ArcSight IdentityView 產品簡介

原文：HP-ArcSight 提供　翻譯整理：叡揚資訊 資訊安全事業處

現今企業花費數不盡的時間和資金在身分管理及目錄服務上，但依舊無法回答一些基本問題，例如：

- 是否有共用帳號，是誰在使用？
- DBA 上週對系統有任何異動？是否有發生問題?
- 離職員工是否仍在存取公司內部系統？

組織不易取得足夠透明的資訊去回答上列法規或風險相關問題。一些必要的資訊都包含在目錄服務，包括微軟的 AD。其他的資訊則在規則中、含有人力資源系統以及身分辨識管理(IDM)應用程式的工作流程中，或者是儲存在跨企業日誌檔內。想全面性瞭解企業整體的使用者活動和相關的風險，需要從這些不同的系統連接和關聯訊息。

ArcSight IdentityView 利用系統之間不同的活動日誌，針對企業整體使用者、角色和目錄服務的群組資訊等提供全視野的使用者活動。透過分析使用者行為並對應其在企業內角色，ArcSight IdentityView 可以偵測到潛在風險活動，包括資料竊取以及未經授權存取機密資料等。監控使用者活動可使管理人員能確認其內部控制是有效的，減少資料被竊取的風險和審核失效。

內建使用者監視控制、規則和報表

ArcSight IdentityView 協助企業監控常見使用者情境：

- 高權限使用者及帳號管理

藉由結合目錄服務或身份管理(IDM)系統內使用者及角色之間的資訊，以及資料庫、檔案和其他活動，ArcSight IdentityView 可以主動監控高權限帳號的操作風險或異常活動，這是符合許多法規的關鍵要求。

- IP 位置和使用者帳號的映射

許多重要系統的日誌，如代理伺服器未記錄使用者訊息，只記錄唯一的 IP 位置。調查這些系統的使用者活動需要知道哪個 IP 位置被使用者在特定的時間使用。ArcSight IdentityView 透過關聯資料(包括 DHCP，Kerberos 和使用 IP 位置的所有來源日誌檔)並歸納未經認證活動及個人使用者。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京　營業範圍：兩岸三地及日本　www.gss.com.tw

- 共用帳戶追蹤

透過關聯身份資料、IP 位址和應用程式日誌，ArcSight IdentityView 可解析某單一人於一定時間使用某個共用帳戶。應用在開發應用程式系統裡，可幫助組織遵循法規，如 PCI 標準，其明確禁止使用共用帳戶。基於這樣的結果，企業可以遵循法規且不用重新開發既有的應用程式系統。

- 離職員工/承包商控管

雖然可在目錄管理或身分辨識系統去停用使用者帳號，這些帳號卻可能仍在應用程式或其他系統中活動。ArcSight IdentityView 連結本地目錄管理和身份管理系統的活動，以確保這些帳號在系統或應用程式中已停用。

- 以角色為基礎的控制報告

運用角色或部門的資訊對應到每個標識帳戶，ArcSight IdentityView 可以依照角色、群組或者是其他條件，自動產生完整的活動報告。這功能使管理者瞭解內部控制情況和處理流程是有效的在運作。

- 連結多個帳戶，進行分析

ArcSight IdentityView 能聯結多個帳戶對應到特定的使用者，進而關聯這些帳戶的活動，並發現在不同帳戶的風險；例如，使用資料庫帳戶提取提取機密資料，使用 Windows 帳戶新建一個檔案，並將機密資料存放在檔案中，再用電子郵件帳戶將檔案寄出。此功能有助於研究特定使用者活動，資安團隊可以產出針對單一使用者的報告，而不是針對每個系統上可疑活動的調查。

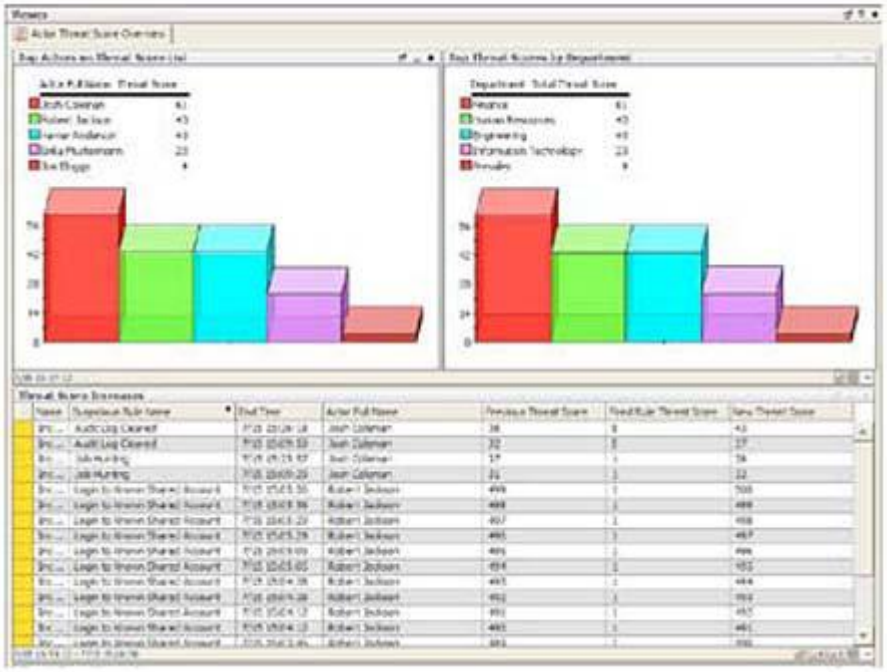
- 權責區分的違規偵測

使用 ArcSight IdentityView，組織可以建立須由二人以上才能執行的規則，並在違反規則時觸發警報。例如：某一使用者提出變更申請，並自行批准同一個申請，此時 ArcSight IdentityView 就會告警。

管理階層的儀表板及報告

利用 ArcSight IdentityView，管理者可以清楚知道資安告警及法規遵循風險，是來自哪位使用者、部門或群組。ArcSight IdentityView 可於安全及活動日誌紀錄到使用者資訊，讓管理者可以輕鬆一致地了解公司資安狀況(如下圖)。

GSS Galaxy Software Services 叡揚資訊
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京 營業範圍：兩岸三地及日本 www.gss.com.tw



圖說: ArcSight IdentityView 提供威脅數據，並依部門標示出最危險的使用者，列出他們的危險行為

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京　營業範圍：兩岸三地及日本　www.gss.com.tw