cpl.thalesgroup.com

THALES

CipherTrust Security Intelligence

挑戰：建立企業範圍內機敏資料威脅能見度

為了避免已經發生資安事件(例如資料外洩)後才察覺，IT管理者需要一種簡單的方法以辨識和關聯所有潛在安全事件的相關資料，以便能夠快速且即時舒緩威脅。一些最有效的工具就是安全情資與事件管理(Security Intelligence and Event Management; SIEM)方案。

解決方案：CipherTrust Security Intelligence有效追蹤和調查整個企業組織的可疑活動

如果沒有CipherTrust Transparent Encryption的Security Intelligence提供詳細資料，SIEM方案可能產生盲點，無法察覺資料的潛在威脅。CipherTrust Security Intelligence登錄並報告法規遵循狀態，以及利用領先SIEM系統加速威脅偵測。

效益

- **提供分級且可據以行動的安全情資**
  傳統上，SIEM仰賴防火牆、IPS和NetFlow裝置提供的日誌資料。由於這項情資是在網路層捕捉，因此這些系統會產生龐大資料，使得管理者難以辨識需要處理的事件。這些系統也存在一個常見的盲點：它們沒有提供伺服器的資料存取與事件能見度。CipherTrust Security Intelligence排除此一盲點，提供有關檔案存取活動的針對性關鍵資訊。因此，它能協助避免非法或盜用帳號者竊取機敏資料。CipherTrust Security Intelligence日誌會產出有關使用者與程序「被允許」或「拒絕」存取資料的可稽核報表。詳細的日誌可檢視使用者與程序何時存取資料、在何種政策下執行、以及存取請求是否被允許或拒絕。
- **簡化稽核與法規遵循**
  CipherTrust Security Intelligence提供詳細的能見度與整合，協助簡化稽核工作與法規遵循報告。為符合許多法規義務，企業必須證明已建置並且運作資料保護措施。CipherTrust Security Intelligence可用於向稽核者證明加密、金鑰管理與存取政策皆有效運作。

- **預先建置的SIEM整合**
  CipherTrust Transparent Encryption日誌在系統階層收集和報告合法與非法的加密檔案與磁碟存取，包括使用者、程序等。CipherTrust Security Intelligence日誌與報表簡化法規遵循報告，並利用領先SIEM系統加速威脅偵測。合法的授權使用者存取資料可提供SIME平台建立使用資料的參考基準，與其他安全資料整合，例如使用者位置和存取點，以找出確切的威脅點。

功能

CipherTrust Security Intelligence日誌：

- 產出有關使用者與程序「被允許」或「拒絕」存取資料的可稽核報表。這些日誌能有效的和SIEM平台共享，協助發現異常程序和使用者存取型態，加速進一步的調查。
- 偵測可能的惡意軟體或進行非法存取的惡意內部使用者。
- 找出使用者對受保護資料的不尋常存取型態，防範惡意軟體(或惡意內部使用者)竊取資料。
- 監控程序對受保護資料的異常存取型態，防範程序遭惡意軟體侵入。
- 辨識非法使用者對CipherTrust Manager設備的攻擊。

CipherTrust資料安全平台

CipherTrust Security Intelligence是CipherTrust資料安全平台的一部分。CipherTrust平台統合資料發現、分類、資料保護，並提供前所未有的分級存取控制，以及集中化金鑰管理。這可以簡化資安營運，加速法規遵循時程，確保雲端轉移安全以及降低整體企業風險。企業可仰賴Thales CipherTrust資料安全平台以協助發現、保護和管控企業機敏資料，不論資料駐留在任何地方。

關於Thales

那些保護您隱私的組織仰賴Thales保護他們的資料。企業在維護資料安全上面對越來越多重要的決策，不論是建置加密策略、轉移到雲端、或者資料法規的遵循義務等，您可以仰賴Thales確保安全的進行數位轉型。

Thales為關鍵決策提供關鍵技術。