中華資安國際
CHT Security

# 日誌管理系統

## 概述

- 本系統可以整合收容各式日誌與不同廠牌的資安事件，支援加密儲存，且提供原始日誌資料查詢與中文化報表管理介面，以符合日誌收集、保存及查詢之需求

## 特色

- 支援收集多種設備日誌格式，事件收集時內建過濾、聚合、正規化、分類、壓縮、加密功能。事件收集正規化後能自動歸類設備種類、行為類別、行為結果及事件嚴重等級等資訊。
- 事件傳遞支援過濾與聚合設定，可自訂過濾與聚合條件，且至少需包含來源 IP、目的 IP、連接埠、設備類型、設備 IP、事件類型、事件嚴重程度。
- 需保存正規化(Normalization)後之原始日誌資料，支援加密雜湊演算法確保事件完整，包含 SHA-256、SHA-512。日誌一經儲存後，系統僅提供唯讀方式，可避免資料遭竄改。
- 事件查詢提供關鍵字輸入查詢，並可加入條件限制至少包括必要條件、排除條件與最少條件等。
- 使用者可以在查詢結果中，直接以滑鼠點選關鍵字進行查詢條件新增以精進查詢。
- 若事件不需正規化的情況下，可透過系統直接收集，並且提供關鍵字查詢。
- 系統提供預設報表，包括設定監控報表等。
- 報表格式需支援 Excel、PDF、CSV、Word 並可直接輸出為 HTML 格式。使用者可以在匯出時，選擇匯出事件的相關欄位。
- 報表需具備中文管理介面

## 產品畫面