產品型錄

radiflow

iSID工控安全威脅偵測

- 自動學習工控環境中的網路拓樸(Network Topology)與操作行為(Operational Behavior)
- 本地部署iSID或分散部署iSAP Smart Collector的彈性部署架構
- 利用深度封包檢測(Deep Packet Inspection, DPI)技術針對SCADA網路流量進行分析
- 監督PLCs中的配置變更
- 利用模型分析進行網路異常偵測以及特徵比對方式發現已知漏洞
- 非侵入式網路運作機制
- 低誤報率 (Low False-Alarm Rate)
- 透過iCEN中央管控系統整合分散於各處的iSID系統

多層次資安防護提供全面的威脅檢測

iSID採取多種資安防護技術，毋須中斷現行運作中之工控網路即可分散部屬於各處並監視網路活動與拓樸架構。 這些技術個別針對特定類型的網路活動提供獨特的功能：

1. **網路可見度：**
   透過被動掃描(Passive Scanning)來檢視所有OT網路流量，iSID便可為所有設備、網路通訊協定及連線數據建立視覺化網路模型，並在檢測到有可疑變更時（如：出現未知的設備或連線）主動發出告警。
2. **網路攻擊：**
   根據來自研究實驗室的數據以及Radiflow所屬的研究結果，處理針對工控網路所設計的已知威脅，包括PLCs, RTUs和工業通訊協定。
3. **政策監控：**
   為每個網路連線定義/修改防護政策，用於驗證特定命令（例如：寫入控制器）和操作範圍（如：不可將渦輪機轉速設置高於800轉）。
4. **維護管理：**
   當特定設備在特定時間內的維護工作進行時，可透過設定來限制維護期間的網路暴露風險。當維護階段完成後，可產生所有維護工作的活動日誌報告。
5. **異常檢測：**
   使用多種參數來建立網路行為分析模型，包括設備序列採樣時間、操作值的頻率等，用於檢測異常行為。
6. **操作行為：**
   監視和稽核外部站點設備（PLC, RTU & IED）的管理，並可發出韌體變更或配置修改（如：軟體更新或是開啟/關閉了設備）以及活動紀錄的告警。

ABOUT RADIFLOW

Radiflow 為關鍵基礎設施 (Critical Infrastructure, CI)業務運營開發單位所值得信賴的工業網路安全解決方案。

Radiflow改變了ICS/SCADA網路安全防護的遊戲規則，其解決方案組合使客戶能夠保持對其OT網路的可見度和控制。

Radiflow的智慧工業網路安全威脅檢測和分析平臺可最大限度地減少OT環境中的潛在業務中斷和損失。

Radiflow的團隊由來自不同背景的專業人士，來自精英軍事單位的網路專家以及來自全球網路安全供應商的自動化專家組成。

Radiflow解決方案成立於2009年，以成功部署於主要工業企業和公用事業單位，保護了全球3,000多個關鍵設施。

常見使用情境

技術人員到場維護

iSID會自動在預先定義的維護時間內監控技術人員的維護活動，超過維護工作所定義的範圍會觸發告警。

未經授權的PLC配置變更

iSID會檢測可能影響PLC配置的已知協定命令。

Black Energy (BE) 惡意程式

iSID可明確地識別出Black Energy惡意程式並發出告警，並檢測來自Black Energy SCADA外掛程式的未授權的SCADA命令，以及整體工控運作程序中的異常行為。

間諜軟體

iSID會透過掃描網路活動來發覺試圖針對SCADA設備（如：PLCs和RTUs）進行滲透攻擊的間諜軟體。

中間人（Man-in-the-Middle, MITM）攻擊

iSID會透過MAC偽冒或IP位址盜竊來檢測網路中冒充合法伺服器、工作站或SCADA控制器的惡意設備並發出告警。

SCADA伺服器攻擊

iSID會檢測工控系統中的變化並告警，包括命令序列和時序中的命令序列以及時序異常。

集中管控與分散部署iSID

iSID可部署在企業中心，搭配iSAP為各處外地站點提供威脅檢測；或是直接在每個外地站點使用iSID進行本地威脅檢測（亦可兩者組合使用）。

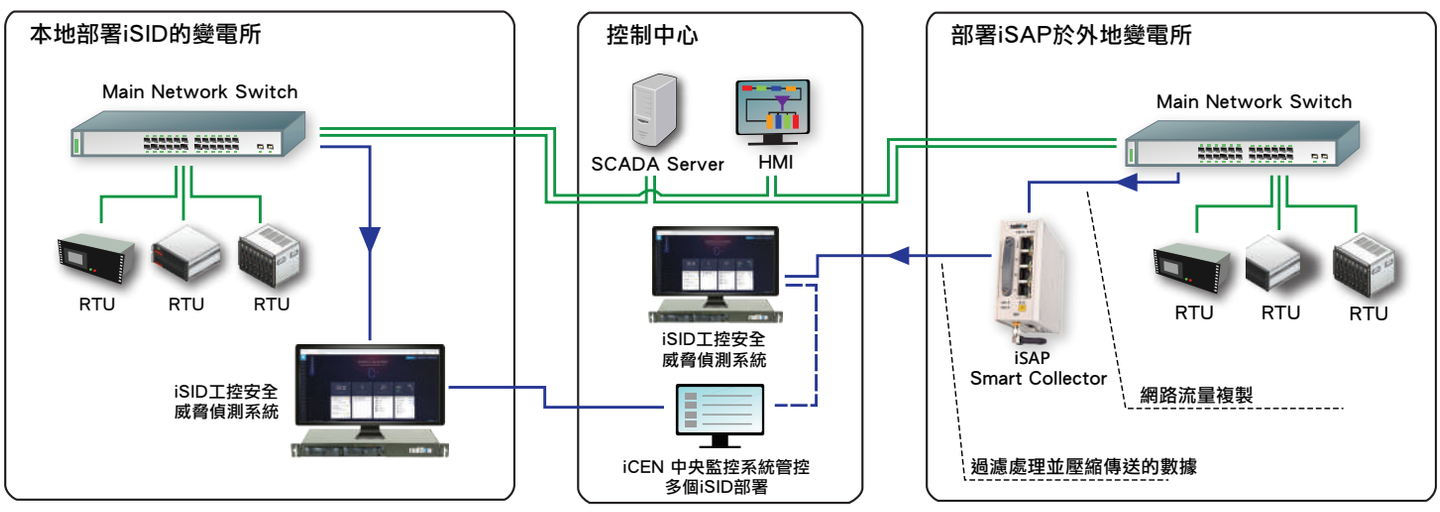
由於從每個站點向中央部署的IDS發送大量資料，通常會造成網路過載(Network Overload)的問題。

Radiflow的 iSAP Smart Collector就是為了解決這個問題而設計：部署於各處外地站點，透過當地網路交換器所提供的網路資料來篩選過濾與分析，只保留有用的SCADA傳輸封包（如：ModBus數據）。

為了進一步防止網路過載，過濾後的資料會透過加密的VPN通道壓縮傳送至中央部署的iSID系統。

使用Radiflow的iCEN中央監控系統對多個iSID系統（一般來說大型網路架構的站點建議使用）進行監視與管理。iCEN提供每個iSID的運作狀態、持續檢測的摘要資訊（如：網路風險狀態、檢測到的事件）和系統運行狀況等資訊。並可用於遠端軟體更新和維護作業。

部署架構



iSID部署示意圖：結合位於控制中心的中央監控系統（iCEN）以及分散部署於各處變電所的iSAP Smart Collector。