GFi LANguard

Security Event Log Monitor

Event log based intrusion detection & event log management

Multe companii presupun, in mod eronat, ca accesul neautorizat provine doar din exterior. Realitatea este ca majoritatea amenintarilor intr-o organizatie provin din interior, de la utilizatorii care acceseaza date confidentiale, si impotriva carora firewall-ul instalat la intrarea in retea nu ofera protectie. Si in plus, este necesara o modalitate de a verifica daca firewall-ul chiar blocheaza toate atacurile provenite din exterior. GFI LANguard S.E.L.M. monitorizeaza jurnalele de securitate de pe serverele si statiile Windows NT/2000/XP si transmite alerte in timp real despre posibilele tentative de intruziune/atac.

Pe lânga jurnalele de securitate, GFI LANguard S.E.L.M. poate analiza jurnalele aplicatiilor, jurnalele sistem si orice alte jurnale specificate. Se pot creea copii de siguranta si se pot sterge jurnalele de pe toate masinile din retea in mod automat; se pot creea rapoarte, filtra evenimentele din intreaga retea, nu doar pentru o masina. GFI LANguard S.E.L.M. aduna toate evenimentele intr-o singura baza de date centrala. Astfel, este mai usor sa creati rapoarte pentru intreaga organizatie, precum si filtre personalizate. Folosind reguli personalizate, puteti creea propriile alerte bazate pe identificatorul evenimentului, conditii si continut. Poate genera rapoarte zilnice, saptamânale, si lunare despre evenimentele importante petrecute in retea. Deoarece GFI LANguard S.E.L.M. nu este un sistem de detectie a intrusilor prin retea, nu este impiedicat in functionare de prezenta switch-urilor, criptarea traficului IP sau transferul de date la viteze mari.

Faciliteaza analiza jurnalelor de securitate

-Ofera monitorizare si notificare in timp real
-Elimina fragmentarea urmelor prin utilizarea unei singure baze de date
-Permite arhivarea centralizata a evenimentelor pentru generare de rapoarte si copii de siguranta
-Traduce descrierile (deseori criptice) ale evenimentelor in explicatii clare si concise, si ofera sugestii pentru actiuni ce se pot lua
-Elimina evenimentele neimportante ce reprezinta un procent ridicat din toate evenimentele legate de securitate.

Avantaje si beneficii

Monitorizeaza evenimentele critice de securitate din intreaga retea (atacuri si utilizatori rauvoitori).

Primirea de alerte in legatura cu evenimentele critice de pe serverele Exchange, ISA, SQL si IIS.

Crearea unei copii de siguranta si apoi stergerea event log-urilor din intreaga retea.

Nu este nevoie de agenti/clienti software pentru distribuirea in retea.

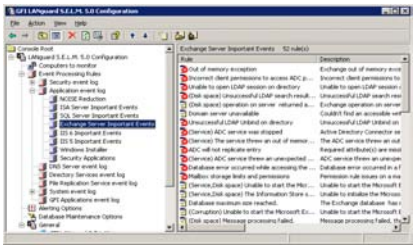
Monitorizeaza IIS, Exchange, ISA&SQL Server

Folosind GFI LANguard S.E.L.M. puteti supraveghea serverele importante. Event-urile de monitorizare generate de Microsoft ISA Server, Exchange Server si IIS pot preveni producerea unor dezastre in retea.

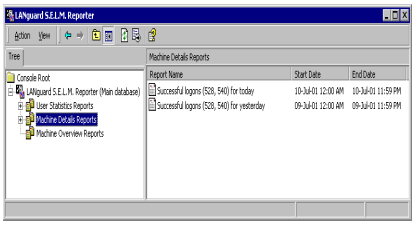
Permite vizualizarea rapoartelor referitoare la ce se întâmpla in retea

Generatorul de rapoarte din GFI LANguard S.E.L.M. ajuta la identificarea tendintelor asupra securitatii retelei. Folositi rapoartele standard pe care le puteti personaliza sau pur si simlu creati propriile rapoarte. Rapoartele standard includ:

-Toate incercarile de logon care au esuat
-Utilizatorii care nu au reusit sa se logheze datorita unui nume de utilizator sau a unei parole incorecte
-Toate conturile blocate pentru un interval de timp
-Pe care computere s-au logat utilizatorii
-Tentative de modificare a jurnalelor
-Evenimente de acces blocat la anumite obiecte (spre exemplu, fisiere securizate)
-Evenimentele importante din ziua, saptamâna, sau luna trecuta

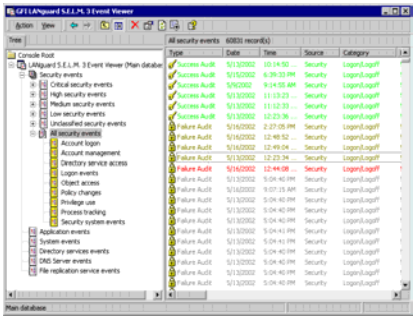


Alerte bazate pe e-mail
Dupa ce a fost detectat un intrus, GFI LANguard S.E.L.M. poate trimite alerte catre una sau mai multe persoane prin intermediul e-mailului. Deoarece puteti configura mai multe adrese, puteti seta ca alertele sa fie trimise si catre pager sau telefon GSM prin intermediul e-mailului, prin directionarea catre un gateway email-to-pager sau email-to-SMS. Alertele pot fi configurate, in functie de nivelul acestora



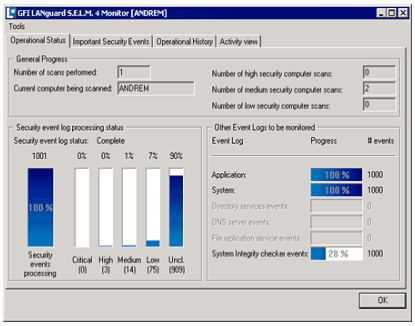
Filtrare avansata a evenimentelor de securitate
Programul de vizualizare a evenimentelor oferit de Windows (Event Viewer) are facilitati limitate si poate oferi date despre un singur computer la un moment dat. GFI LANguard S.E.L.M. ofera o imagine asupra evenimentelor de securitate de pe toate computerele, oferind si posibilitati avansate de filtrare . Spre exemplu, puteti filtra in functie de utilizator, computer, nivelul de securitate al PC-ului, etc. Include si un constructor de conditii pentru a permite crearea de filtre avansate pe baza combinatiilor intre aceste variabile.

Detecteaza intrusii si bresele de securitate
GFI LANguard S.E.L.M. se comporta ca un sistem de detectie host-based a intrusilor prin analizarea in timp real a evenimentelor de securitate. Nu mai este necesara instalarea unui sistem de detectie a atacurilor bazat pe retea.



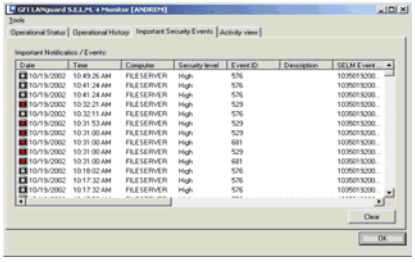
Poate fi configurat sa suporte WAN-uri si LAN-uri
GFI LANguard S.E.L.M. are un agent foarte eficient de colectare a event log-urilor, permitand acumularea evenimentelor de securitate in timp real fara a afecta performanta retelei. Pentru retele mari sau WAN-uri, scanarea evenimentelor poate fi distribuita catre instalari multiple ale GFI LANguard S.E.L.M. Astfel, fiecare instalare a GFI LANguard S.E.L.M. va monitoriza o anumita parte a retelei si va determina evenimentele critice/importante din aceasta sectiune. Acestea vor fi trimise mai departe catre baza centrala GFI LANguard S.E.L.M. Se reduce astfel traficul pe retea, cantitatea de banda si de spatiu de stocare folosite.

Gestiunea bazata pe reguli a event log-urilor
GFI LANguard S.E.L.M include o interfata de reguli puternica care permite stabilirea unor reguli pentru evenimente bazate pe datele de indentificare, conditia si continutul proprietatilor unui eveniment. Poate fi folosita de asemenea interfata interactiva pentru reguli in scopul monitorizarii anumitor aplicatii.



Monitorizeaza accesul la fisierele importante
Prin monitorizarea accesului esuat la fisiere importante puteti verifica cine anume incearca sa aiba acces la acele fisiere. Aceasta permite prevenirea unor atacuri si tentativele de intruziune bazate pe inginerie sociala (prin care, spre exemplu, hackeri devin amabili cu persoana ce are acces la fisierele respective, pentru a afla parola sau indicii despre parola). GFI LANguard S.E.L.M. poate monitoriza si accesul reusit la fisiere, pentru a inregistra cine a accesat fisierele si când anume.

Alte caracteristici sau facilitati
-Monitorizarea starea procesului de colectare a atacurilor si a evenimentelor
-Suporta Access, SQL Server si MSDE
-Monitorizare in timp real sau programat
-Detectia atacurilor asupra serverului web
-Detectia schimbarilor asupra fisierelor importante de pe statii sau servere



Clientii GFI sunt firme mari...
Multe firme cunoscute au ales sa foloseasca GFI LANguard S.E.L.M. Iata doar cateva dintre acestea: Primerica, Pepsico France, UOB Group, Royal&Sunalliance USA Inc., ATP, Ceridian Canada, si multe altele.

CS-SOFTWARE International SRL
Str. Izv. Crisului nr. 7, Sector 4, Bucuresti.
Tel: (021) 450.39.49, Fax: (021) 450.54.27, Mobil: 0722-25.22.11, 0744-55.22.11
E-mail: info@norman.ro, suport@norman.ro.
Web: www.norman.ro, www.css.ro
CUI: R 5247967, Nr. Inreg: J40/1387/1994

Authorised reseller