NTFS Change Auditor

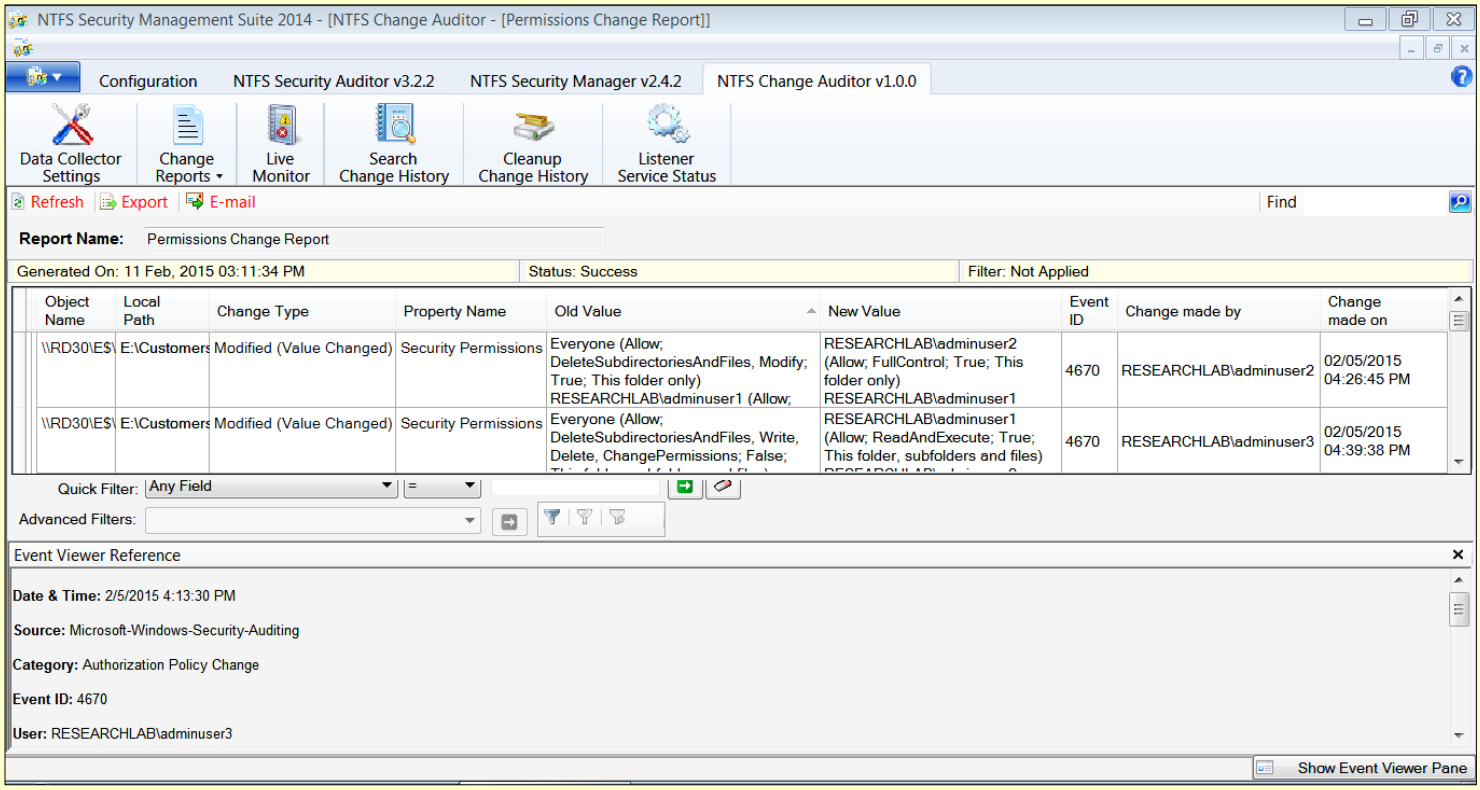
NTFS 檔案伺服器的異動與存取稽核工具

概述

- 稽核所有使用者對敏感與關鍵目錄與檔案的存取
- 追蹤對目錄與檔案所做的所有異動，包括權限異動
- 找出誰在任何時候存取了什麼?
- 使用即時警報Real-time Alerts即時監控所有檔案存取
- 根據您的舉證分析Forensic Analysis與法規遵循需求提供異動歷史記錄

NTFS Change Auditor 提供有關使用者存取檔案與目錄以及對 NTFS 共享、目錄與檔案所做異動的重要問題的答案。

- 誰存取了您的共享Shares？ 對您的共享Shares 進行了哪些類型的修改？
- 誰存取了您的目錄與檔案？ 存取了什麼，對目錄與檔案做了什麼類型的修改？
- 誰異動了目錄與檔案的所有權Ownership？
- 是否因為底層權限結構中的安全漏洞而存在任何未經授權的存取？
- 我的目錄與檔案中經常發生什麼類型的活動？權限與所有權是否不斷變化？



優點

- NTFS 共享上的目錄與檔案存取報告，例如（存取accessed、 建立created、修改modified與刪除deleted）以及有價值的資訊，例如何時與誰進行了異動以及共享名稱Share Name、本地路徑Local Path與使用者端地址Client Address等。

- 目錄與檔案異動報告，例如（ 建立created、修改modified、刪除deleted與所有權異動ownership changes）確切異動的內容、舊值與新值、異動時間、檔案系統中的異動位置以及異動者。基於安全、舉證分析forensic analysis與法規遵循目的，SQL 資料庫中的幾年異動與使用者存取資料的歷史記錄。

- 一旦您的伺服器與工作站中的共享、目錄與檔案發生稽核異動事件就會透過電子郵件發出即時警報Real Time Alerts。

- 從多個主機的安全事件日誌中蒐集已設定事件 ID 的整合資料。

- 強大的搜索查詢可搜索整個事件歷史記錄 - 搜索事件 ID、日期範圍、主機名稱與自由本文free text。

- 現場事件Live Events可在存取與異動發生時立即檢視看所有已設定事件 ID 的事件發生。

- 使用強大的搜索條件清理事件歷史記錄 - 搜索事件 ID、日期範圍與主機名稱。

詳細Vyapin Software產品資料請洽 商丞科技
02-2914-8001 ext 2251 李經理