elastic

Obtén más valor operativo de tu SIEM

elastic.co/es →

Tabla de contenido

Introducción

A medida que las organizaciones adoptan iniciativas de transformación digital para adaptarse a los cambios del mercado, muchas se han visto obligadas a reevaluar su enfoque de seguridad. Los nuevos productos y servicios web, las aplicaciones móviles y la necesidad de brindar soporte a una fuerza de trabajo remota están avanzando hacia nuevos tipos de ciberataques. **Abordar estos ataques requiere que los equipos de seguridad evolucionen rápidamente para mantenerse al día**.

Un desafío fundamental para mantenerse al día es evitar las ineficiencias que pueden amenazar la empresa a pesar de los mejores esfuerzos de los equipos de seguridad. La explosión de la adopción de SaaS, los mandatos de privacidad continuos y las directivas para consolidar las funciones de seguridad solo agregan complejidad operativa.

La clave para mantener el control mientras se mantiene la eficiencia operativa comienza con los datos que tienes fácilmente disponibles dentro de tu plataforma de gestión de eventos e información de seguridad (SIEM). El volumen y la variedad de datos que necesitan los equipos de seguridad se están disparando: el cloud, Internet de las cosas (IoT), fuentes móviles y datos de observabilidad, por nombrar algunos. El resultado es un aumento masivo de la actividad de eventos que es fundamental para descubrir los conocimientos necesarios para proteger el negocio.

Esta explosión de datos a menudo presenta desafíos operativos debido a las limitaciones de SIEM. **Tal vez sea el momento de revisar tu enfoque de SIEM** para asegurarte de que estás preparado para estos nuevos desafíos.

175 ZB

IDC predice que para 2025, los datos a nivel mundial crecerán a 175 zettabytes.

41.6 MM

Para 2025, 41.6 mil millones de dispositivos conectados generarán 79.4 zettabytes de datos

42 MM

Losencuestados de la Encuesta mundial sobre delitos y fraudes económicos 2020 de PwC reportaron $42 mil millones en pérdidas totales por fraude

Los requisitos de seguridad están evolucionando

A medida que las organizaciones adoptan un modelo de negocio más centrado en el cloud, los equipos de seguridad tienen la tarea de garantizar que los activos más valiosos de sus negocios (usuarios, aplicaciones, endpoints y datos) estén protegidos. Considera las siguientes tendencias que dificultan que los equipos de seguridad cumplan con sus KPI y métricas.

Gente

Es esencial mantenerse a la vanguardia de las metodologías de ataque nuevas y más sofisticadas.

- Las habilidades de seguridad son escasas
- Equipos de seguridad agobiados se esfuerzan por trabajar mejor juntos, más rápido y de manera más eficiente

Proceso

La presión está aumentando para mantener la eficiencia y la velocidad operativas a medida que aumentan las iniciativas del cloud.

- Grandes cantidades de datos se están trasladando al cloud
- Los trabajadores y socios remotos necesitan soporte para más soluciones en el cloud

Tecnología

El soporte para fuentes de datos de gran volumen es vital para proporcionar visibilidad de la actividad evasiva y los detalles necesarios para contextualizar una amenaza.

- Es difícil realizar consultas y análisis receptivos en las instalaciones y en el cloud.
- En muchos sistemas, acceder a fuentes de datos de gran volumen puede tener un costo prohibitivo

Los equipos de seguridad están dolorosamente conscientes de que la transformación digital agrega más superficie de ataque: cada nuevo dispositivo conectado o servicio en el cloud puede introducir un nuevo vector potencial para que un adversario lo explote y podría dar lugar a amenazas de seguridad graves o activos expuestos que se suman al riesgo comercial. **El requisito más fundamental es tener el contexto adecuado en el momento adecuado para tomar decisiones mejores y más rápidas**.

Reconsidera tu estrategia de seguridad usando los datos como tu marco de trabajo

Mantener la visibilidad de una superficie de ataque dinámica y en crecimiento a menudo no es práctico. Los modelos de licencia por ingesta o por evento o las arquitecturas que no cumplen con los requisitos de escala del cloud pueden forzar compensaciones. Los equipos suelen dedicar tiempo y recursos a decidir qué datos incluir y excluir de las operaciones diarias, lo que deja a la organización con una visibilidad limitada en su SIEM, lo que da como resultado silos operativos: silos de datos, silos de equipo y silos de proceso.

En lugar de trabajar a través de compensaciones y enfoques únicos para preservar datos que son difíciles de incluir en SIEM, como fuentes de datos de gran volumen o datos históricos, los equipos de seguridad adoptan cada vez más un enfoque diferente centrado en las necesidades de datos. La base de la SIEM moderna debe adecuarse a todos y cada uno de los datos, lo que permite que los equipos de seguridad rompan los silos. **La SIEM moderna permite a los equipos de seguridad buscar a escala** en cantidades masivas de cualquier tipo de datos —ya sean fuentes de datos tradicionales, no tradicionales o de gran volumen— en un ecosistema de múltiples capas con velocidad y precisión. Una vez que esa base está en su lugar, los equipos de seguridad pueden obtener beneficios masivos para **poner en funcionamiento cualquier caso de uso de seguridad a escala** —monitoreo y cumplimiento, detección y prevención de amenazas, búsqueda y respuesta ante incidentes— y abordar el fraude, las violaciones de la privacidad y otros problemas prioritarios que pueden poner en riesgo el negocio. La clave radica en la capacidad de los equipos de operaciones de seguridad para **recopilar, analizar, visualizar y actuar sobre la información de seguridad de una manera unificada**.

Cómo tu SOC se beneficia de un enfoque unificado

Un enfoque unificado ofrece a los equipos de seguridad una serie de ventajas. Un único almacén de datos, con potentes capacidades de visualización, procesamiento y seguridad de datos, proporciona el contexto necesario en los entornos distribuidos para extraer información valiosa de seguridad de todos tus datos. Con la analítica de seguridad adecuada (detecciones de alta fidelidad, trabajos de machine learning validados y otros métodos listos para usar que abarcan las instalaciones y el cloud), los equipos de seguridad pueden mejorar la postura de seguridad, detectar datos conocidos y desconocidos y responder rápidamente para evitar daños y prevenir incidentes futuros. Estratégicamente, **a medida que se producen cambios dinámicos, los equipos de seguridad pueden evolucionar rápidamente**. Los especialistas pueden adquirir conjuntos de habilidades más amplios a medida que:

Aprovechan más contexto para manipular mejor los datos y analizar las técnicas profesionales.

Colaboran para descubrir nuevas investigaciones o implementar nuevas detecciones.

Desarrollan nuevas visualizaciones y procedimientos operativos.

Perfilan a los actores de amenazas y emulan el comportamiento adversario

Más equipos pueden asumir responsabilidades de búsqueda. Las sólidas capacidades de integración a nivel de plataforma pueden permitir procedimientos altamente eficientes que simplifican la adaptación a nuevas clases de amenazas y mandatos regulatorios emergentes.

Con un enfoque unificado, tu SOC puede resolver problemas de seguridad complejos para una multitud de funciones de seguridad, incluida la búsqueda de amenazas, SIEM, investigación de amenazas, cumplimiento, monitoreo e investigación de seguridad, análisis forense digital y respuesta a incidentes, protección de endpoints, antifraude y más.

Visibilidad holística

Recopila información sobre seguridad e incluye cualquier fuente de datos necesaria para lograr resultados alineados con el negocio.

Escalabilidad del cloud

Obtén el contexto necesario de toda la organización para verificar las amenazas, incluidos años de contexto histórico.

Alta eficiencia de SOC

Encuentra los problemas de mayor prioridad de manera rápida e integra fácilmente con otras herramientas y tecnologías para una investigación y respuesta más rápidas.

Valor para todo el equipo de seguridad

Ingeniero de seguridad y administrador

- Analizar de forma centralizada logs, flujos y datos contextuales en todo tu entorno, sin importar qué tan dispares sean tus fuentes de datos
- Búsqueda rápida y federada para acceder y buscar rápidamente en un entorno complejo y distribuido
- Indexar y acceder fácilmente a fuentes de datos de gran volumen sin un costo exorbitante

Analista de seguridad

- Precisión para detectar amenazas complejas más rápido
- Velocidad para acelerar la respuesta y la eficiencia
- Realice una detección automatizada de amenazas y minimice el MTTD

Administrador de SOC

- Mantener un alto nivel de conciencia en todo el entorno para mejorar la postura de seguridad
- Evitar la recurrencia de problemas conocidos mientras se identifica problemas desconocidos
- Cumplir con los KPI de seguridad sin incurrir en altos costos

elastic

¿Tu SIEM te está frenando?

Hoy en día, los datos relevantes para la seguridad pueden provenir de servicios en el cloud, actividad de red y usuarios, endpoints, aplicaciones, dispositivos conectados y muchas otras fuentes. Muchas soluciones de SIEM que intentan acceder a todas estas fuentes de datos dan como resultado tiempos de análisis lentos de "pausa para café" o despliegues con costos prohibitivos.

Algunas SIEM se construyen en almacenes de datos separados para diferentes tipos de analíticas de seguridad —uno para machine learning, otro para correlaciones basadas en eventos—, lo que permite a los equipos archivar datos en otro almacén de datos separado para el contexto de búsqueda de amenazas o evidencia forense, y así sucesivamente. Como se mencionó anteriormente, estos silos causan ineficiencias en la forma en que los equipos comparten el contexto, colaboran, administran los casos y responden a las amenazas.

SIEM debería ayudar a que tu SOC evolucione más rápido, pero muchos productos de SIEM no brindan la escala ni la flexibilidad para ayudar a los equipos de seguridad a romper los silos de datos o de tareas, lo que da como resultado flujos de trabajo de investigación que están limitados por esos silos. El resultado son silos operativos que evitan que los equipos de seguridad se muevan de manera más rápida, inteligente y eficiente.

Los desafíos comunes en la eficiencia operativa con las soluciones de SIEM tradicionales incluyen:

- Las fuentes de datos de seguridad no están consolidadas y residen en almacenes de datos dispares en toda la empresa, lo que dificulta la visibilidad integral.
- Los tiempos de retención son demasiado cortos, lo que obliga a comprometer las detecciones, el contexto de investigación y la búsqueda de amenazas. Es difícil determinar las infracciones de alcance en ataques con tiempos de permanencia más largos.
- Los analistas de seguridad carecen de las fuentes de datos adecuadas necesarias para obtener un contexto sobre la actividad que puede no indicar una amenaza persistente avanzada, pero que sigue siendo una amenaza real para la empresa.
- Los equipos de SOC no pueden aprovechar las herramientas de machine learning, a menos que tengan científicos de datos internos para desarrollar modelos y buscadores de amenazas capacitados para interpretar el contexto.
- Los ingenieros de seguridad deben realizar grandes inversiones en proyectos de normalización de datos o reestructurar continuamente la estructura de datos subyacente de su SIEM cuando necesiten agregar nuevas fuentes de datos enriquecidas por el contexto (como datos de gran volumen). Ya deben "conocer" sus datos.
- Los equipos de investigación dedican una cantidad excesiva de tiempo a desarrollar reglas de SIEM que son frágiles y no resistentes a las técnicas evasivas, y carecen de un contexto de alta fidelidad a partir de los datos correctos.
- Los analistas de nivel 1-2 pasan demasiado tiempo buscando alertas que acaban en callejones sin salida o requieren recuperar contexto adicional de otros almacenes de datos, lo que provoca retrasos e ineficiencias.
- Los desarrolladores pasan la mayor parte de su tiempo solucionando problemas de integración o tratando de mantenerse al tanto de las actualizaciones de los proveedores.

Obtén una mejor protección con una SIEM moderna

Una SIEM moderna puede acceder a todos los datos de seguridad, independientemente del tamaño, la escala o la ubicación. Con visibilidad de todo el entorno, los equipos de seguridad tienen acceso a un contexto enriquecido y períodos de retroceso históricos necesarios para detectar y responder mejor a las amenazas con mayor rapidez y precisión para priorizar las amenazas.

Acceso a todos y cada uno de los datos

Información histórica y en tiempo real

Logro de la máxima velocidad de SOC

Obtén eficiencia operativa con Elastic Security como tu SIEM

Los equipos de seguridad están administrando una cantidad cada vez mayor de datos y necesitan poder buscar, analizar y realizar una detección automatizada en todos ellos, de manera rápida y precisa. La respuesta a las amenazas modernas requiere una correlación instantánea para un trabajo de investigación eficaz, búsqueda, creación de perfiles de amenazas y más en los datos de seguridad tradicionales, la infraestructura del cloud, los datos de aplicaciones y años de datos históricos.

Los equipos de seguridad usan Elastic Security para acceder a datos consolidados, contextualizar los hallazgos con amenazas y contexto comercial y usar datos históricos para encontrar rápidamente la mejor ruta de resolución. Elastic Security resuelve SIEM, seguridad de endpoints, búsqueda de amenazas, monitoreo en el cloud, detección de fraude y muchos otros casos de uso para que tu SOC pueda aprovechar el poder de la búsqueda y la visualización para proteger a la organización con un enfoque unificado para la detección, prevención y respuesta de amenazas.

Trabaja de forma más inteligente con Elastic Security

Gana visibilidad holística

Recopila datos normalizados de Elastic Common Schema con Beats e indexa todos los datos relevantes de seguridad para eliminar los silos de datos en toda la organización. Interactúa con dashboards intuitivos listos para usar y desarrolla visualizaciones personalizadas de arrastrar y soltar que se adapten a tus necesidades con Kibana, Lens y Canvas.

Obtén información sobre seguridad rápidamente

Ingesta datos usando tanto el esquema en escritura como el esquema en formatos de lectura, para un rendimiento de consulta óptimo y la flexibilidad de agregar o cambiar campos después de la ingesta. Lleva los resultados a los dashboards en segundos con la velocidad por la que el Elastic Stack es conocido. Destruye las alertas de fatiga con correlaciones priorizadas.

Incluye años de datos históricos

Aprovecha los snapshot buscables para aprovechar de manera rentable tantos datos de seguridad como necesites para incluirlos en detecciones, contexto de investigación, búsqueda de amenazas, monitoreo del cloud y más. Infracciones de alcance con tiempos de permanencia de meses o incluso años.

Reduce los tiempos de permanencia

Automatiza la detección con detecciones listas para usar mapeadas en MITRE, desarrolladas por el equipo de investigación de seguridad interna de Elastic, y detecciones personalizadas que aprovechan el poderoso e intuitivo Lenguaje de búsqueda de eventos (EQL) para realizar correlaciones que detectan herramientas, tácticas y procedimientos de amenazas avanzadas.

Encuentra actividades anómalas maliciosas

Aplica trabajos de machine learning sin supervisión a cualquier fuente de datos con una marca de tiempo para identificar anomalías independientes o anomalías asociadas que constituyan una amenaza potencial. Combina machine learning supervisado y no supervisado para detectar métodos, como algoritmos de generación de dominio (DGA) con tasas bajas de falsos positivos.

Optimiza los flujos de trabajo de operaciones de seguridad

Usa el espacio de trabajo interactivo de Elastic Security para detectar y responder a amenazas, clasificar eventos y recopilar evidencia en una línea de tiempo interactiva e intuitiva. Aprovecha la gestión e integración de casos integrada con los principales proveedores de flujo de trabajo, automatización y orquestación de seguridad (SOAR) para acelerar la respuesta y la resolución.

Implementa el SOC moderno

Elastic Security sirve como la base tecnológica de los equipos de seguridad modernos en todas partes. El enfoque de seguridad de plataforma abierta de Elastic facilita la integración, la flexibilidad y el poder de aprovechar las contribuciones y colaboraciones impulsadas por la comunidad para ayudar a los equipos de SOC a evolucionar rápidamente y tomar decisiones mejores y más rápidas.

Conclusión

A medida que los equipos de seguridad protegen a sus organizaciones contra un panorama de seguridad en constante expansión, no deben perder de vista la necesidad de mantenerse operativamente eficientes. Con acceso a todos los datos relevantes de seguridad y métodos rentables para acceder a datos históricos, puedes resolver más casos de uso desplegando Elastic Security como tu SIEM y aumentar el valor operativo de tu despliegue de SIEM en general. Los **equipos de seguridad líderes eligen Elastic Security como su SIEM porque necesitan un enfoque unificado para la detección, prevención y respuesta**.

Elastic proporciona visibilidad holística en todo el entorno con velocidad y eficiencia para identificar y resolver problemas, ofrece escalabilidad en el cloud en todo tu entorno híbrido y permite que tu SOC alcance la máxima eficiencia independientemente de qué tan distribuidos estén los equipos o cuántos silos operan en la actualidad. Mantén tu empresa protegida con un nuevo enfoque de SIEM con Elastic Security.

¿Quieres comprobar Elastic Security por ti mismo?

Prueba Elastic Security en Elastic Cloud (14 días gratis, no se requiere tarjeta de crédito). O despliégalo localmente, donde siempre es gratuito.

Comienza Elastic Security de forma gratuita →

Search. Observe. Protect.

Elastic hace que los datos puedan usarse en tiempo real y a escala para la búsqueda empresarial, observabilidad y seguridad. Las soluciones de Elastic están desarrolladas a partir de una sola pila de tecnología gratuita y abierta que se puede desplegar en cualquier lugar para encontrar de forma instantánea información procesable de cualquier tipo de datos: desde encontrar documentos hasta monitorear infraestructuras y buscar amenazas. Miles de organizaciones de todo el mundo, como Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia y Verizon, usan Elastic para impulsar los sistemas de misión crítica. Fundada en 2012, Elastic cotiza en NYSE con el símbolo bursátil ESTC. Conoce más en elastic.co/es.

OFICINA CENTRAL EN AMÉRICA
800 West El Camino Real, Suite 350, Mountain View, California 94040
General +1 650 458 2620, Ventas +1 650 458 2625

info@elastic.co