Ciberseguridad a prueba: los desafíos que vienen para los SOCs en 2024

Los Centros de Operaciones de Seguridad, mejor conocidos como SOCs en la industria TI, son unidades clave para las empresas desde hace varios años. Ahora su rol se vuelve todavía más importante, en un escenario de amenazas crecientes y cada vez más sofisticadas.

Los ataques de ransomware operados por humanos tuvieron un incremento de casi 200% en 2023, según el más reciente Digital Defense Report de Microsoft, y se espera que este año la tendencia siga al alza. El aumento de la superficie de ataque no es el único tema desafiante para las empresas. La complejidad con la que se presentan estos ataques es cada vez más insólita y, ante eso, las posturas de seguridad tradicionales ya no son suficientes y el rol de los Centros De Operaciones de Seguridad, conocidos como SOCs, se vuelve más relevante.

Nicolás Corrado, socio líder de Cyber Risk en Deloitte, considera que en 2024 los SOCs enfrentarán desafíos muy relevantes como el aumento de ataques a cadenas de suministro y dispositivos IoT. Esto requerirá, entre otras cosas, un enfoque de seguridad de Zero Trust. Asimismo, la gestión de la creciente complejidad y el volumen de amenazas cibernéticas será fundamental para las organizaciones, advirtiendo que los SOCs 'deberán alinearse más estrechamente con las estrategias empresariales y participar en la toma de decisiones a nivel ejecutivo'.

'Los equipos más tradicionales de TI simplemente no pueden seguir el ritmo. Por ello, los SOCs se han convertido en una pieza fundamental de la seguridad digital de las organizaciones, pues permiten una visibilidad completa sobre el estado de todos los activos de la organización, tienen una mirada experta e informada sobre las amenazas y una capacidad para llevar a cabo una detección temprana de potenciales incidentes de ciberseguridad', explica Marcelo Felman, director de Ciberseguridad de Microsoft para Latinoamérica, y agrega que estas unidades también desempeñan un papel crucial en la implementación de estrategias preventivas.

Su importancia al interior de las empresas viene creciendo con los años. En 2022, un análisis de Kaspersky reveló que los ciberincidentes contra empresas hechos por humanos habían aumentado un 50%, y los analistas de los SOCs fueron quienes lo detectaron.

Eduardo Chavarro, especialista en Respuesta a Incidentes de esa firma de ciberseguridad, explica que cuando en la industria hablan de 'ciberincidentes hechos por humanos' se trata de ataques manuales donde el atacante realiza la infección, o una parte de ella, con sus propias manos. 'La consecuencia directa de esto es que el delincuente evitará las detecciones automatizadas de las soluciones de seguridad; y por ende, la detección de incidentes provocados por humanos se llevará a cabo mediante análisis humanos o mediante el uso de Threat Intelligence. Este análisis humano es hecho por los equipos de SOCs. Es una batalla de ocultarse versus enfocarse en cada detalle', dice.

El aporte de La IA generativa

Aunque no es una novedad en el segmento de ciberseguridad, la IA generativa, o GenIA, seguirá siendo de gran valor en el 2024, coinciden los expertos.

'Cada vez generamos más información y la identificación de amenazas, fugas o acciones sospechosas será cada vez más difícil y hasta imposible sin la IA', asegura Corrado, socio de Deloitte, mientras destaca que una mayor integración de capacidades avanzadas en torno a esta tecnología y al aprendizaje automático van a marcar la diferencia.

El socio de Deloitte añade que ahora la GenIA empezará a tener un uso que permita a los analistas de ciberseguridad hacer búsquedas, correlaciones y hasta informes 'sin necesidad de conocer técnicamente las sentencias a ejecutar, cómo correlacionar en un SIEM, o incluso cómo configurar un orquestador'. Esto se traduce, a su juicio, en una menor fatiga para los analistas, mayor concentración y foco en el monitoreo de amenazas y análisis forenses 'más profundos'. Asimismo, el ejecutivo de Kaspersky subraya que la suma de la GenIA y el análisis experto permite entregar resultados 'más oportunos y eficientes', que ayuden a las organizaciones a tomar decisiones y contener ataques en etapas tempranas, disminuyendo al máximo los falsos positivos en la detección de amenazas.

Pero no solo seguirá abriendo oportunidades. 'Cualquier tecnología es a la vez una herramienta y una potencial arma', enfatiza el ejecutivo de Microsoft, subrayando que la ciberdelincuencia también tiene acceso a tecnologías de punta como la IA para la creación, sofisticación y operación de sus actividades criminales.

Sobre la base de los resultados del Digital Defense Report de Microsoft, dice que la humanidad está entrando 'en una era de proliferación' para la creación y manipulación de medios basados en IA que permiten refinar los mensajes de phishing, mejorar la creación de materiales falsos y perfeccionar ataques de ingeniería social, en un escenario donde en 2023 había 29.300 millones de dispositivos conectados a Internet, emitiendo y recibiendo información, acota, citando un informe reciente de Cisco.

El socio de Deloitte coincide y dice que mientras la GenIA seguirá siendo una aliada para los SOCs, estos también deben ser muy conscientes de que los ciberdelincuentes pueden aprovecharla para llevar a cabo ataques más sofisticados y convincentes. 'Las empresas deben estar preparadas para las implicaciones normativas y éticas de su uso', concluye.

Nicolás Corrado
Socio Líder Cyber Risk
nicorrado@deloitte.com