EVENTSENTRY

Sepa cuándo necesita actuar.

Brindando información significativa sobre los datos de su red.

EventSentry es una potente solución de supervisión que proporciona a su equipo de TI datos de red procesables que impulsan decisiones de TI inteligentes, en tiempo real. Fiable, seguro, escalable y fácil de implementar, EventSentry mejorará el rendimiento, el cumplimiento y la seguridad de su red. Ahorre tiempo, evite desastres y reduzca el coste total de propiedad con una de las soluciones de supervisión más rentables del mercado. Los nuevos usuarios se ponen en marcha en cuestión de minutos y pueden adaptar fácilmente la solución a sus necesidades, con un galardonado servicio de atención al cliente a su alcance.

CARACTERÍSTICAS PRINCIPALES:

- Correlacione y supervise los registros de eventos y los archivos de registro en tiempo real, así como el rendimiento, el espacio en disco, los servicios, los procesos y mucho más en servidores y estaciones de trabajo físicos y virtuales (en la nube).
- Rastree los cambios de Active Directory™ de cualquier objeto hasta el nivel de atributo, incluidos los cambios de políticas de grupo. Detecte contraseñas comprometidas y duplicadas. Incluye informes de estado de usuario y recordatorios de caducidad de contraseñas para usuarios finales.
- Los informes de cumplimiento y los paneles de control listos para usar, impulsados por un motor de seguridad orientado a Windows™, ayudan a poner en marcha varios requisitos de cumplimiento, como PCI, CMMC, NIST y CJIS.
- Visualice los datos con paneles de control y una potente función de informes y tareas. Los informes admiten autenti-cación granular y búsquedas sofisticadas en los registros..
- Los scripts automatizados de seguridad, conformidad y refuerzo aumentan la seguridad, reducen la superficie de ataque y validan la configuración de conformidad.

COMENTARIOS DE CLIENTES:

"EventSentry se ha convertido rápidamente en una herramienta esencial para supervisar la salud de los sistemas de infraestructuras críticas."
"La navaja suiza de las soluciones de supervisión de redes!"
"Escala muy por encima de la competencia."
"Su servicio de atención al cliente ha sido impecable!"
"Nos pusimos en marcha en cuestión de minutos!"
"Más allá de la supervisión de los registros de sucesos."
"Funciona como se supone."
"La visibilidad de nuestros sistemas era alucinante."

Version 5.2

Para más información, llame al 312.624.7698
www.eventsentry.com

Descripción de características

EVENTSENTRY

Monitoreo y Correlación de Registro
Supervisión y correlación de registros de eventos en tiempo real con detección de anomalías y funciones avanzadas como umbrales, eventos recurrentes, temporizadores, detección de movimientos laterales, puntuación de amenazas y mucho más.

Cumplimiento de Normativas y Seguridad
Realice un seguimiento de la actividad de archivos/registros/procesos, inicios de sesión de consola, inicios de sesión de red correctos o fallidos, gestión de cuentas y mucho más para ayudar con los requisitos de cumplimiento de PCI, CMMC, NIST, CJIS y otros. Gestione automáticamente Sysmon en toda la red.

Monitoreo y Correlación de Archivos de Registro
Supervisa y correlaciona cualquier archivo de registro (por ejemplo, IIS, DHCP, copia de seguridad, cortafuegos) en tiempo real y envía alertas en caso de coincidencia de texto. Cree vistas personalizadas para archivos de registro estructurados.

NetFlow
Visualiza y mejora los datos NetFlow y sFlow con GeoIP, información sobre amenazas y detección de escaneado de puertos. La integración de Sysmon correlaciona la actividad de la red de procesos con NetFlow.

Inventario Extensivo
Realiza un inventario del software instalado, las extensiones del navegador, los parches y la información de hardware, incluido el inventario de máquinas virtuales (VMWare© e Hyper-V©). Muestra asignaciones de puertos de conmutadores físicos e información de hardware gestionado.

Monitoreo Integral de la Salud del Sistema
Realiza un seguimiento de todas las métricas importantes del sistema, como el uso de discos y carpetas, métricas de rendimiento, reinicios, archivos críticos del sistema operativo y mucho más.

Monitoreo de Procesos, Servicios y Tareas Programadas
Supervisa proactivamente servicios, tareas programadas y procesos. Amplio seguimiento y supervisión de la actividad de los procesos (puede requerir Sysmon).

Notificaciones y Correcciones
Envíe notificaciones en tiempo real por correo electrónico o API web, reenviar registros a través de Syslog, enviar trampas SNMP, automáticamente procesos personalizados, scripts, reinicios, control de servicios y mucho más.

Monitoreo Avanzado de Active Directory
Rastrea los cambios en los objetos de AD hasta el nivel de atributo, incluidos los valores anteriores y posteriores, los cambios en las directivas de grupo, los informes de estado de los usuarios y los correos electrónicos de caducidad de las contraseñas. Identifica contraseñas comprometidas y duplicadas.

Inventario de Permisos
Un inventario de permisos NTFS de carpetas seleccionadas que permite identificar rápidamente los permisos de acceso y auditoría asignados a usuarios y grupos.

Agentes Inteligentes y Livianos
Los agentes supervisan sus hosts sin afectar al rendimiento de los hosts supervisados, al tiempo que minimizan el uso del ancho de banda de la red. Los agentes pueden instalarse automáticamente y no tienen dependencias.

Automatización de Seguridad, Cumplimiento de Normativas y Fortalecimiento de seguridad
La colección de scripts de seguridad y estado personalizables detecta configuraciones inseguras, parches y actualizaciones que faltan, infracciones de la normativa y configuraciones erróneas en los servidores y puntos finales supervisados.

Informes Web
Informes web modernos con cuadros de mando, control de acceso granular, informes flexibles, motor de trabajos y herramientas de visualización. Amplia API para acceder a datos de software de terceros. Funciona con los principales navegadores y dispositivos móviles.

Monitoreo de Latidos
Supervisa de forma centralizada el tiempo de actividad de hosts y servicios TCP y proporciona estadísticas de disponibilidad.

Syslog/SNMP/ARP Daemon
Recoge mensajes Syslog y traps SNMP (v1-v3) de forma centralizada desde hosts Unix/Linux y/o dispositivos de red. Las alertas que coincidan con las reglas configuradas pueden enviarse en tiempo real.

MIA: Monitoreo de la Integridad de Archivos
Rastrea sumas de comprobación, tamaño, versión, entropía y firmas de archivos críticos para detectar y rastrear cambios. Las alertas en tiempo real y la generación de informes los requisitos de seguridad.

Version 5.2

Para más información, llame al 312.624.7698
www.eventsentry.com