Cómo afrontar los retos clave de los entornos de seguridad de múltiples proveedores

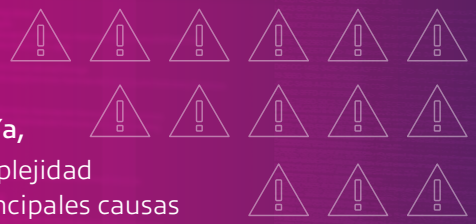
Una guía para superar el agotamiento en el área de seguridad y reforzar sus defensas con Insight y Microsoft Sentinel

La Seguridad bajo tensión

de los encuestados en la Encuesta Comparativa CISO 2020 de Cisco afirman que están sufriendo fatiga por ciberseguridad (que se define como prácticamente renunciar a la defensa proactiva contra actores maliciosos).

De los que la sufren, el **93 % recibe más de**

5.000 **alertas cada día,**



lo que indica que la complejidad parece ser una de las principales causas de agotamiento en el área de seguridad.[1]

Para gestionar un entorno de amenazas complejo, la mayoría de las organizaciones aprovechan varias soluciones de seguridad. Pero gestionar y organizar alertas de varias fuentes dispares no solo es un reto, sino que también expone a las empresas a más riesgos.

Una sobreabundancia de alertas significa que puede haber demasiadas para abordar, lo que afecta a la concienciación y visibilidad del equipo y, potencialmente, expone al negocio a amenazas más grandes y perjudiciales en el futuro.

Según Fady Younes, director de ciberseguridad de Cisco, "No integrar varias soluciones de seguridad también puede dejar brechas en la cobertura o crear una situación en la que el equipo de TI no comprenda correctamente qué protección proporciona una solución en particular o cómo funciona, lo que afecta a la visibilidad y la concienciación sobre el verdadero estado de seguridad de la red".[2]

Saber qué riesgos y alertas priorizar se vuelve menos claro en estos entornos.

No todas las alertas tienen la misma gravedad, y las mejores estrategias de seguridad personalizan los controles de seguridad y asignan recursos según el nivel de riesgo.

En entornos diversos y multinube, la recuperación ante desastres se vuelve increíblemente compleja, lo que requiere una cultura de seguridad proactiva en lugar de reactiva.

"Abordar las incidencias de integración y un gran volumen de alertas de seguridad puede distraer a los ingenieros de seguridad de abordar otros desafíos a los que se enfrentan..."

— **Fady Younes, director de ciberseguridad para Oriente Medio y África en Cisco**

SIEM y SOAR

Los equipos de seguridad tienen dos objetivos principales: saber qué está pasando en sus entornos de TI y responder a esa información. Las soluciones de gestión de eventos e información de seguridad (SIEM) y de orquestación, automatización y respuesta de seguridad (SOAR) existen para ayudar a lograr estos objetivos.

Las herramientas SIEM recopilan y agregan datos de eventos de diversas fuentes dentro de un entorno de TI, luego analizan y clasifican los eventos en orden de prioridad o criticidad. Los equipos de seguridad asumen la responsabilidad de la búsqueda y respuesta a amenazas, así como el ajuste y la corrección de la plataforma SIEM.

Las herramientas SOAR proporcionan análisis y automatización avanzados que se basan en las capacidades de las herramientas SIEM, para una respuesta a amenazas más autónoma. Las herramientas SOAR aprovechan tantos datos en tiempo real como sea posible y son sensibles a la habilidad de los gerentes; estas herramientas son más o menos eficaces en función de cómo se utilizan.

dicen que SOAR es muy o extremadamente importante para la postura de seguridad general de su organización.

Casos de uso clave para SOAR:

- 65% Clasificación SIEM
- 62% Ataques de phishing
- 62% Inteligencia sobre amenazas

Resultados de las implementaciones de SOAR:

- Resolución de incidentes más rápida
- Mejora de la eficiencia del personal
- Reducción de los costes generales[3]

¿Qué diferencia a Microsoft Sentinel?

SOAR es la funcionalidad de Sentinel que la diferencia de la competencia. Permite a los equipos de seguridad escribir código o cuadernos de estrategias dentro de Sentinel para responder automáticamente a las amenazas a medida que entran en acción, ayudando así al equipo de SOC a reducir la fatiga por alertas y centrarse en las cosas en las que realmente debe centrarse.

A nuestros clientes les gusta mucho que se puedan correlacionar alertas e incidentes, trazando un mapa de cada incidente asociado con una entidad específica. Lo que normalmente mostraré a los clientes en una demostración es un escenario en el que un atacante aleatorio ha obtenido acceso al entorno, ha elevado sus privilegios, ha realizado una descarga masiva de datos empresariales y, a continuación, ha eliminado su cuenta. Estas son cuatro alertas separadas que usted recibiría dentro de cualquier SOAR o SIEM. Pero en Microsoft Sentinel, puede ver un gráfico de una entidad con cuatro líneas diferentes para cada alerta que han generado, así como una línea temporal cronológica de esos eventos. Microsoft Sentinel facilita la búsqueda de amenazas."

— Consultor asociado, InfoSec, Insight

El caso de Microsoft Sentinel

Microsoft Sentinel™ combina la potencia de un SIEM y un SOAR en una sola solución. Si ya ha invertido en Microsoft® Sentinel, está en el camino hacia una seguridad más sólida.

La plataforma Sentinel puede ayudarle a:

Identifique las amenazas antes de que afecten a su negocio.

Responda rápidamente y con mayor precisión.

Simplifique la seguridad en entornos híbridos, multicloud, sin servidor y otros entornos modernos.

Reduzca los costes en comparación con las soluciones SIEM heredadas para investigación de amenazas, licencias, almacenamiento, infraestructura, gestión e implementación.

La herramienta se basa en la profunda experiencia de Microsoft en seguridad y las últimas capacidades de inteligencia artificial, y funciona armoniosamente con otros productos de Microsoft. Es rápida de configurar y fácil de escalar.

Un centro, muchos puntos de datos

Los entornos de soluciones de múltiples proveedores se vuelven menos complejos de gestionar con Microsoft Sentinel. La capacidad de Sentinel para extraer fuentes de datos de todo el ecosistema de soluciones de seguridad de múltiples proveedores proporciona a las organizaciones visibilidad y control para simplificar la búsqueda de amenazas, reducir la fatiga por alertas y capturar una imagen real de su postura de seguridad.

Mejores prácticas para la implementación

Comenzar a usar Microsoft Sentinel es relativamente sencillo. Antes de la implementación, aconsejamos establecer políticas y una gobernanza claras. Las consideraciones incluyen estándares de conformidad, requisitos de costos, planes de almacenamiento, recuperación ante desastres, niveles de personal del equipo de seguridad y planes de respuesta ante incidentes.

Día 1:

Habilite Microsoft Sentinel.

Conecte fuentes de datos.

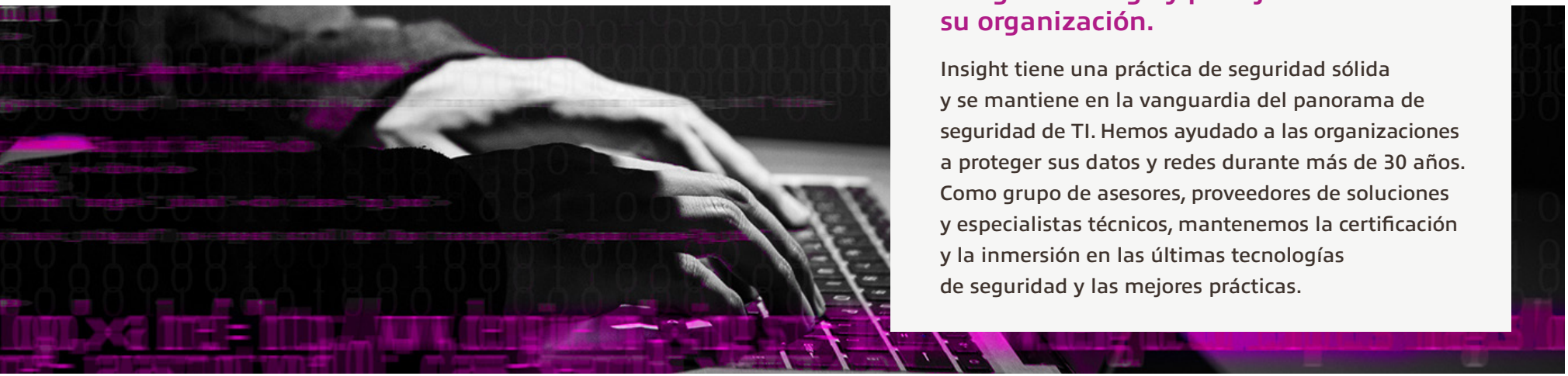
Comience a crear consultas para investigar los datos.

Como muchas otras herramientas SIEM, Syslog y CEF sirven como puntos de ingestión. Puede utilizar cualquier distribución preferida de Linux®, incluida la propia distribución Linux de Microsoft, e instalar reenviadores CEF y Syslog para reenviar registros a Microsoft Sentinel para su ingestión.

Microsoft ha creado Sentinel para albergar también registros de formato genéricos en formato común de eventos, de modo que incluso los registros de dispositivos heredados o especializados se puedan integrar y analizar.

Seguro en todos los ámbitos.

Microsoft Sentinel es más eficaz cuando forma parte de un enfoque programático más amplio de la ciberseguridad. Asegúrese de que su organización emplea las mejores prácticas en todo el espectro de ciberseguridad: Identificar, proteger, detectar, responder y recuperar.



SOLUCIÓN INSIGHT

Mitigue el riesgo y proteja su organización.

Insight tiene una práctica de seguridad sólida y se mantiene en la vanguardia del panorama de seguridad de TI. Hemos ayudado a las organizaciones a proteger sus datos y redes durante más de 30 años. Como grupo de asesores, proveedores de soluciones y especialistas técnicos, mantenemos la certificación y la inmersión en las últimas tecnologías de seguridad y las mejores prácticas.

Día 2+:

La flexibilidad y el dinamismo de la plataforma se harán evidentes en este punto. A continuación, le mostramos varias formas de maximizar drásticamente los beneficios de Microsoft Sentinel para las necesidades específicas y el perfil de riesgo de su organización.

1.

Compruebe sus reenviadores de registros.

Si no presta mucha atención al estado de su reenvío de registros y a la capacidad de su directorio de registros de VAR, las cosas pueden complicarse rápidamente y la ingesta de registros cesará. Cuando los consultores de Insight realizan la implementación de Microsoft Sentinel, utilizamos distribuciones de Linux con una partición para el punto de montaje del registro del VAR que es independiente del sistema operativo. De esta manera, si el directorio se llena, no afecta tanto al sistema operativo.

2.

Observe sus tasas de ingestión.

Es difícil calcular cuántos registros puede ingerir al principio, pero después de uno o dos meses, tendrá suficientes datos históricos para respaldar una mejor toma de decisiones en torno a una tasa de ingesta de datos adecuada. Esto le ayudará a obtener un mejor resultado de costes.

3.

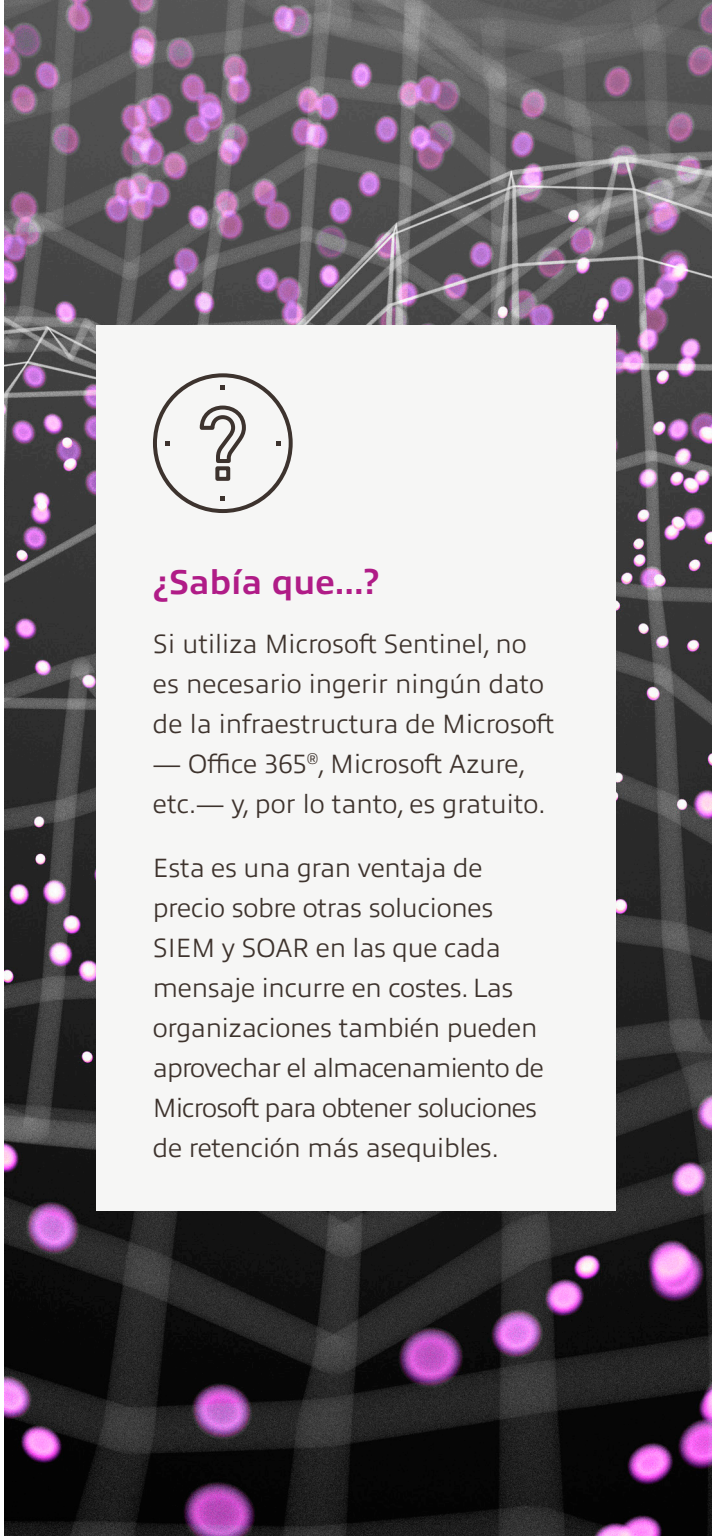
Minimizar los falsos positivos.

Muchas reglas listas para usar que proporcionan informes sobre funciones administrativas mediante análisis de comportamiento pueden generar falsos positivos. Microsoft ha publicado una función de Sentinel llamada Lista de seguimiento para ayudar a reducir estos falsos positivos, el ruido resultante y la fatiga por alertas. La Lista de seguimiento le permite integrar consultas (o CSV de diferentes atributos) en reglas analíticas que examinan una lista de seguimiento, o par de identificadores clave, y no alerta sobre actividades específicas.

4.

Utilice un tenant centralizado.

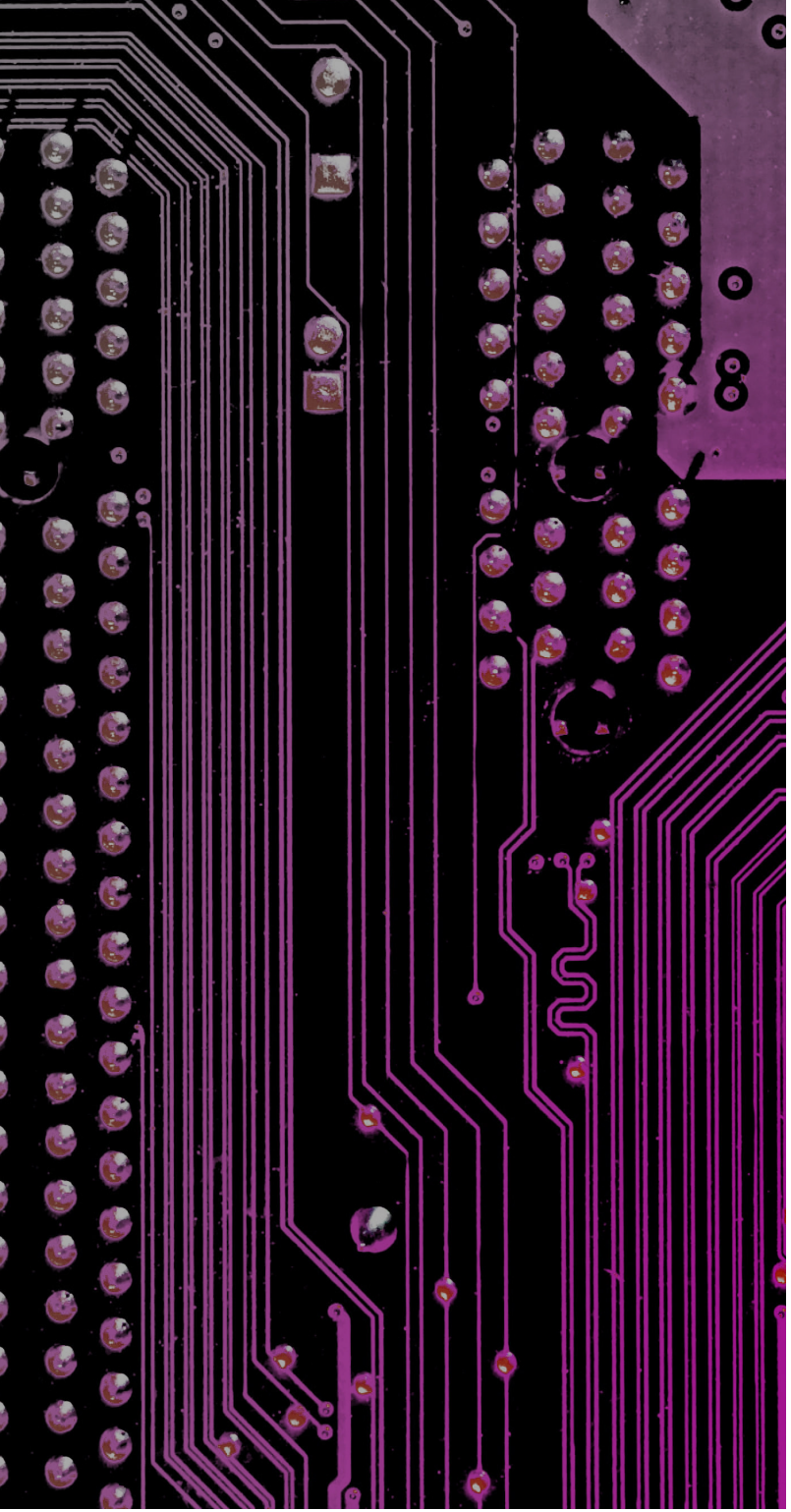
Si está supervisando diferentes tenants de Azure®, debe crear diferentes instalaciones de Microsoft Sentinel y registrar áreas de trabajo de análisis en cada uno de esos tenants. Al utilizar Azure Lighthouse para supervisar estas áreas de trabajo en un tenant centralizado, puede ajustar las reglas analíticas, llegar a la fuente fidedigna e implementar reglas para todos los tenants. Esto le ayudará a establecer una línea base coherente para umbrales, frecuencia de funcionamiento y otros ajustes.



¿Sabía que...?

Si utiliza Microsoft Sentinel, no es necesario ingerir ningún dato de la infraestructura de Microsoft — Office 365®, Microsoft Azure, etc.— y, por lo tanto, es gratuito.

Esta es una gran ventaja de precio sobre otras soluciones SIEM y SOAR en las que cada mensaje incurre en costes. Las organizaciones también pueden aprovechar el almacenamiento de Microsoft para obtener soluciones de retención más asequibles.



5.

Desintonice las soluciones listas para usar.

Microsoft Sentinel ofrece el beneficio distintivo de integrarse fluidamente con su ecosistema de Microsoft. Nuestros consultores aconsejan regularmente a los clientes que utilicen Microsoft Defender for Identity (MDI) para Active Directory® (AD) en las instalaciones, por ejemplo. Sin embargo, al conectar MDI a Sentinel, la configuración predeterminada reenviará automáticamente todas las alertas que salgan de MDI. Es probable que desee ir al conector del plugin y desintonizarlo para que no reciba alertas sobre información no urgente y solo reciba alertas dentro de un rango de gravedad especificado.

También examine la gravedad de las reglas analíticas existentes y escálelas, desescaléelas o elimínelas, según sus necesidades. Muchas reglas analíticas preconfiguradas se ejecutan con una frecuencia establecida que puede ser demasiado frecuente para gestionarlas. Recomendamos usar reglas analíticas que se ejecutan cada 15 o 30 minutos para alertas de alta gravedad, y ejecutarlas solo una vez al día para alertas de baja gravedad o informativas que no tienen mucho impacto en el negocio. En última instancia, el desintonizado le ayudará a minimizar la fatiga y el ruido por las alertas.

6.

Evaluar la paridad.

¿Qué utilizaba para proteger su entorno de TI antes de Microsoft Sentinel? ¿Cuáles son las similitudes y diferencias? Nuestros consultores sugieren que mire su antiguo sistema y el entorno de Microsoft Sentinel uno junto al otro y compare resultados visuales, paneles, alertas, fuentes de registro y otros atributos clave para garantizar que esté obteniendo paridad. No se debe obviar ninguna fuente de datos. Esto también le ayuda a asegurarse de que comprende completamente el nuevo alcance de las tareas diarias, el cuidado y la alimentación, y los requisitos de personal para respaldar la nueva plataforma.

7.

Considere la orientación proporcionada por Microsoft.

Microsoft ha publicado recomendaciones para realizar actividades regulares con el fin de garantizar que Sentinel le ofrece la mejor seguridad posible. Revíselas para obtener sugerencias sobre tareas diarias, semanales y mensuales, integraciones para configurar y procesos para gestionar y responder a incidentes.

Oportunidades de automatización

Uno de los puntos fuertes de la plataforma Microsoft Sentinel son sus capacidades de automatización. Aproveche la automatización para lograr una eficiencia y seguridad óptimas.

A continuación le indicamos un par de formas con las que puede automatizar con Sentinel:

Retención

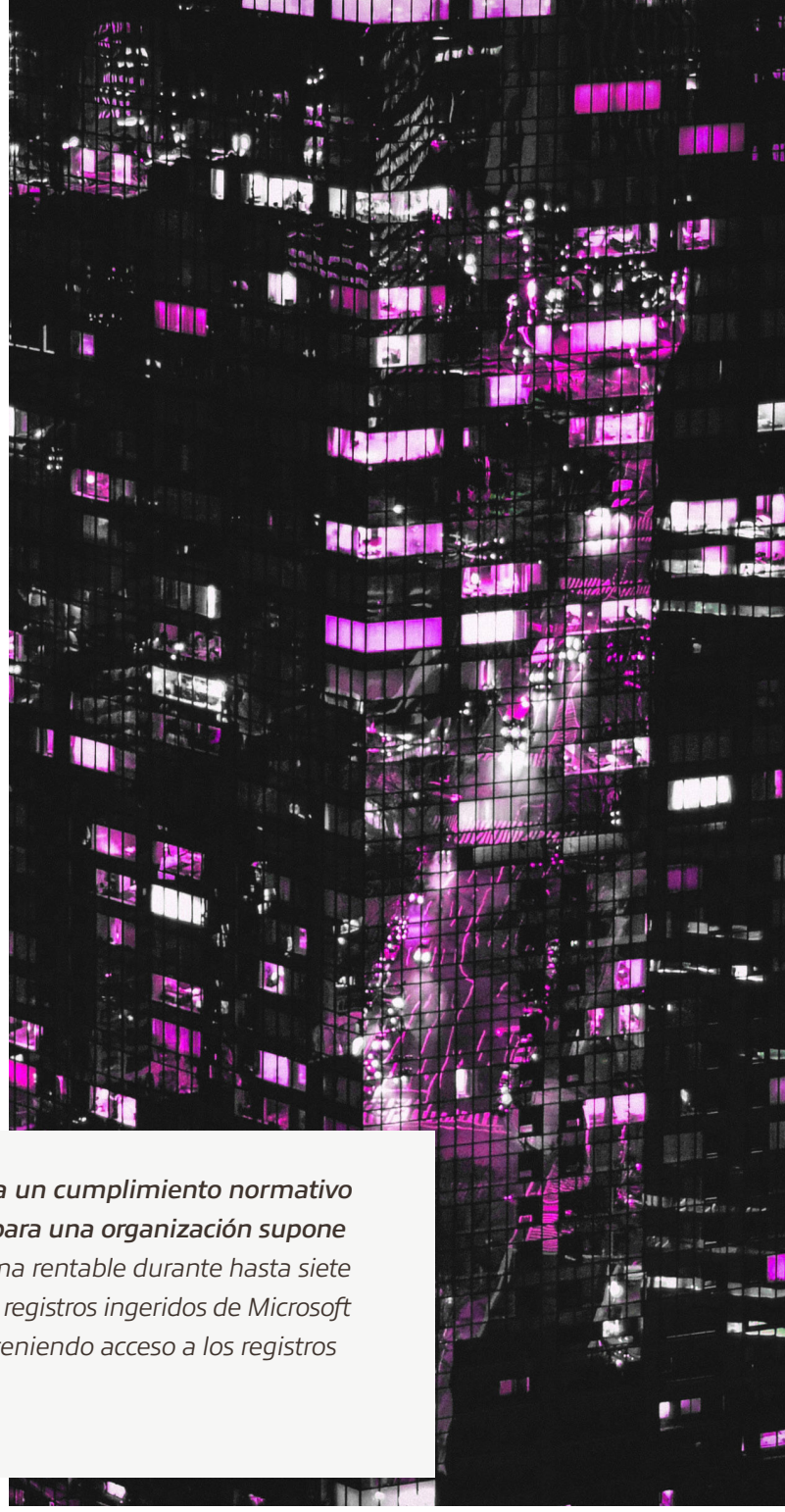
Cada organización tiene diferentes necesidades en torno a la retención de datos, en función de los requisitos legales y de conformidad del sector. Microsoft Sentinel ofrece la capacidad de automatizar el almacenamiento durante períodos de tiempo establecidos, lo que hace que sea increíblemente fácil para su equipo realizar esa tarea sin tener que establecer recordatorios ni preocuparse por la capacidad.

Cuadernos de estrategias

Para automatizaciones más complejas, los cuadernos de estrategias son una excelente opción. Los cuadernos de estrategias de Microsoft Sentinel se pueden configurar para una serie de tareas, como:

- Bloqueo de un usuario después de una alerta de inicio de sesión fallida
- Creación de un incidente de ServiceNow® que alimenta a su sistema de tickets
- Modificación de la CMDB en ServiceNow tras cambios en dispositivos bloqueados en la red

GitHub, propiedad de Microsoft, alberga muchos cuadernos de estrategias e ideas para la personalización, así como automatizaciones específicas de proveedores dentro de Microsoft Sentinel para explorar.



> ***Tenemos clientes que quieren siete años de retención de datos para HIPAA, o un año para un cumplimiento normativo gubernamental o NIST, por ejemplo. Averiguar qué esquema de retención funciona mejor para una organización supone un reto.*** *Blob Storage de Microsoft es una buena opción: le permite conservar registros de forma rentable durante hasta siete u ocho años. Para simplificar esto, creamos Azure Logic Apps que mueven automáticamente los registros ingeridos de Microsoft Sentinel a Blob Storage para que se conserven durante siete años. Las organizaciones siguen teniendo acceso a los registros si son necesarios para una investigación o indagación de seguridad."*
>
> — Consultor asociado, InfoSec, Insight

Mirando hacia el futuro

Existen innumerables formas de expandir y mejorar Microsoft Sentinel, y las oportunidades siguen creciendo a medida que la plataforma y la comunidad de usuarios maduran.

BYO ML

Traiga su propio aprendizaje automático (BYO ML) es un área que está recibiendo mucha atención. Esta página de Microsoft GitHub actúa como repositorio de la información más reciente y una biblioteca creciente de cuadernos de formación de muestra. Las organizaciones utilizan BYO ML para crear Databricks y ofrecer la formación y el análisis a través de un entorno Spark que extrae todos los datos de Sentinel, crea modelos para el acceso remoto o el comportamiento anómalo, y mucho más.

> ***No necesita tener un doctorado para poder hacerlo.*** *Gran parte de la formación y de los modelos creados por la comunidad son una aproximación bastante buena que solo necesita personalizarse para su entorno. Otros SIEM tienen algo similar a esto, pero la idea de que se puede tener una experiencia muy nativa basada en la ciencia de datos, donde básicamente tenemos un cuaderno Jupiter, un montón de bibliotecas de ciencia de datos Python, y se extraen datos directamente del entorno donde se está ejecutando el cuaderno, es muy interesante para mí."*
>
> **— Arquitecto principal (ciberseguridad, redes, ciencia de datos), Insight**

Visualización avanzada

Azure Monitor Workbooks dentro de Microsoft Sentinel ofrece una visualización de datos enriquecida. Por supuesto, esto es extremadamente útil para los equipos de seguridad. Ver los datos puede facilitar la identificación de puntos débiles y vulnerabilidades, ayudando a los equipos de seguridad a priorizar. La visualización también puede ayudar a los equipos de seguridad a justificar los presupuestos a la alta dirección con un impacto rápido. En el futuro, creemos que la visualización de datos será un enfoque clave, con comunidades de usuarios desarrollando libros de trabajo personalizados para abordar cualquier necesidad de seguridad o de negocio.

SOLUCIÓN INSIGHT

Nuestros consultores de servicios de seguridad pueden ayudarle a considerar las implicaciones de seguridad de sus actividades empresariales y adoptar soluciones que se alineen con sus necesidades y objetivos. Comenzamos por evaluar su entorno, desafíos y requisitos actuales.

Servicios gestionados

Debido a la falta de tiempo y recursos, las organizaciones de hoy en día solo pueden remediar  **50%** de las amenazas de seguridad legítimas.[1]

A muchas organizaciones les resulta difícil atraer y retener profesionales de la seguridad con experiencia que estén al día de los últimos conjuntos de herramientas de SIEM, SOAR y Centro de operaciones de seguridad (COS). Ya estamos viendo una consolidación general del talento en el área de seguridad dentro de las organizaciones de servicios que pueden gestionar con competencia los entornos de seguridad, así como proporcionar soporte crítico en torno a la preparación para ransomware, la arquitectura de seguridad, la respuesta a incidentes y la remediación.

En muchos casos, la gestión del tiempo es el mayor desafío. Aprender sobre formas de aumentar la automatización o aprovechar el aprendizaje automático para mejorar la búsqueda de amenazas puede verse eclipsado por las innumerables demandas diarias que supone dirigir un equipo de seguridad.

¿La clave para amplificar su seguridad? Servicios gestionados.

Insight ofrece servicios de seguridad gestionados (MSS) que se basan en las capacidades de Microsoft Sentinel y proporcionan supervisión ininterrumpida de su entorno. Al combinar las mejores prácticas reforzadas de la industria con técnicas de vanguardia para la minimización de riesgos, ayudamos a los clientes a liberar la pesada carga de cuidar y mejorar un entorno de seguridad dinámico.

Un enfoque avanzado.

Nuestros consultores de servicios de seguridad pueden ayudarle a considerar las implicaciones de seguridad de sus actividades empresariales y adoptar soluciones que se alineen con sus necesidades y objetivos. Comenzamos por evaluar su entorno, desafíos y requisitos actuales.

16 años

de experiencia en gestión de incidentes y amenazas

Más de 1.500

arquitectos, ingenieros y expertos en seguridad y prestación de servicios

Resultados de seguridad gestionados:

 Tiempos de respuesta más rápidos

 Gobernanza y cumplimiento más sólidos

 Mayor contexto y visibilidad

 Detección de amenazas mejorada

 Reducción de la carga del equipo de seguridad

Todo es posible

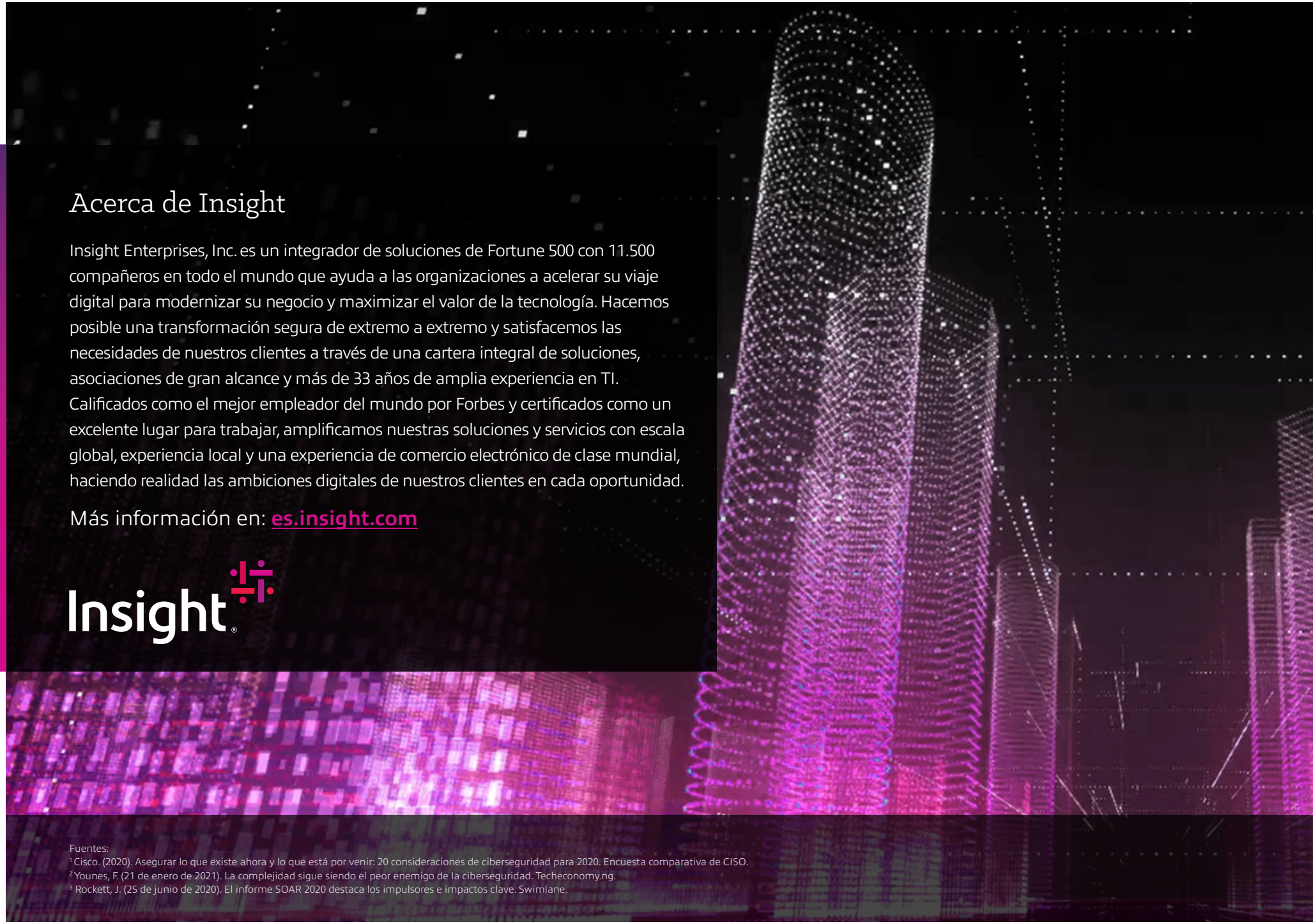
Microsoft Sentinel es fácil de implementar, pero requiere habilidades adicionales para optimizarlo bien.

Afortunadamente, hay pocos límites en cuanto a lo lejos que la plataforma puede llevarle en su camino hacia una seguridad completa, y con un equipo de confianza como Insight, es más fácil que nunca conseguir realizar el valor de su inversión. Nuestros consultores, técnicos y arquitectos tienen experiencia de primer nivel en el sector en torno a Microsoft Sentinel en una amplia variedad de entornos de clientes.

Independientemente de dónde se encuentre en su viaje de Sentinel, puede trabajar con Insight para:

- Evaluación de su entorno de seguridad actual
- Una evaluación de preparación de Microsoft Sentinel
- Implementación, integración y personalización de Microsoft Sentinel
- Servicios de seguridad gestionados para gestionar Microsoft Sentinel
- Optimización, automatizaciones y ajuste avanzado de funciones de Microsoft Sentinel

Póngase en contacto con nuestro equipo hoy mismo para comentar sus necesidades



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.

Más información en: **es.insight.com**

Insight®

Fuentes:
[1] Cisco. (2020). Asegurar lo que existe ahora y lo que está por venir: 20 consideraciones de ciberseguridad para 2020. Encuesta comparativa de CISO.
[2] Younes, F. (21 de enero de 2021). La complejidad sigue siendo el peor enemigo de la ciberseguridad. Techeconomy.ng.
[3] Rockett, J. (25 de junio de 2020). El informe SOAR 2020 destaca los impulsores e impactos clave. Swimlane.