雲智維科技
Cloud Intelligent Operation

雲智維資通安全監控平台

www.cio.partners

雲智維資通安全監控平台採用訂閱制商務模式，用戶可以選擇月付或是年付方式等支付方式。資通安全監控平台負責 SNMP Polling 以及日誌(Log)接收，並將所得 SNMP 數值以及收到的日誌透過加密壓縮方式轉發至雲智維的分析中心。雲智維採用 SNMP Polling 方式監控用戶端網路設備的健康狀態，包括 CPU/Memory 使用率，介面(Interface)流量與 Broadcast/Error 訊息等，透過適當告警值(Threshold)的設定，針對超過告警值的狀況發出告警提醒維運人員。

平台功能

提供資通安全威脅偵測、資安威脅預警以及情資回傳作業等功能。監控範圍完整收容指定設備所產出之日誌(Log) 以及網路連線紀錄 NetFlow/sFlow 數據，前述所指設備至少包括 Core Switch、Firewall、IPS、Web Filtering、AAA、WAF、Mail SPAM、Anti-Virus 等，同時能透過 SNMP 監控前述設備之硬體健康狀態，確保各系統運作無虞，並可調閱查詢一年之內的日誌紀錄(Log)，機關視實際需求得調整監控設備範圍。

- 透過對上述網路連線紀錄 NetFlow/sFlow 數據的收集與分析，提供針對流量型 DDoS 攻擊和擴散型病毒爆發之即時偵測以及聯防阻擋之能力。DDoS 攻擊偵測功能至少包括 Host Scan、Flooding、Burst Session 等
- 根據日誌與網路連線紀錄 NetFlow/sFlow 數據的分析，產出「資安事件(Event)告警」，並進行影響性評估，針對確有存在有資安風險的事件再生成「資安通報單」，內容包括事件主旨、事件說明、MITRE ATT&CK Techniques ID、建議措施等。
- 遵循國家資通安全研究院訂定之「政府領域聯防監控作業規範 _GSOC 2.0」，辦理情資回傳，包含【資安監控單】、【設備狀況單】、【情資分析單】等。
- 可以電子檔、網頁呈現等方式定期產出月報、季報。內容包含但不限於下列：

服務月報：

(1) 資安監控與情資回傳分析：

(a) 當月「資安通報單」之產生數量以及回傳數量等資訊。

(b) 當月「資安監控單」之產生數量以及回傳數量等資訊。

(c) 當月「監控設備狀況單」，呈現其監控設備運作情形。

(d) 當月「情資分析單」之產生數量、回傳數量以及通知機關數量等資訊。

(e) 威脅情資之統計分析：提供當月來自外部的威脅連線 IP 清單資訊，協助機關用於黑名單阻擋以利資安強化。

(2) 資安威脅預警：

(a) 當月資安威脅訊息彙整，包含安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現安全漏洞與補救措施、資通安全事件報導、漏洞分析、修補方式或對策。

(b) 總結

服務季報：

(1) 資安監控與情資回傳分析：

(a) 當季統計分析

(b) 當季資安通報事件統計，包含事件主旨、

事件觸發規則及事件類別統計，近期機關遭受資安威脅的趨勢。

(c) 提供來自外部的威脅連線 IP 清單資訊，協助機關用於黑名單阻擋以利資安強化。

(d) 提供當季受監控設備產出之日誌量 EPS(Event Per Second) 資訊，檢視監控部署的成效。

(2) 資安威脅預警：

(a) 資安威脅預警訊息:資安威脅類型、摘要說明、可能造成之影響。

(b) 總結

- 提供資安威脅預警訊息，涵蓋自有以及其他資安組織所發布之資料。預警訊息內容包含：
  - (1) 案例分享：近期國內外資安事件案例。
  - (2) 資安威脅情資：提供惡意中繼站、高風險惡意特徵之清單(IP 與域名)。
  - (3) 病毒資訊警訊：如趨勢科技及 Symantec 等防毒廠商中級以上病毒警訊。
  - (4) 系統弱點公告：如 NCCST、Microsoft、各國 CERT 等國內外資安組織公告。
  - (5) 網頁攻擊資訊：如 Zone-H、OWASP 資安組織公告等。
  - (6) 新聞事件：如 CNN、Google 及 Yahoo 等國內外資安新聞資訊。
  - (7) 廠商發現之威脅：如 Zero-Day 事件。
- 提供可視化資安戰情儀表板(Dashboard)，能夠呈現即時告警事件與流量排行等訊息，並可根據需求自行定義與調整 Dashboard 呈現內容、圖形樣式、格框大小與畫面排列位置，提供多種時間區段(一小時/一天)選項，儀表板(Dashboard)內容至少包含：
  - (1) 資安事件依據嚴重等級統計分析
  - (2) 嘗試入侵本機關之外部 IP 且名列威脅情資之即時資訊呈現與排名統計
  - (3) 機關內部 IP 連線外部威脅情資之即時資訊呈現與排名統計
  - (4) 即時呈現機關內部發生 DDoS 攻擊如 Host Scan、Flooding、Burst Session 等之攻擊來源 IP 和受害主機資訊
  - (5) 即時呈現來自外部的 DDoS 攻擊如 Host Scan、Flooding、Burst Session 等之攻擊來源 IP 和受害主機資訊
  - (6) 帳號鎖定以及密碼猜測行為
  - (7) 外部訪問本機關網站之連線數(Session)以及封包(Packet)大小(64/128/256/512 Bytes)分時圖
  - (8) 提供網站的瀏覽延遲(Latency)監控

雲智維科技 (Cloud Intelligent Operation, CIO)

Tel : 04-23755010 www.cio.partners

技術支援 : center@cio.partners

業務聯繫 : sales@cio.partners