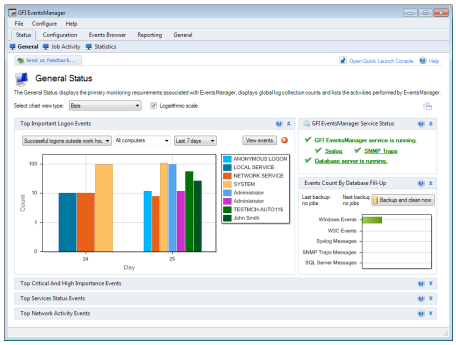
企業資訊事件稽核管理

Automated network-wide event log management

GFI EventsManager™

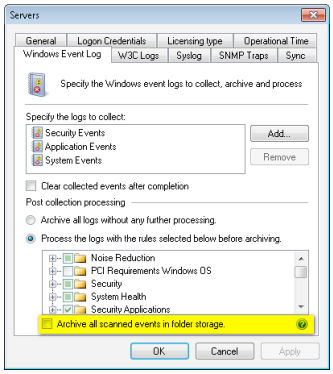
GFI EventsManager 可將企業內的Windows Server 與 workstation 上所有的事件集中，即時進行分析、歸類與處理，當重大事件記錄產生時也會透過電子郵件、簡訊或是啟動程式的方式做出即時警告。對於有稽核師固定進行稽核的企業，GFI EventsManager更內建了許多稽核報表，這些報表完全符合 SOX, PCI DSS, HIPAA...等資訊安全管理標準而產出，可以用來直接提交給稽核師。GFI EventsManager 也是一台log server，可以接收來自 Unix主機、防火牆、資料庫、網路設備、網站伺服器 ...等資訊設備送出的log以及SNMP traps，並進一步地分析與產出報表。

GFI EventsManager 功能特色



資安監控中心般的系統主畫面

GFI EventsManager主畫面顯示了所有監控電腦的登入事件統計、系統本身的狀態、各種格式事件發生的統計、關鍵事件發生的趨勢、應用程式活動、網路事件活動的圖形資訊，讓管理人員對監控對象記錄一目了然。



Rule-based日誌事件處理

EventsManager內建有許多的'處理原則'(Rule Sets)。當來自不同日誌源所產生的日誌進入系統時，EventsManager便會即時地檢查並套用這些原則對日誌進行處理。像是忽略重複的事件、開機關機的警告、記錄的保存...等。管理者也可修改這些內建原則，或是自定原則。

Windows事件來源的自動掃描

若您將EventsManager布置於Windows網域內，系統便可以自動地發現網域內的網域控制站、Exchange server、伺服器與工作站、ISA server等並將發現的個主機加入已分類好的事件來源中。

多樣的日誌格式支援

不同於其他產品需要透過3rd party程式來轉送Windows事件、EventsManager直接支援了各種Windows平台事件的抓取(包括Windows server 2008 R2 與 Windows 7)。此外，EventsManager也可以log server方式接收W3C、Syslog、SNMP等的設備日誌。

事件瀏覽器

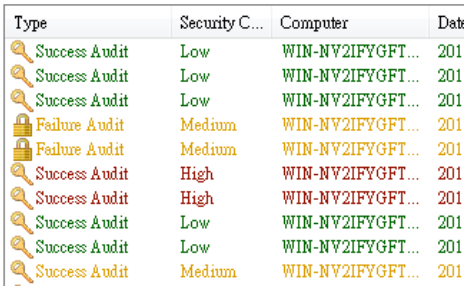
EventsManager的事件瀏覽器提供了在同一個畫面下，在Windows、W3C、Syslog、SNMP及MS-SQL Audit瀏覽切換的強大功能。管理者可以選擇任一種希望觀看的事件，便可直接看到事件細節，不需另外開啟或連接個別設備。

監看SQL Server的運作

EventsManager特別針對SQL Server的事件作了優化，藉由處理SQL server的日誌對SQL Server進行滴水不漏的監看 -- 如Server的啟動、登入活動、備份、Server端的程序等，對於資料庫關機與連續登入失敗等重要事件，也會透過Mail或SMS傳送警訊。

以顏色辨視事件的重要性

如何讓管理者對事件的重要性容易辨識？當然是透過顏色。EventsManager所搜集到的事件會自動以顏色分類 – 關鍵的、重要的、普通的、一般的。透過顏色就可以知道哪些是需要優先注意的。



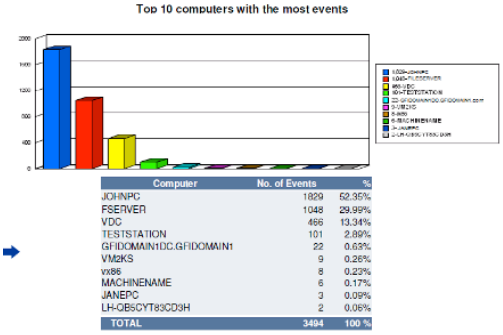
Type	Security C...	Computer	Date
Success Audit	Low	WIN-NV2IFYGFT...	201
Success Audit	Low	WIN-NV2IFYGFT...	201
Success Audit	Low	WIN-NV2IFYGFT...	201
Failure Audit	Medium	WIN-NV2IFYGFT...	201
Failure Audit	Medium	WIN-NV2IFYGFT...	201
Success Audit	High	WIN-NV2IFYGFT...	201
Success Audit	High	WIN-NV2IFYGFT...	201
Success Audit	Low	WIN-NV2IFYGFT...	201
Success Audit	Low	WIN-NV2IFYGFT...	201
Success Audit	Medium	WIN-NV2IFYGFT...	201

事件精簡處理

GFI EventsManager 能檢查並移除日誌中不需注意的事件 (比如重複的系統事件 or 背景處理程序記錄)，留下那些真正重要並有用的事件記錄，加速事件過濾與減少資料庫空間。

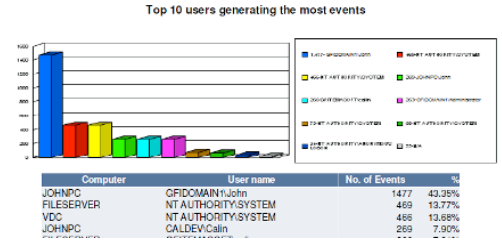
符合稽核要求的報表

內建超過120種以上的報表，客戶可以直接點選觀看，或是將報表匯出成 HTML、PDF、EXCEL、WORD、RTF等，管理者也可選擇想要的日誌種類與相關事件、過濾條件等來自定報表內容，產出客製報表。 EventsManager的報表完全符合國際法規（PCI DSS、SOX、HIPAA、GLBA...）的資安稽核要求，對於政府機關、金融證券、醫療單位的日常稽核特別有幫助。



Top 10 computers with the most events

Computer	No. of Events	%
JOHNPC	1829	52.35%
FSERVER	1048	29.99%
VDC	466	13.34%
TESTSTATION	101	2.89%
GFIDOMAIN1DC.GFIDOMAIN1	22	0.63%
VM2KS	9	0.26%
vx86	8	0.23%
MACHINENAME	6	0.17%
JANEPC	3	0.09%
LH-QBSCYT83CD3H	2	0.06%
TOTAL	3494	100 %



Top 10 users generating the most events

Computer	User name	No. of Events	%
JOHNPC	GFIDOMAIN1\John	1477	43.35%
FILESERVER	NT AUTHORITY\SYSTEM	469	13.77%
VDC	NT AUTHORITY\SYSTEM	466	13.68%
JOHNPC	CALDEV\Calin	269	7.90%

使用 GFI EventsManager 為企業帶來的4大效益

日誌事件集中管理

GFI EventsManager 將企業內伺服器或設備每日所產生的大量事件與日誌進行集中收集，減少管理成本

關鍵服務的監控

GFI EventsManager 協助資訊管理人員對 Microsoft ISA server、Exchange server、SQL 與 IIS Server等鍵服務主機進行重大資訊監視，以便在出問題時立即可知。

即時告警機制

GFI EventsManager可從即時事件收集中分析，一旦發現了不尋常的跡象便會觸發以電子郵件或是簡訊發出警告。對企業來說，GFI EventsManage就成了經濟有效的防護系統！

企業稽核與個資舉證

事件日誌的保存與報表一直是稽核師稽核企業的重點之一。而個資法因應更需要完善的報表以防不時之需。GFI EventsManager的內建報表符合近年來各種相關法規資安要求。當企業有稽核需求，或是因個資外洩造成法律上的訴訟爭議需要提出證明時，EventsManager的報表便成了企業最好的護身符。

系統需求

硬體需求*:*

- 處理器：2.5GHz Dual-Core
- 記憶體：8 GB
- 儲存空間：500 GB 可用空間以上

支援安裝的作業系統 *[32bit / 64bit]*

- Windows Server 2008 (Standard/Enterprise,含R2)
- Windows Server 2003 sp2 (Standard/Enterprise)
- Windows 2000 sp4 (Server/Advance server)
- Windows 7 (Professional/Enterprise/Ultimate)
- Windows Vista (Enterprise/Business/Ultimate)
- Windows XP Professional
- Windows SBS 2003/2008

原廠優質夥伴

podTech 東邦科技
Tel: (02) 2625-7817
Fax: (02) 2394-2530
e-mail: wecare@podtech.com.tw
網站: www.podtech.com.tw