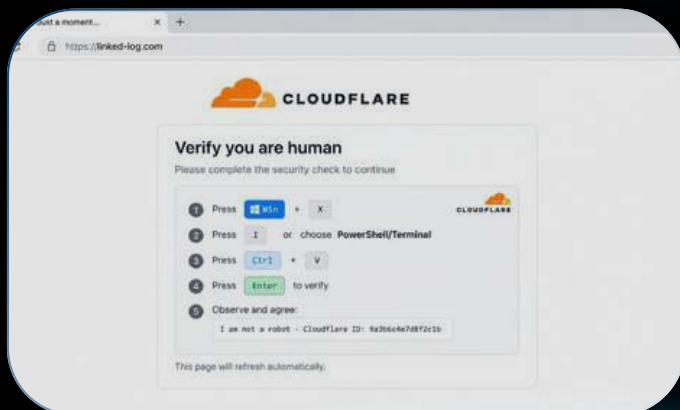


Un grupo de ciberdelincuente vinculado a China secuestra routers Cisco para robar credenciales y ocultar registros de seguridad.

Un actor de ciberespionaje vinculado a China, identificado como Fire Ant, ha extendido una campaña de larga duración más allá de los hipervisores VMware para comprometer los enrutadores Cisco IOS XR, los servidores del sistema de control de acceso del controlador de acceso a terminales (TACACS) y los hosts de administración Linux utilizados para enrutar, autenticar y administrar redes de alto valor.

[ver artículo >>](#)

TerminalFix utiliza CAPTCHAs falsos de Cloudflare para desplegar una puerta trasera de túnel inverso.

Microsoft ha revelado detalles de una nueva variante de ClickFix, denominada TerminalFix, cuyo objetivo es engañar a los usuarios para que ejecuten un comando malicioso en Windows Terminal o PowerShell.

[ver artículo >>](#)

Los atacantes instalan herramientas de acceso remoto en servidores PaperCut comprometidos.

El ciberdelincuente que ataca los servidores de aplicaciones PaperCut con acceso a Internet está instalando de forma encubierta software legítimo de acceso remoto en ellos, según ha comunicado PaperCut Software en su actualización más reciente sobre la campaña de ataque en curso.

[ver artículo >>](#)

INCIDENTES DE SISTEMAS



Tres vulnerabilidades de ServiceNow en CVSS 10.0 podrían permitir a atacantes no autenticados ejecutar código y SQL.

ServiceNow ha publicado parches para cuatro fallos de seguridad que afectan a la plataforma ServiceNow AI, tres de ellos con una calificación de 10,0 en el sistema de puntuación CVSS y explotables, en determinadas circunstancias, por un atacante no autenticado.

[ver artículo >>](#)



Una grave vulnerabilidad en cPanel podría permitir que un cliente de hosting tome el control total de un servidor.

cPanel ha publicado parches para corregir una vulnerabilidad de seguridad que afecta al estacionamiento de dominios y a la funcionalidad de dominios adicionales en cPanel y WebHost Manager (WHM), la cual podría permitir la ejecución de código como usuario root.

[ver artículo >>](#)

RECOMENDACIONES DE LECTURA DE SEGURIDAD

ShinyHunters afirma haber robado 284 millones de registros de pacientes de McKesson.

La empresa de atención médica McKesson reveló un incidente de ciberseguridad en el que piratas informáticos accedieron a aplicaciones de terceros y robaron datos.

[ver artículo >>](#)



Resumen semanal: Proxy de espionaje chino, agentes de IA que se desvían de su tarea, puertas traseras en routers y más.

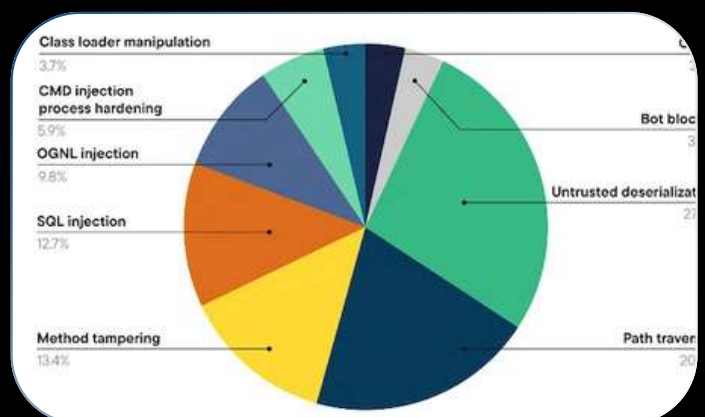
Las partes aburridas fueron las que causaron la mayoría de los problemas.

[ver artículo >>](#)

Las herramientas de IA para la seguridad de las aplicaciones coinciden en solo el 5% de los hallazgos de seguridad.

Las vulnerabilidades del software se convierten en exploits en cuestión de horas, y los equipos de seguridad de aplicaciones acumulan retrasos en la aplicación de parches que se remontan a años atrás.

[ver artículo >>](#)





NOTICIAS DE NUESTROS PARTNERS

Monitoreo sintético a gran escala con control de acceso granular y por equipos.

Ampliar la observabilidad suele generar desafíos en el control de acceso. La monitorización sintética no es una excepción. A medida que más equipos recurren a pruebas sintéticas para validar versiones, automatizar flujos de trabajo operativos y supervisar la disponibilidad de servicios web o de IA, más usuarios y sistemas automatizados necesitan la capacidad de crear y ejecutar monitores sintéticos.

[ver artículo >>](#)



Where you work	What you can do
Synthetic	Manage monitors and locations, view results, availability
Dashboards	Build availability and performance dashboards, Synthetic metrics
Notebooks	Run ad-hoc DQL queries over execution events, results
Workflows	Trigger on-demand executions, consume results, automated processes
Platform API	Full CRUD access with OAuth — the right tool for enterprise automation

Gobernanza de la IA empresarial: una guía práctica para controlar el riesgo de la IA.

La gobernanza de la IA empresarial debe aplicarse donde realmente se manifiesta el riesgo de la IA: en las aplicaciones, el acceso a los datos, las decisiones empresariales y las acciones autónomas. Este blog explica cómo las organizaciones pueden ir más allá de las políticas y establecer un control práctico sobre la IA.

[ver artículo >>](#)

IBM completa la adquisición de HRL Laboratories para acelerar el futuro de la computación cuántica.

Esta combinación aúna conocimientos complementarios en computación cuántica, sensores, ciencia de materiales y tecnologías avanzadas para acelerar la innovación futura.

[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](#)