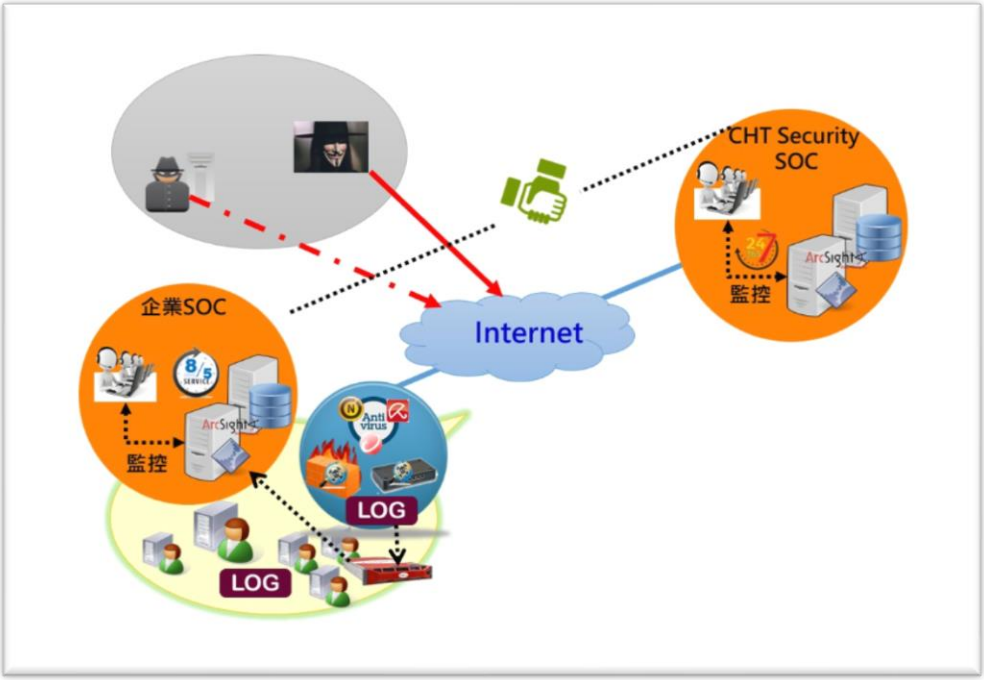
中華資安國際
CHT Security

SOC 監控

概述

網際網路的普及以致於資訊網路環境中充斥駭客入侵、攻擊、網路釣魚、探測、電腦病毒、蠕蟲和間諜軟體等威脅事件，也因技術的不斷進步，駭客攻擊模式也就更加多元化，面臨到的資訊安全事件也日趨複雜。

企業與組織在遭受資安威脅或駭客入侵時，往往無法於第一時間得知情況並處理，透過資安監控服務，讓企業與組織可以即時瞭解內外部資安威脅，以便在第一時間內對資安事件做應變處理，將損害降至最低。



特色

- 透過 EDR、NDR 及巨量資料技術進行多維度分析，挖掘未知威脅，提高偵測率
- 建立戰情中心，整合事前檢測、事中監控與端點鑑識，快速提供決策應變
- 介接全方位聯防機制，分享威脅情資，防範事件於未然
- 結合日誌巨量資料分析、網路軌跡分析(NDR)與威脅情資，挖掘未知威脅與潛伏攻擊，提高偵測率

- 結合端點入侵威脅評估(EDR)關聯分析，提升監控通報的準確率
- 建立日常連線基礎值，分析差異與特徵，找出未知惡意中繼站
- 接收威脅情資並即時回饋採取聯防應變措施，建構預警防護體系，縮短資安事件回應時間
- 協助客戶緊急應變、定位入侵管道、評估受影響範圍及回復受駭系統

需求規格

本產品依客戶需求，可分三個規格，分別為如下：

1. 低流量-EPS (Event Per Second): 900 / 故障總時間小於 104 小時
2. 中流量-EPS (Event Per Second): 2300 / 故障總時間小於 78 小時
3. 高流量-EPS (Event Per Second): 4900 / 故障總時間小於 52 小時

機關訂購前可根據日誌種類 EPS 參考表，加總機關內擁有的資安設備 EPS，計算監控所需要的 EPS 總量。