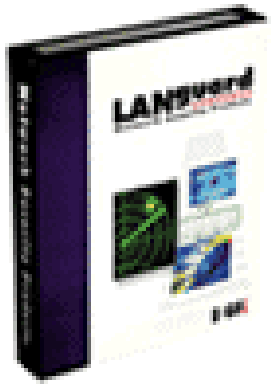


LANguard
Security Event Log Monitor

Intrusion detection using
NT/2000 event logs

安全事件記錄觀察器提供安全記錄闖入探測器、管理及分析整個本地網絡的安全事件記錄。

目錄

爲何使用 GFI LANguard 安全事件記錄觀察器? I

1. 安全理由 - 監控內部安全事件！

- 防火牆並不提供對公司內部侵襲的保護。
- 網絡一定要受到稽核才能確保防火牆操作正常。
- 內部安全的威脅很大：

「80%的侵襲起源來自防火牆內部。」
– *電腦世界，2002年一月*

「在美國，內部侵襲導致每年高達十億美元的損失。」
– *Business Week, 2000年十二月*

爲何使用 GFI LANguard 安全事件記錄觀察器? II

2. **使用事件記錄管理的理由：**

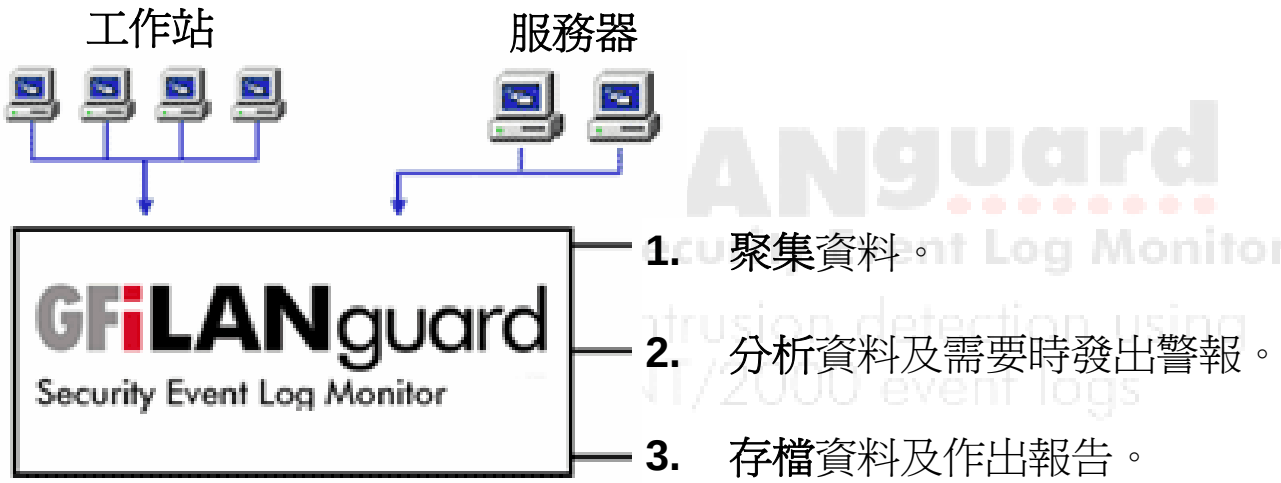
- 在遠端機自動支持及清除事件記錄。
- 監控危急任務的服務器及應用程序 (Exchange 服務器、ISA 服務器及病毒掃描軟件)。
- 簡易過濾及重要事件分析。

甚麼是 LANguard 安全事件記錄觀察器

使用 **GFI LANguard** 安全事件記錄觀察器能：

- 對用戶企圖進入共享及機密的文件時進行監控。
- 對您的網絡發生特殊事件或情況時會作出警報。
- 探測本地網用戶的侵襲。

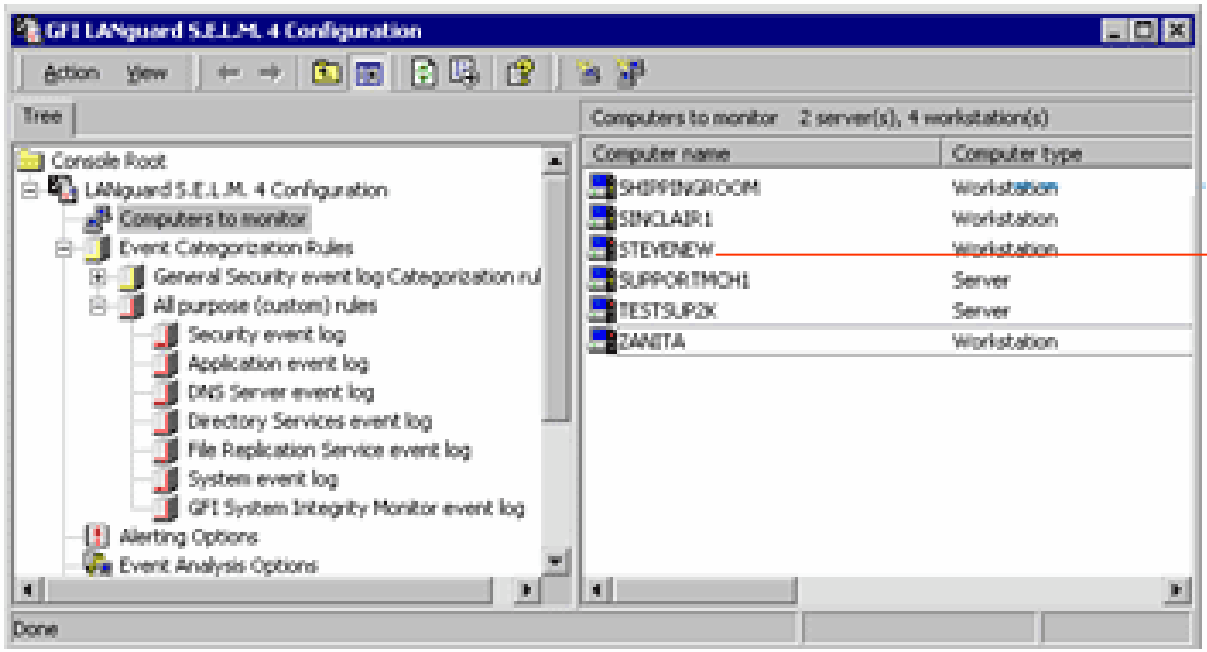
GFI LANguard 安全事件記錄觀察器怎樣操作



- 無需代理/客戶軟件。
- 沒有在網絡交通上的沖突。
- 擴充性良好 - 可在多樣的用戶之中分布極度的負載。
- 搜集應用程序及系統事件。

GFI LANguard 安全事件記錄觀察器的結構 I

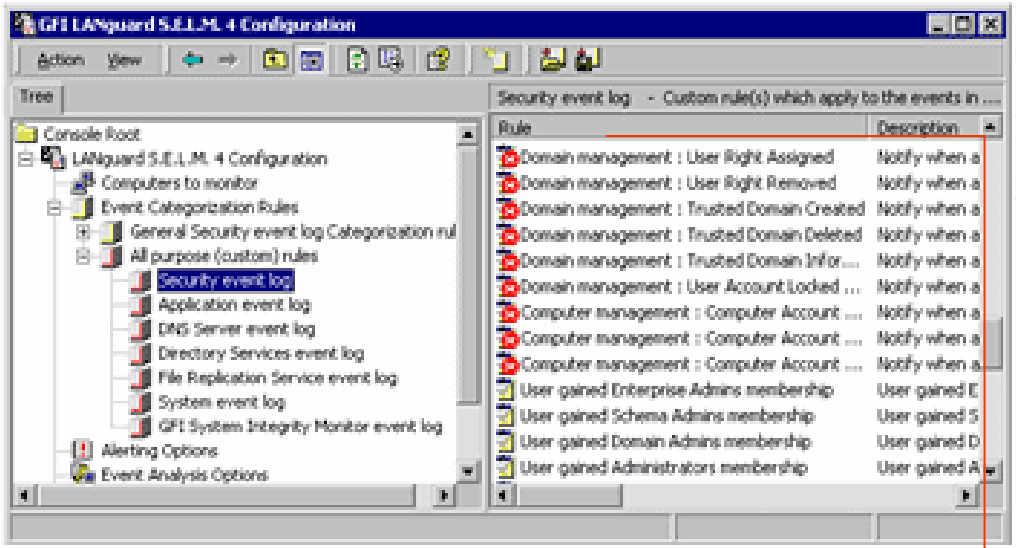
設定怎樣監控哪部電腦。



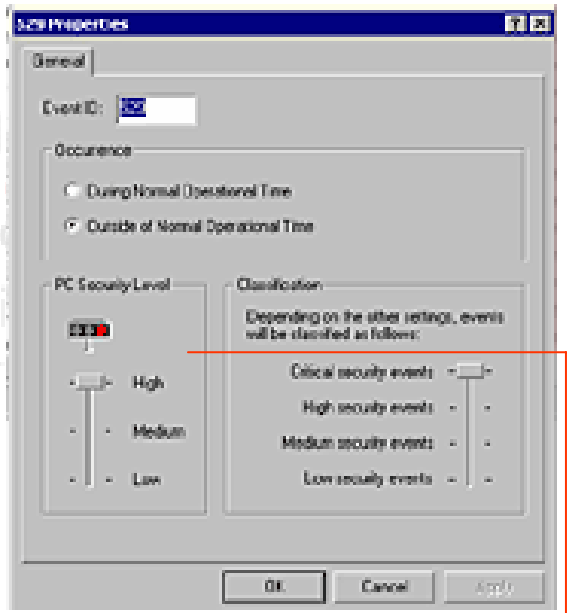
您可以指定監控哪部電腦

GFI LANguard 安全事件記錄觀察器的結構 II

設定怎樣監控哪部電腦。



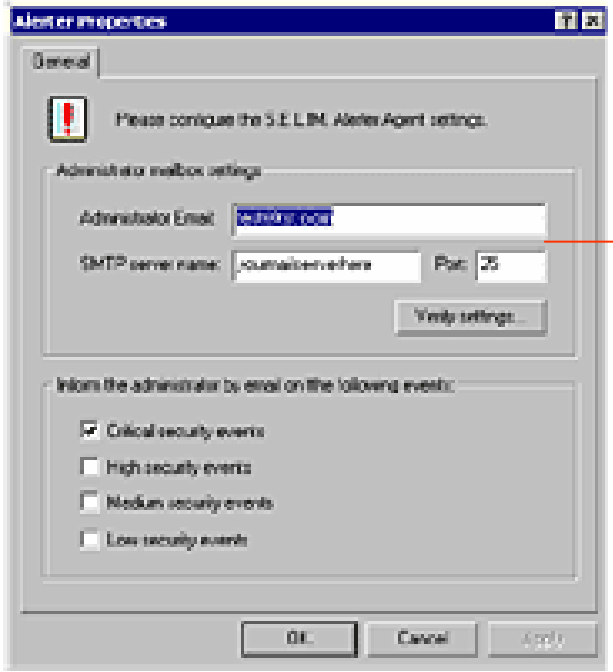
及事件應該怎樣分類



事件可根据監控中的電腦安全水平更進一步地分析

GFI LANguard 安全事件記錄觀察器的警報

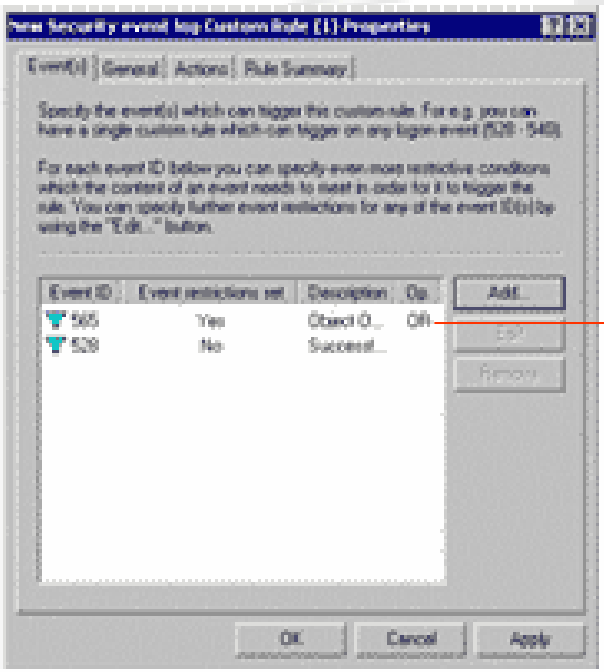
安全事件記錄觀察器發現危急事件後立即發送電郵警報。



設定電郵地址及什麼時侯發送警報

增加自定的規則

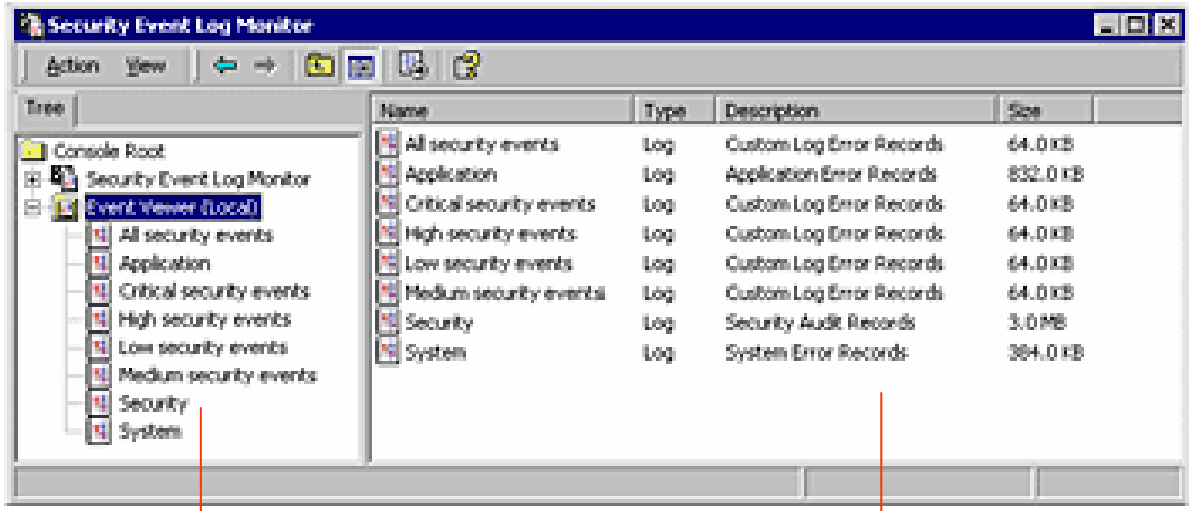
爲特殊的事件情況自定警報。



當一位特殊的用戶存取特殊的檔案，警報將會發出：例如

事件閱讀器 I

LANguard 事件閱讀器和其他的視窗事件閱讀器很相似，卻比它更多的先進搜尋及過濾選項。使用它在中央的位置回顧所有您的網絡事件，允許您偵查及調查網絡闖入。

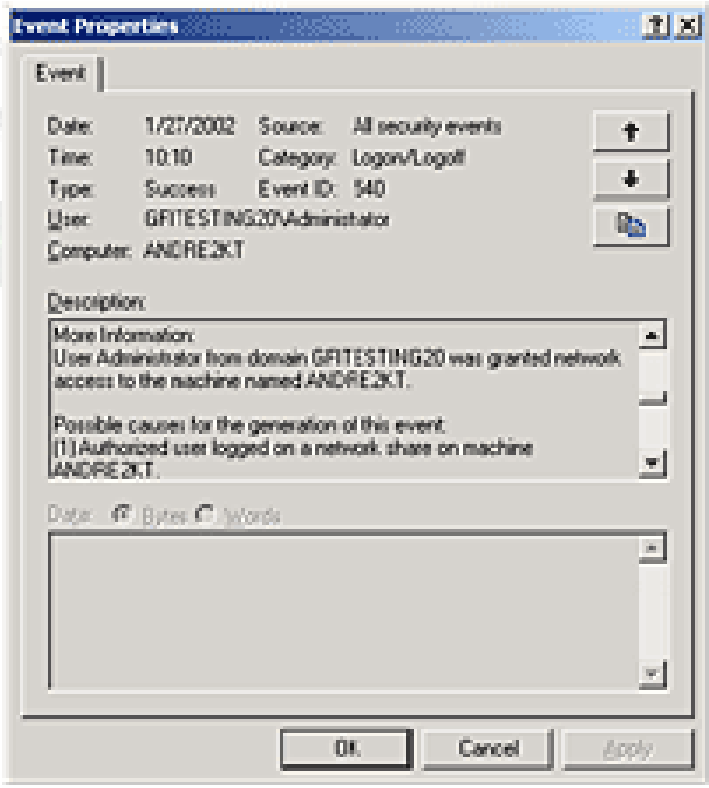


顯示所有在安全水平上已分類的事件

經事件類型進行更進一步的分類

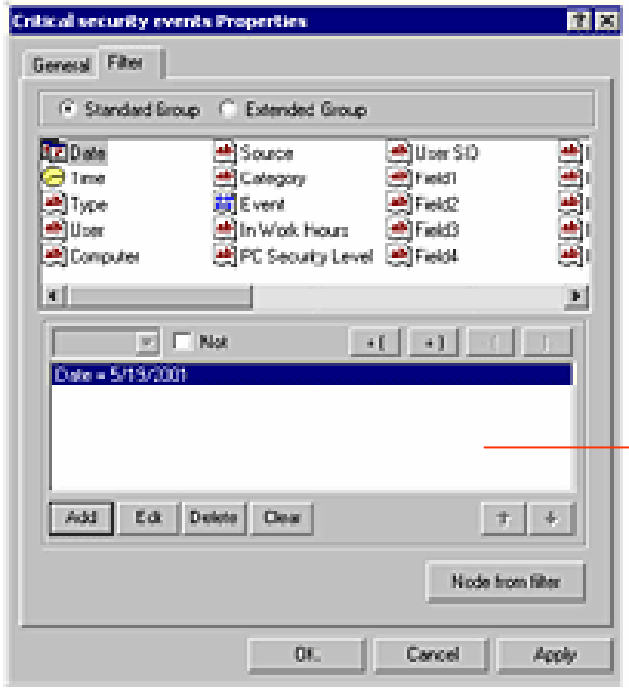
事件閱讀器 II

雙擊在事件之上能看到詳細資料及可能的原因。



事件閱讀器的搜尋性能

事件閱讀器包含一個強大的過濾器，它能確保您能分析特殊的用戶、電腦、事件類型、等等。



創造先進的過濾器條件建造器

GFI LANguard 安全事件記錄觀察器通訊員

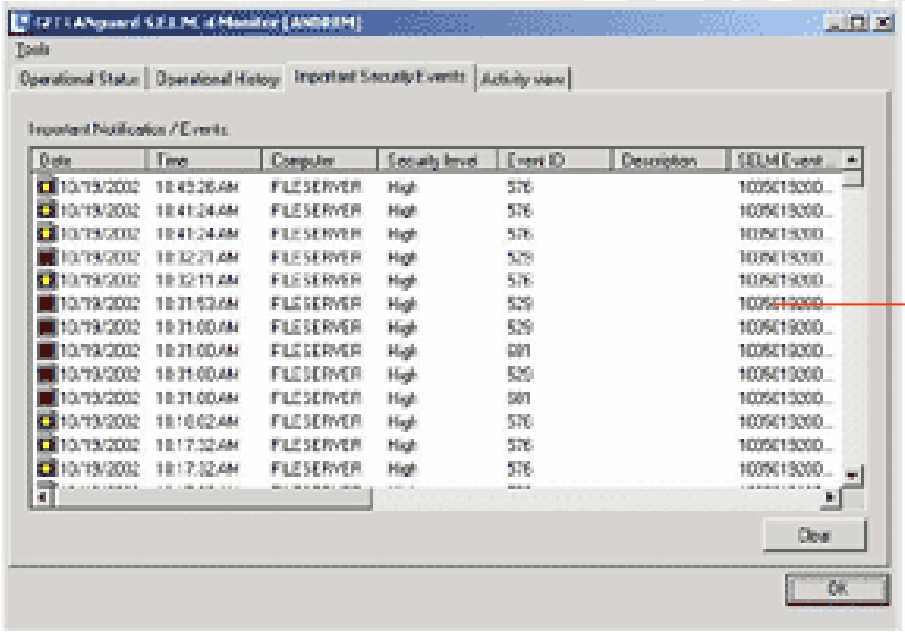
安全事件記錄觀察器能遞送關於您的網絡上行爲的詳細報告，包括：

- 所有失敗的登錄。
- 所有用戶登出。
- 用戶的第一次登錄時間 - 也使您能檢查雇員何時到達。
- 目標訪問報告。
- 哪個用戶產生最多報告。

觀看雇員的到達時間

狀況觀察器

實時觀看高度安全及其他危急的事件發生。



直接觀看危急的事件

GFI LANguard 安全事件記錄觀察器怎樣勝過其他產品

與其他標準的事件記錄回取器不同，**安全事件記錄觀察器**能：

- 包一個含嵌入的事件記錄分析引擎 - 無需復習使用手冊。
- 提供廣泛的安全報告。
- 優惠的價格。

Pricing in US$			
Product	for 10 servers	for 100 workstations	Total
TNT Software Event Log Monitor	3,450.00	6,500.00	9,950.00
GFI LANguard S.E.L.M.	1,395.00	995.00	2,390.00

免費起動包

從這里下載 **GFI LANguard 安全事件記錄觀察器**一個服務器及五個工作站專用版的免費拷貝：

http://www.gfi.com/downloads/downloads.asp?pid=6&lid=1

推薦書

「我對 **GFI LANguard 安全事件記錄觀察器**的觀察性能及報告感到十分滿意。無需多說，它意味深長地縮小我每日回顧服務器事件記錄的時間。」
- John Vargo, 網絡管理員, Atlantic Tool & Die Company, Cleveland,俄亥俄州, 美國

「與 **GFI LANguard 安全事件記錄觀察器**，視窗管理員能在第一次執行詳細的視窗安全事件記錄分析，及作出即時的事件安全增值,感謝 **GFI LANguard** 的高度詳盡及容易理解的事件記述與實時警報的結合。」
-Bob Walder, 主任, The NSS Group, Cambs,英國

「感謝你們的幫助及關注我電郵給你們的問題。感激你們迅速解決問題的轉變時間。」
- Jason Lopes MCSE, MCP + I, 系統管理員, R/GA, 紐約, 美國

客戶名單

多間大型公司於世界各地也使用此產品，他們包括：

- 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
- 等等

下載

請瀏覽這里取得關於 **GFI LANguard 安全事件記錄觀察器**的 PDF 資料冊及白皮書：

http://www.gfi.com/lanselm/lanselmpapers.htm

關於 GFI

GFI 分別在美國、英國、德國、澳大利亞及馬耳他設有辦公室，及擁有全球性的經銷商網絡。

GFI 是個領導 GFI FAXmaker、GFI MailSecurity、GFI MailEssentials 及 GFI LANguard 產品行列的市場開發者。

GFI 榮獲美國微軟公司 2000年最佳應用軟件伙伴冠軍。

請瀏覽 www.gfi.com 取得更多資料。