Proofpoint Managed SIEM

Refuerce la seguridad de su entorno Splunk

Ventajas principales

- Detección mejorada para disponer de una mayor visibilidad. Identifique las amenazas ocultas gracias a indicadores de nuestra inteligencia de amenazas emergentes.
- Caza de amenazas inteligente para ofrecer respuestas proactivas. Investigamos a los ciberdelincuentes y buscamos pruebas en su entorno. Al proporcionar información en profundidad de factores contextuales como el alcance de los objetivos, el calendario y otros aspectos, permitimos la respuesta y la corrección proactivas.
- Supervisión y detección permanentes. Ofrecemos una optimización rápida de su entorno. Y nuestro equipo de caza de amenazas respaldará su programa SIEM con supervisión permanente y una reducción del tiempo medio de respuesta y corrección.
- Ingeniería de seguridad especializada. Nuestro equipo de ingeniería es de los mejores del mundo y garantiza el buen estado de su entorno Splunk.

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.

Proofpoint Managed SIEM le da acceso a un equipo de expertos cuya única misión es detectar, analizar y mitigar las amenazas. El servicio ofrece una protección avanzada para entornos Splunk. Gracias a él, puede desplazar parte de la carga de trabajo asociada a la administración de información y eventos de seguridad (SIEM) y conseguir funciones avanzadas de caza de amenazas.

Proofpoint Managed SIEM ayuda a aliviar los retos cotidianos a los que se enfrentan sus equipos de TI y seguridad de la información cuando intentan gestionar grandes volúmenes de alertas y responder a ellas rápidamente. Sin nuestro servicio, estas tareas pueden resultar abrumadoras. Y el problema no hace sino empeorar con la incorporación de nuevas tecnologías de detección y el creciente número de alertas que generan. Esto puede dar lugar a fatiga de alertas, incluso si sus equipos aplican las mejores prácticas, runbooks y las últimas herramientas y métodos de análisis.

Simplifique las operaciones de seguridad

Los clientes de Splunk que utilizan Proofpoint Managed SIEM consiguen las siguientes ventajas:

- **Detección optimizada.** A diferencia de otros servicios que sencillamente operan al margen de las alertas que proporcionan otras soluciones SIEM, Proofpoint Managed SIEM mejora las detecciones con inteligencia e indicadores de amenazas. Eso nos permite ver amenazas que otras soluciones no ven.
- **Caza de amenazas y cambios.** Nuestra cartera de seguridad abarca muchos vectores de detección, con un potente gráfico de amenazas impulsado por aprendizaje automático e inteligencia artificial de más de 1 billón de nodos, y más de 100 investigadores de amenazas. Esta amplitud y profundidad no solo nos permite detectar amenazas, sino establecer conexiones entre incidentes que podrían parecer desconectados.
- **Protección frente a amenazas permanente.** El servicio Proofpoint Managed SIEM se proporciona a través de un equipo global de profesionales de seguridad y detección de amenazas. Nuestros expertos se encuentran en centros de operaciones de seguridad repartidos por todo el mundo. Además, identifican, clasifican e investigan amenazas para nuestros clientes de manera ininterrumpida.

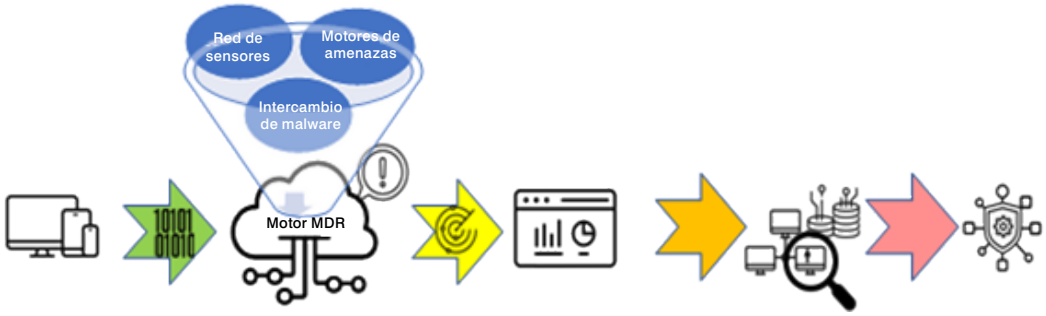

Figura 1: Las fuentes reenvían los registros al motor de detección y respuesta gestionadas (MDR), que utiliza la inteligencia de amenazas de Proofpoint para optimizar las alertas. Nuestro equipo clasifica, analiza y prioriza las alertas, a continuación lleva a cabo análisis correlacionales y realiza acciones de caza proactiva de amenazas para contener y responder a ellas.

Enriquezca los registros de Splunk con inteligencia de amenazas de Proofpoint

La inteligencia de amenazas de Proofpoint enriquece los registros de su red para identificar amenazas que podrían haber pasado desapercibidas y crear nuevas alertas de Proofpoint. Cuando aparecen las alertas, las clasificamos e investigamos más afondo. Los detalles de las amenazas (como usuarios clave, objetivos de alto valor y patrones de ataque) se identifican para su priorización y mitigación. Evaluamos las amenazas para realizar cazas de amenazas avanzadas cuando sea necesario.

El equipo de Proofpoint utiliza un flujo de trabajo de aprobación optimizado para corregir rápidamente las amenazas activas. El flujo de trabajo también garantiza que los recursos de seguridad de su organización quedan libres y disponibles para trabajar en proyectos de seguridad más importantes o estratégicos.

Detección avanzada de amenazas para su organización

Proofpoint mejora las funciones SIEM tradicionales con detección avanzada basada en servicios y tecnologías de vanguardia. Proporciona:

- **Experiencia incomparable y capacidades proactivas.** La inteligencia de amenazas de Proofpoint nos permite ser proactivos mientras le protegemos. Nuestra red de sensores mundial y nuestro equipo de analistas e investigadores de amenazas realizan actividades de caza de amenazas y correlación en múltiples plataformas. Nuestros expertos tienen además visión de futuro. Crean defensas adaptadas a sus necesidades. Además, se basan en las mejores prácticas del sector y en las últimas actualizaciones de los productos de Proofpoint.
- **Operaciones de seguridad continuas y rentables.** La contratación, formación y retención de personal de seguridad es uno auténtico desafío. Esto es particularmente así en lo que respecta a conocimientos especializados, como la identificación y gestión de incidentes. Nuestros servicios gestionados le dan acceso a un equipo de expertos, siempre a su disposición. Esto le ayuda a reducir al mínimo el tiempo, dinero y recursos que debe destinar a resolver los desafíos de personal específicos.
- **Informes periódicos e información a nivel ejecutivo.** Proporcionamos indicadores que pueden ofrecerle información de gran valor sobre las tendencias de seguridad, identificar las oportunidades para nuevos enfoques de seguridad y ayudarle a tomar decisiones informadas.

Proofpoint Managed SIEM integra estas capacidades para proporcionar una defensa eficaz. Nuestro equipo ayuda a garantizar el buen estado de su entorno. Además, optimizamos la configuración de reglas en Splunk para detectar las amenazas de manera precisa. Esto incluye la implementación de actualizaciones del sistema, parches y ajustes cuando sean necesario. Combinamos la detección avanzada, la priorización y la corrección de amenazas de alta prioridad con mitigaciones rápidas. En pocas palabras, nuestro equipo ofrece la mejor ingeniería de seguridad. Permítanos ayudarle a reducir sus deficiencias de seguridad y la superficie de ataque global.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.