¡Bienvenidos al primer newsletter sobre tendencias tecnológicas e innovación en el mundo productivo!

Esta iniciativa conjunta del **Banco Macro** y **Trampoline Network** es una herramienta ofrecida a las empresas para que puedan conocer el futuro de los negocios en la Argentina, la región y el mundo y así impulsar su desarrollo.

En este tercer número abordaremos las tendencias de la implementación de Inteligencia Artificial en las empresas.

¿Qué es Trampoline Network?

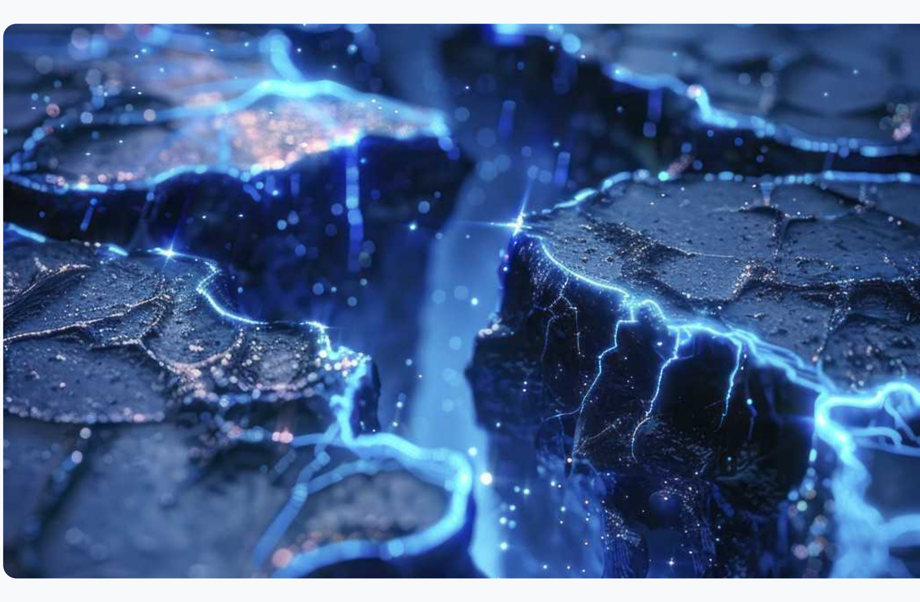
Trampoline Network es un marketplace de innovación, conocimiento y propiedad intelectual que funciona como una plataforma de vinculación entre las empresas y las universidades más relevantes de Latinoamérica.

Si estás buscando soluciones innovadoras para tu empresa, escribinos a info@trampoline.network *que un asesor te contactará.*

Desde Trampoline Network y gracias a un acuerdo firmado con la **Universidad Hebrea de Jerusalén** estamos potenciando start-ups israelíes innovadoras en diferentes sectores que están buscando ampliar sus mercados en Argentina.

ARTÍCULO

Principales amenazas de ciberseguridad en 2024



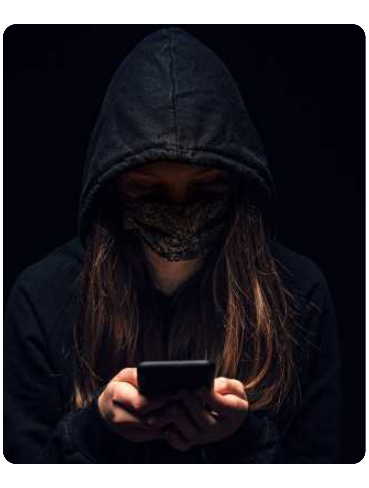
Al entrar en 2024, el panorama de la ciberseguridad sigue evolucionando, con nuevas amenazas emergiendo y otras más antiguas volviéndose más sofisticadas. Este año, una de las preocupaciones más urgentes es el **aumento de los ataques a la cadena de suministro y las vulnerabilidades de día cero**, ambas siendo explotadas por ciberdelincuentes altamente capacitados y actores estatales.

Además, los ciberataques impulsados por IA están en aumento, con atacantes que utilizan el aprendizaje automático para crear ataques de phishing más avanzados y malware que puede evadir las defensas tradicionales.

Principales amenazas a seguir en 2024

/ 01.

Ataques a la cadena de suministro

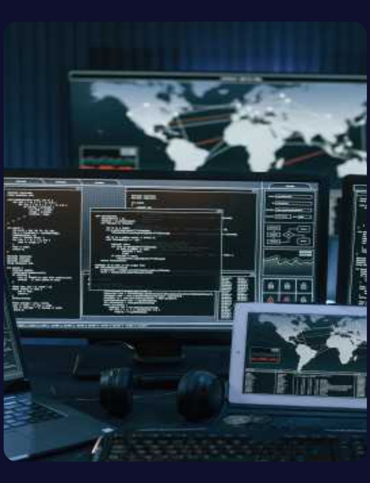


Los ciberdelincuentes están atacando cada vez más a proveedores y terceros para infiltrarse en organizaciones más grandes.

Este método de ataque indirecto puede eludir muchas medidas de seguridad tradicionales, lo que lo convierte en un área crítica de preocupación.

/ 02.

Ataques impulsados por IA

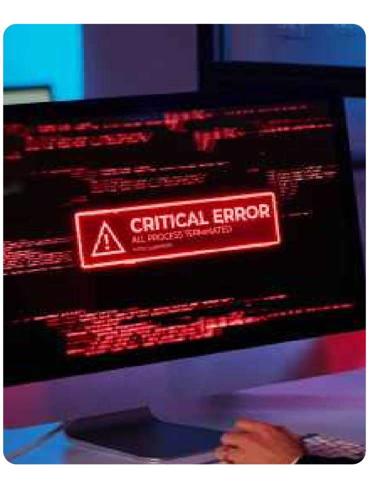


Los hackers están aprovechando la inteligencia artificial para elaborar esquemas de phishing sofisticados, desarrollar malware indetectable y automatizar ataques.

Esta tecnología les brinda herramientas que superan las defensas estándar.

/ 03.

Exploits de día cero

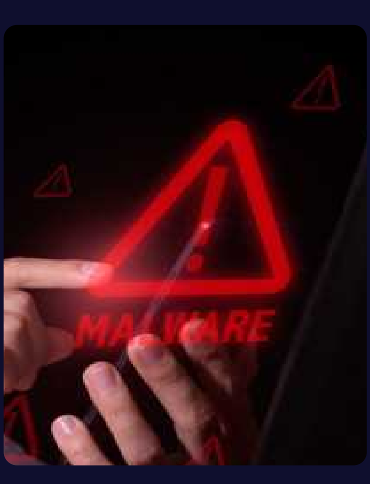


Las vulnerabilidades en software ampliamente utilizado están siendo descubiertas y explotadas más rápido que nunca.

Las empresas luchan por corregir estas vulnerabilidades antes de que se conviertan en puntos de entrada para los ciberdelincuentes.

/ 04.

Ataques a la capa de aplicación



Las aplicaciones web y móviles son objetivos principales para los atacantes, quienes explotan vulnerabilidades para acceder a datos sensibles o lanzar ataques de denegación de servicio distribuido (DDoS).

¿Cómo Palantir Security puede ayudar?

En **Palantir Security Cyber Services**, proporcionamos soluciones de vanguardia para proteger su empresa de estas amenazas emergentes.

Nuestra gama integral de servicios asegura que su compañía esté un paso adelante de los ciberdelincuentes.

Servicios que proporcionamos

Inteligencia de amenazas cibernéticas

Nuestro equipo monitorea continuamente el panorama de amenazas, reuniendo inteligencia procesable para identificar y prevenir ataques antes de que ocurran.

Al aprovechar fuentes de datos globales y análisis en tiempo real, lo ayudamos a mantenerse proactivo ante amenazas emergentes.

Pruebas de seguridad de aplicaciones

Realizamos evaluaciones de seguridad exhaustivas para aplicaciones web y móviles, identificando vulnerabilidades antes de que puedan ser explotadas.

Nuestro proceso de pruebas asegura que sus aplicaciones se mantengan seguras, cumplan con las normativas y sean resistentes ante los ataques.

Al asociarse con **Palantir Security**, obtiene acceso a una detección avanzada de amenazas y estrategias de defensa proactivas adaptadas a las necesidades de su organización. No espere a que ocurra una brecha: fortalezca su postura de seguridad ahora con Palantir Security Cyber Services.

El autor de este artículo es **Palantir Security.** Por cualquier consulta adicional, pueden enviar un mail a la siguiente casilla: eladf@palantirsecurity.com ó a info@trampoline.network

¡Accedé a nuestro formulario de contacto!