

# 網路資訊集納系統ED-CIC

除了外部攻擊、內部機敏資料外洩之外，「使用者的網路使用習慣」常常成為資安漏洞，造成資安防護上的困擾。就算每年例行性做滲透測試或是資安演練，還是可能會有使用習慣不佳或疏忽造成資安事件發生。

「ED-CIC」是使用者網路行為分析/威脅分析工具，除了詳細的行為紀錄及多樣的視覺化統計圖表，明確呈現用戶網路活動及可能的威脅分析，並具備原始封包保留機制，可將保留的封包提供給檢調機關。

「ED-CIC」部署容易，支援導入4Gbps鏡像流量，接收PCAP封包。系統具備網路深層解析技術(DPI)，內建第七層封包處理功能，只需要將被監控流量導入，可關聯相關資料加以統計分析，提供包含網路行為、封包流向、用量統計等資訊。除了支援外掛Storage，提供封包保存功能(option)之外，並可以1:1封包複製輸出至其他系統。

「ED-CIC」具備IP/網段/群組之流量排名和分析、TOP N流量統計、攻擊行為統計(option)、攻擊類型統計(option)、嚴重等級統計(option)等視覺化統計圖表，更容易且直觀判讀網路狀況。

若要進一步檢視使用者行為內容，「ED-CIC」還可將封包輸出至「網路封包鑑識系統CFS」，進行網路內容解譯還原。

高彈性的監測機制，多樣化的視覺化統計圖表，「ED-CIC 網路資訊集納系統」適用不同網路環境，能夠有效監看使用者網路活動，協助診斷網路問題。

