檔案完整性監控與相關應用

保護重要系統與資料，防範特權或已授權使用者未經授權的存取及變更

企業面臨的挑戰
一旦特權使用者做出未獲授權的重要檔案與系統變更，企業所面臨的組織風險便會升高。

解決方案的優點
我們的檔案完整性監控解決方案協助您：

- 遵循各項法規與隱私權標準，例如 PCI DSS、ISO、個資法
- 以 SIEM 解決方案整合即時的智慧型警示，彌補安全情報的不足
- 監控特權或已授權使用者的活動，偵測並防堵潛在威脅
- 更快速地偵測重要檔案、系統和應用程式的變更

簡介

如果您必須保護機密資訊和關鍵系統，您的組織就必須因應特權或已授權使用者未經授權活動所帶來的風險。偵測未經授權的存取和變更是非常困難的工作，需要借助一套即時偵測並警示重要資產變更的安全解決方案，才能掌握安全漏洞或不合法規的事件。

檔案完整性監控是涵蓋範圍更廣的資安計畫的其中一環，協助降低下列特定風險：

- 資料外洩 – 尤其是因濫用特許存取權限
- 系統可用性 – 因檔案、系統與應用程式遭意外或未授權的變更
- 未遵循法規 – 因未能善盡監督存取及變更機密資料的責任

解決問題

針對關鍵業務系統和資料檔案，若要解決特權或已授權使用者未經授權的存取與變更的問題，最佳作法包括即時警示：

- 將警告功能整合至安全性資訊與事件管理 (SIEM) 系統
- 立即提供極為詳細的安全資訊
- 監控特權或已授權使用者的活動

此外，解決方案必須遵循要求使用檔案完整性監控解決方案的法規，並偵測最重要平台上的變更。

NetIQ 的作法

NetIQ 檔案完整性監控解決方案藉由對重要檔案、系統與應用程式未經授權的存取和變更的智慧型警示，協助 IT 資安人員即時偵測和回應潛在威脅。

我們的即時檔案完整性監控方法：

- 監控特權或已授權使用者的活動
- 針對重要檔案、系統與應用程式未經授權的存取和變更，提供即時的智慧型警示
- 確保智慧型警示提供極為詳細的安全資訊，例如變更時間、變更者身分、變更內容、變更位置，以及變更是否經過授權
- 將智慧型警告功能整合至頂尖的 SIEM 解決方案，更快速地回應潛在威脅
- 證明企業監控機密資料存取及變更的能力，以協助達成法規要求
- 偵測最重要平台上的變更，包括 Microsoft Windows 與 Active Directory、UNIX 與 Linux

安全資訊簡單明瞭，不需具備各種事件類型的專業知識也能辨識，並降低因應可疑活動的時間與複雜性。我們的解決方案支援異質 IT 環境，會簡化並集中回應整個企業的威脅，協助團隊迅速識別威脅並積極因應。

NetIQ

此外，我們的檔案完整性監控解決方案能增強由您的 SIEM 解決方案提供的「可作為行動依據的情報」，其中具備必要的安全事件詳細資料，以偵測並防堵威脅。由於 SIEM 本身依賴原生記錄，因此難以深入掌握事件的人、事、時、地、物。我們的檔案完整性監控解決方案提供團隊所需豐富且詳細的安全資訊，以偵測內部或目標式攻擊的跡象。

檔案完整性監控相關應用

檔案完整性監控相關應用是更廣泛的系統完整性監控問題。識別未經授權的檔案存取與變更至關重要，因此這類監控必須納入更廣泛的安全與法規遵循管理方案。

我們進行檔案完整性監控的方法，包括緊密整合 SIEM 解決方案，呈現具關連性的豐富相關資訊給安全與法規遵循團隊。在進一步結合身分識別管理解決方案之後，完整的解決方案便具備身分偵測功能，增加即時身分識別資訊，能立即準確地提供整個組織有關使用者存取權限的其他內容。其後您就能全面掌握安全情報，藉此能更快速地識別並因應特權或已授權使用者活動，辨識其中的安全漏洞或不合法規的前兆。

產品

- **NetIQ Change Guardian™** 提供 SIEM 解決方案即時的智慧型警示，涵蓋多個伺服器、作業系統、裝置和應用程式 (包括 Microsoft Windows、Active Directory、UNIX 與 Linux) 的存取、變更及特權或已授權使用者活動。
- **NetIQ Sentinel™** 從單一中央位置進行安全性事件管理、記錄彙總和鑑識分析。
- **NetIQ Identity Manager** 讓您將使用者管理標準化，且為組職建立單一且豐富的身分識別儲存區。

如需檔案完整性監控的詳細資訊，請瀏覽：**www.netiq.com**，或是致電當地 NetIQ 業務代表或合作夥伴。

全球總部

1233 West Loop South, Suite 810
Houston, Texas 77027 USA
全球：+1 713.548.1700
美國/加拿大免付費電話：
888.323.6768
info@netiq.com
NetIQ.com
http://community.netiq.com

歐洲、中東與非洲總部

Raoul Wallenbergplein 23
2404 ND Alphen aan den Rijn
Netherlands
電話：+31(0)172.50.55.55
傳真：+31(0)172.50.55.51
info@emea@netiq.com

如需本公司在北美、歐洲、中東、非洲、亞太地區和拉丁美洲分公司的完整列表，請瀏覽 NetIQ.com/contacts

追蹤我們的動態：

SB60001FIM -A4 PO 04/13 F
577-TW1022-001 DS 05/13