto grado de plataforma de seguridad informan que sus inversiones en ciberseguridad han ayudado a obtener resultados comerciales como eficiencias operativas y generación de ingresos.

PyPI presenta el estado de archivo para alertar a los usuarios sobre paquetes de Python sin mantenimiento

Los encargados del mantenimiento del registro Python Package Index (PyPI) han anunciado una nueva característica que permite a los desarrolladores de paquetes archivar un proyecto como parte de los esfuerzos para mejorar la seguridad de la cadena de suministro .

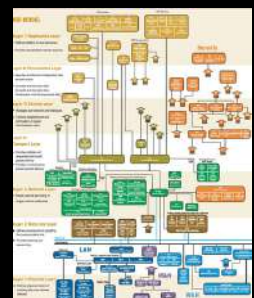


¿Qué es la gestión de la superficie de ataque?

Las superficies de ataque están creciendo más rápido de lo que los equipos de seguridad pueden seguir: para mantenerse a la vanguardia, necesita saber qué está expuesto y dónde es más probable que ataquen los atacantes.

Los 10 mejores firewalls de aplicaciones web (WAF) – 2025

Un firewall de aplicaciones web (WAF) es una solución de seguridad diseñada para proteger las aplicaciones web mediante la supervisión, el filtrado y el bloqueo del tráfico HTTP/S malicioso.



NOTICIAS DE NUESTROS PARTNERS



Reimaginando su SOC: superando la fatiga de alertas con investigaciones dirigidas por IA

Cómo reinventar su SOC, partes 2 y 3: Este blog explora cómo se pueden abordar los desafíos que enfrenta el SOC moderno transformando el proceso de investigación y desbloqueando la eficiencia y la escalabilidad en las operaciones del SOC con IA.

Novedades de la versión 1.307 de Dynatrace SaaS

Esta página muestra nuevas características, cambios y correcciones de errores en la versión 1.307 de Dynatrace SaaS.

Para obtener más información sobre las nuevas aplicaciones de Dynatrace y las actualizaciones de funciones con esta versión, seleccione un elemento de la siguiente tabla.



Telefónica Tech e IBM firman un acuerdo de colaboración para una tecnología cuántica segura

Telefónica Tech integrará la tecnología de seguridad cuántica de IBM en sus servicios de ciberseguridad para crear casos de uso específicos destinados a abordar riesgos nuevos y futuros asociados con el avance de las computadoras cuánticas criptográficamente relevantes.

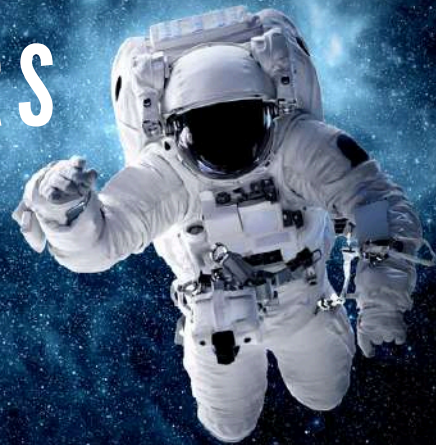
BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainssoft, 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](#)

 **CYLANCE**

[Más Información](#)


Gold Partner

[Más Información](#)

