GFI EventsManager

Gestione dei log degli eventi, protezione e monitoraggio centralizzati

I log degli eventi costituiscono uno strumento prezioso per controllare la protezione e le prestazioni della rete, e sono spesso sottoutilizzati per via della loro complessità e del loro volume. Man mano che le organizzazioni si ingrandiscono, richiedono un approccio più strutturato alla gestione e conservazione dei log di eventi. Una recente indagine, condotta dal SANS Institute, ha rilevato che il 44% degli amministratori di sistemi conserva i log per non oltre un mese.

Una gestione dei log adeguata aiuta a conseguire numerosi obiettivi, compresi:

- la protezione del sistema informatico e della rete
- il monitoraggio dello stato di salute del sistema
- la conformità a leggi e normative
- le indagini legali

GFI EventsManager raccoglie dati da tutti i dispositivi che si avvalgono di log degli eventi di Windows, W3C e Syslog e, per identificare dati fondamentali, applica le regole e il filtraggio migliori del settore. In questo modo, è possibile sapere quando il personale inserisce un portachiave digitale, alza la cornetta per telefonare a casa, accende il computer, nonché si è in grado di sapere quello che il personale fa sul computer e i file cui ha avuto accesso durante la giornata lavorativa. GFI EventsManager invia inoltre avvisi in tempo reale non appena si verificano eventi critici di sistema e di sicurezza e suggerisce azioni correttive.

Benefici

Perché adoperare GFI EventsManager?

- Perché centralizza gli eventi Syslog, W3C e Windows generati da firewall, server, router, commutatori, centralini telefonici, PC e altro
- Perché il programma di configurazione guidata semplifica la gestione e manutenzione da parte dell'utente finale
- Per le prestazioni di scansione degli eventi - senza rivali - scalabili fino a oltre 6 milioni di eventi all'ora
- Per le regole di elaborazione di eventi preconfigurate, che consentono una classificazione e gestione degli eventi immediata ed efficace
- Per il monitoraggio costante dell'attività degli eventi e l'invio di avvisi automatizzati
- Per le potenti capacità di reporting, che offrono un monitoraggio dell'attività della rete efficace e un ROI (ritorno sull'investimento) immediato.

Semplificazione dell'analisi dei log di eventi di tutta la rete

In veste di amministratore di rete, ci si sarà sicuramente trovati di fronte a log voluminosi ed enigmatici, che avranno scoraggiato il processo di analisi degli stessi. GFI EventsManager è una soluzione di elaborazione dei log che offre il controllo e la gestione, su tutta la rete, dei log di eventi di Windows, di W3C ed eventi Syslog, generati dalle risorse di rete. GFI EventsManager comprende un processore di eventi intelligente che elabora i log e presenta le informazioni in modo centralizzato, facile e user-friendly.

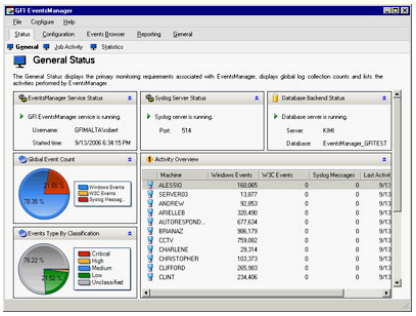
"Traduzione" degli eventi di Windows dal significato "enigmatico"

Log enigmatici allungano il processo di analisi. GFI EventsManager “traduce” le descrizioni spesso enigmatiche degli eventi in spiegazioni e consigli chiari e concisi sugli eventuali provvedimenti da adottare.

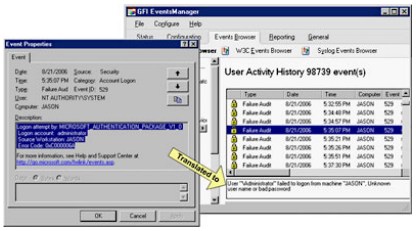
Registrazione centralizzata degli eventi

I log di eventi sono generati continuamente e in modo automatico da un utente o da un processo automatico o in background, e i log sono spesso archiviati in diverse locazioni. GFI EventsManager archivia tutti i log di eventi acquisiti su un unico database SQL, che può anche risiedere in remoto. Inoltre, è possibile configurare backup pianificati dei propri log di eventi.

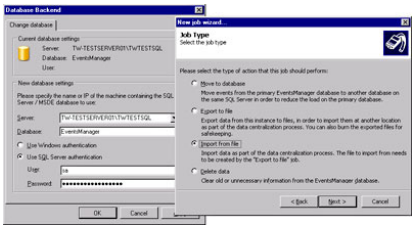
GFI EventsManager



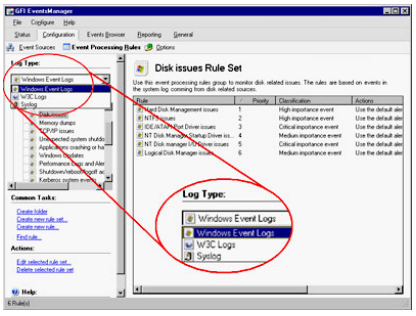
Consolle di gestione di GFI EventsManager



Migliore comprensione dei log cifrati/enigmatici

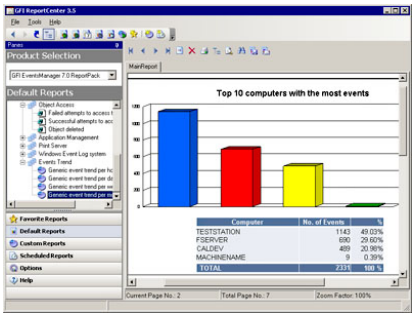


Registrazione centralizzata degli eventi



Supporto di diversi tipi di log (log di eventi di Windows, W3C, Syslog)

GFI EventsManager ReportPack



Rapporto che illustra i primi 10 computer che generano eventi

Motore di scansione dalle prestazioni elevate

GFI EventsManager incoropora un motore di scansione degli eventi completamente riprogettato, del tutto sintonizzato per offrire le massime prestazioni di scansione. Test dimostrano che è in grado di eseguire la scansione e raccogliere fino a 6 milioni di eventi all'ora. Inoltre, la sua metodologia "plug-in" consente l'integrazione di ulteriori caratteristiche e moduli, senza che si verifichino interferenze con il codice esistente.

Avvisi in tempo reale

GFI EventsManager è in grado di inviare avvisi quando individua eventi critici o intrusioni. Si possono attivare azioni quali script o inviare avvisi ad almeno un soggetto tramite email, messaggi di rete e notifiche SMS inviate tramite un gateway o servizio "email verso sms".

Ampio supporto di log di eventi

GFI EventsManager elabora vari tipi di log degli eventi, ivi compresi log di eventi di Windows, Syslog e W3C. Di conseguenza, è possibile raccogliere più dati dai vari sistemi hardware e software più comuni su una tipica rete aziendale.

Raccolta, in un singolo database centrale, dei dati degli eventi distribuiti su una WAN

Il modulo Database Operations (Operazioni di database) consente di raccogliere in un database centrale i dati degli eventi dalle installazioni di GFI EventsManager situate in più sedi e locazioni della rete. Così, è possibile monitorare con facilità migliaia di stazioni di lavoro e di server su tutta la rete, senza che ne risentano l'utilizzo di larghezza di banda e/o di memoria. Tale componente aggiuntivo, da acquistare separatamente, integra e centralizza gli eventi raccolti ed elaborati, e consente di eseguire il salvataggio in back-up o di ripristinare gli eventi su richiesta. Grazie alle operazioni di database si può gestire la dimensione del database stesso, senza dover intervenire manualmente, non soltanto attraverso la centralizzazione, ma anche grazie alla possibilità di esportare gli eventi e salvarli in backup a seconda delle necessità.

Gestione dei log di eventi basata su regole

GFI EventsManager è provvisto di una serie preconfigurata di regole di elaborazione, che consente di filtrare e classificare eventi che soddisfano determinate condizioni. È possibile adoperare tali regole predefinite senza eseguire ulteriori configurazioni oppure si può scegliere di personalizzarle o crearne di nuove, per adeguarle all'infrastruttura della propria rete.

Caratteristiche avanzate di filtraggio degli eventi

Il potente filtro di GFI EventsManager "passa al setaccio" i log di eventi registrati e consente di sfogliare quelli desiderati senza eliminare alcun record dal terminale database. È inoltre possibile evidenziare in modo selettivo eventi specifici, adoperando un colore o lo strumento di ricerca integrato.

Profili di scansione dei log di eventi

I profili di scansione consentono di configurare la serie di regole di monitoraggio degli eventi da applicare a un computer o gruppo di computer, e forniscono un modo centralizzato per mettere a punto l'ottimizzazione delle regole di elaborazione dei log di eventi. Si può anche impostare una serie di regole da applicarsi unicamente alle stazioni di lavoro di un determinato reparto. Questo software offre altresì la possibilità di creare profili complementari distinti, che forniscono regole supplementari e più specializzate, computer per computer.

Visualizzazione dei rapporti sulle principali informazioni di sicurezza che si verificano sulla rete

Con il generatore di rapporti di GFI EventsManager, è possibile creare o personalizzare i rapporti, compresi quelli standard, quali:

- rapporti sull'utilizzo dell'account
- rapporti sulla gestione dell'account
- rapporti sulle variazioni dei criteri
- rapporti sull'accesso agli oggetti
- rapporti sulla gestione delle applicazioni
- rapporti sul server di stampa
- rapporti sul sistema dei log degli eventi di Windows
- rapporti sull'andamento degli eventi

Ausilio nell'ottemperanza alle norme PCI DSS e ad altri regolamenti

A decorrere dal settembre 2007, tutte le aziende che gestiscono dati di titolari di carte di credito, indipendentemente dalle dimensioni delle aziende stesse, sono tenute all'osservanza di rigide norme di sicurezza emanate dalle maggiori società di carte di credito mondiali. La registrazione dei dati è fondamentale per rispettare i requisiti PCI DSS, poiché i log (registri) forniscono "audit trail" di tutte le attività eseguite in un ambiente di dati di titolari di carte di credito; di conseguenza, un sistema completo di gestione dei log come GFI EventsManager fornisce le funzionalità necessarie per poter ottemperare alle norme PCI DSS.

Un "coltellino svizzero" per soddisfare le varie esigenze aziendali

GFI EventsManager aiuta l'azienda ad occuparsi delle seguenti 4 aree:

- Protezione del sistema informatico e della rete, in quanto rileva intrusi e violazioni di sicurezza
- Monitoraggio stato di salute del sistema, poiché controlla i server attivamente
- Conformità a leggi e normative, in quanto è un ausilio per ottemperare alle normative in materia di conservazione di registrazioni!
- Indagini legali, poiché rappresenta un punto di riferimento per quando qualcosa va storto.

Altre caratteristiche:

- rimozione degli eventi di disturbo (noise) o irrilevanti che costituiscono una grossa quota di tutti gli eventi di sicurezza
- monitoraggio e avvisi in tempo reale e continui
- controllo grafico dello stato di GFI EventsManager e della rete grazie al monitor di stato interno
- pianificazione dei rapporti e distribuzione automatica via email.

Molti altri ci hanno scelto...

Molte aziende importanti hanno scelto GFI EventsManager. Ecco solo alcuni esempi: Primerica, Pepsico France, Royal & Sunalliance USA Inc., ATP, Ceridian Canada e molte altre.

Requisiti di sistema

- .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.6 o successivi
- Accesso a MSDE/SQL Server 2000 o successivi

Premi

Scaricate la copia di valutazione da http://www.gfi-italia.com/eventsmanager/

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Software GmbH
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49 (0)40 3068 1000
Fax +49 (0)40 3068 1010
sales@gfisoftware.de

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

www.gfi.com

© 2008 GFI Software – Windows Vista, 2003, XP, 2000 e NT sono marchi commerciali di Microsoft Corporation.
GFI EventsManager è un marchio commerciale registrato e GFI e il logo GFI sono marchi commerciali di GFI SOFTWARE in Germania, negli Stati Uniti, nel Regno Unito e in altri paesi.
Tutti i prodotti e le aziende nominati nel presente documento possono essere marchi commerciali dei rispettivi proprietari.