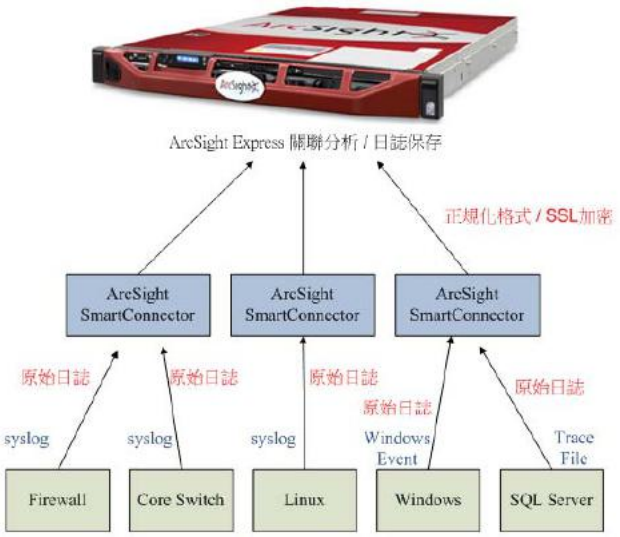
ArcSight 資安事件管理解決方案
- Logger 簡介

ArcSight Logger 可從任何生成記錄資料的系統收集資訊。它可視需求調整處理的資料量，並可生成跨資料的超快速搜尋。因此，任何規模的組織皆可使用此高效能的記錄資料儲存庫，以協助加快 IT 作業、應用程式開發及網路安全性問題的蒐證分析，並可同時因應多重法規。

今日，就記錄所作的分析來解答的疑問越來越偏重於使用者方面，而且可能擴及任何基礎結構。傳統記錄管理工具無法擴充來分析整個企業的記錄，因為受限於來源類型；不但搜尋/報告能力有限，也無法進行延展。ArcSight Logger 是通用記錄管理解決方案，可擷取與分析所有企業記錄資料以回答個別團隊的問題，並可在必要時輕鬆擴充成適用於整個企業的記錄管理解決方案。

Logger運作架構



ArcSight Logger 是一個功能強大的事件收集中心，透過 ArcSight SmartConnector 收集前端資訊設備所產生的原始 Log，並將原始 Log 做正規化處理，將 Log 轉換成 CEF 格式的日誌，再傳送至 ArcSight Logger 上做分析及保存，若有需要對原始 Log 做資料備份的需求，也可以在 Connector 上設定保留原始日誌，以達到同時保存原始日誌及正規化後的日誌。

ArcSight Logger

Logger 可以將日誌做長期的歷史儲存及產生相關報表，並提供一個有效的日誌儲存方式和管理多達最大 42TB 的日誌資料。可儲存原始日誌資料或是經過正規化處理的日誌。Logger 本身預設提供多種符合安全性法律規範的報表格式，以及支援即時事件查詢的功能。

Log 格式正規化與保護機制

未正規化日誌所會遭遇的問題：

下圖是一個正規化的範例，在未正規化的日誌中可以看到兩筆 Firewall 的日誌記錄，但因為每家廠商的日誌格式都不相同，導致管理者閱讀的困難，即使將這些日誌都收進同一個日誌管理的設備中統一保存，但管理者若要同時查出這兩筆日誌記錄所需輸入的查詢指令相對較困難。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

正規化日誌的好處：

當日誌經過正規化後會將所有的日誌分門別類的欄位化，在查詢時可以快速依欄位值直接輸入統一的關鍵字，就可以輕易的查出全部想要的日誌資料，例如可輸入 CategoryOutcome = /Failure 就可以查出所有設備結果為失敗的日誌資訊，就可以透過這個方式快速的找出您要的資訊。

安全的LOG保護機制構

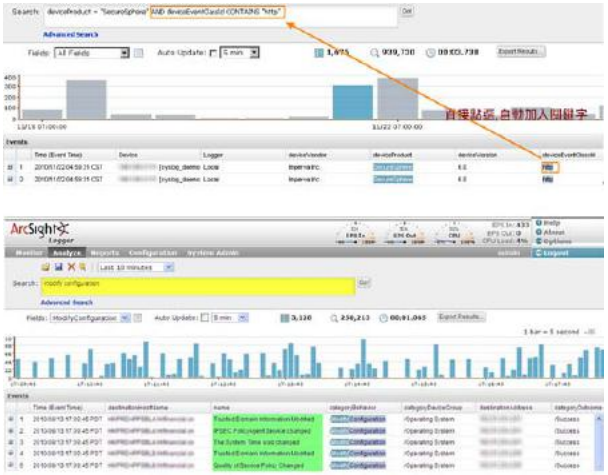
在網路犯罪行為發生或追查事件時, LOG 關係到舉證或是追查事件的方向是否正確，ArcSight 在 Log 的保護上提供以下的安全措施，以確保 Log 的安全性：

- 儲存在 ArcSight 或 Connector 中的 Log 使用 HASH (MD5 or SHA) 加密
- Log 在傳輸過程中使用 SSL 加密
- Log 無法也不允許修改,以避免遭有心人士竄改

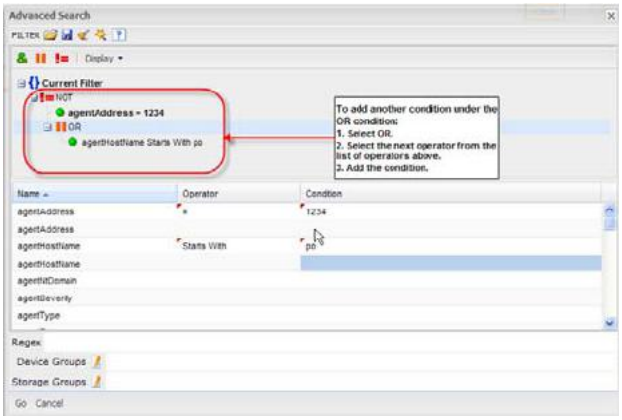
直覺化查詢

透過 Web 介面搜索對事件做簡易的查詢，可直接在查詢頁面輸入關鍵字，（例如 IP 或 Hostname）就可快速的查詢出您要的資訊，也可輸入正規表示式（Regular Expression）及布林邏輯運算式（Boolean logic）執行進階查詢。

支援 Drill down 功能，直接點選想查詢的文字，即自動加入關鍵字，可搜尋並報告大量的資料，以迅速、輕鬆地調查中斷狀況和事件。

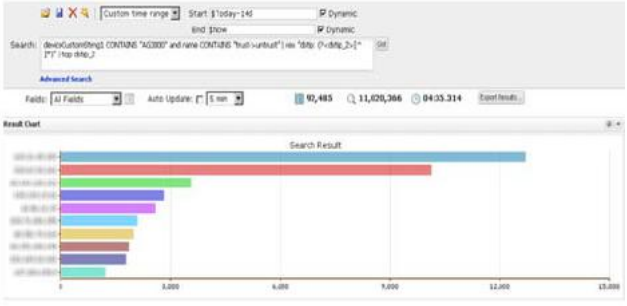


也可透過查詢精靈選擇需要的查詢條件。



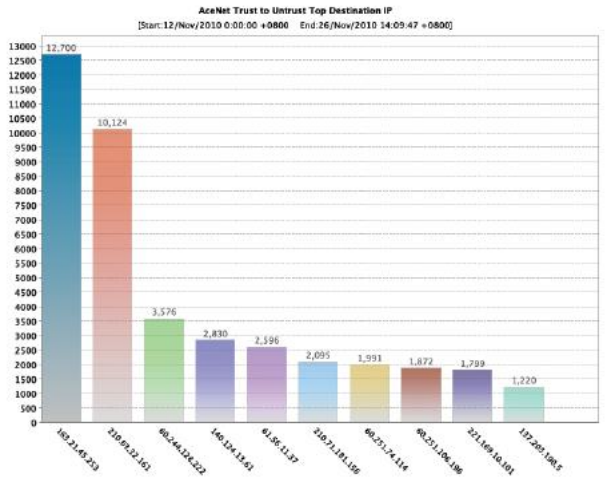
即時產生統計圖表

可直接在查詢畫面輸入查詢條件，馬上產生您想要的報表。



GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

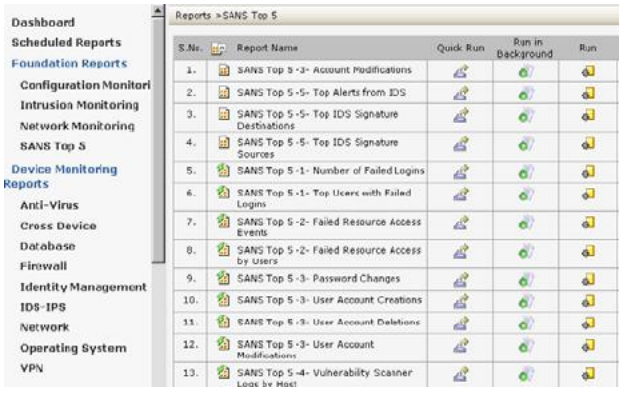
直接滙出成報表 (PDF或CSV)



廣泛的報表功能

提供大量的預設報表，大大降低再自行手動建立報表所耗費的人力。也提供 SQL EDITOR 可依需求彈性調整報表條件，客製化所需求的報表。

- 100% web base 操作
- 可設定排程定期滙出報表
- 明確分類報表類型
- 提供法規報表 Package



自訂Dashboard更方便管理

可將常用的報表放在首頁或鍵結到其它設備的 Web 管理平台或其它外部網站。

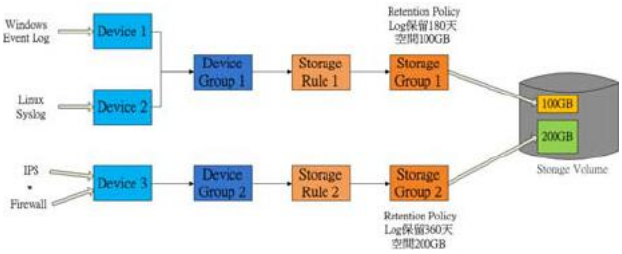
Drill Down 報表

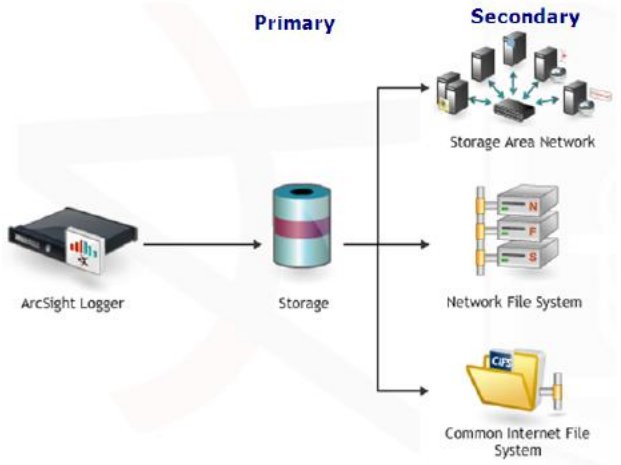
部份報表提供 Drill Down 功能，能直接點選即可查詢在彙總資料後面的細節，更方便使用者閱讀及查詢。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787

彈性的儲存機制

可依 Log 重要性或依法規規定自訂 Log 的保留時間及空間大小，另外 Log 本身除了可儲存在 ArcSight 上，也可以透過ＣＩＦＳ或ＮＦＳ或是ＳＡＮ將 Log 儲存在另外的儲存區。

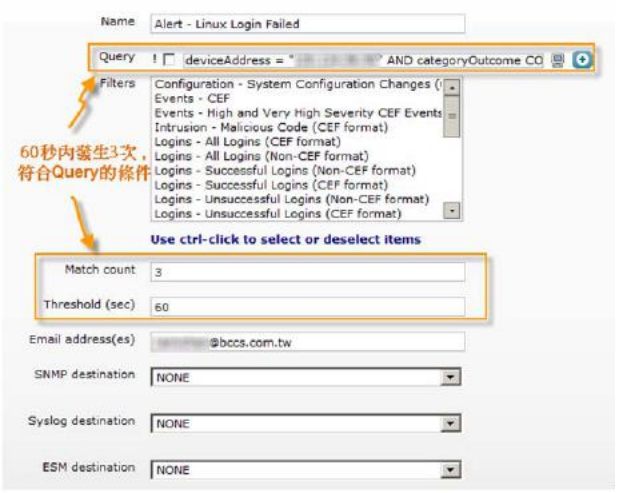




即時告警功能

可設定多組即時告警條件：

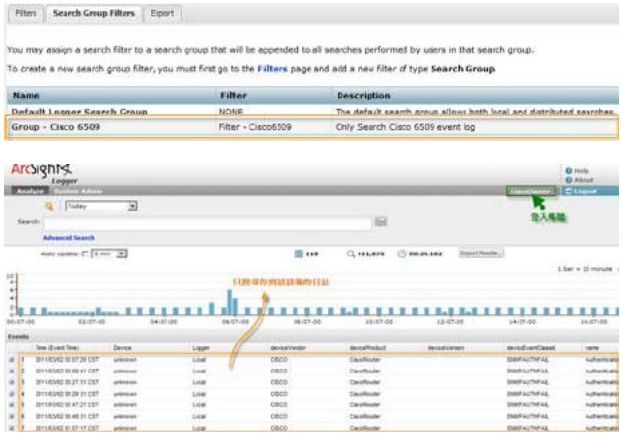
自訂告警條件



設定帳號控管權限

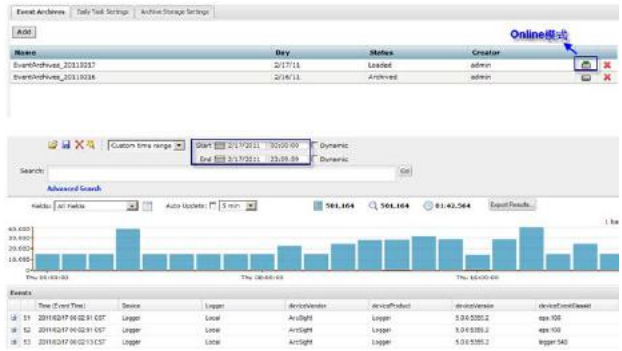
可依需求限制該某些帳號只能查詢的到某些設備的 Log。

GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787



日誌Archive保存機制

Archive 出去的日誌，當設定成 Online 模式後，可直接讀取 Archive 目錄中日誌，依然可以查詢，且不需將日誌回存到 Logger 本機的硬碟上。



GSS 叡揚資訊 Galaxy Software Services 地址：台北市 10461 中山區德惠街 9 號 5 樓 電話：+886-2-2586-7890 傳真：+886-2-2586-8787