securonix

FICHA TÉCNICA

Securonix + Snowflake

Detección y respuesta de amenazas a escala de nube

Desafíos de la seguridad de los macrodatos

A medida que las empresas se trasladan a la nube, las soluciones tradicionales de SIEM (gestión de eventos e información de seguridad) no pueden seguir el ritmo de la escala y la complejidad de los datos de seguridad. Las brechas de la visibilidad y las limitaciones resultantes dificultan la eficaz detección de amenazas y respuesta a ellas. Los primeros intentos de resolver este problema no lograron procesar, enriquecer ni formatear los datos para transformarlos en casos de uso prácticos para los analistas.

Por otra parte, las plataformas de datos en la nube se han creado para llevar a cabo análisis rentables a gran escala, pero carecen de las integraciones de seguridad y de los análisis innovadores que necesitan los equipos de seguridad.

La solución: Securonix + Snowflake

En una nueva y emocionante asociación, Securonix y Snowflake han creado una solución de arquitectura dividida que permite a los clientes utilizar los análisis de Securonix además de su actual plataforma de datos en la nube Snowflake. La solución conjunta permite a los clientes de Snowflake mantener sus datos dentro de su implementación de Snowflake mientras siguen aprovechando Securonix Next-Gen SIEM para aumentar la visibilidad, la seguridad, el análisis y la respuesta a incidentes basada en la inteligencia.

A diferencia de las soluciones tradicionales de SIEM que utilizan un modelo de consumo de datos, este enfoque híbrido permite que los datos, los servicios y las aplicaciones se implementen de forma óptima entre la nube de datos Snowflake y la infraestructura nativa en la nube de Securonix. Con la solución conjunta, las organizaciones pueden consolidar todos sus datos empresariales y de seguridad en una sola ubicación y aprovechar los análisis avanzados para la detección y la respuesta.

Beneficios de la solución

Obtención de una fuente única de información

Todos los registros, activos y configuraciones se analizan juntos, para eliminar los "silos" y reducir la complejidad.

Precios transparentes y ahorros de costos

Los precios económicos del almacenamiento y de eventos por segundo reducen los costos del SIEM. Pague directamente a Snowflake para evitar el aumento vertiginoso de los costos del procesamiento de datos.

Detección de amenazas y respuesta a ellas más rápidas

La solución centralizada de Securonix Next-Gen SIEM optimiza la investigación y actúa como una extensión de la nube de datos Snowflake del cliente.

Los clientes pueden utilizar la arquitectura de un solo nivel de Snowflake para contar con un almacenamiento rentable e ilimitado en la nube con una política de retención flexible que se controle dentro de la organización.
La potencia del cómputo es prácticamente ilimitada y puede escalarse según sea necesario para llevar a cabo investigaciones rápidas en terabytes y petabytes de datos. Además, el precio de Snowflake basado en el consumo significa que solo se paga por los recursos cuando se utilizan, lo cual se traduce en un importante ahorro de costos en general.

Detalles de la arquitectura de implementación

- Securonix aloja los servicios centrales de la aplicación de SIEM, el monitoreo, los microservicios y la recuperación de catástrofes para la solución.
- La cuenta de Snowflake existente del cliente recibe datos de seguridad normalizados y enriquecidos.
- Los recursos existentes de la nube de datos Snowflake se utilizan para un almacenamiento ilimitado que permite hacer consultas desde la consola de Securonix.
- Los conjuntos de datos empresariales de la cuenta de Snowflake del cliente se pueden cargar de forma independiente y combinar con los datos de seguridad para el enriquecimiento del contexto.
- El cliente es propietario de todos los datos de registro recopilados y puede aprovecharlos para los casos de uso que trasciendan la SIEM, como la observabilidad operativa, las métricas de seguridad y la validación de controles.

Securonix + Snowflake para la detección y la respuesta

A diferencia de los modelos tradicionales de consumo de datos, este modelo de implementación compartido ofrece Securonix Next-Gen SIEM como una extensión perfectamente integrada del entorno de la nube Snowflake del cliente. Todos los registros de seguridad se almacenan y analizan en un solo lugar, lo que permite una detección de amenazas y respuesta a ellas más rápida en el entorno del cliente. Las organizaciones pueden conseguir una visibilidad completa, conocimientos prácticos, una mejor automatización y un ahorro significativo al utilizar Securonix con Snowflake.

Para obtener más información sobre Securonix + Snowflake, programe una demostración en **www.securonix.com/request-a-demo**

securonix