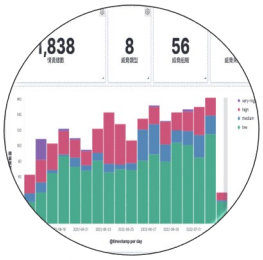
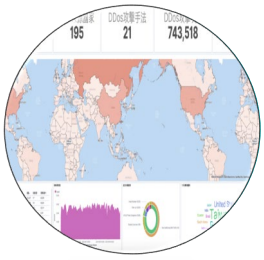
以零信任為基礎
資安戰情中心

現今的網路駭客攻擊，正在產生巨大的轉變，充斥著各種大量的，持續性的針對式攻擊，企業在佈署防火牆等資安設備建立邊際防禦時，應該參考NIST SP 800-207零信任架構，建立資安戰情中心(安全事件資訊管理系統，SIEM），導入以情資驅動的防禦策略，快速攔截攻擊，降低駭客的攻擊面，減輕防火牆等資安設備的負擔。



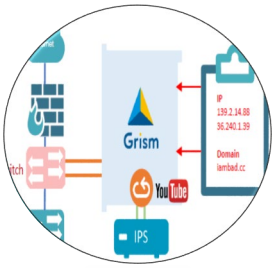
政策管理者 (PA)

透過API取得雲端情資中心的最新情資資訊以及入侵特徵指標(IoCs)情資，與戰情中心建立聯防機制。內建IoC事件分析報表，可一覽政策執行點的偵測與攔截報表，快速了解企業資安現況。



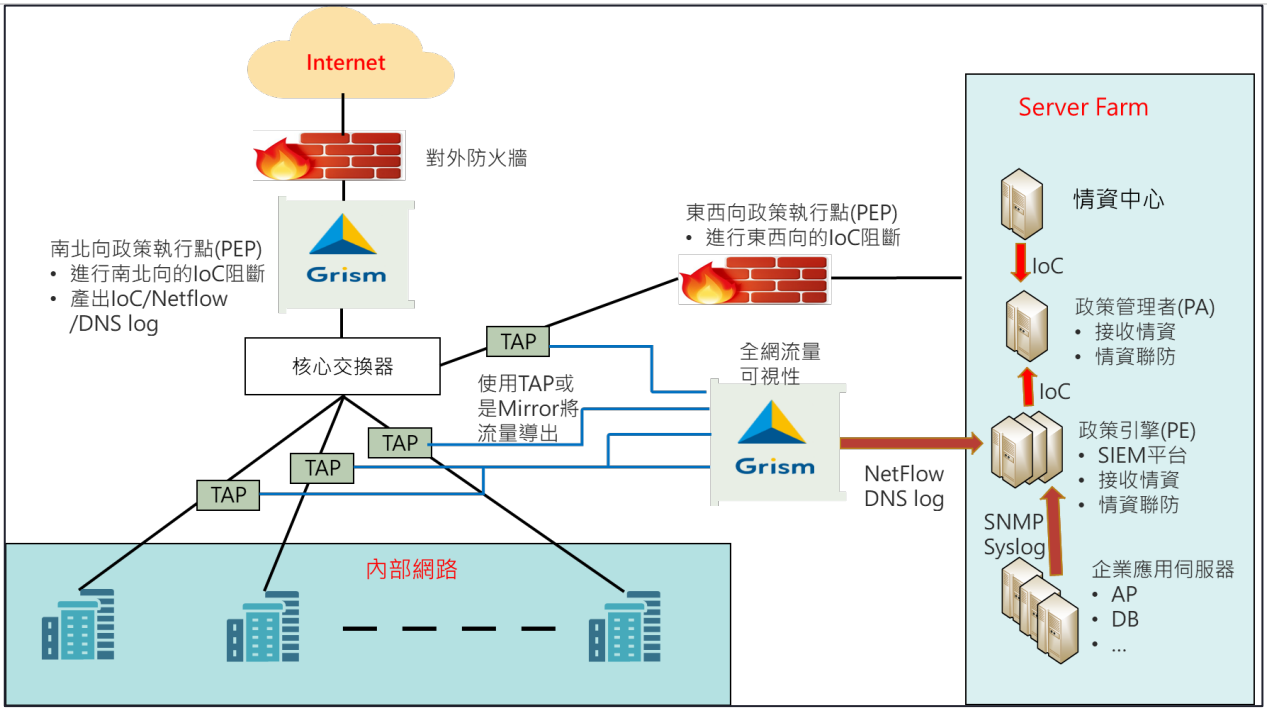
政策引擎 (PE)

完整的資安戰情中心功能，可收集大量網路資安日誌，包括政策管理者的情資資訊以及政策執行點的偵測與攔截事件。內建各式儀表板和報告功能，可將情資資訊與企業內的資安事件進行比對分析。



政策執行點 (PEP)

即時比對網路流量，包括IoC，NetFlow、DNS log、SSL log以及HTTP/HTTPS等等，可將偵測到的事件傳送到政策管理者或是戰情中心進行事件分析，針對IoC指標，可選擇即時阻斷。

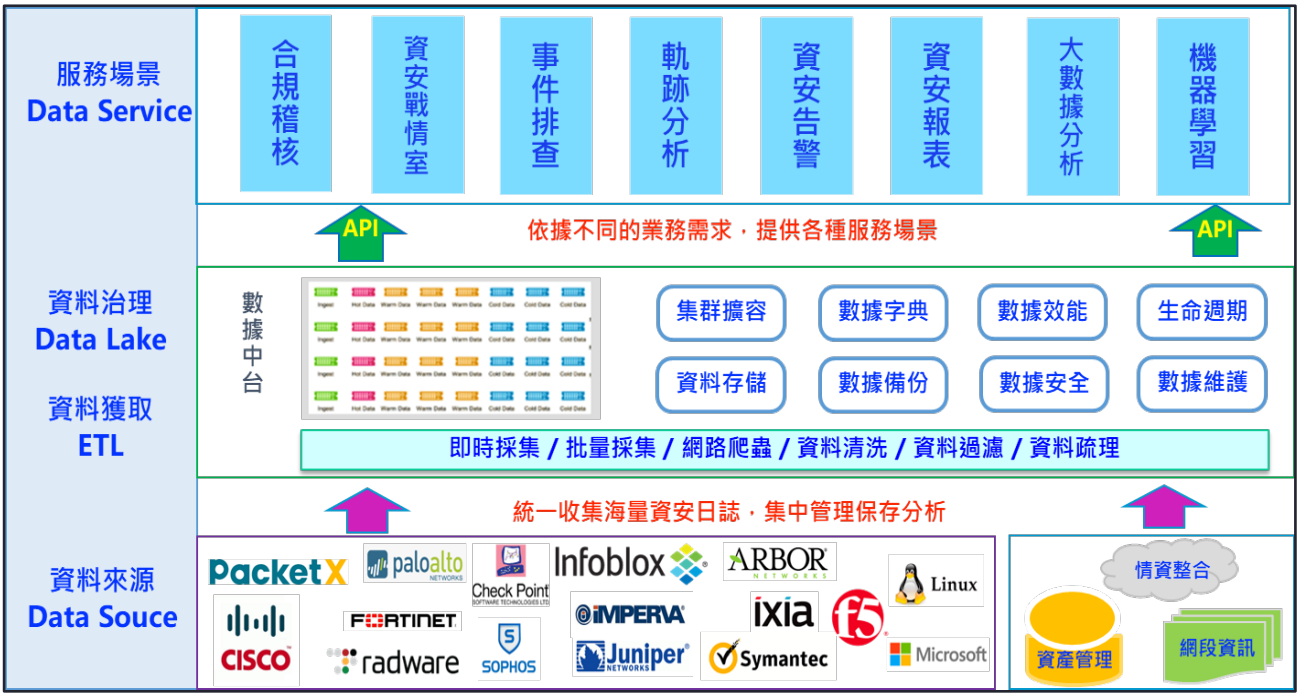


全網可視性與精準防禦

NIST指出，企業要能監控內部網路流量，（從連線中，依照資料的描述 (或 metadata)，取篩出目的、時間等所需資料，以便動態決定權限，所以企業設置戰情中心時，同時擔任政策引擎的工作，能夠統一收集多個資安設備所偵測到的事件以及Netflow等資訊，並建立儀表板與事件通報機制，與內建的或外部情資資訊，進行事件關聯分析，找出具備威脅性的事件，進行追查以及情資聯防。

政策執行點可以設置於於網際網路出口，或是在重要的網路節點上，統一由政策管理者(獨立運作，或是可安裝於SIEM平台)，派送情資至多個政策執行點上，進行情資聯防，補強次世代防火牆的情資功能，達到縱深防禦的效果。

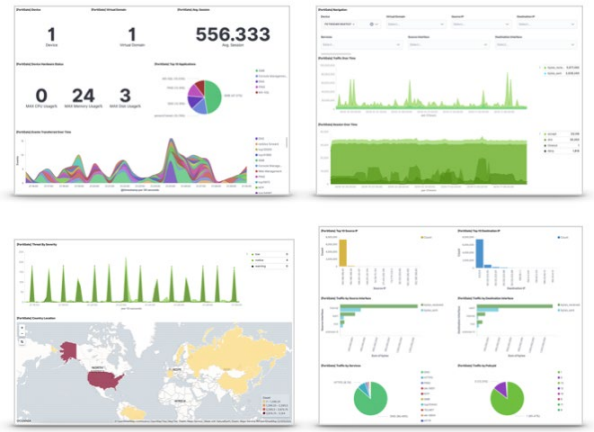
戰情中心(政策引擎，PE)



高速穩定的SIEM平台

集中不同的結構化資料和非結構化日誌，並進行關聯性的大數據整合，客製化儀表版、自訂事件告警、機器學習等等，以滿足各種大數據的應用場景和解決方案。可建置橫向擴容的資料集群系統，保證數據的安全和運行效能，並提供開放API以存取大數據資料。

可大量收容網路資安日誌，沒有日誌容量的限制，並提升資安事件的查詢時間，進一步整合情資、企業資產等資訊，打造完整資安戰情中心



創建多維度關聯分析彈性報表

- 效能與錯誤分析
- 流量分析
- 用戶連接分析
- 資安事件分析
- 符合ISO27001 的資安報表規範
- 檢查特權帳號的行為軌跡分析
- 情資報表

政策管理者(PA)

自動化取得雲端情資中心的最新情資資訊以及入侵特徵碼情資，同時與政策執行點建立聯防機制。

- 全自動化更新，無須人員介入
- 達到縱深防禦的效果
- 補強次世代防火牆的情資功能

企業快速檢視事件與追查

當企業面對駭客24小時不間斷的高低速的攻擊時，產生的告警風暴極為驚人，為了因應如此高效率的年代，需透過新世代解決方案，提供企業輕易的從不同角度進行分析和調查。

- 靈活的時間區間分析
- 內部連線惡意網址的IP列表

政策執行點(PEP)

情資驅動的防禦策略，進行偵測與阻斷，並可以依據監控策略，進行在線流量監控，將網路流量再進行複製、過濾與分配。

情資中心

每一至三小時提供最新IP名譽情資列表，將惡意訪問第一時間阻擋。所有IP名譽情資都經過分析、過濾、權重計算。IP名譽情資筆數約在數萬筆，依時間動態更新。

即時更新清單種類:

- 高風險惡意訪問 IP 清單。
- 洋蔥路由 IP 清單。

台元碼科技有限公司
www.softforce.app
台北市大同區太原路11巷29號

授權經銷商: