LITORALPRESS

Fecha: 06-05-2025
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: **“Juntos podemos ayudar a las organizaciones a reducir su ciber exposición de forma proactiva”**

Pág. : 38
Cm2: 487,7

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

> VISIONES DE MARCA

Mario Benedetti, Tenable Chile

“Juntos podemos ayudar a las organizaciones a reducir su ciber exposición de forma proactiva”

En medio de un panorama de amenazas y riesgos inédito en la historia, Tenable entrega un mensaje consistente: confiar en defensas reactivas ya no basta. Es imprescindible evolucionar hacia estrategias proactivas de ciber exposición. En estas Visiones de Marca, Mario Benedetti, Gerente de Territorio de Tenable Chile, comparte la estrategia de la marca para el mercado de distribución y su apuesta por un canal capaz de acompañar a los clientes en el camino de la ciberseguridad proactiva.

¿La IA es un factor que marcará el futuro de las estrategias de ciberseguridad de las empresas?

La inteligencia artificial se ha convertido en una oportunidad de innovación tan grande como en un vector de riesgo que está cambiando la ciberseguridad. Estamos viendo un incremento del uso de IA sin precedentes: tras años de pocos cambios, la penetración global de la IA pasó del 20% en 2017 al 72% en 2024, y el uso de IA generativa subió del 33% al 65% entre 2023 y 2024 (Encuesta mundial de McKinsey sobre IA). Pero la nube e IA juntas también crean riesgos cibernéticos inéditos. En el uso de IA en la nube no está en juego solo la protección de datos sensibles: componentes de IA suelen contener propiedad intelectual, algoritmos propietarios y PII, lo que los vuelve objetivos de alto valor.

Hay nuevos riesgos, como se advierte en un reciente informe de Tenable...

Efectivamente. Nuestro informe de Tenable Cloud Research revela que más de dos tercios de las cargas de trabajo con paquetes de IA instalados contienen al menos una vulnerabilidad crítica, y que, en el 30% de esos entornos, se halló la vulnerabilidad capaz de facilitar accesos no autorizados. Otro nuevo riesgo es el “concepto Jenga”, introducido por Tenable Cloud Research, que describe la tendencia de los proveedores de nube a construir un servicio sobre otro, como si fueran bloques de Jenga. Basta con un servicio mal configurado para poner en riesgo toda la estructura: una sola pieza débil puede comprometerlo todo. El informe revela cómo 8 de cada 10 organizaciones mantienen la cuenta de servicio predeterminada de Compute Engine (con privilegios excesivos) en Google Vertex AI Notebooks, lo que pone en riesgo todos los servicios que dependen de ella.

¿Qué se hace ante este panorama?

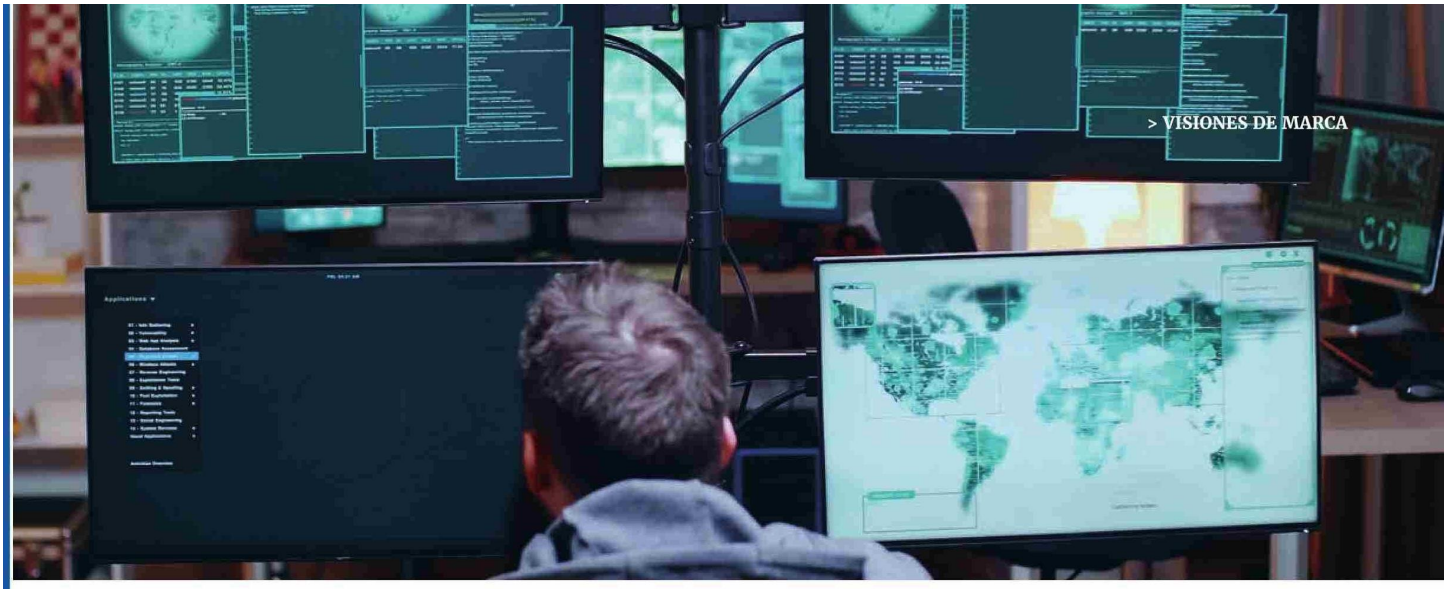
Lo primero que hay que señalar es que confiar en defensas reactivas, ya no basta. Es imprescindible evolucionar hacia estrategias proactivas de ciber exposición, basadas en visibilidad continua de cargas de trabajo, escaneo y remediación automatizada de vulnerabilidades, validación de modelos en “shift-left” y gobernanza colaborativa.

LITORALPRESS

Fecha: 06-05-2025
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: “Juntos podemos ayudar a las organizaciones a reducir su ciber exposición de forma proactiva”

Pág. : 39
Cm2: 463,1

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida



Solo así las empresas podrán aprovechar el potencial transformador de la IA sin convertirse en víctimas de sus propias innovaciones.

¿Con qué herramientas cuenta el Canal para afrontar los desafíos de seguridad en la nube?

Para ello, nuestros partners cuentan con Tenable Cloud Security, una solución que brinda a las organizaciones la capacidad de adaptarse a la velocidad de la innovación sin renunciar al control. Gracias a su análisis automatizado de riesgo contextual y su cobertura nativa de servicios de nube pública (AWS, Azure, GCP, ICU), Tenable Cloud Security ayuda a priorizar esfuerzos y a aplicar el principio de menor privilegio a escala, detectando configuraciones erróneas, identidades con permisos excesivos y puntos ciegos en entornos híbridos y multinube.

¿Y fuera de la nube?

Por supuesto que la protección no se limita al perímetro de nube. Con la cartera completa de Tenable, los clientes pueden defenderse de incidentes que se originan en la infraestructura de TI tradicional, en cargas de trabajo de IA y hasta en entornos de tecnología operativa (OT). Nuestra plataforma unificada Tenable One, integra visibilidad, conocimiento y acción en toda la superficie de ataque.

¿Preparan a sus canales para esta etapa de explosión de amenazas?

Frente al panorama actual de ciberseguridad, marcado por la adopción masiva de IA, la explosión de datos distribuidos y el avance de tecnologías como edge computing y, a futuro, la computación cuántica, las organizaciones deberán implementar IA a escala sin dejar de proteger sus activos; al mismo tiempo, el crecimiento de entornos multinube y los ataques cada vez más impulsados por IA, elevarán la complejidad de la defensa.

Más de dos tercios de las cargas de trabajo con paquetes de IA instalados contienen al menos una vulnerabilidad crítica, y en el 30% de esos entornos, se halló la vulnerabilidad capaz de facilitar accesos no autorizados.

Las organizaciones necesitan hoy -más que nunca- canales que entiendan cómo las organizaciones en Chile pueden anticipar vulnerabilidades críticas, gestionar, medir y reducir su riesgo cibernético.

Esta tecnología, ¿cómo se complementa con la estrategia de canales de Tenable?

Nuestra estrategia se seguirá enfocando en nuestros partners como foco central. Seguiremos trabajando mano a mano con socios de negocio y clientes en toda América Latina, entendiendo sus puntos de dolor y ofreciéndoles las soluciones más efectivas para sus necesidades de ciberseguridad. Creemos que la verdadera diferenciación de un buen canal no proviene de vender un producto, sino de adoptar un enfoque empático y colaborativo: escuchamos los retos locales, compartimos nuestra experiencia global y ajustamos conjuntamente las mejores prácticas de gestión de exposición.

¿Cómo está conformado el ecosistema de canales de Tenable en Chile?

En Chile, colaboramos con un ecosistema que combina distribuidores mayoristas (encargados de logística y facturación local), resellers especializados en seguridad de red y nube, MSSPs que integran nuestras soluciones en servicios gestionados de vulnerabilidades y SOC, y consultoras de integración que acompañan implementaciones avanzadas en sectores como finanzas, energía y Gobierno. Este tejido de partners permite cubrir desde proyectos puntuales de evaluación de riesgo hasta programas globales de exposición continua.

¿Tienen un programa de canales activo?

Sí. El programa Tenable Assure Partner Program está plenamente operativo en toda la región LATAM, con más de 60 empresas certificadas solo en Chile. Nuestro equipo regional tiene como objetivo acompañar a cada socio en preventa, implementación y postventa para asegurar que, juntos, podamos ayudar a las organizaciones a reducir su Cyber Exposure de forma proactiva. ChN