4 Formas en las que Microsoft Sentinel aborda las principales inquietudes de seguridad de TI

Maximice los beneficios y las capacidades de su inversión en seguridad.

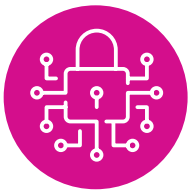
Insight

Microsoft

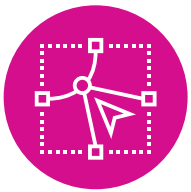
Sondeando el panorama de amenazas

Encontrar la combinación adecuada de herramientas, tecnologías y conjuntos de habilidades es fundamental para dirigir un Centro de operaciones de seguridad (COS) con éxito. Esto es especialmente cierto a raíz del rápido aumento del volumen de ciberataques que se han producido últimamente. Ahora, tenga en cuenta que el coste medio de una violación de seguridad causada por ransomware en 2021 fue de unos increíbles 4,62 millones de dólares.[1] Eso son muchos daños potenciales. Por lo tanto, no es de extrañar que se presione a los equipos de seguridad de TI de todo el mundo para mejorar el tiempo de respuesta y evitar pérdidas futuras.

Para combatir esta tendencia en crecimiento, se espera que las empresas gasten de media 24,4 millones de dólares en su presupuesto de seguridad de TI en 2022.[2] Aquellas que quieran alojar datos on-premise y en la nube tendrán que reevaluar sus soluciones existentes para garantizar una cobertura completa en todas las ubicaciones operativas, oficinas domésticas, sistemas de comunicación y cualquier otro lugar entremedias.

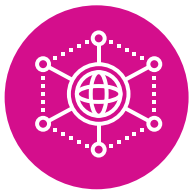


El aumento en el número de endpoints y de los volúmenes de datos exige una seguridad escalable.



Las soluciones puntuales ofrecen un alcance limitado y retos de integración adicionales.

Encontrar y retener talentos clave en el campo de la seguridad se ha vuelto más difícil.



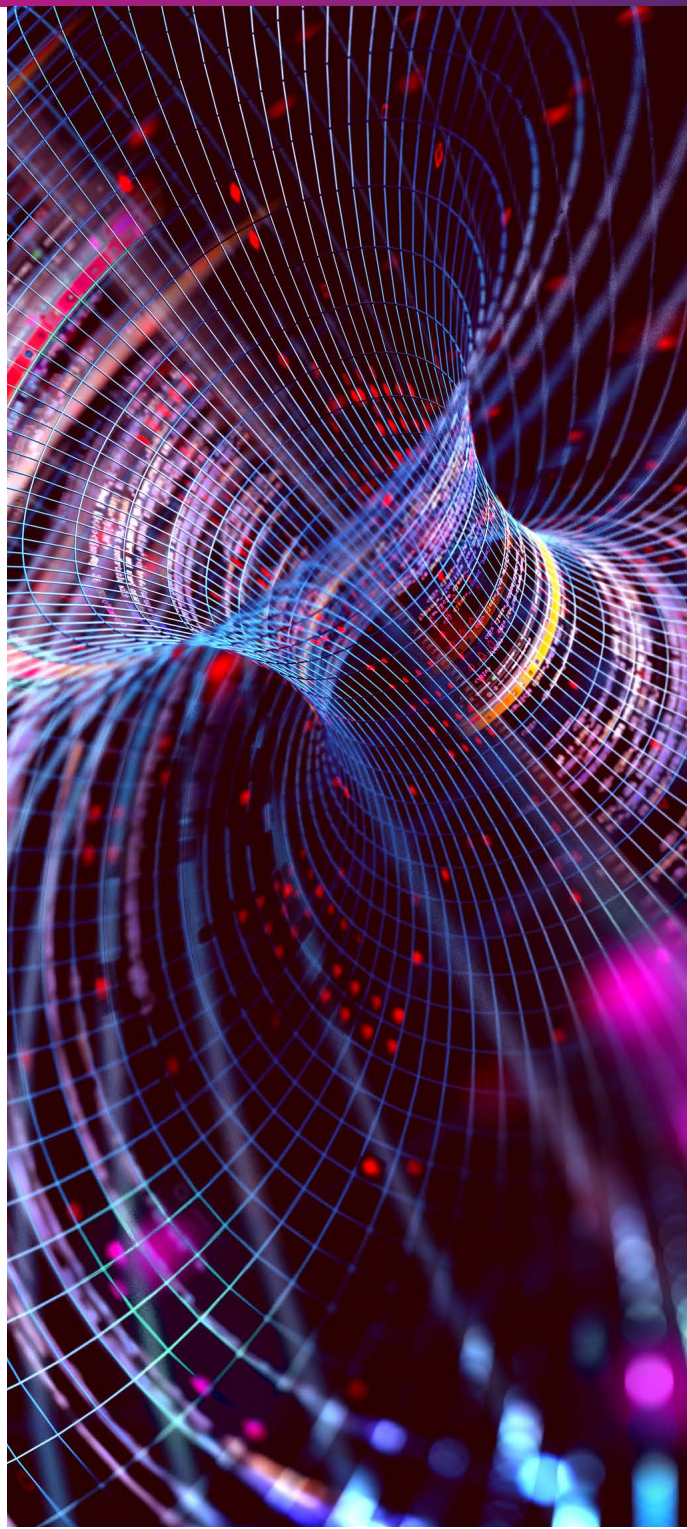
La complejidad de los entornos de TI está aumentando con innumerables vectores de ataques.

Piense en sus datos, usuarios y sistemas.

Tener una visión completa es fundamental para detectar y frustrar posibles daños, así como para poder explotar múltiples sistemas desde un único punto de partida y obtener el control de todo el entorno de TI. Las empresas tardan una media de 280 días en detectar una violación, lo cual supone que una cantidad innumerable de datos, registros y sistemas pueden verse comprometidos antes de que se tomen medidas para combatir la intrusión. Una forma de mejorar la visibilidad y reducir este obstáculo es implementar la gestión de identidades y acceso. Poder realizar un seguimiento de las tendencias de comportamiento de los usuarios para descubrir patrones puede ayudar a las empresas a acotar el plazo de tiempo para aplicar remedios y abordar las brechas que anteriormente no se habían observado.

Al implementar la gestión de identidades y acceso, considere hacer las siguientes preguntas:

- ¿Qué tan sensibles son sus datos?
- ¿Quién realmente necesita acceder a archivos específicos?
- ¿Cuándo y durante cuánto tiempo se necesita acceso?
- ¿Necesita iniciar un programa de clasificación de datos?
- ¿Ha establecido tipos de usuarios?
- ¿Cuándo fue la última vez que revisó los permisos?
- ¿Cómo verifica las identidades y los puntos de acceso?
- ¿Qué alternativas a la autenticación ha considerado?
- ¿La biometría sería una opción que valdría la pena?
- ¿Ha notado alguna brecha o patrón evidente?
- ¿Cómo podría hacer la transición de su enfoque actual a uno más seguro?



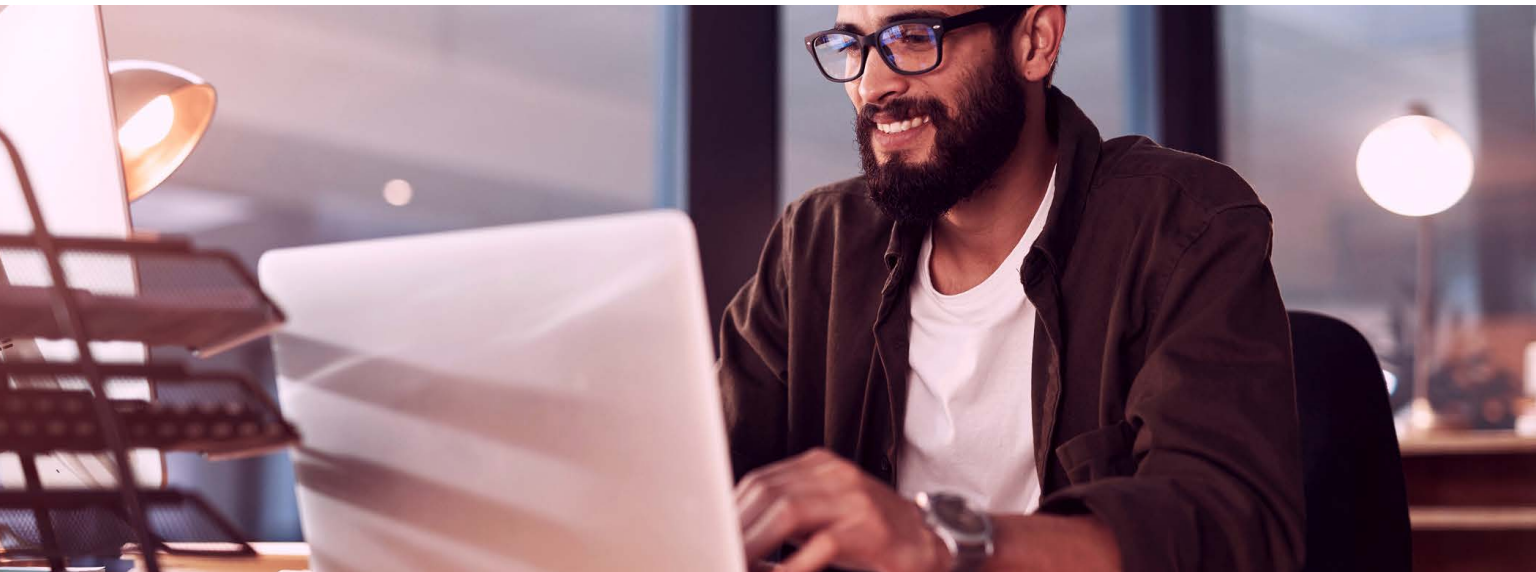
Las bases de un programa de seguridad moderno

Puede ser útil tener en cuenta que el 89 % de las empresas ya han adoptado, o están planeando adoptar, un enfoque multinube.[4] Si su negocio forma parte de esta mayoría, puede tener un entorno de TI diverso a mano. Poder realizar con éxito un seguimiento de los datos, de los hackers maliciosos y de otros aspectos, mejorará la eficacia de los esfuerzos preventivos realizados por su equipo de seguridad de TI. Otra característica clave de un programa sólido es la gobernanza integral que aborda la posesión y la responsabilidad. Al definir los objetivos, roles y procesos de seguridad, las empresas pueden organizar mejor las directrices y la formación, así como validar usuarios y procesos.

Otra consideración a tener en cuenta es que el 57% de las empresas encuestadas en el informe "El estado de la modernización de TI 2020" dijeron que actualizar la infraestructura y los procesos de seguridad era uno de los principales obstáculos en su recorrido para modernizar sus entornos operativos de TI.[3] Aquí es donde un partner externo puede proporcionar valor añadido a través de servicios de automatización.

La automatización dentro del COS ofrece:

- Capacidades de detección, respuesta y corrección más rápidas
- Menos errores y menor "fatiga por alertas"
- Recursos de seguridad liberados de tareas repetitivas
- Mejora de la experiencia y satisfacción del usuario



Invertir en una solución SIEM nativa de la nube

Microsoft Sentinel es una solución de gestión de eventos e información de seguridad (SIEM) y de orquestación, automatización y respuesta de seguridad (SOAR) nativa de la nube que se proporciona como un servicio en la nube. Al aprovechar su capacidad para proporcionar análisis de seguridad inteligentes para todo el entorno, las empresas pueden detener las amenazas antes de que causen daños. Como solución escalable y perenne, Microsoft Sentinel mejorará o reemplazará sus herramientas de seguridad existentes para aumentar la visibilidad de su panorama de amenazas.

- Obtenga una vista completa de su negocio.
- Mejore la detección y la respuesta con inteligencia artificial (IA).
- Elimine la configuración y el mantenimiento de la infraestructura de seguridad.
- Escale para satisfacer las siempre en evolución necesidades de seguridad.

Como ventaja adicional, esta solución reduce los costes hasta un 48% y se implementa un 67% más rápido que los SIEM tradicionales.[5] Como resultado, las empresas pueden dedicar más tiempo a encontrar amenazas reales rápidamente cultivando operaciones de seguridad más estratégicas. ¿Cómo funciona exactamente? ¿Cómo utiliza la IA y el aprendizaje automático para detectar, analizar e investigar amenazas? Profundizaremos en el proceso de cuatro pasos en la página siguiente.

4 pasos para las operaciones de seguridad de última generación

1. Recopilar

Hoy en día, las empresas alojan documentos, datos, registros y mucho más en una multitud de dispositivos, aplicaciones e infraestructura, tanto on-premise como en múltiples nubes. Además, los usuarios acceden a todos estos archivos confidenciales prácticamente en cualquier momento y desde cualquier lugar. Microsoft Sentinel recopila datos a escala de la nube, agregando dispositivos de infraestructura y seguridad como firewalls.

2. Detectar

Encontrar incidencias regulares y patrones de ciberataques puede ayudar a las empresas a protegerse de las amenazas. El análisis y la incomparable inteligencia frente a amenazas ayudan a las empresas incluso a descubrir amenazas que antes eran indetectables y a minimizar las posibilidades de falsos positivos. Imagine poder supervisar y correlacionar millones de anomalías a la vez y luego obtener valor rápidamente del informe. Eso es lo que ofrece esta solución.

3. Investigar

Aprovechando décadas de trabajo en ciberseguridad en Microsoft, Microsoft Sentinel busca actividades sospechosas a escala siguiendo instrucciones de la IA, eliminando la necesidad de hardware o máquinas virtuales. Aprende a eliminar el ruido gracias a los registros diarios, para que los equipos de seguridad puedan centrarse en las señales esenciales.

4. Responder

Con la orquestación incorporada y la automatización de tareas comunes, las empresas pueden responder a los incidentes rápidamente. Al aprovechar la tecnología inteligente, su equipo de seguridad de TI no solo ahorrará tiempo, sino que también mejorará la precisión. Por ejemplo, los cuadernos de estrategias activados por reglas de análisis o automatización se pueden ejecutar dentro de Microsoft Sentinel para mejorar el tiempo de respuesta y bloquear a los actores maliciosos.

¿Por qué Insight para Microsoft Sentinel?

En Insight, creemos que nunca ha habido un mejor momento para perfeccionar su postura de seguridad, especialmente con el aumento del trabajo remoto e híbrido. Confíe en nuestros años de experiencia para proteger a su empresa contra las amenazas cibernéticas en evolución. Juntos, ayudaremos a su empresa a obtener una solución flexible y escalable que aproveche las capacidades de la IA y del aprendizaje automático de vanguardia. El objetivo: mejorar la seguridad, la visibilidad y el control de todo su entorno de TI.

Somos uno de los principales partners de Microsoft y uno de los únicos 12 partners mencionados públicamente por Microsoft para ofrecer consultoría y servicios Microsoft Sentinel:

- 18 competencias Gold y Silver de Microsoft
- Más de 25 años como partner de Microsoft
- Más de 1.000 ingenieros y profesionales de servicio centrados en Azure
- Un proveedor de servicios gestionados (MSP) experto de Azure y el mayor partner de Azure
- Ganador del premio Microsoft Security 20/20 en la categoría de Partner de Implementación de Seguridad Azure del Año
- Soporte en todo momento y prestación de servicios de consultoría

Acerca de Insight

Insight Enterprises, Inc. es un integrador de soluciones de Fortune 500 con 11.500 compañeros en todo el mundo que ayuda a las organizaciones a acelerar su viaje digital para modernizar su negocio y maximizar el valor de la tecnología. Hacemos posible una transformación segura de extremo a extremo y satisfacemos las necesidades de nuestros clientes a través de una cartera integral de soluciones, asociaciones de gran alcance y más de 33 años de amplia experiencia en TI. Calificados como el mejor empleador del mundo por Forbes y certificados como un excelente lugar para trabajar, amplificamos nuestras soluciones y servicios con escala global, experiencia local y una experiencia de comercio electrónico de clase mundial, haciendo realidad las ambiciones digitales de nuestros clientes en cada oportunidad.

Insight®

es.insight.com

Fuentes:

[1] IBM Security. (2021). Coste de un informe de violación de la seguridad de los datos.

[2] Channel Futures. (febrero de 2022). El alto coste del ransomware.

[3] Insight. El estado de la modernización de TI 2020.

[4] Flexera. (marzo de 2022). Informe sobre el estado de la nube 2022.

[5] Forrester. (noviembre de 2020). El Impacto Económico Total™ de Microsoft Sentinel. Ahorro de costes. y beneficios empresariales facilitados por Microsoft Sentinel.

MKT6231