Microsoft GOLD CERTIFIED Partner

GFI EventsManager

Monitorización, administración, y archivo de sucesos

■ Miles de instalaciones a clientes

¡Monitorización, administración, y archivo de sucesos sencilla!

El enorme volumen de los sucesos de sistema generados diariamente es para las organizaciones una valiosa fuente de información para cumplir obligaciones legales y reguladoras y para dirigir los riesgos de la seguridad de TI. Las crecientes amenazas para la continuidad de los negocios exigen una estrategia que incluya monitorización en tiempo real de la red y además la capacidad de generar informes y de analizar esta información para cumplir las rigurosas y más demandadas obligaciones legales o reguladoras.

Esta es, sin embargo, una tarea abrumadora sin las herramientas apropiadas. Con miles de clientes y a precios competitivos, GFI EventsManager™ 8 alivia la carga de los administradores y simplifica la complejidad de la gestión, archivado y generación de informes sobre sucesos.

GFI EventsManager es una solución de monitorización, administración y archivo de sucesos que ayuda a las organizaciones a ajustarse al cumplimiento legal y regulador tal como SOX, PCI DSS e HIPAA. Este galardonado software soporta un amplio rango de tipos de suceso tales como W3C, sucesos Windows, Syslog y, en la última versión, traps SNMP generador por dispositivos tales como cortafuegos, enrutadores y sensores así como dispositivos genéricos.

Proporcionando soporte para dispositivos de los 20 principales fabricantes del mundo así como dispositivos a medida, GFI EventsManager le permite monitorizar una amplia familia de productos hardware, generar informes sobre el estado operativo de cada uno y recoger información para el análisis.

BENEFICIOS

- **Centraliza los sucesos Syslog, W3C, Windows y SNMP Traps generados por cortafuegos, servidores, enrutadores, switches, sistemas telefónicos, PCs y más**
- **Incrementa el tiempo de actividad e identifica problemas mediante alertas en tiempo real**
- **Monitorización y administración de toda la red rápida y económica**
- **Auditoría SQL Server para SQL Server 2000, 2005, 2008 y también MSDE y SQL Express**
- **Rendimiento sin igual de escaneo de sucesos de hasta 6 millones de sucesos por hora**
- **Certificado para Windows Server 2008; Soporta Windows Vista**

Alertas en tiempo real - incluyendo alertas SNMPv2

La más reciente compilación de GFI EventsManager mejora el nivel de alertas cuando se detectan en la red sucesos importantes o intrusiones. GFI EventsManager le permite activar acciones tales como ejecución de secuencias de comandos o envío de alertas a una o más personas por correo electrónico, mensajes de red y notificaciones SMS enviadas mediante una pasarela o servicio de correo-a-SMS y ahora SNMPv2. La generación de alertas SNMP también permitirá a los administradores integrar GFI EventsManager con mecanismos de monitorización pre existentes o genéricos.

Instalación y funcionalidad

La última compilación de GFI EventsManager ha sido optimizado para proporcionar a los usuarios un proceso de instalación mejorado. Algunos de los cambios incluyen optimización de varias partes ejecutables del producto, documentación de instalación actualizada, nuevas guía de inicio rápido para ayudarle a agregar orígenes de sucesos, crear reglas y trabajar más rápida y eficazmente con operaciones de base de datos así como la capacidad de descargar e instalar el ReportPack desde la página de informes. El ReportPack contiene también informes específicos para el estándar de la Industria de Tarjetas de Pago (PCI).

Vea informes sobre información clave de seguridad que están ocurriendo en su red

El generador de informes de GFI EventsManager, que se entrega con el producto, le permtie crear o personalizar informes, incluyendo informes estándar, tales como:

- Informes de la Industria de Pagos con Tarjeta (PCI)
- Informes de uso de cuentas
- Informes administrativos de cuentas
- Informes de cambios de directiva
- Informes de acceso a objetos
- Informes administrativos de aplicaciones
- Informes de servidor de impresión
- Infomes de sistema del registro de sucesos Windows
- Informes de tendencias de eventos

Registro de sucesos centralizado

Los registros de sucesos son contánte y automáticamente generados por los usuarios o por procesos automáticos/de segundo plano y a menudo son almacenados en lugares distintos. GFI EventsManager almacena todos los registros de sucesos capturados en una base de datos SQL que además puede ser remota. También puede configurar copias de seguridad programadas de sus registros de sucesos.

Análisis de registros de sucesos incluyendo SNMP Traps, registros de Sucesos Windows, registros W3C y Syslog

Como administrador de red usted ha experimentado los crípticos y voluminosos logs que hacen abrumador el proceso de análisis. GFI EventsManager es una solución de procesamiento de registros que proporciona control y administración en toda la red de registros de sucesos Windows, registros W3C y eventos Syslog generados por sus recursos de red. GFI EventsManager ya soporta Protocolo Simple de Administración de red (SNMP) versión 3 que es el idioma hablado por los dispositivos de bajo nivel como enrutadores, sensores, cortafuegos, etc. Mediante SNMP los usuarios pueden ahora monitorizar una completa familia de dispositivos hardware en sus infraestructuras con la habilidad de generar informes sobre el estado operativo de cada dispositivo.

Certificado para Windows Server 2008; Soporta Vista

GFI EventsManager ha conseguido el estado 'Certificado para Windows Server 2008' y se puede instalar en, y recoger sucesos de Windows Vista y Windows 2008. Aunque estas nuevas plataformas utilizan un formato diferente de registro, GFI EventsManager presenta los sucesos de varios sistemas operativos de la misma forma, permitiendo al usuario acostumbrarse a una estructura común, irrespectivamente de la plataforma monitorizada. GFI EventsManager también soporta Windows 2000, Windows XP y Windows 2003.

Control granular más profundo de sucesos

GFI EventsManager le ayuda a monitorizar una mayor familia de sistema y dispositivos mediante el registro y análisis centralizado de varios tipos de registro incluyendo sucesos Windows, Syslog, W3C y ahora SNMP Traps que son generados por recursos de red. Los administradores puede recoger información de equipos Windows y de dispositivos de terceros con un mayor nivel de granularidad y además procesa la información del nivel extendido de etiquetas y basa la decisión sobre qué hacer en el acto, sin mayor gestión de información.

Consola de administración de GFI EventsManager

Consola de Inicio Rápido de GFI EventsManager

Requerimientos del sistema

- **Requerimientos del Sistema - Equipos de Instalación:** .NET Framework 2.0., Microsoft Windows 2000, XP, 2003 o 2008, Soporte de MS SBS 2003 & 2008 (MS SBS no requerido), Microsoft Data Access Components (MDAC) 2.8 o posterior, Access, MSDE o MS SQL Express (Gratuito y descargado automáticamente durante la instalación), o MS SQL Server 2000 , 2005 o 2008.
- **Requerimientos del software – Equipos Escaneados:** Escaneo de registros de sucesos Windows: El servicio Rgistro Remoto debe estar habilitado, el servidio de auditoría de Windows deber estar habilitado, los equipos VISTA deben estar en el mismo dominio del servidor escáner así como UAC deshabilitado, escaneo de registros W3C: Las carpetas deben ser accesibles vía recursos compartidos Windows.
- **Syslog y SNMP Traps:** Los orígenes/remitentes deben ser configurados para enviar mensajes al equipo/dirección IP en el que esté instalado GFI EventsManager

↓ Para más información y para descargar su versión de evaluación gratuita por favor visite http://www.gfihispana.com/es/eventsmanager/

GFI

Microsoft GOLD CERTIFIED Partner