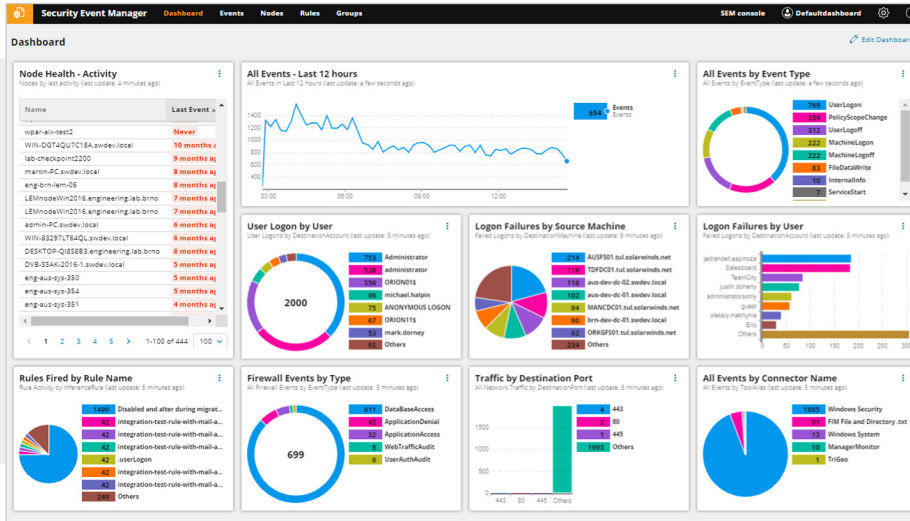


Security Event Manager



Una solución SIEM todo en uno para la recopilación de registros, almacenamiento, análisis y generación de informes diseñados para ayudar a los profesionales de TI a identificar y responder a la ciberamenazas y demostrar el cumplimiento.

Miles de profesionales de seguridad y de TI con recursos limitados confían en SolarWinds® Security Event Manager (SEM) para lograr una detección de amenazas, análisis y respuesta ante incidentes automatizados e informes sobre cumplimiento eficientes y rentables. Nuestro SIEM todo en uno combina administración de registros, detección de amenazas, normalización y correlación, reenvío, informes, monitoreo de la integridad de los archivos, monitoreo de la actividad de los usuarios, detección y prevención de USB, investigación sobre amenazas y respuesta activa en un dispositivo virtual fácil de implementar, administrar y usar. Hemos diseñado nuestro SIEM para brindarle la funcionalidad que necesita sin la complejidad ni el costo de la mayoría de las demás soluciones de SIEM.

BAJAR PRUEBA GRATIS

Totalmente funcional por 30 días

SECURITY EVENT MANAGER DE UN VISTAZO

- » Recopila, consolida y estandariza registros y eventos desde firewalls, dispositivos y aplicaciones IDS/IPS, conmutadores, routers, servidores, registros de sistema operativo y otras aplicaciones.
- » Realiza correlaciones en tiempo real de datos de máquinas para identificar las amenazas y los patrones de ataque.
- » Actúa ante actividad sospechosa de manera automática con Active Response, que incluye bloqueo de dispositivos USB, detención de procesos maliciosos, cancelación de sesión de usuarios, etc.
- » Facilita los informes y las auditorías sobre cumplimiento con informes y listas para usar para HIPAA, PCI DSS, SOX, ISO, DISA STIGs, FISMA, FERPA, NERC CIP, GLBA, etc.
- » La interfaz intuitiva y la amplia selección de contenido listo para usar le permiten no tener que ser un experto en seguridad ni en cumplimiento para obtener todo el valor de nuestra solución SIEM
- » Licencias asequibles y escalables basadas en fuentes emisoras de registros no en volumen de registros

Recopilación y normalización fáciles de dispositivos de red y registros de máquina

Security Event Manager incluye cientos de **conectores listos para usar** que el proceso de recopilar, estandarizar y catalogar datos y registros de eventos generados en su red. Nuestra tasa de compresión de registros líder del sector permite almacenar más datos con menos recursos.

Panel y vistas personalizables

Identifique rápidamente patrones importantes o sospechosos en datos de máquinas con una amplia variedad de visualizaciones personalizables y un panel flexible. Investigue en profundidad en patrones interesantes con un clic y vea toda la lista de registros relacionados y sus detalles.

Búsquedas simples y potentes para análisis forenses y detección y solución de problemas

Security Event Manager se ha diseñado para permitir a los usuarios encontrar rápidamente datos de registros importantes mediante búsquedas de palabras clave sencillas en datos de eventos en tiempo real además de en datos históricos en periodos de tiempo predefinidos o personalizados. Los filtros listos para usar o de datos rápido.

Correlación de eventos en memoria en tiempo real

Mediante el procesamiento y la normalización de los datos de registros antes de que se escriban en la base de datos, Security Event Manager puede brindar correlación de eventos y registros en tiempo real. Las reglas de correlación predefinidas y personalizadas permiten a Security Event Manager alertar automáticamente sobre brechas de seguridad potenciales y otros problemas críticos.

Plantillas listas para usar de informes de cumplimiento y seguridad

Con Security Event Manager es fácil generar y programar informes de cumplimiento con rapidez usando más de 300 plantillas de informes y una consola que le permite personalizar los informes en función de su organización.

Grupos y fuente de investigación sobre amenazas

Las reglas de correlación están mejoradas con una fuente de investigación sobre amenazas plenamente integrada que se actualiza con regularidad y que automáticamente detecta y etiqueta la actividad maliciosa desde IP maliciosas conocidas. Cree fácilmente grupos que contengan valores pertinentes para su entorno, como nombres de usuario y computadora, ubicaciones de archivos esenciales y dispositivos USB aprobados. Estos grupos se pueden autocompletar a través de reglas de correlación y pueden alertar a los administradores de sistemas a través de la generación de informes.

Respuesta activa integrada

Security Event Manager puede hacer mucho más que activar alertas de correo electrónico. SEM se ha diseñado para responder de manera inmediata a eventos de seguridad, operativos y activados por políticas mediante respuestas predefinidas, como poner en cuarentena máquinas infectadas, bloquear direcciones IP, detener procesos sospechosos y la configuración de Active Directory®.

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

El monitoreo de la integridad de los archivos incrustado (FIM) brinda compatibilidad más amplia con el cumplimiento e inteligencia de seguridad más exhaustiva para amenazas internas, malware de día cero y otros ataques avanzados. Aproveche las capacidades de FIM mejoradas para un mejor ajuste y reduzca drásticamente el desorden asociado con cambios en archivos de baja prioridad, lo que aumenta la productividad.

BAJAR PRUEBA GRATIS

Totalmente funcional por 30 días

Prevención y detección de USB

Security Event Manager lo ayuda a prevenir la pérdida de datos de punto y protege la información con 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.

Reenvío y exportación de registros

Security Event Manager reenvía datos de registros sin procesar (RFC3164 y RFC 5244) a otras aplicaciones para su uso posterior. Además, los usuarios pueden exportar los registros a un archivo CSV de modo que los datos se puedan compartir con otros equipos y proveedores externos, descargarse en otras herramientas o adjuntarse a tickets del servicio de ayuda.

Analice datos históricos

Seleccione tendencias clave mediante el análisis de datos históricos a través de búsquedas de eventos de red El generador de consultas intuitivo presenta consejos y recomendaciones a medida que introduce los parámetros de la consulta. Después, el histograma de eventos y el selector de tiempo personalizado le permite enfocarse en r

BAJAR PRUEBA GRATIS

Totalmente funcional por 30 días

REQUISITOS DEL SISTEMA DE SECURITY EVENT MANAGER

Para ver todos los requisitos del sistema y determinar el tamaño de la implementación, consulte los requisitos del sistema SEM [en la guía de instalación o actualización SEM](#).

REQUISITOS DEL SISTEMA DE SECURITY EVENT MANAGER

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 Security 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 (NYSE:SWI) es un proveedor líder de software de administración de infraestructuras de TI eficaz y asequible. Nuestros productos ofrecen a las organizaciones de todo el mundo, con independencia del tipo, el tamaño y la complejidad de la infraestructura de TI, la capacidad de monitorear y administrar el desempeño de sus entornos de TI, en modelos locales, de nube o híbridos. Interactuamos continuamente con todo tipo de profesionales de TI (profesionales de operaciones de TI, de DevOps y proveedores de servicios gestionados) para comprender los retos que enfrentan a la hora de mantener infraestructuras de TI de alto desempeño y disponibilidad. La información que obtenemos a través de esta interacción como, por ejemplo, mediante nuestra comunidad en línea **THWACK** nos permite crear productos que resuelven los retos conocidos de gestión de TI de la forma que los gestores de tecnología quieren resolverlos. Este enfoque en el usuario y el compromiso de ofrecer la mejor calidad en la gestión integral del desempeño de TI híbrida ha posicionado a SolarWinds como líder internacional en software de gestión de redes y soluciones de MSP. Obtenga más información hoy mismo en www.solarwinds.com.

BAJAR PRUEBA GRATIS

Totalmente funcional por 30 días



PÓNGASE EN CONTACTO CON NOSOTROS

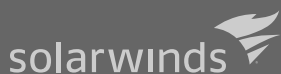
ZALTOR Mayorista de Soluciones TIC

Teléfono: +34 916 625 945

c/Caléndula, 93 - Edif. E - Miniparc III

28109 · El Soto de La Moraleja · Alcobendas · Madrid

Correo electrónico: misp@zaltor.com



© 2020 SolarWinds Worldwide, LLC. Todos los derechos reservados

Las marcas comerciales SolarWinds, SolarWinds & Design, Orion y THWACK son propiedad exclusiva de SolarWinds Worldwide, LLC y es posible que estén registradas o pendientes de registrarse en EE. UU. y en otros países. Todas las demás marcas comerciales, marcas de servicio y logotipos de SolarWinds pueden ser marcas de hecho o estar registradas o pendientes de registro. Todas las demás marcas comerciales aquí mencionadas se utilizan solo para fines de identificación y no pertenecen a sus respectivas compañías (y pueden, incluso, ser marcas registradas de estas).

Este documento no puede ser reproducido, copiado, distribuido, publicado, transmitido, almacenado en un sistema de recuperación de información, o de cualquier otra manera, en forma física o electrónica, sin la autorización por escrito de SolarWinds. Todos los derechos, títulos e intereses relativos al software, los servicios y la documentación son propiedad exclusiva de SolarWinds y sus licenciantes.

SOLARWINDS NO SE HACE RESPONSABLE DE LAS GARANTÍAS, CONDICIONES U OTROS TÉRMINOS, EXPRESOS O IMPLÍCITOS, DE NATURALEZA LEGAL O DE OTRO TIPO, COMO, ENTRE OTROS, LA FALTA DE INFRACCIÓN DE DERECHOS, LA PRECISIÓN, LA EXHAUSTIVIDAD O LA UTILIDAD DE LA INFORMACIÓN INCLUIDA EN EL DOCUMENTO. EN NINGÚN CASO SOLARWINDS, SUS PROVEEDORES O SUS LICENCIANTES SERÁN RESPONSABLES DE DAÑOS, YA SEA QUE SURJAN DE AGRAVIO, CONTRATO U OTRAS TEORÍAS LEGALES, INCLUSO SI SE HUBIERA ADVERTIDO A SOLARWINDS DE LA POSIBILIDAD DE TALES DAÑOS.