Log & Event Manager

Demuestre el cumplimiento y mejore la seguridad

> *"Interfaz intuitiva y fácil de usar que extrae todos los datos empresariales de la red convertidos en información relevante y comprensible."*
>
> – Marie Karaffa,
> Directora de TI,
> John Roberts Co.

Más de 3500 profesionales de seguridad con recursos limitados confían en SolarWinds® Log & Event Manager para una gestión de la información de seguridad y de eventos efcaz, asequible y efciente (SIEM). Nuestro SIEM todo en uno combina gestión de registros, correlación, generación de informes, monitoreo de la integridad de archivos, monitoreo de la actividad del usuario, detección de USB y prevención, inteligencia de amenazas y respuesta activa en un appliance virtual que es fácil de implementar, gestionar y utilizar. Hemos diseñado nuestro SIEM para proporcionar la funcionalidad que necesita sin la complejidad y costo de otras soluciones SIEM empresariales.

RESUMEN DE LOG & EVENT MANAGER

- Recopila, consolida y analiza registros y eventos desde frewalls, dispositivos y aplicaciones IDS/IPS, conmutadores, routers, servidores, registros de sistema operativo y otras aplicaciones.
- Correlación en tiempo real para identifcar los ataques.
- Detecte infracciones con inteligencia de amenazas.
- Admite análisis de causa raíz con inteligencia integrada que se aplica a redes, aplicaciones y gestión de la seguridad.
- Bloquea y pone en cuarentena actividad maliciosa y sospechosa, lo que incluye uso inapropiado de USB.
- Brinda inteligencia más exhaustiva y compatibilidad con cumplimiento más amplia mediante Monitoreo de la integridad de los archivos (FIM) incrustado.
- Genera informes sobre cumplimiento listos para usar para HIPAA, PCI DSS, SOX, ISO, DISA STIGs, FISMA, FERPA, NERC CIP, GLBA, GPG13, etc.

FUNCIONES DESTACADAS

Recopilación de registros de nube, máquinas y dispositivos de red fácil y adaptable

Log & Event Manager recopila y cataloga datos de eventos y registros en tiempo real, desde cualquier lugar de la infraestructura de TI donde se generen datos. Analice los recursos de datos admitidos.

Correlación de eventos en memoria en tiempo real

Mediante el procesamiento de los datos de registro antes de que se escriban en la base de datos, Log & Event Manager ofrece correlación de eventos y registro en tiempo real verdadero, lo que le permite detectar y solucionar problemas e investigar infracciones de seguridad y otras cuestiones esenciales de manera inmediata.

Fuente web de inteligencia de amenazas

Aproveche la información lista para usar sobre IP dañinas para identifcar actividad maliciosa. La fuente web se actualiza con regularidad desde una recopilación de orígenes de investigación y etiqueta automáticamente los eventos a medida que se introducen en el appliance. A partir de ahí, puede ejecutar rápidamente búsquedas o informes para ver la actividad sospechosa, o bien crear reglas para realizar acciones automáticas.

Búsqueda de TI avanzada para análisis forenses de eventos

La avanzada capacidad de búsqueda de TI ad-hoc de Log & Event Manager facilita la detección de problemas por medio de una interfaz de tipo "arrastrar y soltar" que permite realizar instantáneamente seguimiento de eventos. Incluso puede guardar búsquedas comunes para referencia futura.

Retención y compresión de datos de registro

Log & Event Manager permite almacenar terabytes de datos de registro a una elevada tasa de compresión para generación de informes de cumplimiento, compilación y alivio de la carga, lo que reduce los requisitos de almacenamiento externo.

Monitoreo de la integridad de los archivos incrustado y en tiempo real

El monitoreo de la integridad de los archivos incrustado brinda compatibilidad más amplia con el cumplimiento e inteligencia de seguridad más exhaustiva para amenazas internas, malware de día cero y otros ataques avanzados.

Respuestas activas integradas

Log & Event Manager le permite responder inmediatamente ante eventos de seguridad, operativos y originados por políticas por medio de respuestas activas incorporadas, que realizan acciones como poner en cuarentena máquinas infectadas, bloquear direcciones IP, detener procesos o ajustar los parámetros de Active Directory®.

Prevención y detección de USB

Log & Event Manager lo ayuda a prevenir la pérdida de datos de punto fnal y protege la información confdencial con notifcaciones en tiempo real cuando los dispositivos USB se conectan, con capacidad para bloquear su uso y con informes integrados para auditar el uso de USB.

Monitoreo de la actividad de los usuarios

Mejore el conocimiento de su situación mediante información sobre actividades críticas de los usuarios. Conozca cuándo se utilizan cuentas con privilegios, cómo se utilizan y desde dónde.

Plantillas listas para usar de informes de cumplimiento y seguridad

Con Log & Event Manager, es fácil generar y programar informes de cumplimiento con rapidez usando más de 300 plantillas probadas para auditoría y una consola que le permite personalizar los informes en función de las necesidades de cumplimiento específcas de su organización.

Facilidad de uso e implementación

La implementación de Log & Event Manager es rápida y simple. Es posible comenzar a auditar registros sin dilación, por medio de la intuitiva interfaz, la consola basada en web y el modelo de implementación de aplicaciones virtuales.

¿QUIÉN DEBERÍA UTILIZAR LOG & EVENT MANAGER?

Profesionales con recursos limitados que enfrentan el desafío de:

- Falta de visibilidad de los ataques además de tiempo limitado para el monitoreo con personal.
- Demandas de cumplimiento que necesitan automatización y/o monitoreo de la integridad de los archivos.
- Incapacidad para priorizar, gestionar y responder ante incidentes de seguridad.
- Tiempo de respuesta ante incidentes lento.
- Incapacidad para determinar la causa raíz de la actividad sospechosa.
- Incapacidad de monitorear el uso aceptable de los usuarios internos y amenazas internas.
- Necesidad de compartir datos de registros y actividades de seguridad, red, aplicaciones y sistemas.
- Implementaciones SIEM inefcientes, inoperables o costosas .

CÓMO LOG & EVENT MANAGER RESPALDA SU PROGRAMA DE SEGURIDAD

- Automatización e inteligencia incrustadas brindan un Centro de operaciones de seguridad virtual para el monitoreo 24x7.
- Detección de eventos más rápida y alertas sobre correspondencias de inteligencia de amenazas basada en IP.
- Detección más inteligente y precisa de actividad sospechosa y maliciosa, lo que incluye malware de día cero y amenazas avanzas e internas.
- Elimina los procesos de informes manuales que consumen mucho tiempo.
- Acelera la respuesta mediante capacidades forenses efcaces.
- Bloquea de forma automática el uso inadecuado u ofensivo mediante respuestas activas para infracciones de red, sistema y políticas de acceso.
- Monitorea y bloquea el uso de USB según reglas de políticas de comportamiento.
- Proceso de inicio de sesión intuitivo con integración de inicio de sesión único: uso de ID de usuario y contraseña, tarjeta inteligente, contraseña de un solo uso y dispositivo biométrico.

REQUISITOS DEL SISTEMA

HARDWARE	REQUISITOS MÍNIMOS
CPU	Procesador dual, 2,0 GHz
Memoria	8 GB RAM
Disco duro	250 GB
SOFTWARE	**REQUISITOS MÍNIMOS**
SO/Virtual	VMWare® ESX®/ESXi™ 4.0 y superior
Entornos	HYPER-V® SERVER 2008, 2008 R2, 2012, 2012R2
Base de datos	Integrado con appliance virtual

PRUÉBELO ANTES DE COMPRARLO. DESCARGUE UNA VERSIÓN DE PRUEBA GRATIS.

Compruébelo por usted mismo. En SolarWinds, creemos que debe probar nuestro software antes de comprarlo. Por ello, ofrecemos pruebas gratis completamente funcionales de nuestros productos. No tiene más que descargar Log & Event Manager y, en menos de una hora, estará listo para analizar archivos de registro. Es así de simple. ¡Descargue hoy mismo una prueba gratis y completamente funcional!

ACERCA DE SOLARWINDS®

SolarWinds brinda software de gestión de TI efcaz y rentable a los clientes de todo el mundo, desde empresas Fortune 500® hasta pequeñas empresas, proveedores de servicios gestionados, agencias gubernamentales e instituciones educativas. Hemos asumido el compromiso de concentrarnos exclusivamente en los profesionales de TI, proveedores de servicios gestionados y desarrollo y operaciones, y nos esforzamos en eliminar la complejidad que nuestros clientes se vieron obligados a aceptar por parte de proveedores tradicionales de software empresarial. Independientemente del lugar en el que se encuentre el activo de TI o el usuario, SolarWinds entrega productos fáciles de encontrar, comprar, usar, mantener y escalar, a la vez que proporciona la facultad de atender las áreas clave de la infraestructura, desde las instalaciones hasta la nube. Este enfoque y compromiso con la excelencia en la gestión del desempeño de la TI híbrida han convertido a SolarWinds en el líder mundial en software de gestión de redes y soluciones MSP, y está brindando un crecimiento similar en el espectro completo del software de gestión de TI. Nuestras soluciones se basan en nuestra profunda conexión con nuestra base de usuarios, que interactúa en nuestra comunidad en línea THWACK® para resolver problemas, compartir tecnología y prácticas recomendadas, y participar directamente en nuestro proceso de desarrollo de productos. Obtenga más información hoy en www.solarwinds.com.

OBTENGA MÁS INFORMACIÓN

Para más información sobre los productos de SolarWinds, visite solarwinds.com, llame o envíe un correo electrónico.

CONTINENTE AMERICANO
Teléfono: 866.530.8100
Fax: 512.682.9301
Correo electrónico:
latam.sales@solarwinds.com

7171 Southwest Parkway | Building 400 | Austin, Texas 78735