國立臺北大學資訊工程學系 108 學年度專題

資安圖表分析系統

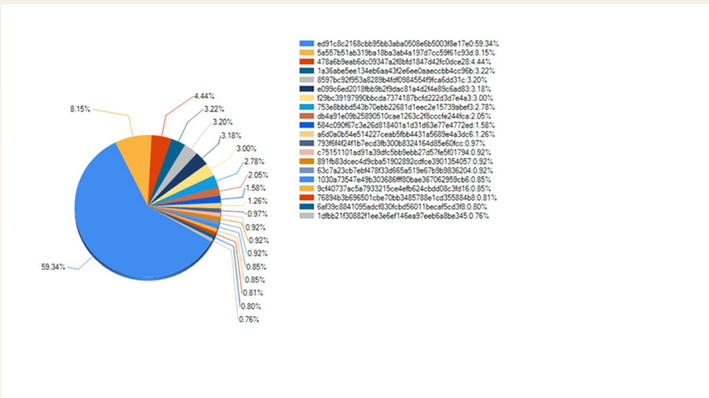
組員：陳致維、張揚鑫、任旻哲

摘要

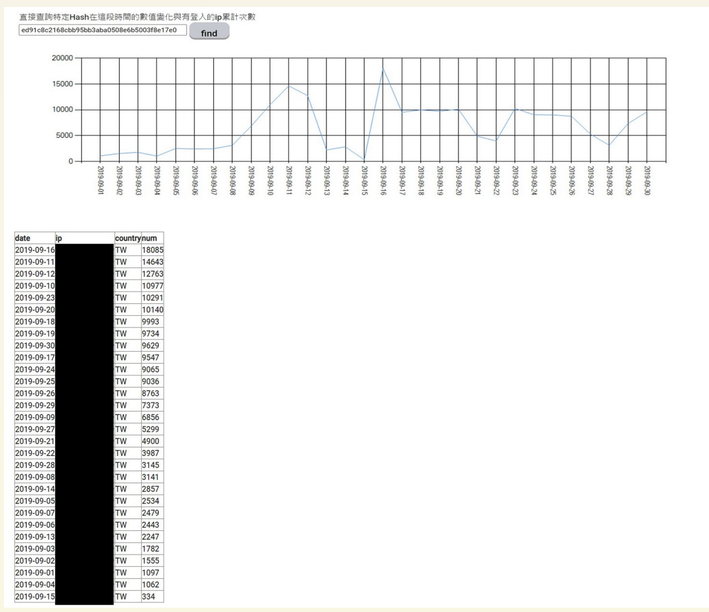
隨著科技的日新月異，網路的蓬勃發展，近年來網路攻擊事件層出不窮，所以現代人會用一些安全資訊和事件管理系統來做網路威脅的管理，進而提升本身的資安防護能力，但網路管理者或相關之研究人員在面對成堆的資訊，肯定是費時且費力。

FTP

FTP 資料來源透過 POP3 及 IMAP4 的電子郵件登入信息來獲取，我們可以拿來分析有沒有人在跳國別，代表著可能有人的帳號被盜取。



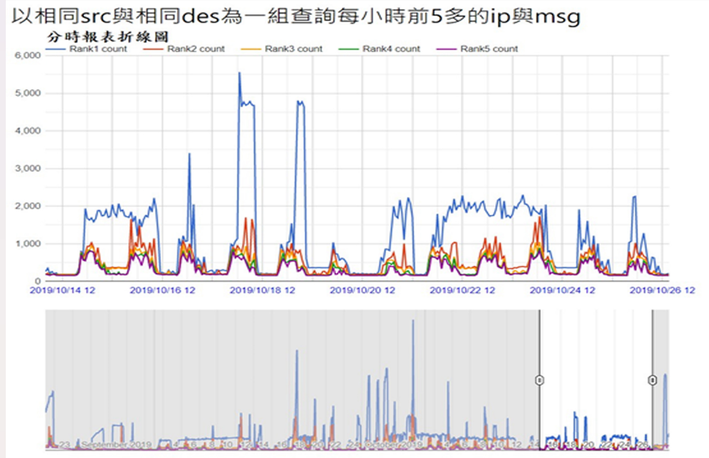
分析特定時間內 HASH 的數量排序之後的圓餅圖



查詢特定 HASH 在特定時間內登入次數變化及登入 IP 之統計

Firewall

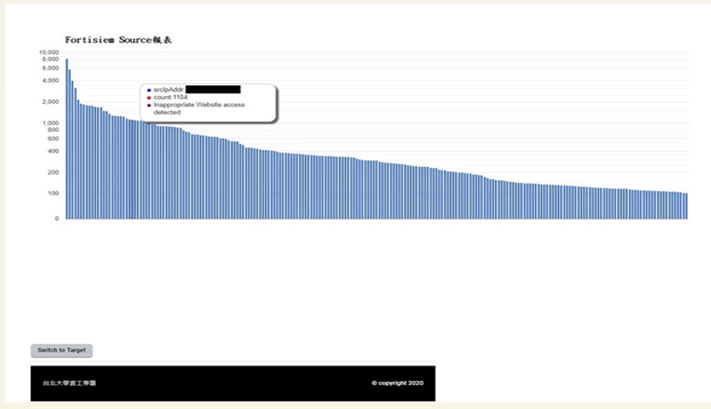
Firewall 資料來源是 PA/Sonicwal 的紀錄檔，我們透過 Kiwi Syslog 來取得。

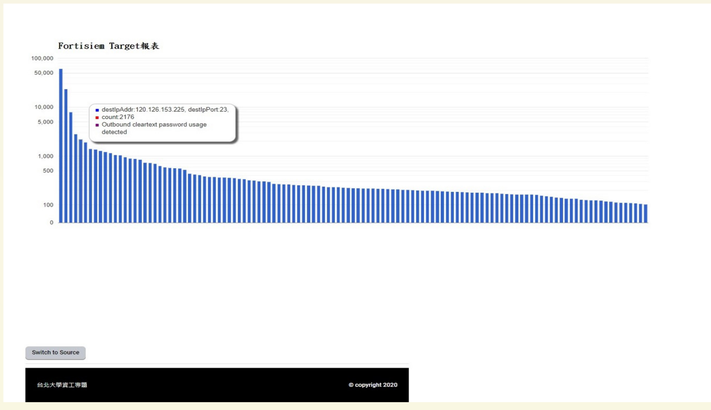


查詢前 5 多的被回報 IP 與其 msg，可以對被回報 IP 進行關注

FortiSIEM

類似 Firewall 的系統，可以分析的事件較多，資料量也很多。





透過 Switch 按鈕，可以切換對 Source 及 Target 的查詢，交叉比對後讓我們能防範某個特定的 Source 或對某個特定的 Target 做防禦的加強