SOOP-CLM
集中式日誌管理平台

Service-Oriented Operation Portal - Centralized Log Management

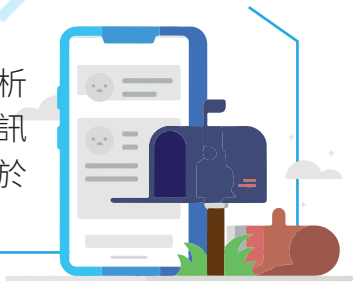
產品定位

SOOP-CLM是一個高性價比的企業級集中化日誌管理解決方案，它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。不但一次滿足符規、稽核及IT維運等需求，也是企業面對大數據資料與AI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。

產品六大特色：

1 強大的集中收容能力，便於資料分析及高效率查找

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；提供儀表板視覺化相關資訊，平均百萬資料秒級回應；亦可將長期歷史資料壓縮儲存於Hadoop，作為倉儲之用。



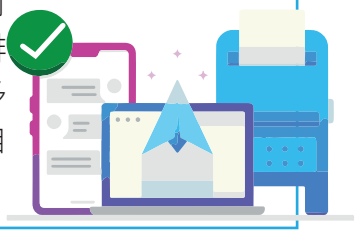
2 功能完整的日誌管理解決方案，易於操作上手及管理使用

支援AD/LDAP及OIDC認證方式，具備密碼管控機制，嚴格的Role-based access control控管存取權限，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，方便使用者彈性運用。

PiExtract 信研科技股份有限公司 台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com

3 穩定可靠的分散式架構設計，有效降低維護負擔及提高服務品質

去中心化架構的分散式運作叢集設計，輕鬆達到簡易擴充，高可用度的目標，大幅降低管理難度；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；內建防呆機制，可阻擋一般性不當之人為操作或管理疏忽；提供多種API，方便用戶擴展開發各種面向的應用服務；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。



4 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。

5 整合其他第三方解決方案，節省維運成本或擴大投資效益

透過SOOP-CLM第三方整合能力，能有效減少許多以流量/CPU/OS或日誌量計價的軟體授權費用，亦不需擔心未來因日誌量增加需負擔的額外授權費用，如利用SOOP-CLM避免SIEM工具的授權費用增加。在IT維運環境中，整合多種監控工具數據提供整合視覺化呈現，減少解決問題時間及降低人力成本，如整合AP/Infra/DB/Docker/Cloud等相關監控管理工具。串接大數據平台，除提供日常資料備份、定時稽核外，並可挖掘其中商業價值，擴大投資效益，如Hadoop/TeraData/MongoDB等大數據平台。整合AIOps工具，加入AI/Machine Learning等演算法建立預測模型，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管理更具智慧化，加速企業數位轉型。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。是企業在面對大數據資料和AI時代的最佳選擇。

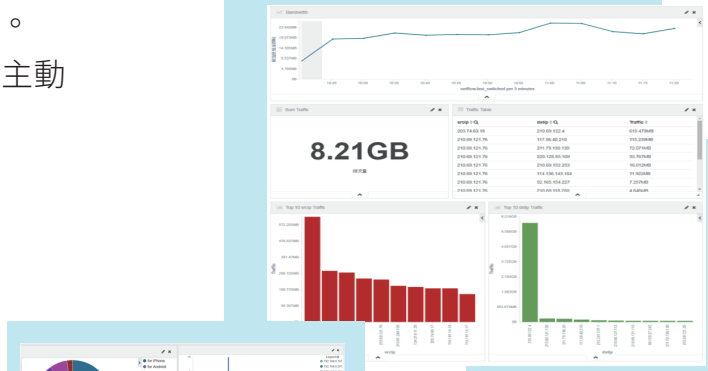
6 高性價比的計價方式，輕鬆擁有無後顧之憂

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。

PiExtract 信研科技股份有限公司 台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com

成功案例 – IT 日常維運

利用SOOP-CLM集中收集400＋台伺服器，200＋台網路設備之日誌資料，每日收集超過 150GB 的日誌資料。
當SOOP-CLM發現系統狀況異常時，SOOP-CLM會主動發出通知，讓維運人員可即時掌握系統狀態。



導入SOOP-CLM的效益

快速查詢，降低問題查找時間

- 在單一平台透過關鍵字查詢相關日誌資料，交叉比對，縮短服務恢復時間： 2小時 => 0.5小時。
- 將日誌視覺化呈現，可一眼看出相關項目是否異常，以便維運人員做出對應的處理。

藉由日誌集中管理，強化日常維運效率

監控『異常登入行為』、『單一IP流量大幅增加』及『不被允許的設定變更』等等行為，強化管理。

成功案例 – 資安/稽核應用 ISO 27001

符合資訊安全稽核需求

符合 ISO 27001 日誌稽核規範

A.12.4 存錄與監控 (目標：紀錄事件與生成證據)

(1) A.12.4.1 事件存錄

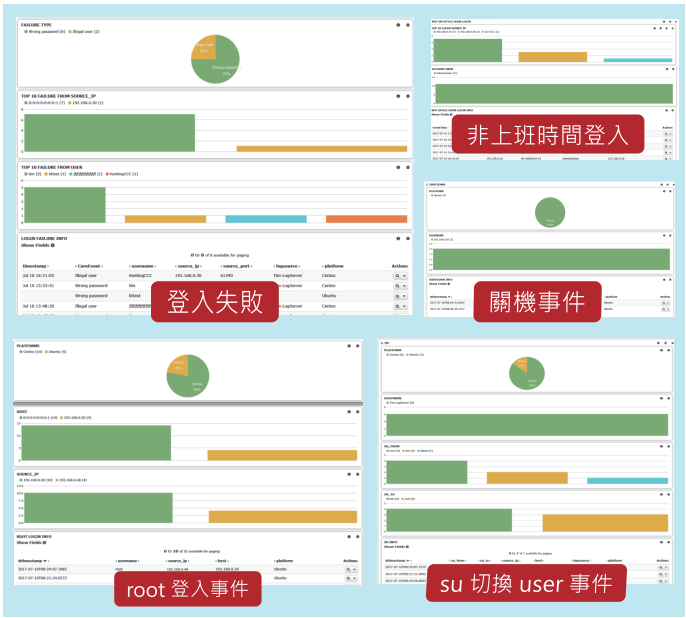
事件日誌係紀錄使用者活動、異常、錯誤及資訊安全事件，應產生並保留且定期審查。

(2) A.12.4.2 日誌資訊的保護

應保護存錄設施與日誌資訊，不受竄改與未經授權的存取。

(3) A.12.4.3 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄、保護並定期審查。



A.12.4 存錄與監控

導入SOOP-CLM的效益

建構 ISO 27001稽核儀表板，提升資訊安全

清楚呈現所有資訊，協助客戶符合ISO 27001日誌稽核項目，以提升整體資訊安全性。

日誌統一管理，簡化稽核流程

- 大幅提升管理效率、減少稽核人力與時間(每季稽核花費時間由 10天縮短至 10分鐘內完成)
- 降低手動稽核可能造成的失誤，更可以即時追蹤違反資安的事件。

維運參考依據

- 可針對特定事件進行關鍵字告警(例如深夜root登入系統事件)，定時產出報表。
- 可透過稽核報表來制定流程或管理的改善計畫。

PiExtract 信研科技股份有限公司 台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com

成功案例 – 日誌減量應用

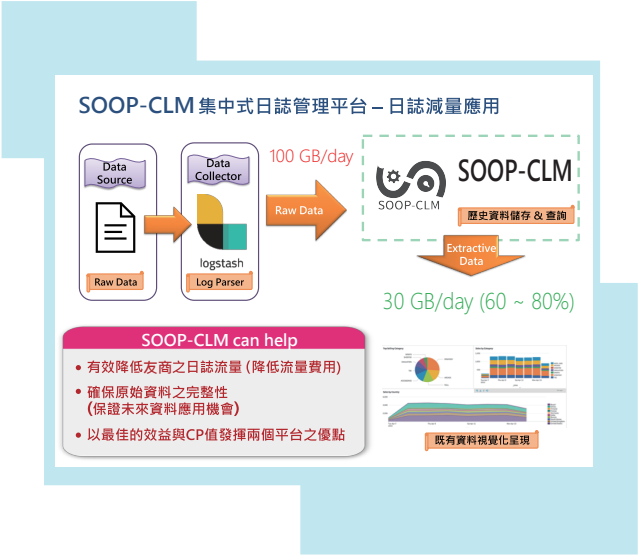
將Raw　Data收集至SOOP-CLM中，確保原始資料之完整性，再透過SOOP-CLM過濾並計算出友商所需的資料，有效降低友商日誌流量。

導入SOOP-CLM的效益

保障既有投資，且大幅降低軟體授權費用

將日誌量減量70%後，僅將有使用到的日誌資料導入友商，以既有的資安事件開單，及資料視覺化儀表板呈現，不僅保障既有投資，更有效降低友商之日誌流量，降低每年支付之流量費用。

SOOP-CLM收集全部日誌資料，維持日誌資料完整性，以利資料稽核及查詢。



日誌擴充收集不受限

日誌收容無流量限制，可完整收集突發性事件所產生之大量日誌資料及新設備日誌，確保原始資料之完整性 。

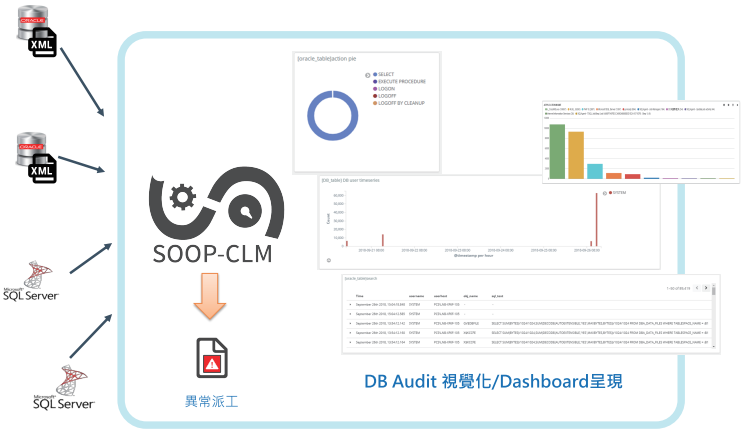
成功案例 – DB Audit Log

利用SOOP-CLM集中收容不同DB之操作行為，完整監控資料庫之狀態。

導入SOOP-CLM的效益

整合跨平台DB Audit Log 資料

透過單一平台，整合不同種類之DB Audit Log 資訊，讓維運人員不用維運多套DB Audit工具，僅須透過SOOP-CLM就可查閱所有DB之Audit Log，並設定相關視覺化圖表。



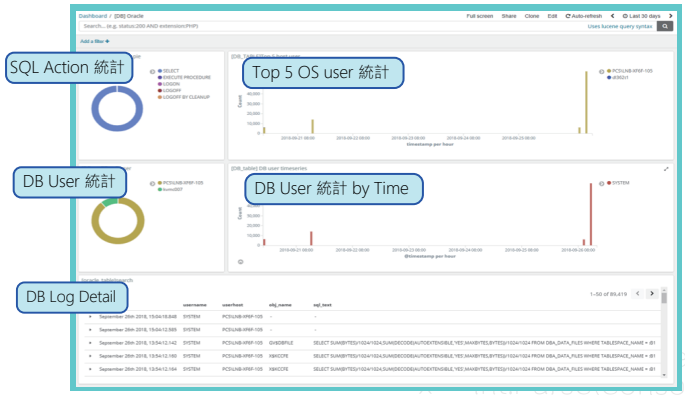
完整記錄DB行為軌跡

利用SOOP-CLM收集DB Audit Log，完整記錄所有DB行為軌跡，例如DB活動之時間、來源、使用者、SQL指令等細節；這些資料除可用於稽核應用外，亦可作為後續分析之用。

即時收集，即時發現DB異常行為

維運人員可自行定義及設定DB異常行為規則，當SOOP-CLM偵測到DB異常活動時（如異常時間的存取行為，大量異常的資料存取紀錄等)，相關維運人員可即時收到SOOP-CLM通知並處理。

當問題發生時，維運人員可透過SOOP-CLM提供之資料視覺化儀表板快速查找相關日誌紀錄，有效減少問題處理時間確保資料庫安全。



PiExtract 信研科技股份有限公司　台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com

內建 Dashboard 及報表

OS

ESXi　Windows　Linux

事件相關
1. 事件級別數量趨勢圖
2. 事件級別分佈圖
3. 設備收容台數
4. 事件級別統計
   (Information、Warning等)
5. 設備收容台數

登入相關
1. AD帳號鎖定統計
2. 登入成功/登出 事件總數
3. 登入成功 來源IP/登入帳號 事件統計及趨勢
4. 登入失敗 來源IP/登入帳號 事件統計及趨勢

排程相關
1. 排程Audit事件分佈圖及趨勢(更新、刪除、停用、建立)
2. 各種排程日誌(刪除、啟用、停用、更新)

開/關機相關
1. 關機時間紀錄
2. 開/關機分佈圖
3. 異常關機統計

效能監控
CPU、Memory、Disk、Top Process、Disk I/O、Network Traffic

網路設備

Flow - Base

1. Services、Autonomous Systems(如Google、AWS、Yahoo等)、IP Version及Protocols等統計圖表
2. Top 10 Applications統計分佈圖 (如SSL、Gmail、Facebook等)
3. Applications 流量圖
4. 來源IP/目的 IP分佈圖
5. flow流量圓餅圖 (Clients 以及伺服器)
6. Geo IP流量圖(國家、城市、Server與Client 流量、Service 流量、Client位置、Server位置)
7. 來源/目的 Autonomous Systems趨勢圖(流量、封包數)
8. Ingress/Egress Interfaces趨勢圖(流量、封包數)
9. Protocols/VLANs圓餅圖(流量紀錄)
10. Protocols/VLANs趨勢圖(流量、封包數)

Fortinet　Checkpoint　Palo-Alto

事件相關
1. 事件級別數量趨勢圖
2. 事件級別分佈圖
3. 設備收容台數

網路設備Config異動相關紀錄

登入相關
1. 登入成功/登出 事件總數
2. 登入成功 來源IP/登入帳號 事件統計及趨勢
3. 登入失敗 來源IP/登入帳號 事件統計及趨勢

Policy Rule異動相關
1. Move Policy
2. Edit Policy
3. Delete Policy
4. Add Policy

Policy Rule Action
1. Deny
2. Allow
3. Close
4. Timeout

F5　Cisco

事件相關
1. 事件級別數量趨勢圖
2. 事件級別分佈圖
3. 設備收容台數

登入相關
1. 登入成功/登出 事件總數
2. 登入成功 來源IP/登入帳號 事件統計及趨勢
3. 登入失敗 來源IP/登入帳號 事件統計及趨勢

Config異動相關紀錄

PiExtract 信研科技股份有限公司　台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com

Middleware

DB

登入相關
1. 登入成功/登入 事件總數
2. 登入成功 來源IP/登入帳號 事件統計及趨勢
3. 登入失敗 來源IP/登入帳號 事件統計及趨勢

服務啟動紀錄

Audit Log

有別於市面上大部分的日誌集中收集平台授權方式，SOOP-CLM授權方式為訂閱制，授權不限流量，由硬體大小決定可收容的日誌多寡！也就是說您不用再為每年日誌收容的高額流量授權費煩惱了，選擇SOOP-CLM可以讓您放心地進行全面的日誌收集！

內建支援之設備及系統清單

網路設備

Cisco

N9K-C93108TC-EX、ASR1002X-5G-K9
Cisco Nessus7010、1841、1721
C3900、C1900、3925、2821、N9K-C9336PQ、C6509、CT3504
C2950 (WS-C2950G-24)
C2960 (WS-C2960-48PST-L、 WS-C2960-24TT-L、WS-C2960-24PC-L、WS-C2960-48TC-L)
C2960G (WS-C2960G-24TC-L)
C2960X (WS-C2960X-48TS-L、WS-C2960X-24TS-L)
C2960S (WS-C2960S-24TD-L、WS-C2960S-48TD-L)
C3560G (WS-C3560G-48TS)
C3750G (WS-C3750G-24TS-1U)
C3750X (WS-C3750X-48P、WS-C3750X-48)
C3850 (WS-C3850-12S-S、WS-C3850-24T)

F5

BIG-IP i2600
BIG-IP LTM 4200
BIG-IP LTM 3900
BIG-IP GTM 1600

Flow-Base

sFlow
NetFlow version 5 / 7 / 9
ipfix

Fortinet

FortiGate 3140B
FortiGate 200D
FortiGate 60D
Fortinet 60E

Palo - Alto

PA-3020

CheckPoint

15400

網路防火牆

OS

Windows/AD Server

Windows Server 2003
Windows Server 2003 R2
Windows Server 2008(Win Server 2008 Standard SP2、Win Server 2008 Enterprise SP2)
Windows Server 2008 R2(Server 2008 R2 Enterprise SP1、Win Server 2008 R2 Standard SP1)
Windows Server 2012Win Server 2012 Standard)
Windows Server 2012 R2(Win Server 2012 R2 Standard)
Windows Server 2016(Win Server 2016 Standard)
Windows Server 2019
Windows 7 Enterprise

Linux

CentOS 7 / 8
Red Hat Enterprise Linux 7 / 8
Ubuntu 18
SUSE Linux Enterprise Server 12 SP 3 / 12 SP4 / 15

Unix

AIX
HP-UX

ESXi

VM Ware ESXi 6.5
VM Ware ESXi 6.0
VM Ware ESXi 5.5

Middleware

DB

Oracle
MS SQL
MariaDB
MySQL
DB2
PostgreSQL
MongoDB
Redis

Container

Docker
Kubernetes

AP

Apache
Nginx
JBoss
Node.js
HAProxy
IIS

PiExtract 信研科技股份有限公司 台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com

功能列表

系統架構
1.具備高可用性，避免單點失效造成系統故障，進而確保資料不遺失
2.具備高擴充性，支援水平擴充或垂直擴充方式，當日誌量增加時，可維持正常的效能運作，且技術上擴充的節點數無上限
3.透過Web UI進行日誌管理，且支援SSL安全加密的Web操作介面
4.可建置於雲環境
5.支援多租戶服務

資料留存設定
1.可依據不同來源設定不同的日誌留存天數，有效精簡硬碟空間的使用

自我監控
1.監控本身狀態及各節點狀況，當監控項目有服務異常，除了發送告警通知，SOOP-CLM各服務也會先自動重啟，以維持系統高穩定度
2.具備系統自我稽核功能，可即時紀錄與稽核使用者的操作記錄，如登入及日誌查詢等紀錄，以符合稽核規範

權限設定
1.提供密碼強度設定，支援強制要求密碼需含大小寫英文字母、數字及特殊符號；提供帳號鎖定機制，在帳號登入失敗三次須立即鎖定，以配合法規稽核需求
2.有效控管使用者日誌查詢權限，提供Role-based access control有效保護日誌資料，可依照不同角色檢視相對應的資料
3.支援群組設定，可針對不同資料來源、事件內容及關鍵字進行群組權限設定，不同群組可查閱的不同的資料內容
4.儀表板支援權限管控功能，可限定特定的使用者或是角色是否可以閱覽或是修改儀表板
5.支援串接AD/LDAP及OIDC

報表及告警功能
1.可定期將儀表板匯出為PDF及MHTML格式，提供日報、週報、月報、季報及年報方式將報表寄送至使用者信箱；定期提供管理人員系統維運報告，且PDF格式支援自定義logo
2.可從日誌資料中偵測系統異常現象，支援關鍵字及條件設定事件告警，當異常發生時，第一時間通知維運人員
3.告警功能支援動態閾值，根據先前的行為模式，辨識系統中異常的事件，提供真實動態趨勢分析，避免僅靠靜態閾值判定造成的誤差
4.提供E-mail方式通知告警事件，告警郵件內容包含告警狀態及相關事件之日誌內容，如事件發生時間及相關日誌內文等內容

日誌收容及豐富內建模組
1.支援多樣日誌蒐集方式，如JDBC、TCP/UDP、SNMP Traps、Syslog、sFlow、NetFlow、Windows Event Files、CSV、TXT、XML等
2.提供大量隨插即用的日誌模板，維運人員僅需將相關日誌資料匯入，即可使用內建之日誌Dashboard，如Windows、Linux、F5、Cisco、Fortinet、Palo-Alto及Middleware等模組

PiExtract 信研科技股份有限公司 台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com

EPS 2300情境舉例

EPS 2,300日誌資料，單次查詢區間1 day，SOOP-CLM保留20天的資料

產品名稱

SOOP-CLM企業版 (HA版本，且資料備份1份)

3台硬體資源

CPU: 16 Core

Memory: 256 GB

Disk:IOPS 500+, 3.5 TB

此規格可收容資料

1. 單筆日誌大小1KB。
2. EPS 2,300日誌資料。
3. 5種不同來源類型的日誌資料(如Windows、Cisco、F5都各自算一類)。
4. 單次查詢區間1 day，並於SOOP-CLM保留20天的資料。

PiExtract 信研科技股份有限公司 台北市松山區八德路二段449號7樓
TEL : +886 2 2751-8123
MAIL : support@piextract.com