Tanium señala que combinando datos en tiempo real e IA es posible detectar amenazas cibernéticas y remediarlas de inmediato

Ciudad de México. 4 de febrero de 2025.- Tanium, proveedor líder de la industria de administración convergente de endpoints (XEM), señala que en cuanto más se adopten dispositivos, software y sistemas adicionales, más podrá la automatización mejorar y aplicar de manera consistente las políticas de seguridad en entornos grandes, al mismo tiempo que identifica patrones para crear una defensa mejor y más proactiva, lo cual la hará esencial para los equipos de ciberseguridad en los próximos años.

Desde la óptica de la empresa, la Inteligencia Artificial (IA) lleva las capacidades de automatización a un nuevo nivel. La combinación de ambos permite a las organizaciones manejar tareas repetitivas y cotidianas para que los expertos humanos en ciberseguridad puedan concentrarse en el trabajo de alto impacto. Junto con los datos en tiempo real sobre el entorno operativo de una organización tal como se ve actualmente, la IA y la automatización pueden detectar amenazas y remediar problemas de manera más rápida y eficiente que hasta hace poco tiempo todavía.

Las empresas que planean implementar la automatización en sus prácticas de ciberseguridad, deben considerar factores sensibles de esta tecnología; especialmente en lo que respecta a la identidad y la autenticación. También, deberán introducir mecanismos de gobernanza sólidos y bucles de retroalimentación transparentes para que los equipos de seguridad puedan monitorear lo que realmente están haciendo la IA y la automatización en conjunto y ajustar las políticas de acuerdo a las necesidades.

“Estamos combinando nuestra capacidad de proporcionar datos en tiempo real sobre el entorno operativo de una organización con IA que puede mostrar información crítica sobre amenazas y vulnerabilidades ciberneticas reales a medida que ocurren y los pasos para remediarlas. Nuestro objetivo es canalizar las tareas rutinarias a la automatización y dejar que la IA se encargue de la detección de amenazas para que los equipos de ciberseguridad puedan concentrarse en ejecutar la remediación más rápido y que su confianza en el producto les permita concentrarse en el trabajo crítico para el negocio”, senaló Harman Kaur, vicepresidenta de Inteligencia Artificial en Tanium.

Para Tanium, la IA ayuda a mejorar la productividad y hacer las cosas más rápido, no obstante, las organizaciones quieren asegurarse de que pueden confiar en los resultados y esos resultados deben ser procesables. Los datos en tiempo real son una herramienta de validación increíble y un facilitador de la acción. Poder encontrar problemas después de que ocurren y usar esa información para garantizar que no vuelvan a suceder es útil, pero poder encontrar problemas a medida que ocurren y remediarlos en tiempo real con el contexto de su entorno operativo real tal como se observa actualmente, es un superpoder y el futuro de la ciberseguridad.

La empresa informó que durante 2025 continuará invirtiendo e investigando en una mejor automatización ya que busca superar los límites y hacer que ésta sea un multiplicador de fuerza aún mayor de lo que ya es en la actualidad. Asimismo, se priorizará la visibilidad en la ciberseguridad proactiva ya que el objetivo es entregar al cliente visibilidad de las cosas antes de que se presente un problema. Lo anterior, junto con el uso fluido de datos para una mejor toma de decisiones. El objetivo es brindar recomendaciones prácticas que las organizaciones puedan implementar antes de que se vean afectadas por la próxima gran vulnerabilidad.

“Para 2025, la IA en ciberseguridad pasará rápidamente de los chatbots a un enfoque más impulsado por agentes. Si bien los chatbots ofrecen valor, los agentes representan un cambio de paradigma. Las organizaciones que aprovechen la automatización utilizarán agentes para la detección de amenazas y respuestas autónomas. Además, los agentes mejorarán la escalabilidad de los recursos de TI así como la higiene cibernética”, finalizó Kaur.