GFI LANguard

Security Event Log Monitor

Scoperta d'intrusione basata sui log degli eventi e gestione dei log degli eventi

Molte compagnie erroneamente suppongono che un accesso non autorizzato possa essere tentato solo da gruppi estranei. Attualmente invece, la maggioranza delle minacce per la sicurezza delle società proviene da sorgenti interne, e contro cui un firewall non offre alcuna protezione. GFI LANguard S.E.L.M. controlla i log del sistema di sicurezza di tutti i vostri server e workstation Windows NT/2000/XP/2003, e vi avvisa in tempo reale di eventuali intrusioni/attacchi.

GFI LANguard S.E.L.M. possiede un motore per l'analisi degli eventi della sicurezza che tiene conto di ciascun evento di sicurezza e di altre informazioni quali, livello di protezione di ciascun computer, quando l'evento accade (fuori o durante l'orario di lavoro), ruolo del computer ed il suo sistema operativo (workstation, server o domain controller). Basandosi su queste informazioni, GFI LANguard S.E.L.M. può decidere se l'evento della sicurezza ha un livello critico, alto, medio o basso. In questo modo è possibile affrontare velocemente gli importanti eventi della sicurezza senza esserne un esperto e conoscendo ciascun evento di Windows.

Oltre ad analizzare i log degli eventi della sicurezza, GFI LANguard S.E.L.M. può anche analizzare i log delle applicazioni, del sistema ed altri eventi. È possibile mantenere o cancellare i log degli eventi su tutte le macchine remote del vostro network automaticamente; e vedere, riportare e filtrare gli eventi di tutto il network, invece che una macchina alla volta. Dato che GFI LANguard S.E.L.M. riporta tutti gli eventi in un database centrale, è facile creare rapporti e filtri personali. Usando le regole personalizzate, potete creare i vostri propri allarmi basati su ID dell'evento, condizioni e contenuti. GFI LANguard S.E.L.M. è l'unico prodotto per la gestione degli eventi in grado di analizzare il contenuto e le proprietà di un evento. Inoltre GFI LANguard S.E.L.M. vi consente di creare dei rapporti per una conoscenza più dettagliata del vostro network.

L'analisi dei log di eventi dei grandi network è stata semplificata

- "Traduce" le descrizioni spesso criptiche degli eventi in un linguaggio chiaro, fornisce spiegazioni coincise, e suggerimenti di azioni
- Rimuove gli eventi di "disturbo" che rappresentano gran parte di tutti gli eventi della sicurezza
- Risolve i problemi della manomissione dei log file per la sicurezza
- Fornisce controllo e notifiche in tempo reale
- Risolve il problema della frammentazione delle tracce di verifica consolidando tutti gli eventi di sicurezza in unico database.

Caratteristiche fondamentali & benefici

Scoprire gli attacchi al vostro network in tempo reale

Controllare gli utenti che tentano di accedere alle condivisioni protette ed ai file confidenziali

Creare degli allarmi per eventi specifici e condizioni che accadono sul vostro network

Back up e rimozione degli eventi automaticamente sulle macchine remote

Archiviare i log degli eventi in un database centrale.

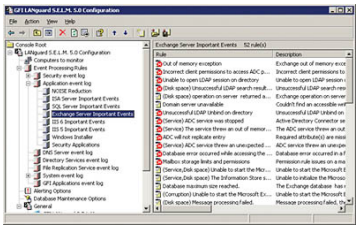
Controlla Microsoft ISA Server, Exchange Server & SQL server

Usando GFI LANguard S.E.L.M., potete controllare i vostri server mission-critical (missione-critica). Controlla gli eventi generati da Microsoft ISA Server, Exchange Server e SQL Server e previene il verificarsi di situazioni disastrose per il network. Per esempio, potete controllare la coda dell'email, i gateway SMTP, la disponibilità MAPI, gli hard disk inefficienti, lo spazio sul disco, ed altro.

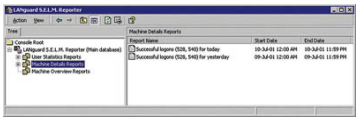
Visualizza i rapporti sulle informazioni chiave per la sicurezza che accadono sul vostro network

Il modulo dei rapporti di GFI LANguard S.E.L.M. vi permette di identificare le tendenze della sicurezza. Utilizzate i rapporti standard - che potete personalizzare - o create rapporti personalizzati. I rapporti standard includono:

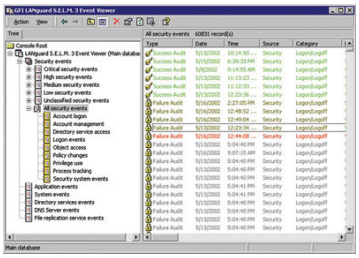
- Tutte le connessioni fallite
- Utenti che hanno fallito la connessione per un errore del nome utente o nella password
- Tutti i blocchi dell'account per un periodo di tempo
- Connessione giornaliera iniziale per ogni utente al di fuori di un periodo di tempo
- I computer a cui gli utenti connessi
- Possibili manomissioni dei log della sicurezza per un periodo di tempo
- Eventi di accesso fallito (per esempio, tentativi di accesso a file protetti)
- Eventi di alta sicurezza per i passati giorni, settimane o mesi.



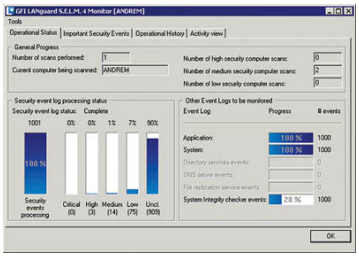
Configurazione snap-in della MMC di GFI LANguard S.E.L.M.



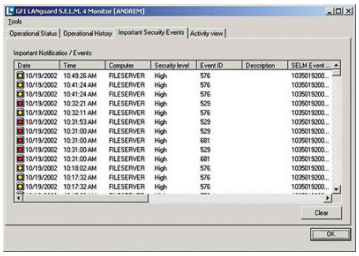
Visualizzare i rapporti su informazioni chiave della sicurezza che accadono sul vostro network



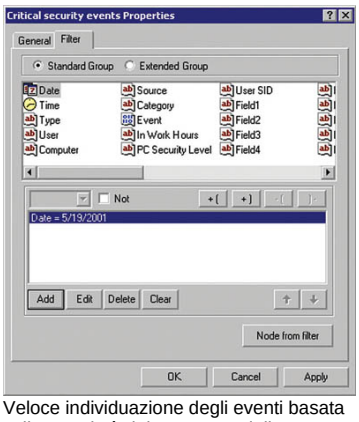
Filtro avanzato degli eventi della sicurezza usando l'Event Viewer di GFI LANguard S.E.L.M.



Monitor d'intrusione e dello della raccolta degli eventi



Notifica immediata di eventi critici



Veloce individuazione degli eventi basata sulle proprietà del contenuto dell'evento

Allarmi in tempo reale

GFI LANguard S.E.L.M. può inviarvi dei messaggi di allarme quando sono scoperte intrusioni o eventi critici. È possibile allertare una o più persone tramite e-mail, oppure inviare un SMS o avvisi di cercapersone tramite il gateway SMS. Gli eventi critici sono inoltre, anche visualizzati nel monitor delle intrusioni.

Filtraggio avanzato degli eventi utilizzando il Visore di Eventi di GFI LANguard S.E.L.M.

Il visore di eventi di Microsoft Windows ha caratteristiche limitate, e può visualizzare solo un computer per volta. Il Visore di Eventi di GFI LANguard fornisce una singola visualizzazione di tutti gli eventi relativi a tutti i vostri computer, ed inoltre offre capacità di filtraggio avanzate. Per esempio, è possibile effettuare un filtraggio basato su un determinato utente, computer, livello di sicurezza del PC, e descrizione/proprietà dell'evento. È contenuta inoltre una condizione che vi consente di creare filtri avanzati o combinazioni delle varie variabili.

Scopre gli intrusi e le brecce nel sistema di sicurezza: Il modo giusto è la scoperta delle intrusioni!

GFI LANguard S.E.L.M. agisce come un sistema di scoperta d'intrusione basato su host che analizza gli eventi della sicurezza in tempo reale. In questo modo è possibile trovare gli intrusi e le brecce nel sistema di sicurezza senza installare un sistema di rilevazione di intrusione basato sul network (IDS). I prodotti per network basati su IDS sono costosi e difficili da dispiegare.

Scalabile per supportare reti WAN e LAN

GFI LANguard S.E.L.M. ha un agente per la registrazione dei log di eventi molto efficiente, che consente una catalogazione degli eventi in tempo reale e senza appesantire le prestazioni del network. Per network di dimensioni elevate o WAN, la scansione degli eventi può essere distribuita mediante installazioni multiple di GFI LANguard S.E.L.M., che possono essere connesse tra loro tramite il connettore WAN. In questo modo, ogni singola installazione di GFI LANguard S.E.L.M. monitorerà una specifica sezione della rete LAN o WAN e riporterà gli eventi critici/importanti per tale "sezione". Il connettore quindi, inoltra tali eventi al database centrale di GFI LANguard S.E.L.M. Questo riduce il traffico della rete, l'utilizzo della banda e lo spazio per la registrazione, consentendo inoltre, di monitorare decine di migliaia di server e di workstation, oltre ai collegamenti WAN.

Gestione dei log degli eventi basata su regole

GFI LANguard S.E.L.M. include una potente interfaccia per l'uso di regole, che permette di impostare facilmente delle regole per gli eventi basate sull'ID, sulle condizioni e il contenuto delle proprietà di un evento. Per esempio, è possibile ricevere una notifica immediata se un particolare utente prova ad eseguire connessioni più di un certo numero di volte, o se tenta di accedere ad un file particolare. È possibile anche utilizzare il wizard delle regole per controllare le applicazioni personali o di terzi.

Controlla l'accesso a file importanti

Per mezzo dell'analisi degli accessi falliti ai file, potete controllare chi sta tentando di accedere a quei file. Questo vi permette di anticipare in modo più ampio gli 'attacchi' alla rete e i tentativi d'intrusione degli hacker basati su tecniche a sfondo sociale. GFI LANguard vi permette inoltre di esaminare gli accessi riusciti ai file, significando che potete registrare chi ha avuto accesso ai file e quando. È possibile, inoltre, controllare quando sono avviati alcuni processi.

Altre caratteristiche

- Controllo dello stato delle intrusioni e della collezione degli eventi
- Supporti per Access, SQL Server e MSDE
- Monitoraggio e pianificazione in tempo reale
- Scoperta delle intrusioni del server web
- Scoperta delle modifiche a file importanti sia su workstation che sui server.

Molti altri ci hanno scelto…

Molte delle principali aziende hanno scelto GFI LANguard S.E.L.M. Le seguenti sono solo alcune di loro: Royal & Sunalliance USA Inc., Primerica, Pepsico France, UOB Group/UOB Bank, Airline Tariff Publishing, Orange County Sheriff IMS, Ceridian Canada, Johns Hopkins University School of Medicine, e molte altre.

Recensioni

GFI LANguard S.E.L.M. named "Best of 2002" - GFI LANguard Security Event Log Monitor has won SC Magazine's Best of 2002 award.

- Secure Computing Magazine, December 2002

GFI LANguard S.E.L.M. awarded NSS Approved logo - The NSS Group has reviewed GFI LANguard Security Event Log Monitor and awarded it the NSS Approved logo that is granted only to products that the group is happy to recommend. In a detailed review, the NSS Group found that GFI LANguard S.E.L.M. enables administrators to perform detailed analysis of Windows security event logs, providing them with real-time security alerts.

- The NSS Group, October 2001

Requisiti del sistema

- Windows 2000 Pro o Server, Windows XP o Windows 2003.
- I server ed i client da controllare devono essere avviati su Windows NT, 2000, XP or 2003.

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

GFI Software Ltd UK
5, Princeton Mews
167-169 London Road
Kingston-upon-Thames
Surrey KT2 6PT, UK
Tel +44 (0) 870 5370
Tel +44 (0) 870 5377
sales@gfi.co.uk

GFI Software USA, Inc.
201 Towerview Court
Cary, NC 27513
USA
Tel +1 (888) 2 GFIFAX
Fal +1 (919) 388 5621
sales@gfiusa.com

GFI Software GmbH
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49(0) 700306810 00
Fax +49(0) 700306810 10
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 Ltd
GFI House
San Andrea Street
San Swann SGN 05 Malta
Tel +356 2138 2418
Fax +356 2138 3419

www.gfi.com

©2003 GFI Software Ltd. - Windows XP/2000/NT are trademarks of Microsoft Corporation.
GFI LANguard Security Event Log Monitor is a registered trademark, and GFI and the GFI logo are trademarks of GFI Software Ltd. in Germany, USA, the United Kingdom and other countries.