雲智維科技
Cloud Intelligent Operation

雲智維 CIO

網路數據與資安事件分析管理平台

www.cio.partners

雲智維網路數據與資安事件分析管理平台採用訂閱制商務模式，用戶可以選擇月付或是年付等支付方式。雲智維自建專屬的維運與數據分析中心，透過電子郵件、電話說明、視訊會議等方式提供服務給訂閱的客戶，Golden 用戶的服務時間為周一到周六 8:00 至 19:00， Premium 用戶則為周一到周日 7:00 至 23:00。

網路數據與資安事件分析管理平台負責 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。支援 Switch Port Mirror Traffic 接入，能產出 1:1 NetFlow 數據以及 DNS 查詢紀錄(DNS Event Log)，並透過加密壓縮將產出數據轉發至雲智維分析中心。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，協助提醒維運人員。每一 Golden 等級的訂閱適用於納管設備低於 20 部(含)以下的環境，而每一 Premium 等級則適合有 21-50 部納管設備的環境。用戶可以根據需求選購多個 Golden 以及 Premium 等級的方案。前述所謂納管設備包含網路設備(Router/Switch/Wireless)、伺服器以及應用服務(Service，ex: Web/DNS/Mail/AD/DHCP/DB)、資安設備(ex: FW/NGFW/IPS/WAF/UTM)。

功能

- 接收來自中繼設備的 SNMP/NetFlow/Log 數據，以主動告警、Dashboard 或是日/周/月/季/年報表形式提供以下分析，幫助機關資訊維運工作：
  - (1) 設備健康顯示
    - (a) 設備總數與障礙數
    - (b) 重要設備 CPU 使用率
  - (2) 網路使用分析
    - (a) 對外頻寬流量圖
    - (b) 內部 IP/電腦名稱使用 Internet 頻寬 TOP N 排名報表
    - (c) 知名服務(Google、Line、Microsoft 等)使用 TOP N 排名報表
    - (d) 瀏覽網站 TOP N 排名報表
    - (e) 網路服務協議(HTTP/HTTPS、Mail、FTP 等)使用 TOP N 排名報表
    - (f) 瀏覽企業官網的外部來源 IP 所屬國家 TOP N 排名報表
  - (3) 資安相關
    - (a) 事件依據嚴重等級統計
    - (b) 資安事件 TOP N 排名報表
    - (c) 內部 IP/電腦名稱出現資安事件 TOP N 排名報表
    - (d) 與威脅情資資料庫比對結果
  - (4) 智慧分析結果
    - (a) 發生異常流量事件
    - (b) 發生異常事件行為事件
    - (c) 原廠證明收集之 SNMP/Flow/Syslog 數據不含郵件內文、通信軟體內容、個資法規範之密碼與金融相關機敏資訊
- 收集 Windows AD 記錄、DHCP 伺服器記錄(DHCP Log)或 IP 對應表，將網路架構裡的 IP 地址轉換成人名或是電腦名稱，掌握人員使用行為。
- 24 小時不間斷收集網路數據，搭配 AI 學習分析技術，監控連線行為，掌握出現異常連線的電腦並隔離。

- 若用戶授權，將遠端協助設定閘道防火牆的封阻策略(Aceess Deny)以啟動聯合防禦，將具有威脅的連線外部來源 IP 阻擋在閘道防火牆設備，以及將來自內網的威脅阻擋，禁止聯外。
- 提供趨勢預測(Prediction)功能，以歷史數據建立走勢模型，包括網路設備與伺服器 CPU/Memory/Disk 使用率、線路頻寬、品質量測 RTT(Round Trip Time)等，提前告警資源不足狀況。

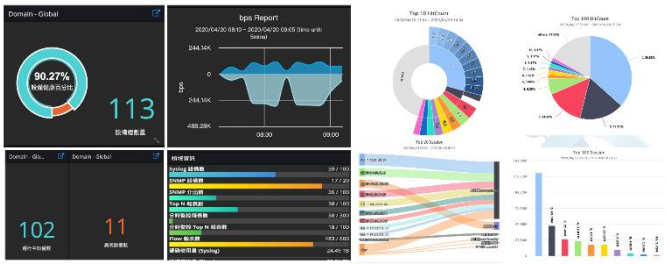
Premium 方案

網路數據與資安事件分析管理平台監控與優化內部網路服務(WEB/DNS)品質，包含兩種延遲監控方式：一是用 ICMP 持續發出測試 Ping 封包用以收集網路的延遲數據(Round Trip Time, RTT)；另一個則是針對被監控的網頁服務(Web Service)定時且持續模擬人們瀏覽該網頁，將整個過程的反應時間記錄下來進行分析。藉由不同角度的模擬瀏覽監控，將更能即時掌握服務的狀態，並在延遲出現非預期的上升時提出告警。

Premium 用戶可以登入雲智維智慧維運系統所提供的專屬網頁(Web Portal)，如同自己在企業內建置了一套網管與日誌分析系統。除了內建的報表與監控可視化面板(Dashboard)以外，Premium 用戶也可以根據自己的需求新增報表。

Web Portal 功能

- 支援 2D/3D 全球視覺的攻擊動態即時呈現。
- 可同時設定多個查詢條件，包括來源設備、事件關鍵字(Keyword)、IP、嚴重等級(Severity)、國家/地區、AS、時間區段、使用者名等。
- 呈現事件紀錄(Event Log)內容，包括發生在哪一台設備、來源 IP/Port/名稱/國家、目的 IP/Port/名稱/國家、發生時間、事件名稱、發生次數(hit count)等。



- 呈現流量紀錄(Flow Record)內容，包括來源 IP/Port/部門名稱/國家/所在 Switch Interface、目的 IP/Port/部門名稱/國家/所在 Switch Interface、Byte/Packet/Session、時間等。
- 可自行定義與製作 TOP N 統計報表，選定時間統計區間、事件關鍵字(Keyword) 、Source/Destination IP、Source/Destination Port、設備、圖表型態等參數，產出時報、日報、週報、月報、季報、半年報與年報等各種報表。報表格式包括：PDF、CSV、HTML、XML 等。
- 儀表板功能(Dashboard)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。

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