PoExtract
SOOP-CLM集中式日誌管理平台

Service-Oriented Operation Portal - Centralized Log Management

SOOP-CLM 是一個高性價比的企業級集中化日誌管理解決方案，由於它吃到飽授權特色，可以集中收容多樣性的日誌來源與不同的日誌格式，並進一步分析、關聯、儲存及視覺化日誌資料。不但一次滿足政府法令及稽核等需求，也是企業面對資訊安全與大數據時代的堅強後盾，更可以結合其他第三方解決方案，節省整體擁有成本，增加企業競爭力。

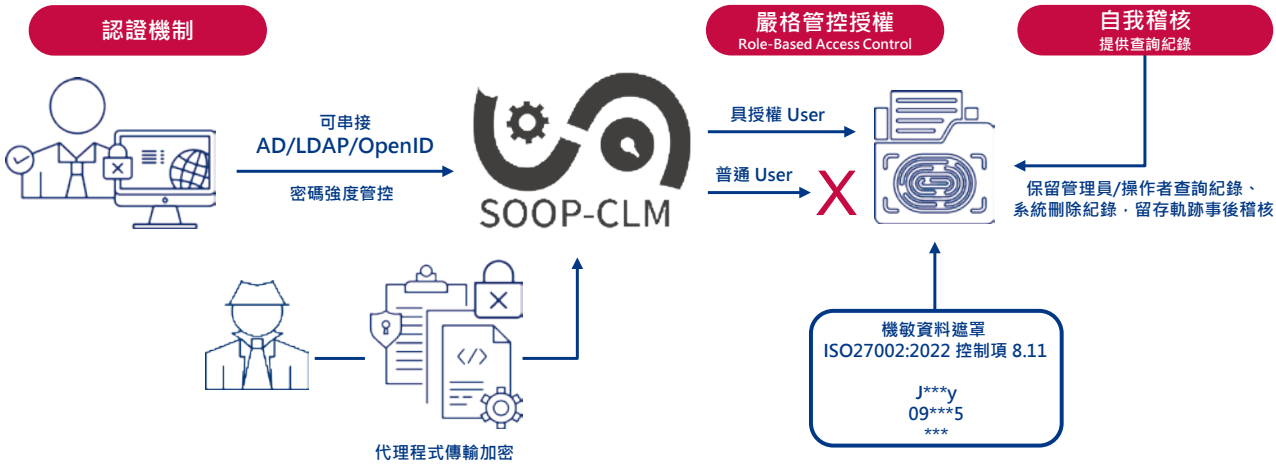
資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌（OS event） 2. 網站日誌（web log） 3. 應用程式日誌（AP log） 4. 登入日誌（logon log）
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄。	

強大的集中收容能力，便於高效率查找及降低資料流失風險

可集中收容眾多裝置上不同格式的日誌資料，透過內建的多樣解析模組分析關聯所收容的各種日誌資料；提供關鍵字查詢並視覺化相關資訊，平均百萬資料秒級回應； 若結合 Data Queue 模組，作為蓄洪池之用，避免突發大量流量衝擊下，資料遺失風險；亦可將長期歷史資料壓縮儲存或整合 Hadoop 作為資料倉儲之用。

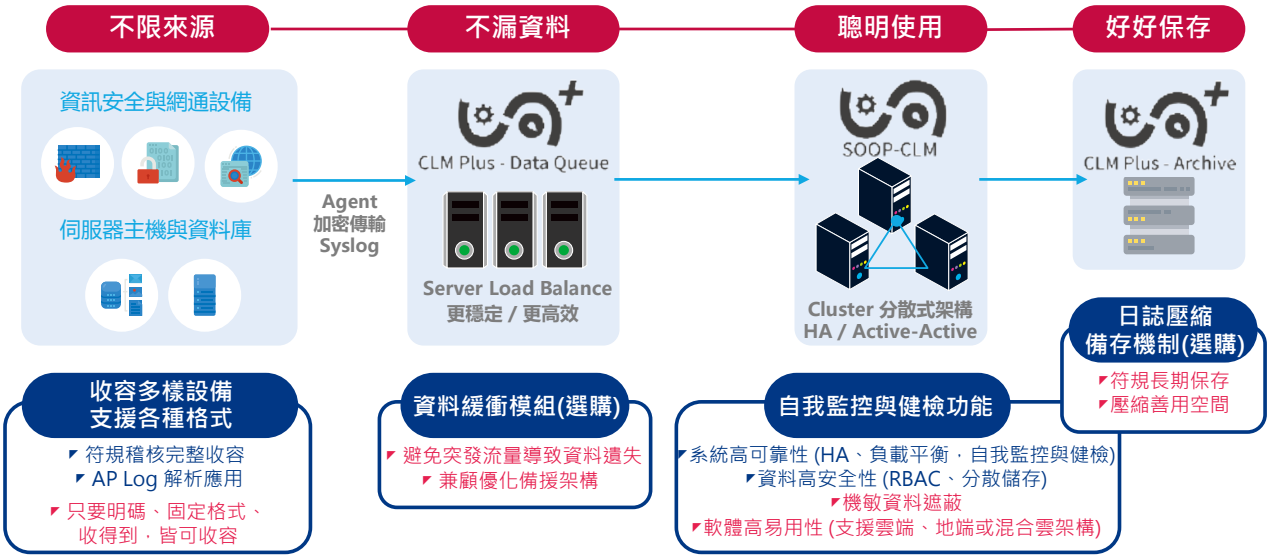
功能完整的日誌管理解決方案，易於操作上手及符合稽核管理要求

支援 AD/LDAP 及 OIDC 認證方式，具備密碼管控機制，嚴格的 Role-based 存取控管權限，內建Document Level Security 以符合 ISO-27001 要求，保護日誌資料且具不可竄改性，並可留存歷史資料以符合 ISO 27001 與 PCI DSS 等日誌稽核項目，達到法規遵循及企業稽核標準；提供簡易人機操作介面，可於 Web UI 上設定告警、報表排程和日誌解析規則等日誌管理功能，降低學習曲線；內建多樣視覺化模組，或運用時間過濾功能和拖拉式自定義儀表板功能，快速滿足不同視覺化需求。



穩定可靠的分散式架構設計，有效降低維護負擔，避免單點失效風險

去中心化架構的分散式運作叢集設計(Active-Active)，內建 Load Balance 機制，支援雲端、地端或混合雲架構，輕鬆達到簡易擴充，高可用度的目標；透過 SOOP-CLM 的自我監控及健檢功能，維運人員可輕易的掌握系統平台當前狀態，當系統平台運作遭遇瓶頸時，可協助迅速排除異常，大幅降低管理難度；內建防呆機制，可阻擋一般性不當之人為操作或管理疏忽。

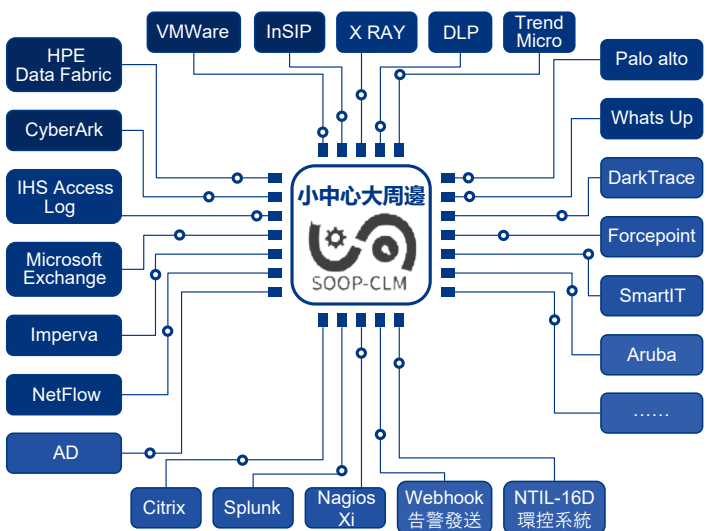


智能告警機制，提供真實的趨勢分析及反映真實狀況

SOOP-CLM 內建的動態閾值透過先進的演算法，自動依據過去的歷史數據，為不同時段定義更貼近現實的閾值，協助判斷是否發生異常，有效提升網路與資安告警的精準度，降低發送 False Alarm 的機率，協助用戶第一時間察覺異常，同時加速排除作業，提升系統可靠度，進一步推升使用者滿意度，達到早期告警、快速定位、高效維運的目標，如此一來，即可快速、精準定位異常範圍，有效減少排除異常時間，降低管理成本，提升維運效率。

小中心大周邊設計理念，整合其他第三方解決方案，擴大投資效益

提供多種 API，方便用戶整合或開發各種面向的第三方應用服務；在 IT 維運環境中，整合多種監控工具數據視覺化呈現，作為 NOC 之用；串接大數據平台，挖掘其中商業價值，擴大投資效益；整合 AIOps 工具，搭配 RPA 等機器人流程自動化工具，進行主動修復及預測分析等應用，讓 IT 管理更智慧化，加速企業數位轉型；結合 SOC 等資安軟硬體產品，不但可作為資安聯防一員，並可留下數位軌跡，以利數位鑑識查找，輔助資安政策制定。SOOP-CLM 的高整合性能發揮各產品的最大效益，節省整體擁有成本，增加企業競爭力。是企業在面對資安風險和 AI 時代的最佳選擇。



高性價比的計價方式，輕鬆擁有無後顧之憂

免費支援新設備的日誌解析處理，不必煩惱往後日誌平台維護支出增加；授權不限流量/EPS/容量/CPU/Memory/日誌來源設備數/日誌量/操作使用者數量，透過擴充硬體資源或節點方式，彈性部署節省使用成本；不斷推陳出新的日誌應用及插件，將投資效益發揮到最大；內建多樣化應用服務，大幅縮減客製化開發的時程及負擔；基於開源具備高自由度及在地支援，有效減少未來轉換成本和使用風險；國外官方維護及本地多方弱掃，雙重保障確實降低資安疑慮；客戶橫跨政府/金融/電信，產品經多方檢驗，品質成熟穩定有保障。