securonix

FICHA TÉCNICA

Gestión NXLog

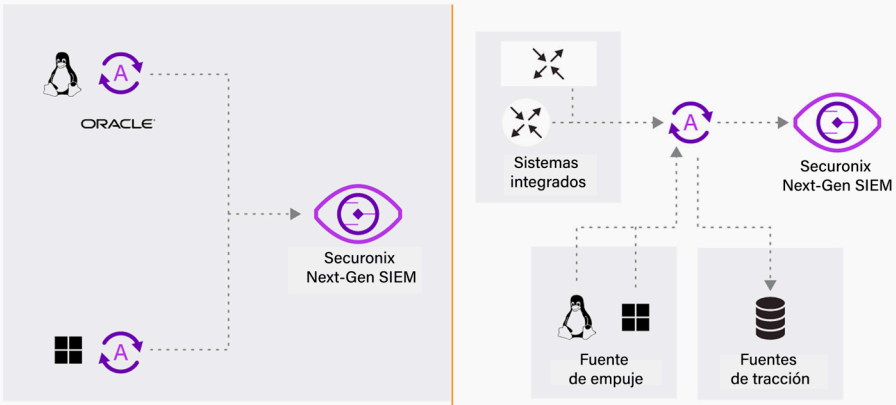
Recopilación definitiva de registros y gestión centralizada

Mejor detección y respuesta de las amenazas utilizando la recopilación centralizada de registros.

Las organizaciones invierten en soluciones de SIEM (gestión de eventos e información de seguridad) para mejorar las operaciones de seguridad, gestionar el riesgo, acelerar la respuesta a incidentes y proporcionar un análisis forense digital. Sin embargo, si la SIEM no proporciona una correlación ni un análisis adecuados debido a una recopilación de registros insuficiente, la organización no puede capitalizar su inversión en la SIEM.

Securonix con NXLog proporciona una solución de recopilación y distribución de registros altamente flexible y fiable. NXLog es un sistema de registro escalable que garantiza que los registros se recopilen de forma eficiente, segura y fiable. NXLog estructura, formatea y filtra los datos. La solución es compatible con la mayoría de los sistemas operativos y puede manejar fuentes de datos que otras herramientas no pueden, lo cual le da a usted una visibilidad adicional de los sistemas de toda su organización.

Soporte de gestión de registros de varias plataformas



Recopilación de registros basada en agentes

Recopilación de registros sin agentes

Beneficios de la recopilación avanzada de registros con NXLog

NXLog es un sistema de recopilación de registros de alto rendimiento que optimiza las funciones de gestión de registros al ingresar sus datos en un lugar central para filtrar, clasificar, convertir y procesar de forma más fácil.

Automatice las operaciones de seguridad de TI

Simplifique la recopilación de registros utilizando un único producto que lea muchas fuentes de registros y los transmita a varios destinos. Securonix ofrece el análisis de los registros de eventos a nivel de alojamiento web, lo cual reduce el costo de distribución y gestión de la recopilación de registros.

Reduzca el riesgo de los registros en tránsito

Securonix con NXLog permite a los clientes enviar los registros de forma segura y fiable a Securonix Next-Gen SIEM.

Mantenga el cumplimiento de los datos

El monitoreo de la integridad de los archivos ayuda al cumplimiento y la detección mediante el monitoreo de los cambios en los archivos y las carpetas importantes.

Recopilación de registros de Securonix con NXLog

Securonix proporciona un sistema de registro escalable al permitir la recopilación de datos en varios entornos.

Gestión centralizada de registros

Adquisición de registros sin fricciones

Amplíe y simplifique el ingreso de datos en diversas fuentes con una sola tecnología.

Recopilación de registros basada en agentes: NXLog se ejecuta como un agente que admite fuentes de datos específicas de la plataforma, como los registros de eventos de Windows, los registros del núcleo de Linux, los registros de Android, la bitácora de eventos del sistema local, etc.

Recopilación de registros sin agentes: Para los sistemas integrados o tradicionales, como los rúteres y los conmutadores, los cuales no admiten la instalación de agentes, un servidor o dispositivo envía los datos de registro a una instancia de NXLog a través de la red utilizando sus protocolos nativos.

Centralización de registros: NXLog recopila y gestiona el flujo de registros de toda la empresa. La centralización de registros ahorra tiempo y garantiza la coherencia de sus datos de registro.

Atienda los mandatos de cumplimiento

Medidas de seguridad para la detección y el cumplimiento

Al proporcionar los mensajes de registro relevantes a Securonix Next-Gen SIEM, puede asegurarse de que está siguiendo los requisitos estándares y de cumplimiento.

Cumplimiento: Obtenga acceso a una colección integrada de registros de auditoría para monitorear los cambios en archivos y directorios en todas las plataformas compatibles, incluido el registro de Windows.

Monitoreo de la integridad de los archivos: El monitoreo de la integridad de los archivos de NXLog proporciona alertas sobre las actividades de los activos, como los posibles cambios no autorizados. NXLog ofrece una mejor respuesta a los incidentes, como la detección de ataques de *malware* o cambios maliciosos hechos por el *malware* en activos cruciales, cuando se utiliza con Securonix Next-Gen SIEM.

Mitigación de riesgos

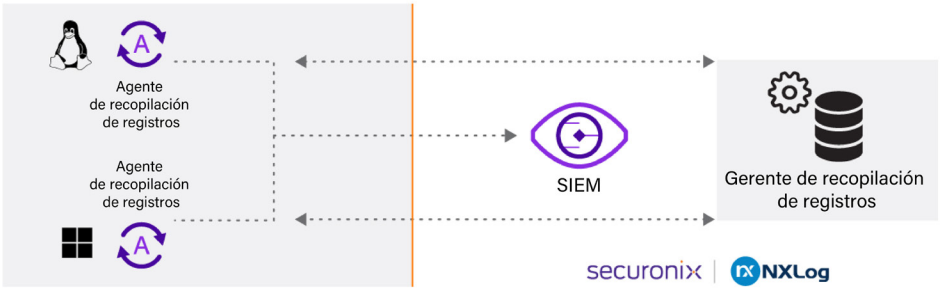
Reduzca el riesgo de los registros en tránsito

La recopilación de registros desde muchos dispositivos con una única solución permite que los registros se transfieran sin perder su integridad. Para disminuir el riesgo, la solución utiliza una transferencia fiable con compresión, un acuse de recibo a nivel de protocolo y una agrupación por lotes.

Encriptación de datos SSL/TLS: La encriptación protege los datos de registro en tránsito para que no sean modificados ni vistos por un atacante. NXLog proporciona una encriptación de datos SSL/TLS; admite muchos módulos de entrada y salida; y garantiza una autenticación sólida, y la integridad y la confidencialidad de los mensajes.

Seguridad de los datos: Asegura la transferencia de registros y permite que usted configure los privilegios especiales.

Gerente de recopilación de registros de Securonix con la tecnología de NXLog



Para obtener más información sobre Securonix Nex-Gen SIEM con la tecnología NXLog, programe una demostración en www.securonix.com/request-a-demo