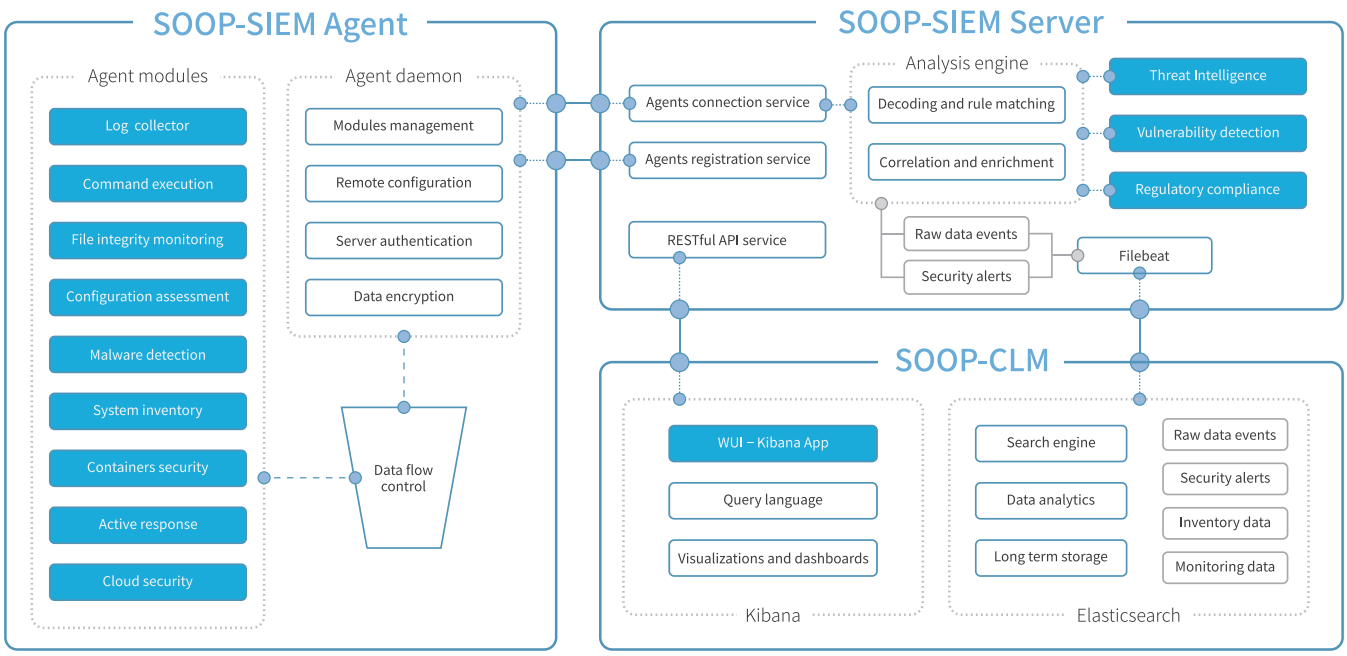
# SOOP-SIEM一站式資訊安全解決方案

## Service-Oriented Operation Portal-
## Security Information and Event Management

## 監控　檢測　分析　回應　合規




SOOP-SIEM 是一套整合 XDR、SIEM 的端點 (EDR) 與雲端 (Cloud) 平台的高 CP 值全方位資安解決方案，在單一資安監控平台上，執行即時分析，為公共雲、私有雲和本地資料中心提供資安威脅預防、檢測和回應 (response) 的保護，具備容易部署及使用簡單的特色，不但協助企業滿足技術合規性要求，且高度支持第三方整合的擴展性並可以客製化。

## 產品十大特色

### 即時的資安監控與分析

可用來收集、聚合、索引和分析安全相關資料，針對入侵、威脅和行為異常。結合資安情報，提供即時監控、分析、回應和快速修復的能力。

### 滿足技術合規性要求

結合其可擴展性和多平台支援，提供了一些必要的安全控制，滿足 PCI DSS、SOC2、GDPR、NIST、GPG13 和 HIPAA 等合規要求，Web 使用界面提供多種報告和儀表板。

### 評估系統安全配置

幫助管理員評估系統安全配置的合規性，定期掃描檢測已知易受攻擊、未修補或配置不安全的應用服務，並提供相關要求的告警。

## 全面性的入侵偵測

多方掃描受監控的系統及網路設備，以查找惡意軟件、後門程式、木馬程式及其他可疑異常。檢測隱藏檔案、隱藏程序或未註冊的網絡監聽器，以及不一致的系統調用回應，並使用其字串樣版 (RegEx) 引擎持續分析收集到的日誌資料特徵比對危害指標 (IOC)。

## 強大的日誌分析能力

可以收集各種日誌數據，例如系統日誌、應用程序日誌、安全設備日誌等，將它們聚合到中控端以進行基於資安政策的分析和儲存。SOOP–SIEM 內的規則設置允許發現應用程式或系統的錯誤、錯誤配置、企圖執行或成功執行的惡意活動、違反政策以及各種其他資安和維運問題。

## 監控機敏檔案完整性(FIM)

可監控檔案系統，識別您需要關注的檔案內容、權限、所有權和屬性的變化，並可識別新增或修改文件的使用者和應用程式。可與威脅情資結合使用識別威脅或受影響主機。此外，也是一些法規標準（例如 PCI DSS）的必要要求。

## 開箱即用的主動回應

主動執行各種對策來應對威脅，例如滿足在 ATT&CK Matrix 某些標準時阻止從威脅源訪問系統。此外，可遠端執行命令或系統查詢，識別危害指標 (IOC) 並幫助執行其他即時鑑識或事件回應任務。

## 內建威脅情資和弱點掃描功能

集成不斷更新的 CVE、NVD 和 OVAL 等多種威脅情資資料庫和弱點掃描工具，識別易受攻擊的關鍵資產，在攻擊者破壞或竊取前採取糾正措施。

## 提供雲平台資安監控的功能

能夠利用整合模組，從知名雲端服務供應商（如 Amazon AWS、Azure 或 Google Cloud）提取資安資料，實現在 API Level 之雲端基礎設施監控。

## 提供容器資安監控的功能

為 Docker 主機和容器提供資安可見性，監控它們的行為並偵測威脅、弱點和異常。SOOP-SIEM 代理程式 (Agent) 與 Docker 引擎原生集成，允許使用者監控 image、volume、網路設置和執行容器，面對可能的威脅發出告警。

PiExtract

信研科技股份有限公司 PiExtract Technology CO., Ltd.
MAIL：support@piextract.com