中華資安國際
CHT Security

中華資安事件管理及戰情牆系統

概述

- 中華資安事件管理及戰情牆系統用來整合內部資安設備威脅告警，提供企業及機關資安維運中心(SOC: Security Operation Center)管理服務。由 SOC 人員從事件單內容判斷發生威脅所在之相關資訊資產，並進行處理，再藉由事件單的自動聚合子單及誤判篩選機制，來降低非資安事件的誤告警比例。

特色

- 採用 SOAP 標準之 Web Service 界面，接收來自 SIEM 產品之威脅告警訊息（目前可收容 Splunk 及 ArcSight ESM，亦可增購客制化費用收容其他 SIEM 設備告警），另外也可透過手動介面自行輸入告警案件，統一納入系統管理
- 完整事件單處理流程紀錄及簽核管理，且結案內容應由主管進行審查，以滿足資安稽核的要求。
- 提供有關組織架構及人員帳號管理功能，可採用 Windows Active Directory 同步及標準 CSV 檔匯入(組織人員名稱)，或可透過 LDAP 身分驗證
- 資訊資產管理：提供資訊資產與處理人員建立連結，於告警威脅案件發生時，可自動寄送給處理人員及簡訊通知
- 提供資產價值及威脅風險指數，以確認是否升高或降低事件風險等級
- 提供案件簽核稽催與每日定期通知，可設定風險等級及所需完成之處理時數，超過通報時間或處理案件時間及可於每日定期稽催信件進行提醒
- 可整合連動 N-SOC 及 N-ISAC 回傳功能，以符合機關或其他領域須回傳事件紀錄之客制化開發作業
- 事件轉派：若原處理人員需將事件移轉給他人處理時，可透過轉派功能將事件移轉其他人員處理。
- 事件結案：事件處理完畢後依其處理人員之組織階層架構及簽屬層級數量，將事件呈請主管審查結案
- 內建提供下列威脅管理相關報表（1）每月事件單總表（2）處理時間總表
- 內建完整通報知識庫內容，並可對應 Mitre ATT&CK v7

產品畫面

中華資安國際
CHT Security
SOC 工作臺 / 通報作業
新增客戶
中華資安國際 / 許楨哲
資安儀表板
AI 巡檢服務報告
個人事件(故)待辦事項
單位事件單管理
代理人處理專區
資安預警情報
惡意中繼站清單下載
SOC 工作臺
通報作業
事件(故)處理作業
通報/事件單管理
通報及處理 SLA 設定
通報單
異常單
誤判單
待通報列表
手動開單
併單
轉異常單
註銷並關單
請輸入關鍵字搜尋
顯示欄位
資料更新時間 : 2020-10-13 15:01:33
重載
事件單號
客戶名稱
開單時間
通報事件名稱
原始紀錄
原始事件發生時間
處理狀態
狀態
暫無資料
共 0 筆
10 筆/頁
跳至
頁
未通報數量
通報完成比例
已完成
未完成 (未通報 & 通報中)
未完成: 1 (0%)