RSM Newsletter

Julio 09 / 2025 – Distribución Gratuita

N° 81

¿Podría el Aumento de Escaneo de MOVEit Transfer Señalar Actividad de Amenaza Emergente?:

Un aumento en la actividad de escaneo dirigida a los sistemas MOVEit Transfer sugiere posibles amenazas emergentes.

La IA Gemini de Google accede a WhatsApp y más en Android:

La IA Gemini de Google ahora se lleva bien con aplicaciones de Android como WhatsApp,

¿Fueron Violadas 16 Mil Millones de Contraseñas? Se Cuestiona la Validez de la Afirmación:

Un informe de Cybernews sugirió una violación masiva de datos que involucraba 16 mil millones de contraseñas.

La Empresa de Tecnología Educativa PowerSchool Anuncia Violación de Datos:

PowerSchool, una empresa de tecnología educativa, informó sobre una violación de datos

Grok – Asistente de IA Actualizado en Google Play:

Grok, el asistente de IA de xAI, ahora está actualizado y listo para responder tus preguntas, generar imágenes y más.

RSM

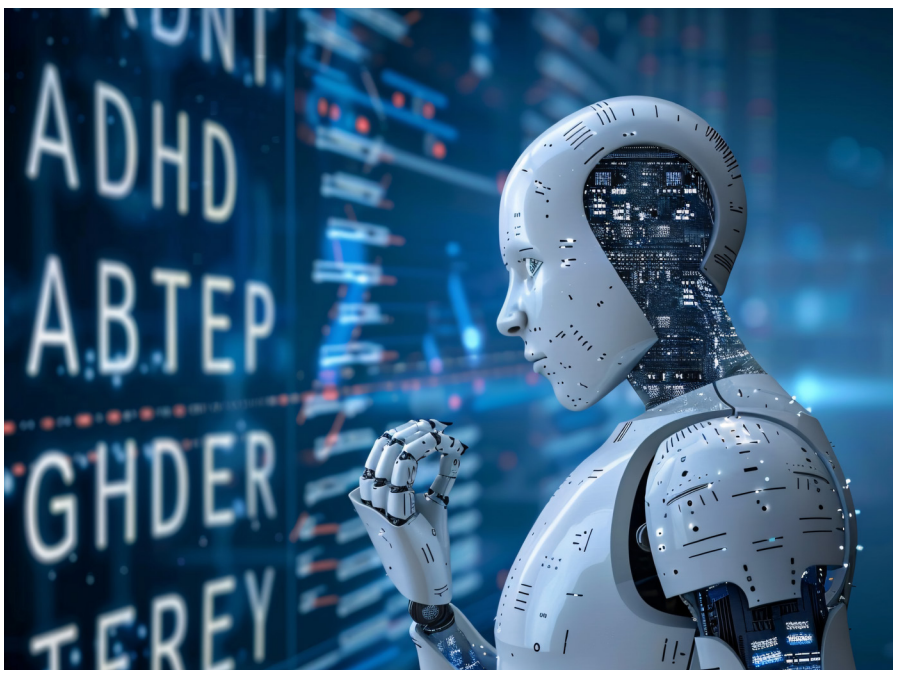
Zumbido Semanal de IA

¡Hola a todos! Estoy aquí una vez más para traerles lo último en noticias de IA. ¡Abróchense el cinturón, porque las noticias de IA de esta semana están más calientes que el reactor de arco de Tony Stark! ¡Vamos a sumergirnos de lleno!

Esta semana, tenemos un festín de acontecimientos de IA: desde el potencial caos del mercado con inversiones guiadas por IA hasta la llegada de la IA Gemini de Google a tus chats de WhatsApp. Mientras tanto, Crescendo está mejorando su experiencia al cliente con algunas nuevas y elegantes capacidades de IA, y Grok está causando sensación en Google Play. Además, si estás ansioso por construir tu propio agente de IA, tenemos algunas joyas de GitHub para ti. ¡Vamos a desglosarlo!

Avances

Crescendo amplía la plataforma CX con nuevas capacidades de IA Agente: La plataforma de experiencia al cliente de Crescendo ahora cuenta con IA Agente con una impresionante precisión del 99.8% en las respuestas. ¡Hablamos de un superhéroe del servicio al cliente! Leer más



Gigantes Tecnológicos Desatados

Grok – Asistente de IA Actualizado en Google Play: Grok, el asistente de IA de xAI, ahora está actualizado y listo para responder tus preguntas, generar imágenes y más. ¡Es como tener tu propio Jarvis personal, sin el sarcasmo! Leer más

La IA Gemini de Google accede a WhatsApp y más en Android: La IA Gemini de Google ahora se lleva bien con aplicaciones de Android como WhatsApp, pero las preocupaciones de privacidad están zumbando más fuerte que un enjambre de abejas. Leer más

Ética de la IA

Cuidado con el riesgo de mercado de la inversión guiada por IA ganando popularidad masiva: Las herramientas de inversión guiadas por IA están en auge, pero podrían ser el Loki del mundo financiero, causando caos y travesuras.
Leer más

Varios

10 Repositorios de GitHub para Dominar Agentes y MCPs: Sumérgete en el mundo de los agentes de IA con estos repositorios de GitHub, porque ¿quién no quiere ser el próximo Tony Stark de la IA? Leer más

INFORME SEMANAL DE

Noticias de Ciberseguridad

Bienvenido al informe de noticias de ciberseguridad de esta semana, donde profundizamos en los últimos desarrollos y tendencias emergentes en el panorama de la ciberseguridad. Como profesional en el campo, mantenerse informado sobre los últimos incidentes, amenazas e innovaciones es crucial para proteger a su organización contra posibles riesgos cibernéticos. Este informe proporciona una visión general completa de las noticias de ciberseguridad más significativas de la semana pasada, ofreciendo perspectivas y análisis para ayudarle a navegar por el siempre cambiante panorama de amenazas digitales.

Esta semana, exploramos una variedad de temas, incluyendo importantes violaciones de datos que afectan a grandes corporaciones, vulnerabilidades recién descubiertas que representan amenazas emergentes y asociaciones innovadoras destinadas a mejorar la infraestructura de ciberseguridad. Además, destacamos los desafíos continuos que enfrentan regiones como África en la construcción de capacidad de ciberseguridad y los últimos productos de infoseguridad diseñados para reforzar las medidas de seguridad. Manténgase informado y preparado mientras nos sumergimos en estas actualizaciones críticas.

Incidentes y Violaciones

La Empresa de Tecnología Educativa PowerSchool Anuncia Violación de Datos: PowerSchool, una empresa de tecnología educativa, informó sobre una violación de datos que involucró acceso no autorizado a su Sistema de Información Estudiantil. La violación, ocurrida a finales de 2024, potencialmente expuso información personal y de salud de los estudiantes, incluidos números de Seguro Social y registros académicos. [1]

¿Fueron Violadas 16 Mil Millones de Contraseñas? Se Cuestiona la Validez de la Afirmación: Un informe de Cybernews sugirió una violación masiva de datos que involucraba 16 mil millones de contraseñas. Sin embargo, los expertos han cuestionado la validez de estas afirmaciones, citando posibles inexactitudes en los datos y el análisis. Esto resalta la importancia de verificar tales afirmaciones sensacionalistas antes de sacar conclusiones. [1]

61 Millones de Registros Listados para la Venta en Línea, Supuestamente Pertenecen a Verizon: Investigadores descubrieron una publicación en un foro que ofrecía una base de datos que supuestamente contenía registros de 61 millones de clientes de Verizon. Los datos, que suman 3.1 GB, parecen legítimos, lo que genera preocupaciones sobre la seguridad de la información del cliente. [1]

Amenazas Emergentes

CISA Añade Una Vulnerabilidad Conocida Explotada al Catálogo: La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ha añadido una nueva vulnerabilidad, CVE-2025-6543, a su Catálogo de Vulnerabilidades Conocidas Explotadas. Esta vulnerabilidad afecta a Citrix Net y está siendo activamente explotada, subrayando la necesidad de vigilancia y aplicación de parches a tiempo. [1]

CLa más crítica es una falla de omisión de autenticación, destacando la necesidad de medidas de seguridad mejoradas en las redes de impresoras. [1]

¿Podría el Aumento de Escaneo de MOVEit Transfer Señalar Actividad de Amenaza Emergente?: Un aumento en la actividad de escaneo dirigida a los sistemas MOVEit Transfer sugiere posibles amenazas emergentes. El número de IPs únicas involucradas en el escaneo ha aumentado significativamente, indicando un interés creciente por parte de actores de amenazas. [1]

Vulnerabilidad en Cisco Unified CM Permite a Atacante Remoto Obtener Acceso de Root: Una vulnerabilidad crítica en Cisco Unified Communications Manager permite a atacantes remotos obtener acceso de root utilizando credenciales SSH codificadas. Esta falla, con un puntaje CVSS de 10.0, representa un riesgo significativo para los sistemas afectados. [1]

Ciberdelincuentes Usan Pantallas Falsas de Verificación de Cloudflare para Engañar a Usuarios a Ejecutar Malware: Una nueva técnica de ingeniería social involucra pantallas falsas de verificación de Cloudflare para engañar a los usuarios a ejecutar malware. Esto resalta la sofisticación en evolución de los ciberdelincuentes y la necesidad de vigilancia por parte de los usuarios. [1]

El Estado de la Ciberseguridad en APAC: Informe de CNC Intelligence Overwatch – Julio 2025: La región de Asia-Pacífico enfrenta amenazas cibernéticas en aumento, con violaciones significativas y aumentos de ransomware. Los esfuerzos para reforzar la ciberseguridad incluyen la expansión de la fuerza laboral y medidas legislativas, pero persisten los desafíos. [1]

Otras Noticias Relevantes

La crisis de ciberseguridad en África y el impulso para movilizar comunidades para salvaguardar un futuro digital: El rápido crecimiento digital de África se ve obstaculizado por desafíos de ciberseguridad, incluyendo una escasez de profesionales capacitados. Iniciativas basadas en la comunidad en países como Ruanda y Nigeria buscan mejorar la conciencia y capacitación en ciberseguridad, aprovechando la joven demografía del continente. [1]

LSU se asocia con CISA, DHS e INL para lanzar un modelo de ciberseguridad de infraestructura crítica: La Universidad Estatal de Luisiana se ha asociado con CISA, DHS y el Laboratorio Nacional de Idaho para desarrollar un modelo de ciberseguridad para infraestructura crítica. Esta iniciativa busca mejorar la ciberseguridad en el sector energético, posicionando a Luisiana como un centro de talento y tecnología cibernética. [1]

Nuevos productos de infoseguridad de la semana: 4 de julio de 2025: Los lanzamientos de productos de infoseguridad notables de esta semana incluyen KnowScam 2.0 de Scamnetic, Tracer Protect para ChatGPT de Tracer AI, las ofertas ampliadas de gestión de identidad de DigitalOcean y StealthMACsec de StealthCores para la seguridad Ethernet. [1]

Desglosando el Agotamiento: Sanando Equipos de Ciberseguridad con las Herramientas y Estrategias Correctas: Los equipos de ciberseguridad enfrentan altos niveles de agotamiento debido a cargas de trabajo aumentadas y falta de personal. Abordar estos problemas estructurales es crucial para mantener operaciones de seguridad efectivas y proteger entornos complejos. [1]

RSM Newsletter

En conclusión, este informe fue generado por un modelo de IA para proporcionarle una visión completa de las últimas noticias de ciberseguridad. Si bien nos esforzamos por la precisión, le animamos a verificar los hechos y mantenerse informado a través de múltiples fuentes. Manténgase vigilante y proactivo en la protección de sus activos digitales.

RSM CHILE

Cruz del sur 133
4th floor
Las Condes
Chile
T 56 2 3253 9050
rsmchile.cl