PoExtract

信研科技股份有限公司

SOOP-CLM 產品介紹簡報

01.關於SOOP-CLM

- 日誌的善加運用，帶來無限的可能
- 在管理日誌時，客戶會面臨什麼挑戰
- 日誌管理平台的建置指導方針
- SOOP-CLM定位-ELK的管理平台
- SOOP-CLM-企業級的集中化日誌管理解決方案

01 日誌的善加運用，帶來無限的可能

- 各式設備都會產出相關的日誌來反應設備的當前狀態，若將這些日誌善加應用，將其多方排列組合，建立關聯，並加以分析，就可以產生無限的可能。

- 因此，日誌的集中管理在近年成為日常管理的顯學，眾多日誌管理平台也如雨後春筍般的問世。

- 但客戶們依舊在找尋某種C/P值合理的方案！

01 在管理日誌時，客戶會面臨什麼挑戰

PyExtract

設備眾多、繁雜

由於在客戶端的設備充斥著各式各樣的品牌型號，因此如何跨品牌及型號的集中收集日誌，就成了客戶面臨的第一個挑戰

日誌格式繁多

也因為品牌及型號的多樣性，各式日誌收集起來後，如何進一步的解析其內容，讓日誌從冷冰冰的文字，變成協助維運的利器

如何應用日誌

因此，如何運用珍貴的日誌來協助日常維運作業、建立大數據平台的基礎，甚至可用來察覺潛在商機，都讓日誌應用變成一門重要的課題

01 日誌管理平台的建置指導方針

By Gartner Guideline 2020

管理機敏資料	例如適當的遮蔽、權限控管及自動偵測機敏資料的機制等。
建立彈性的存取限制	例如不同的人員應該依權限看到不同的資料。
選擇高可靠性的日誌收容平台	例如Server端的Cluster機制、Agent端的buffer機制及是否支援大量及跨地域的收容。
支援常用的日誌型態	例如常見的設備/軟體是否已經內建parser。
應用日誌的方式	例如以儀表板及報表的方式呈現，或是能依要求發出告警。

01 SOOP-CLM定位-ELK的管理平台

- 資料留存
- 權限管控
- 內建解析模組
- 告警設定
- 報表排程

01 SOOP-CLM 企業級的集中化日誌管理解決方案

- 一個高性價比的企業級集中化日誌管理解決方案，一次滿足 符規，稽核及IT維運 等需求：
  - 集中收容多樣性的日誌來源與不同的日誌格式
  - 分析、關聯、儲存及視覺化日誌(Log)資料
  - 是企業面對大數據資料與AI時代的堅強後盾
- 結合其他第三方解決方案，更可節省整體擁有成本，增加企業競爭力
- 支援雲端(IaaS)建置方式，提供更彈性的系統架構規劃

01 03 04 05

02功能介紹

- 認證
- 授權
- 告警
- 報表
- 內建解析模組
- 功能效益

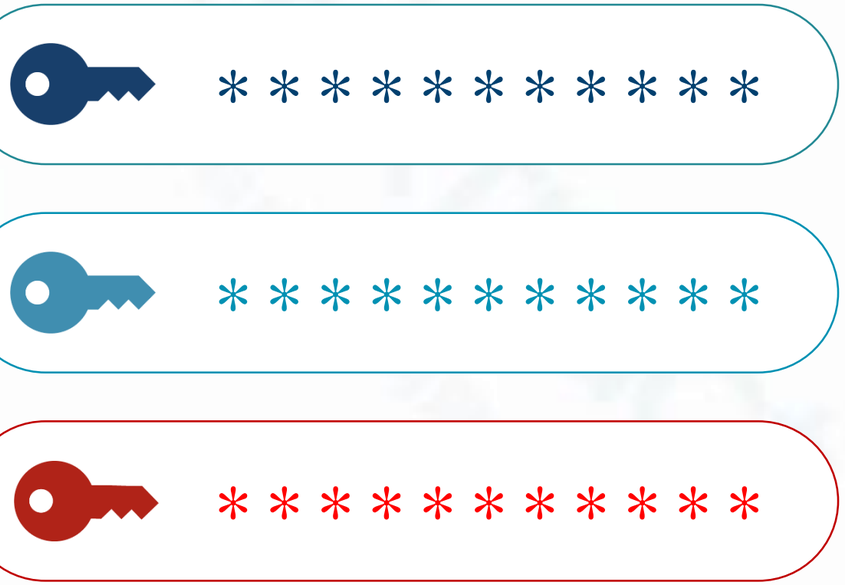
Function features

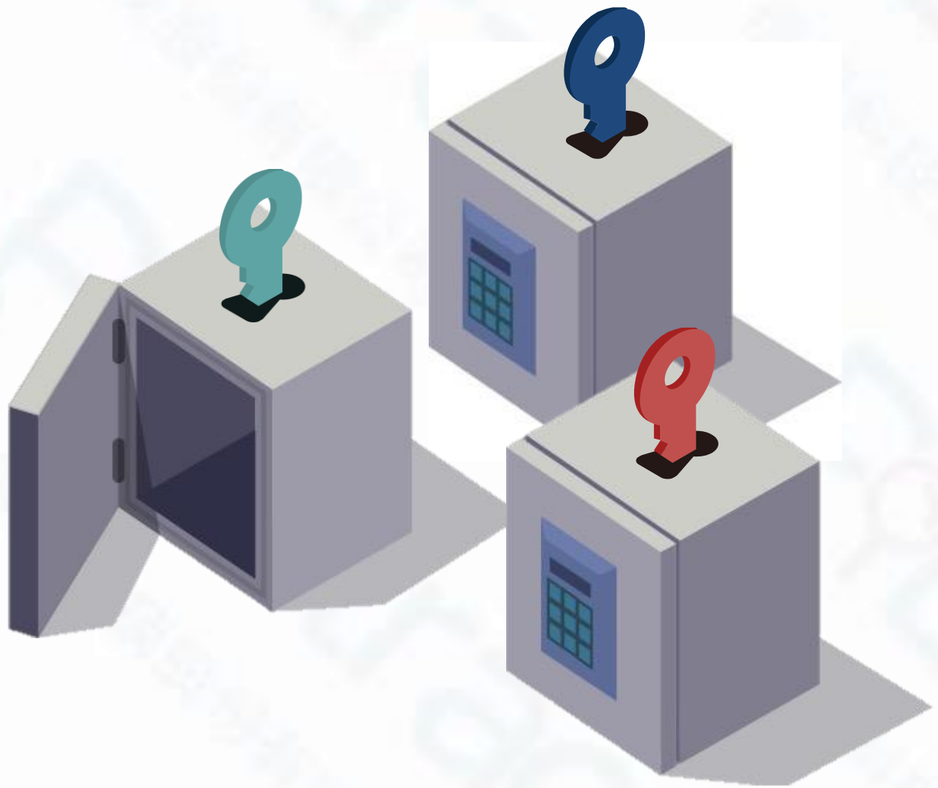
02 功能總介紹-認證

- 認證
- 授權
- 告警
- 報表
- 內建解析模組

提供進階的認證機制，不僅是提供帳密驗證方式，還可以

1. 整合企業內部的AD/LDAP。
2. 設定密碼強度。
3. 設定輸入錯誤三次即鎖定帳號。

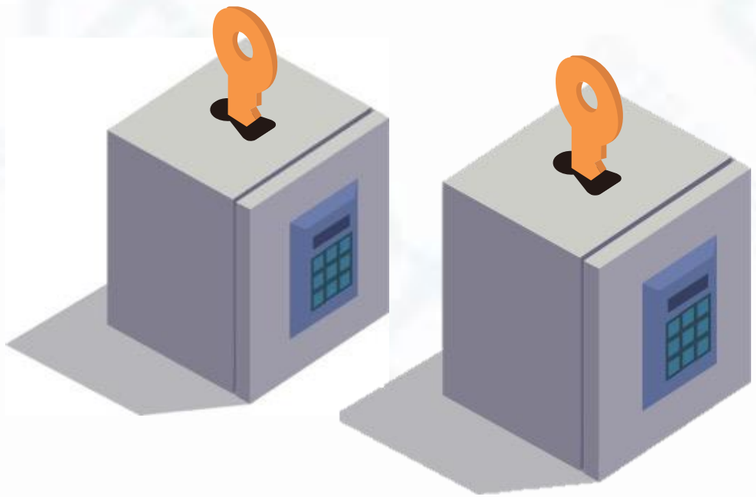




功能總介紹-授權

依不同的使用者及群組，授予不同的資料讀取權限或系統操作權限-Role-Based Access Control。

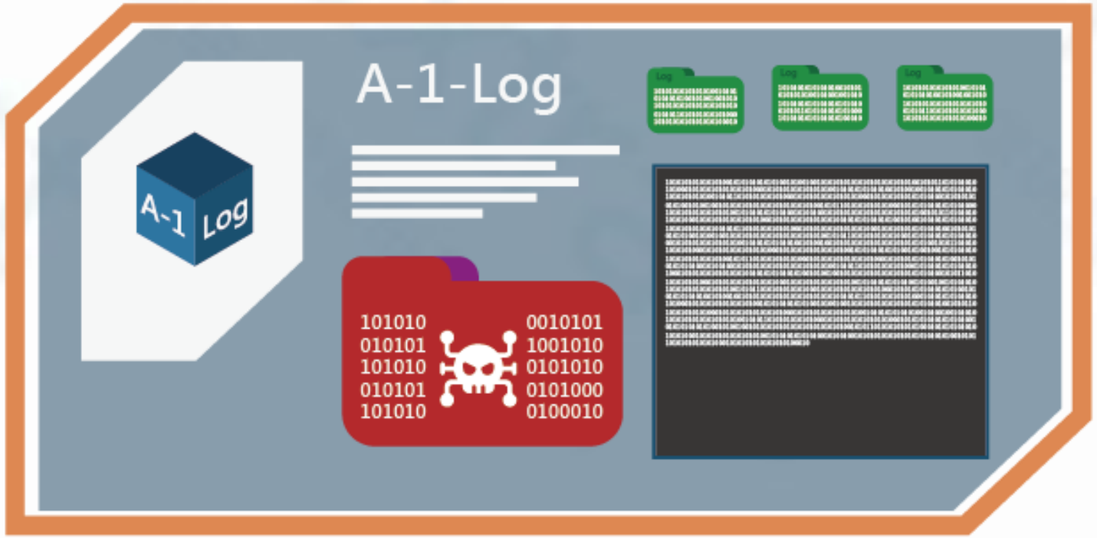
1. 一般用戶只能閱讀儀表板或報表。
2. 群組管理員才能新增/修改/刪除儀表板或報表。
3. 可針對日誌內容做進階的授權管理，例如只有指定群組或使用者才能看到身分證等機敏資料。



功能總介紹-告警

進階的告警功能，讓系統自動判讀日誌內容，並提供主動告警。

1. 依特定關鍵字在單位時間內的數量。
2. 依特定時間內的日誌數量或特定關鍵字的數量。
3. 整合各式告警平台，例如Email, SMS, APPs。
4. 友善及高彈性的設定介面，簡化外部整合機制。
5. 支援動態閾值，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。



PoExtract

認證
授權
告警
報表
內建解析模組

內建業界常用的各式設備的報表介面

1.定期報表：

定期檢視系統狀態，建立長期趨勢分析的基礎。

2. 高度客製化：

除內建報表外，也可支援客戶自定義的報表需求， 滿足所有客戶的一切需求。

3. 高度彈性：

支援各個報表的關聯性分析需求，簡單的點擊即可自動帶入參數，加速異常排除。

4. 附件輸出：

支援PDF及MHTML格式輸出報表內容，簡化操作流程。

功能總介紹-內建解析模組

- 認證
- 授權
- 告警
- 報表
- 內建解析模組

提供大量Plug and Play的日誌模組，讓客戶可以一次性的擁有SOOP-CLM強大的分析功能，並以簡單明瞭的UI介面呈現 。

日誌模組能大幅降低使用上的複雜度，維運人員僅需將相關日誌資料匯入即可。

進階的管理儀表板，讓系統自動以圖形化的方式提供可讀性高的儀表板，主動告警異常。

ESXi

DB

Linux

Windows

Palo-Alto

Flow-Base

Checkpoint

Fortinet

Cisco

F5

PoExtract

Logs

收集的日誌導入

增加整合其他工具

Monitor Tool/Big Data Platform/Automation Tool/AI & ML

減少

減少維運人員負擔

加乘應用情境

War room/SIEM/ISO 27001/ PCI DSS/APM

除去

降低既有流量授權費用

01 02 04 05

03成功案例

- 主動式資安防禦平台
- 資安/稽核應用 – ISO 27001
- 整合儀表板
- 日誌減量應用
- 金融應用服務日誌收容
- 日誌延伸應用-潛在商機發掘

Case study

主動式資安防禦平台

03 成功案例-主動式資安防禦平台

遭遇挑戰 – 無法即時排除資安問題

資訊事件層出不窮，企業需即時反應

- 資安事件總是後知後覺
- 無法即時透過設備日誌查覺異常
- 設備日誌留存時間太短，無法找到資安跡證
- 需要太多人為介入/判斷，失去防堵資安風險的時效

主動式資安防禦平台優勢

- **主動整合**

  主動式的收集資安設備的分析結果，透過內建AI功能協助主動判斷應執行的防堵行為
- **主動防禦**

  整合後台高度彈性的防禦系統，主動控制SDN設備，自動/手動阻斷高風險設備。
- **減少企業資安風險**

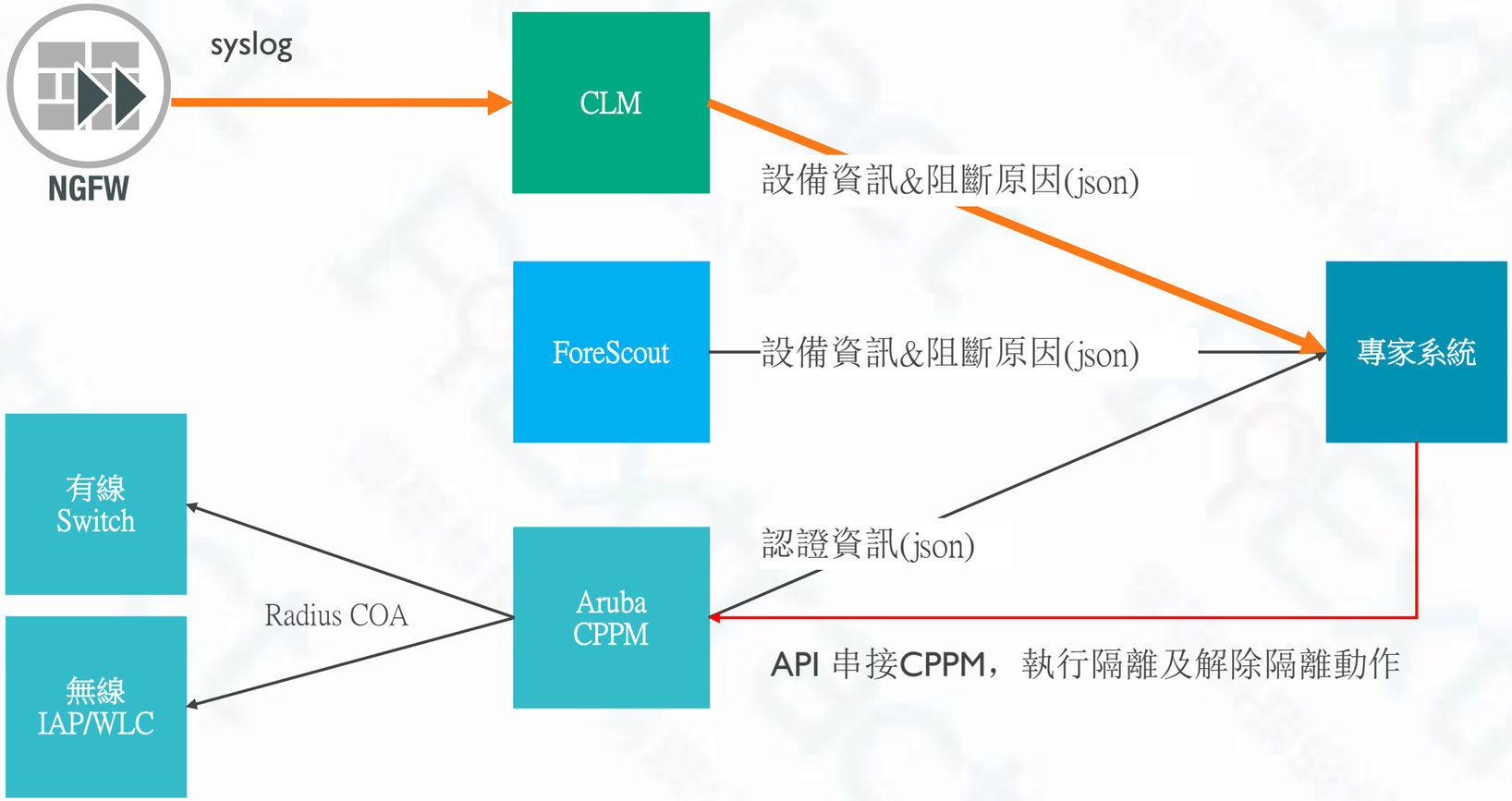
  透過主動整合/主動防禦，提升企業數位轉型時的最佳資安主動防禦方案

03 主動式資安防護平台-架構說明

CLM
- 提供內網網段資訊
- 依據內網來源IP及進行評分
- 評分依據，可參考下述資訊(會再提供的相關資訊)
  type=utm
  subtype=virus,ips…
  eventtype=infected, signature..
  level=warning, alert, critical…
  action=blocked,reset…
  srcip=x.x.x.x
- 當分數超過門檻值時，發告警通知API Server
- Dashboard 內容，提供IP評分表格及其它統計數據
- 可以客製告警Json 格式

API
- 收到CLM 告警 Json
- 用IP比對資料庫，找到對應MAC address
- 手動或自動API 串接CPPM
  1. 用Radius Session ID 執行COA
  2. 更新 Endpoint 資訊

03 主動式資安防護平台-架構說明(cont.)



- ubuntu python wsgi
- Python web socket 收json， 做下一動
- 手動或自動API 串接CPPM
  1. 用Radius Session ID 執行COA
  2. 更新 Endpoint 資訊

03 主動阻斷結果

PoExtract

每頁 10 筆資料　　搜尋字串:

mac_address	status	risk	IP	action
03bfca2bee9a	closed	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
04c3ef25abdc	closed	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
083b7fe4eaba	closed	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
0acb2c3de6b5	closed	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
0adf4f9d7e51	closed	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
0b624a3cfedb	active	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
0fe61d8ca4ce	active	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
106ce29ab74f	active	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
13bdf0495ead	active	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail
14096f5cee7a	active	100	%{Radius:IETF:NAS-IP-Address}	加入隔離區 送出 Detail

1至10/共202筆　　前頁 1 2 3 4 5 … 21 下頁

透過專家系統，提供企業主動或手動式的資安防禦，降低數位轉型時的資安風險。

專案效益

因應數位轉型，提升資訊安全

- 面對未來企業數位轉型的風潮，藉由主動式防禦機制面對未來資訊安全的挑戰，避免企業因資安風險而造成不必要的損失

集中管理資安事件，加強弱點補強

- 統一收集資安日誌並加強稽核，大幅提升管理效率，**大幅降低人為失誤**
- 分析資安事件，避免重覆的問題一再發生，無謂的耗損內部資源在處理重複的事件

維運參考依據

- 可針對特定事件進行**關鍵字告警**，及早得知風險事件
- **定時產出報表**，可透過稽核以及檢討會來制定流程或管理的改善計畫

資安/稽核應用 – ISO 27001

遭遇挑戰 – 符合資訊安全稽核需求

因應法規要求，提升資訊安全

- 為確保終端使用者的資訊安全，企業**必須通過ISO 27001認證**，以提升整體資訊安全性。
- 現況稽核方式須透過人工以指令查詢方式收集相關資料，相當曠日費時。
  (每季需耗費10工作天進行查詢統計)
- 同時部分設備**日誌保留時間太短無法符合稽核規範**。

ISO 27001 日誌稽核項目

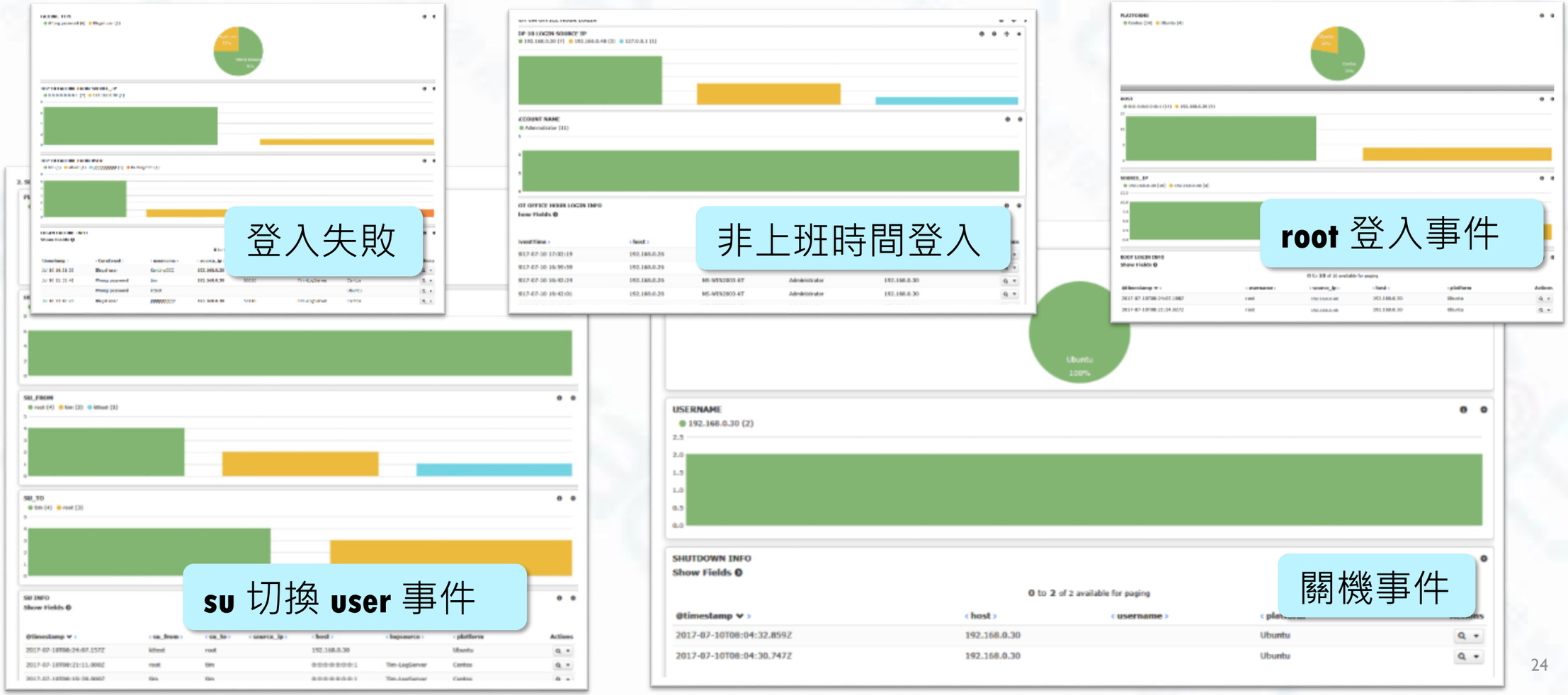
A.12.4 存錄與監控(目標：紀錄事件與生成證據)

- **A.12.4.1 事件存錄**
  控制措施：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、保留並定期審查。
- **A.12.4.2 日誌資訊的保護**
  控制措施：應保護存錄設施與日誌資訊，不受竄改與未經授權的存取。
- **A.12.4.3 管理者與操作者日誌**
  控制措施：系統管理者與操作者的活動應加以存錄、保護並定期審查。

03 成功案例-資安/稽核應用 – ISO 27001

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、保留並定期審查。



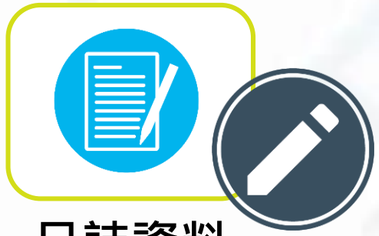
✓ A.12.4.2 日誌資訊的保護

應保護存錄設施與日誌資訊，不受竄改與未經授權的存取。

嚴格控管讀寫權限，寫入SOOP-CLM之日誌資料，只有讀取權限，並無修改/刪除權限。

Role-base 存取控制 (RBAC)

- 日誌來源
  - 寫入權限



日誌資料

- 維運人員:
  - 對應之讀取權限
  - ~~寫入、更新、刪除權限...~~ no permissions

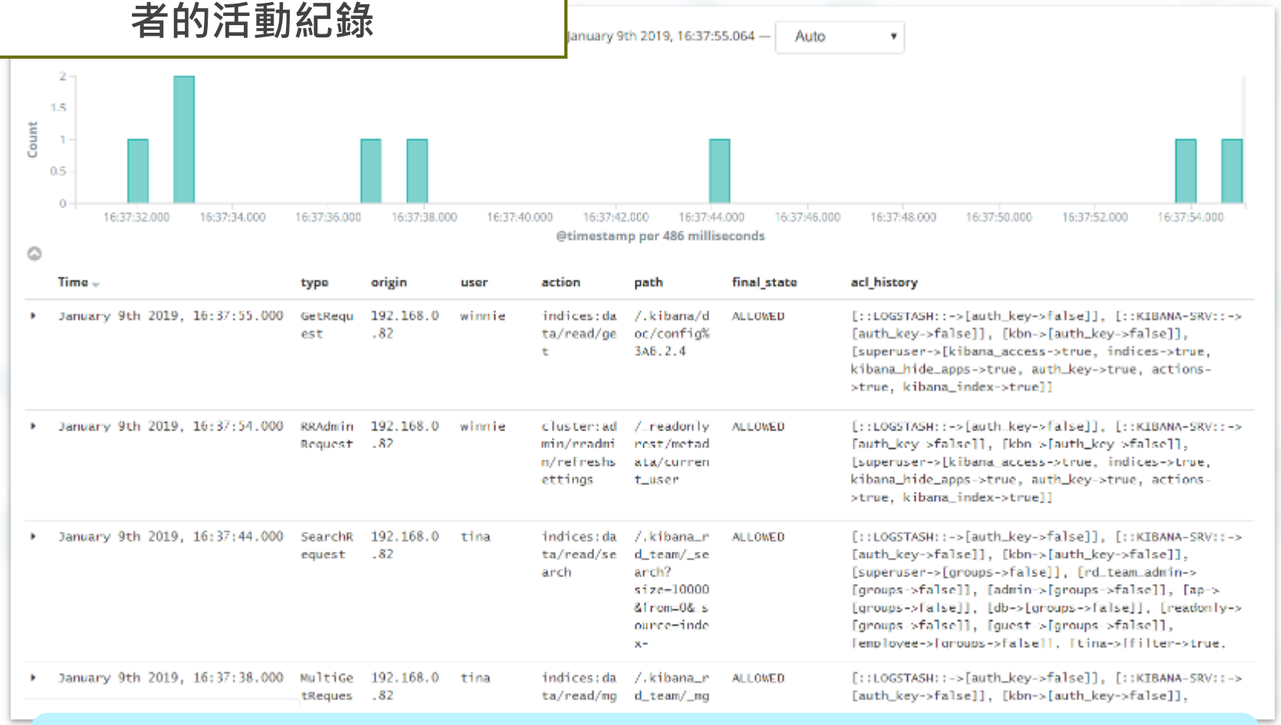
User

03 成功案例-資安/稽核應用 – ISO 27001

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。

SOOP-CLM Audit Log功能
詳細記錄所有系統管理者與操作者的活動紀錄



Time	type	origin	user	action	path	final_state	acl_history
January 9th 2019, 16:37:55.000	GetRequest	192.168.0.82	winnie	indices:data/read/get	/.kibana/doc/config%3A6.2.4	ALLOWED	[::LOGSTASH::->[auth_key->false]], [::KIBANA-SRV::->[auth_key->false]], [kbn->[auth_key->false]], [superuser->[kibana_access->true, indices->true, kibana_hide_apps->true, auth_key->true, actions->true, kibana_index->true]]
January 9th 2019, 16:37:54.000	RRAdminRequest	192.168.0.82	winnie	cluster:admin/readmin/refreshsettings	/_readonlyrest/metadata/current_user	ALLOWED	[::LOGSTASH::->[auth_key->false]], [::KIBANA-SRV::->[auth_key->false]], [kbn->[auth_key->false]], [superuser->[kibana_access->true, indices->true, kibana_hide_apps->true, auth_key->true, actions->true, kibana_index->true]]
January 9th 2019, 16:37:44.000	SearchRequest	192.168.0.82	tina	indices:data/read/search	/.kibana_rd_team/_search?size=10000&from=0&_source=index-	ALLOWED	[::LOGSTASH::->[auth_key->false]], [::KIBANA-SRV::->[auth_key->false]], [kbn->[auth_key->false]], [superuser->[groups->false]], [rd_team_admin->[groups->false]], [admin->[groups->false]], [ap->[groups->false]], [db->[groups->false]], [readonly->[groups->false]], [guest->[groups->false]], [employee->[groups->false]], [tina->[filter->true,
January 9th 2019, 16:37:38.000	MultiGetReques	192.168.0.82	tina	indices:data/read/mg	/.kibana_rd_team/_mg	ALLOWED	[::LOGSTASH::->[auth_key->false]], [::KIBANA-SRV::->[auth_key->false]], [kbn->[auth_key->false]],

操作類型/來源/使用者/存取日誌內容/詳細資訊

SOOP-CLM Report功能
定期寄送Report功能，供維運人員進行定期審查

專案效益

因應法規要求，提升資訊安全

- 建立集中式日誌管理平台，並建構ISO 27001稽核儀表板，清楚呈現所有資訊，協助客戶通過ISO 27001認證，以**提升整體資訊安全性**

日誌統一管理，稽核流程簡單

- 統一各來源日誌、稽核事件集中管理，大幅提升管理效率，**大幅降低人為失誤**
- 稽核報表自動產出並寄送，大幅減少稽核人力與時間(每季稽核可**在10分鐘內完成**)；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**，及早得知風險事件 (例如深夜 root 登入系統事件)
- **定時產出報表**，可透過稽核以及檢討會來制定流程或管理的改善計畫

成功案例-整合儀表板

03 成功案例-整合儀表板

PoExtract

遭遇挑戰

察覺難

大多數的問題由別人告知，並非主動察覺，且常常無法重現服務異常狀況，只能猜測或等待異常再次發生。

究責難

設備廠商會任意異動設備及相關設定，常造成服務異常，但無法追查責任。

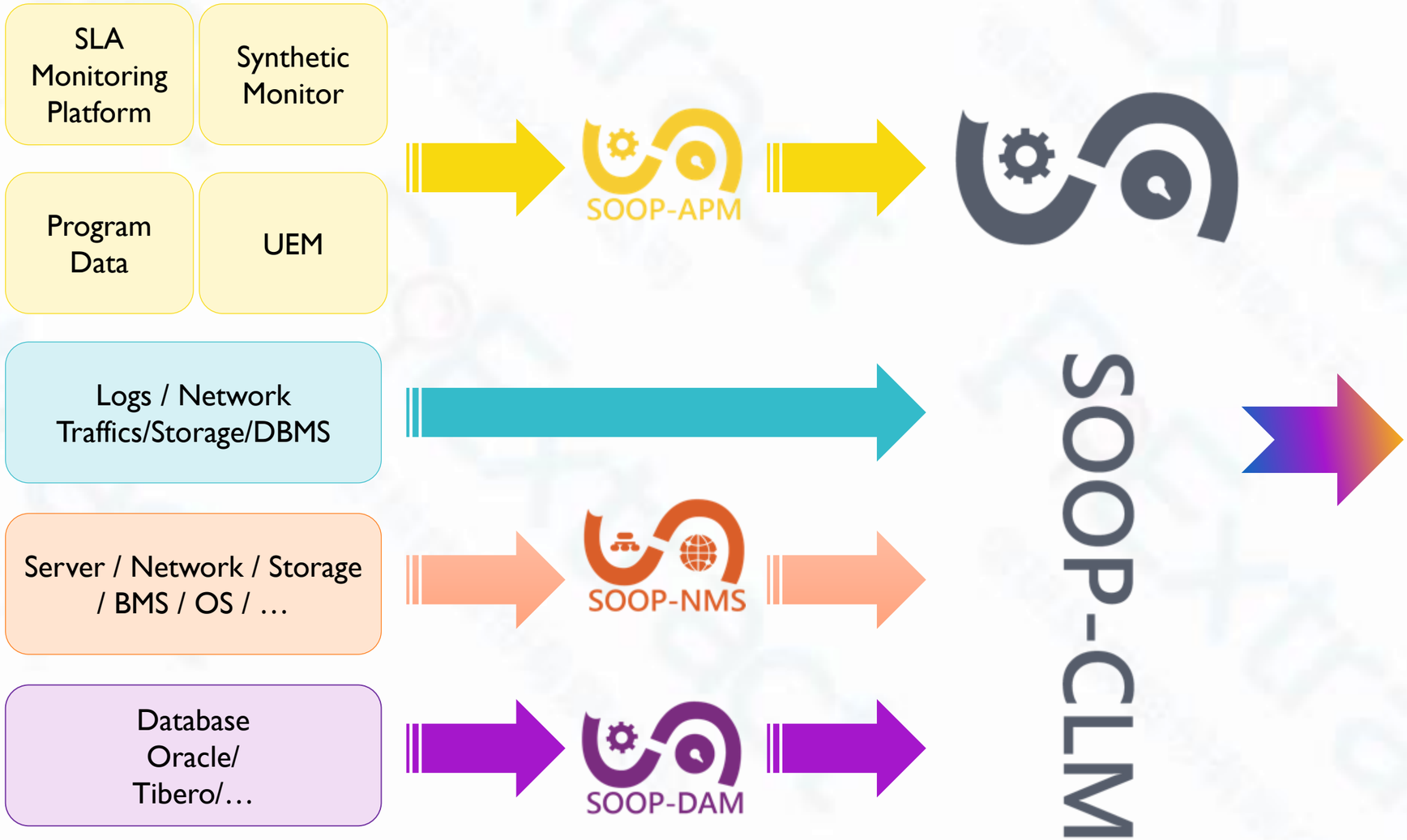
管理難

維運管理大部分外包，監控以基礎設施設備為主，其他監控工具各自獨立且不全面，遇到異常問題，相關維護廠商互相推諉責任。

維護難

維護廠商經常更換，人員更迭頻仍，維護歷史資料無法銜接且經驗無法傳承，解決效率差。

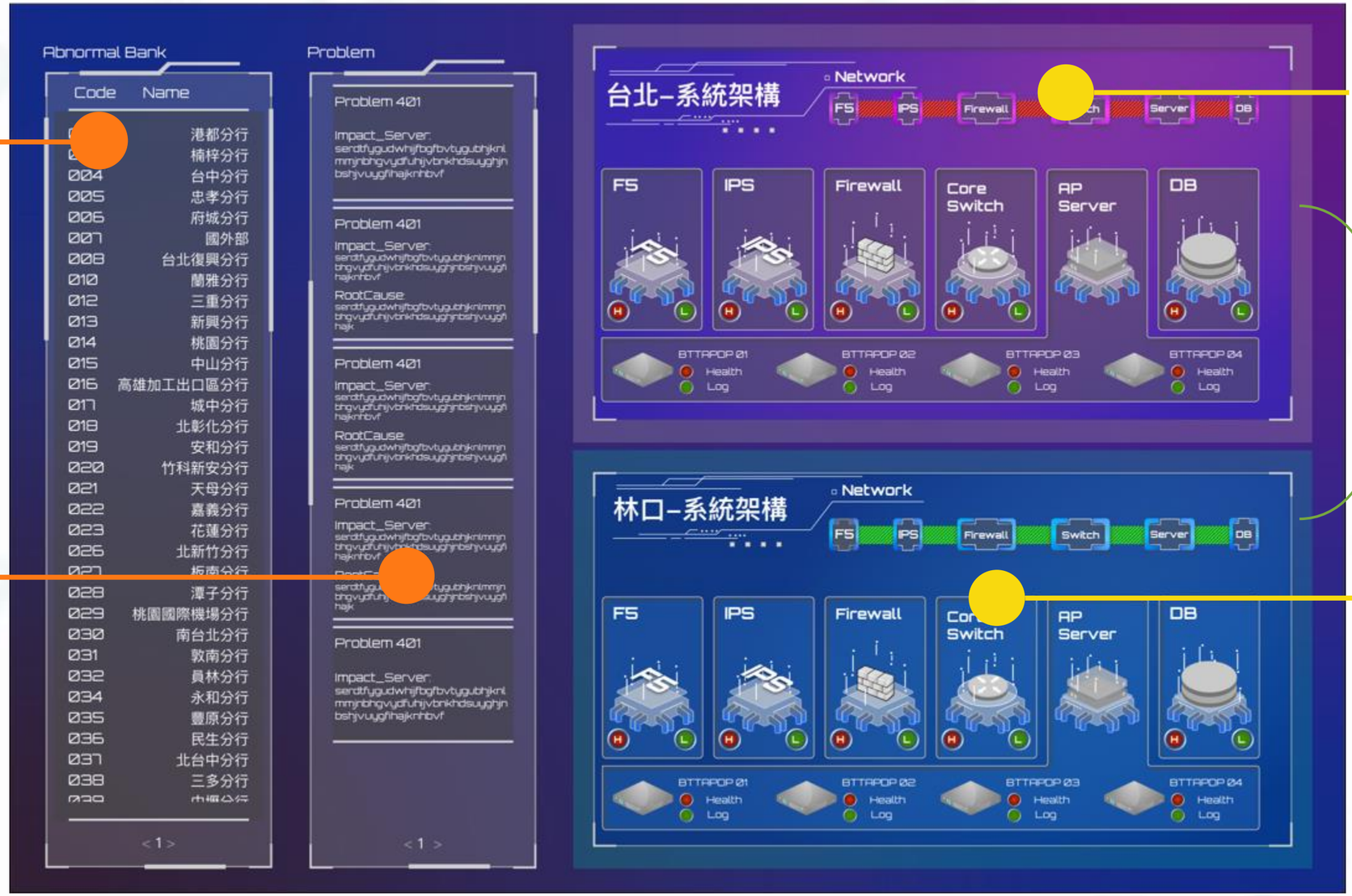
03 成功案例-整合儀表板



03 成功案例-整合儀表板

遭遇異常的分行

自動偵測服務異常



網路流量一覽表

系統資料流

硬體設備健康一覽

03 成功案例-整合儀表板

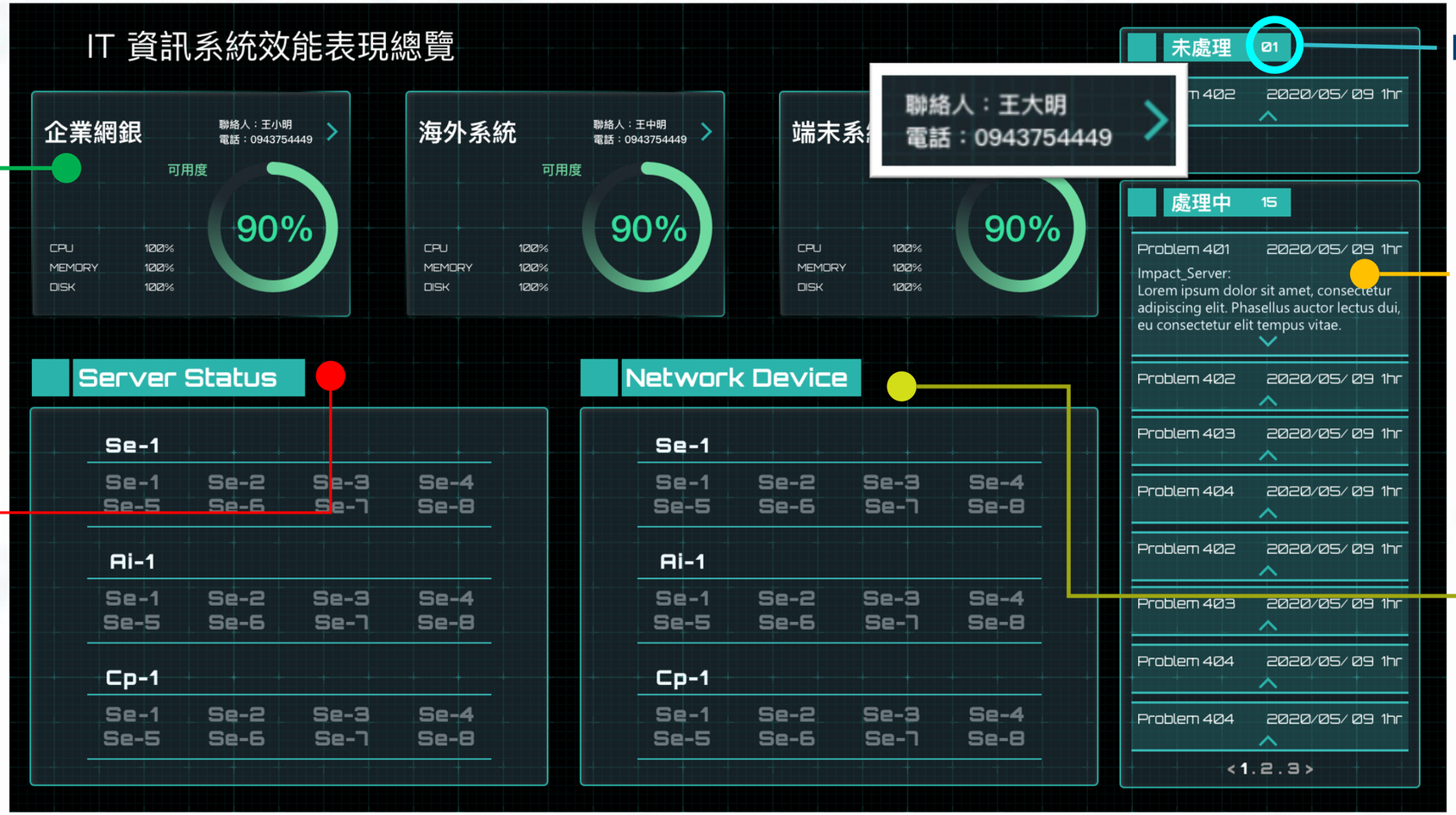
PoExtract

■ 系統負責窗口

OP人員第一時間通知負責維運人員，亦可整合客戶既有之工單處理系統

■ 服務效能總覽

以使用者感受出發，當作效能參考，依據各系統不同的KPI定義不同的SLA



■ 事件處理狀態

介接事件管理系統的資訊追蹤事件處理狀態

■ Problem告知

AI 主動告知問題以及服務異常的主因

■ 基礎設施/網路狀況總覽

直覺性的拓樸圖掌握設備狀況

專案效益

早期告警，即時掌握問題發生狀況

- 透過服務導向維運入口網與告警系統通知，當問題發生的第一時間，能即時掌握網路、基礎設施及各種應用服務的異常狀況

有效降低客訴，提升使用者滿意度

- 從一天平均15件以上，降低為一周1件
- 平均提早客訴發生前2分鐘，發出服務告警

快速定位問題癥結

- 問題解決時間從2周減少為1天

持續優化，提高系統可用度

- 平均服務反應時間從7秒降低為3秒

釐清責任歸屬

- 收集網路設備configuration備份及異動紀錄，釐清網路設備異動的權責歸屬，減少猜測並加速維運

輔助維運決策

- 建立維運用資料倉儲平台，全面及完整收容所有監控數據，並依照智能維運演算法的分析結果，產出相關趨勢報表，做為輔助維運決策之應用

成功案例-日誌減量應用

03 成功案例-日誌減量應用

PoExtract

遭遇挑戰

無法完整收容所有日誌

受限流量限制而**無法完整蒐集事件日誌資料，僅能挑選重要的日誌資料進行蒐集**。

友商軟體授權成本過高

透過以流量計費的日誌蒐集平台進行原始資料蒐集，每年花費大量訂閱及維護費用。

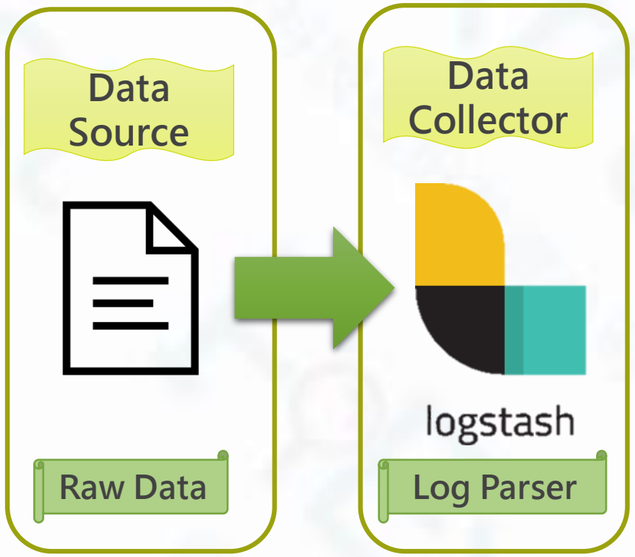
資料實際應用程度低

實際使用的日誌資料僅有20%-40%，**大部分的原始資料僅在特定事件發生時才被查閱**。

不浪費既有投資

已經利用友商建立了大量的儀表板及管理流程，更換系統只會造成**維運的空窗期以及原始投資的浪費**。

03 成功案例-日誌減量應用



100 GB/day

Raw Data

SOOP-CLM

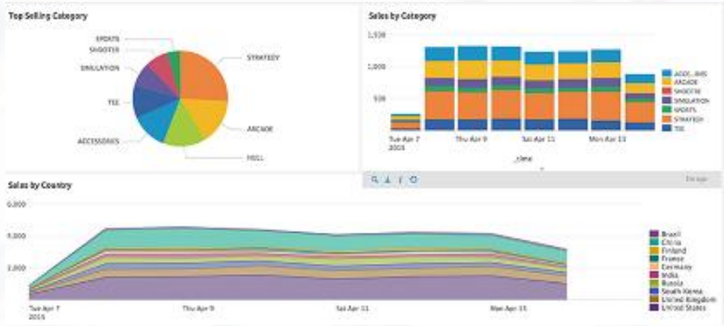
歷史資料儲存 & 查詢

Extractive Data

30 GB/day(↓ 70%)

SOOP-CLM can help

- 有效降低友商之日誌流量(降低流量費用)
- 確保原始資料之完整性(保證未來資料應用機會)
- 以最佳的效益與CP值發揮兩個平台之優點



既有資料視覺化呈現

專案效益

保障既有投資，且大幅降低軟體授權費用

- 透過SOOP-CLM減量，**將日誌量減量70%後**，僅將有使用到的日誌資料導入友商，維持原有的維運機制，及資料視覺化儀表板呈現，不僅**保障既有投資**，更有效降低導入友商之日誌流量，**降低每年支付之流量費用**。
- SOOP-CLM集中式日誌管理平台收集全部所需日誌，維持日誌資料完整性，以利資料稽核及查詢。

日誌擴充蒐集不受限

- 日誌收容無流量限制，可因應突發的事件情境或自由調整收容範圍，提升維運的完整度及發揮日誌的最大價值。

成功案例-金融應用服務日誌收容

03 成功案例-金融應用服務日誌收容

PoExtract

遭遇挑戰

軟體授權成本高

當前數位網銀會員已達200萬人，其應用日誌皆存於商業版Database中。隨著網銀會員人數或使用頻率增加，其產出之日誌也就更多，後續將面臨擴充Database所需之**高昂軟體授權費**。

應用服務效能不佳

網銀常因同一時段（外幣到價或回饋通知時）**大量客戶登入及交易，造成系統緩慢**。
（Log寫入的時間由平時之0.0016秒/筆，延長至10~20秒/筆）

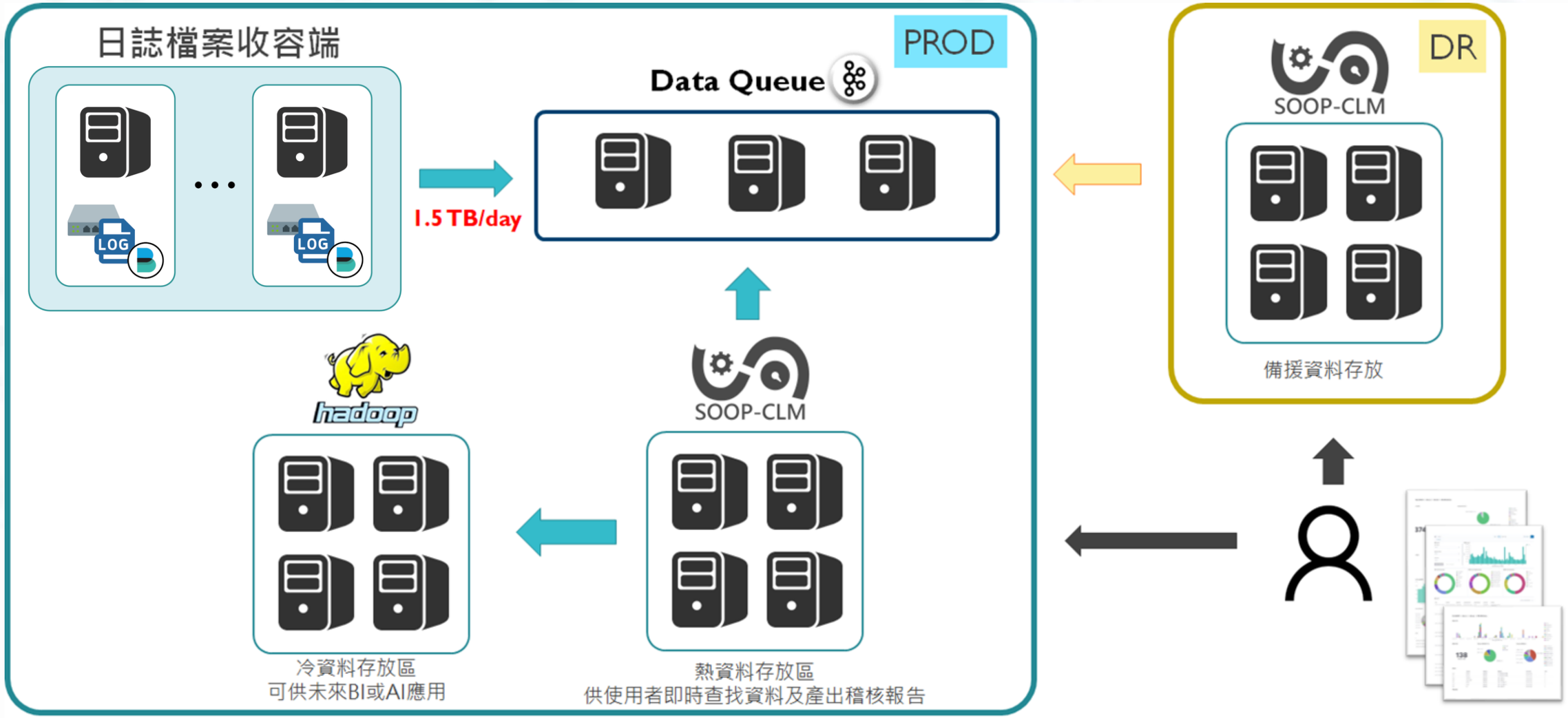
異常排除速度緩慢

當系統發生異常時，需要熟悉資料庫結構/欄位及SQL查詢語法，才查得到想要的資料；加上交易日誌存在Database，而系統及服務日誌存在OS，無法透過單一平台進行查詢，導致異常排除速度緩慢。

長期資料儲存不易

無法壓縮儲存長期歷史資料，難以滿足**稽核及未來Big Data/AI**等需求。

03 成功案例-金融應用服務日誌收容



降低近70%的高額資料庫系統費用

成功案例-金融應用服務日誌收容

專案效益

＋ 增加 系統效能及穩定度

- 基於分散式架構，有效提升系統效能
- 雙中心互為備援，增加系統穩定度

— 減少 維運負擔

- 視覺化查詢與管理介面，降低學習曲線，提升作業效率
- 單一平台查找日誌，加速排除作業
- 關鍵字告警，自動察覺異常，優化人力資源

× 加乘 應用情境

- 彈性整合多種大數據平台，數據再利用，創造未來商機
- 協助客戶分析呈現貸款流程-『進件』、『徵信』、『照會』及『撥款』等關卡之流程瓶頸
- 整合不同種類電文，呈現在同一介面，易於使用者查找

÷ 除去 高額費用

- 不限制流量、設備數量或使用人數，資料收集可以隨心所欲不受授權限制
- 易於佈建，自帶自我健檢功能，有效降低維運人力成本

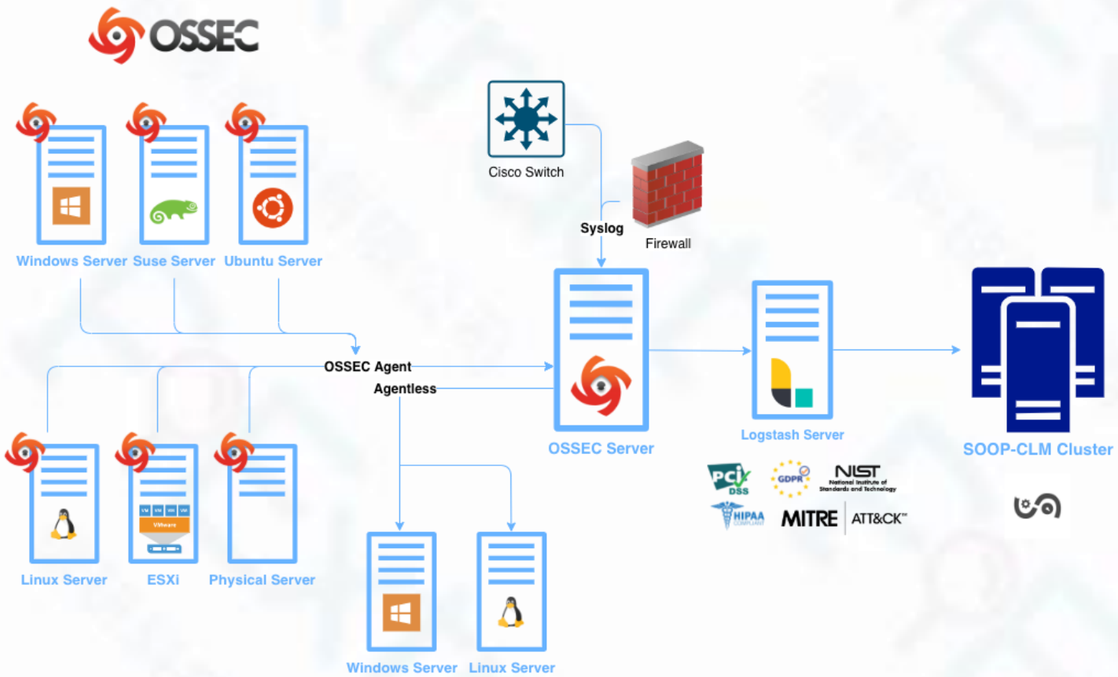
04.資安模組介紹

- 資安模組
- 規則分類
- 產品定位及說明

04 資安模組 - OSSEC

使用CLM-Plus OSSEC 提供完善的 Security Information 協助進行資安的分析監控

1. CLM-Plus OSSEC 提供了多種監控方式， Agent Base、Agentless 以及接收 Syslog
2. 內含著上千種資安規範進行資安分析
3. 整合 MITRE ATT&CK 框架，協助識別資安事件以及詳細資訊
4. 整合SOOP-CLM，以提供權限控管，事件告警、報表產出及儀表板呈現等功能



04 資安模組 - OSSEC

OSSEC 提供了資訊安全的分析功能

系統安全性分析

收集、彙整、分析，幫助企業檢測入侵、資安威脅和異常的行為分析

資安相關日誌分析

透過 Agent 收集系統中的 Syslog,及Ap log ，並將資訊安全相關的資訊回傳至Server 當中

系統合規性

OSSEC 提供了必要的安全規則檢測，以符合各行業的標準以及法規，e.g. PCI DSS(支付卡行業合規性) 、 GDPR (一般資料保護規範)、HIPAA(健康保險便利與責任法案).....等等

入侵偵測

OSSEC 的 Agent 可以協助掃描監控的主機，找到惡意的軟體、rootkit還有可疑的行為。

檔案完整性分析

OSSEC 可以針對系統中的文件進行完整性監控，識別出重要的文件是否有內容、權限以及其他屬性的變化，來保證系統的完整性

PyExtract

OSSEC 將規則區分為多個級別

- 最低級別“00”到最高級別“15”，共有 16 種級別
- 目前有部分級別尚未使用，為將來資安規範發展或演進提供調整空間, 規則如下:

Ignored (可忽略的)

No action taken. Used to avoid false positives. These rules are scanned before all the others. They include events with no security relevance.

None (無)

System low priority notification (系統低順位通知)

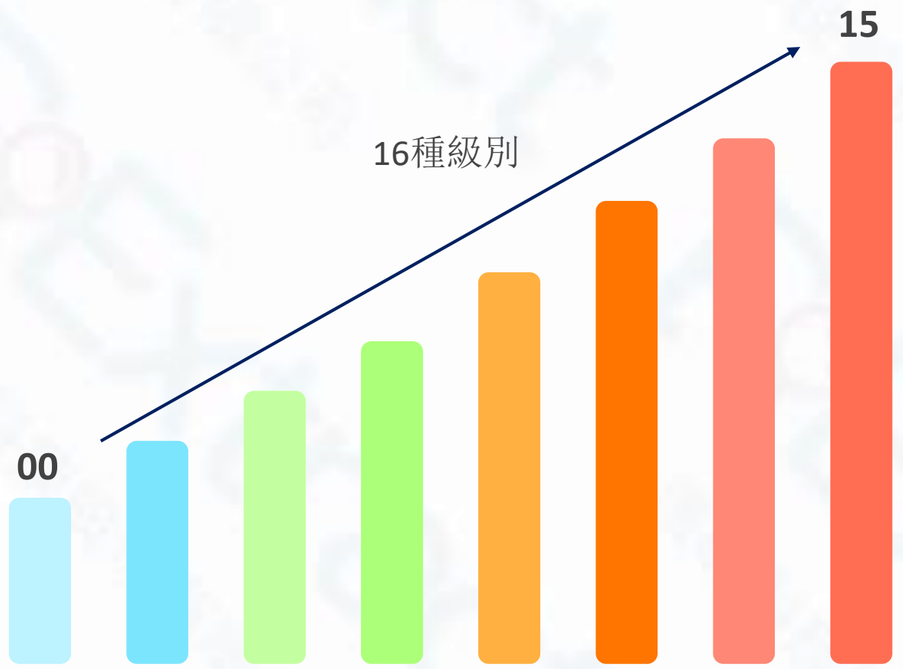
System notification or status messages. They have no security relevance.

Successful/Authorized events (成功授權事件)

They include successful login attempts, firewall allow events, etc.

System low priority error (系統低順位錯誤)

Errors related to bad configurations or unused devices/applications. They have no security relevance and are usually caused by default installations or software testing.



04 OSSEC-規則分類

User generated error (用戶產生的錯誤資訊)

They include missed passwords, denied actions, etc. By itself they have no security relevance.

Low relevance attack (低相關性的攻擊)

They indicate a worm or a virus that have no affect to the system (like code red for apache servers, etc). They also include frequently IDS events and frequently errors.

“Bad word” matching (關鍵字相關)

They include words like “bad”, “error”, etc. These events are most of the time unclassified and may have some security relevance.

First time seen (系統首次出現的行為)

Include first time seen events. First time an IDS event is fired or the first time an user logged in. If you just started using OSSEC HIDS these messages will probably be frequently. After a while they should go away, It also includes security relevant actions (like the starting of a sniffer or something like that).

Multiple user generated errors (使用者多次嘗試產生的錯誤行為)

They include multiple bad passwords, multiple failed logins, etc. They may indicate an attack or may just be that a user just forgot his credentials.

Integrity checking warning (系統完整性驗證)

They include messages regarding the modification of binaries or the presence of rootkits (by rootcheck). If you just modified your system configuration you should be fine regarding the “syscheck” messages. They may indicate a successful attack. Also included IDS events that will be ignored (high number of repetitions).

High importancy event (高重要性事件)

They include error or warning messages from the system, kernel, etc. They may indicate an attack against a specific application.

Unusual error (high importance) (異常錯誤事件)

Most of the times it matches a common attack pattern.

High importance security event (高度重要資安事件)

Most of the times done with correlation and it indicates an attack.

Severe attack (嚴重攻擊事件)

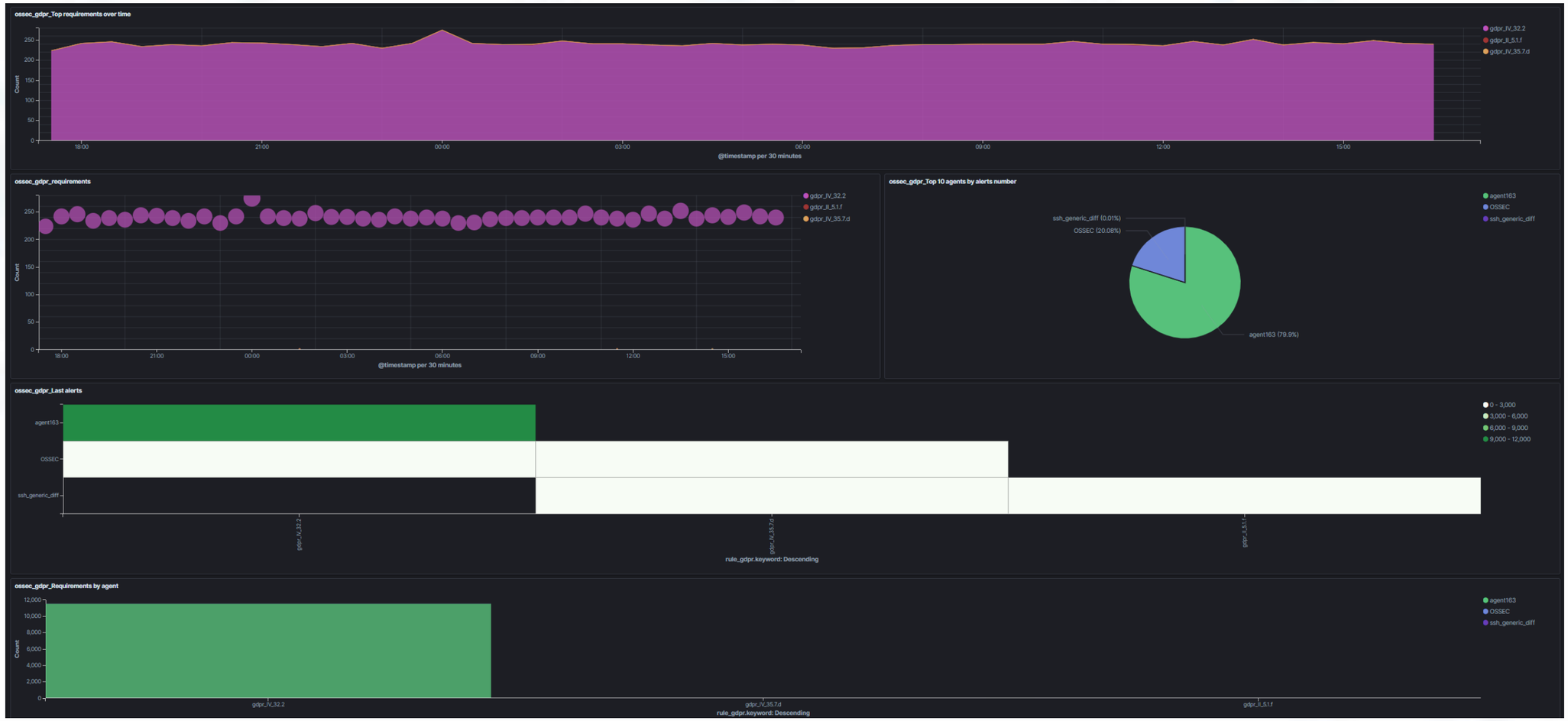
No chances of false positives. Immediate attention is necessary.

04 OSSEC產品定位及說明

- 目前我們可以利用OSSEC做到的程度是：
  - 掃瞄客戶的環境，確認環境中是否有違反現有的資安規範或風險。

04 OSSEC產品定位及說明

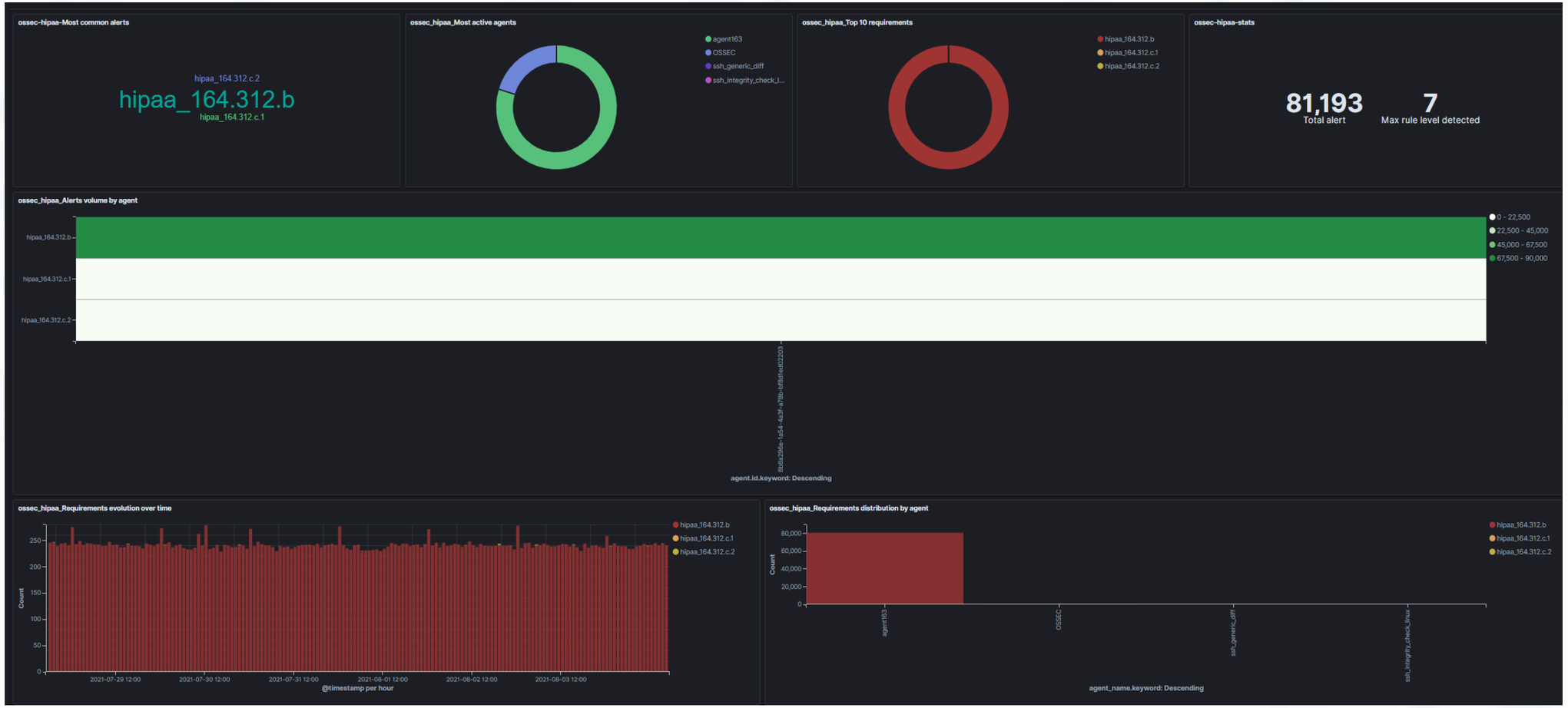
- 目前我們可以利用OSSEC做到的程度是：GDPR
  - 掃瞄客戶的環境，確認環境中是否有違反現有的資安規範或風險。



General Data Protection Regulation

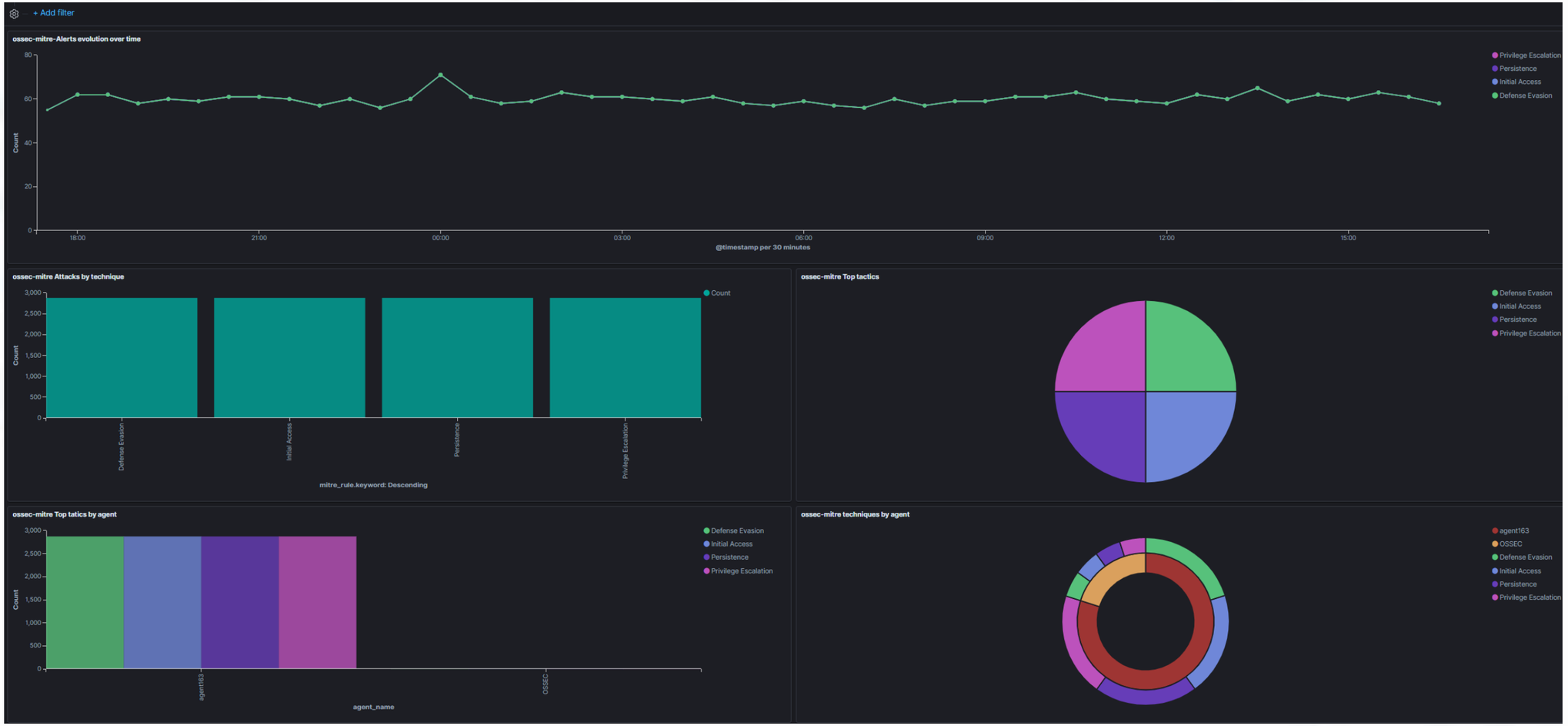
04 OSSEC產品定位及說明

- 目前我們可以利用OSSEC做到的程度是：HIPAA
  - 掃瞄客戶的環境，確認環境中是否有違反現有的資安規範或風險。



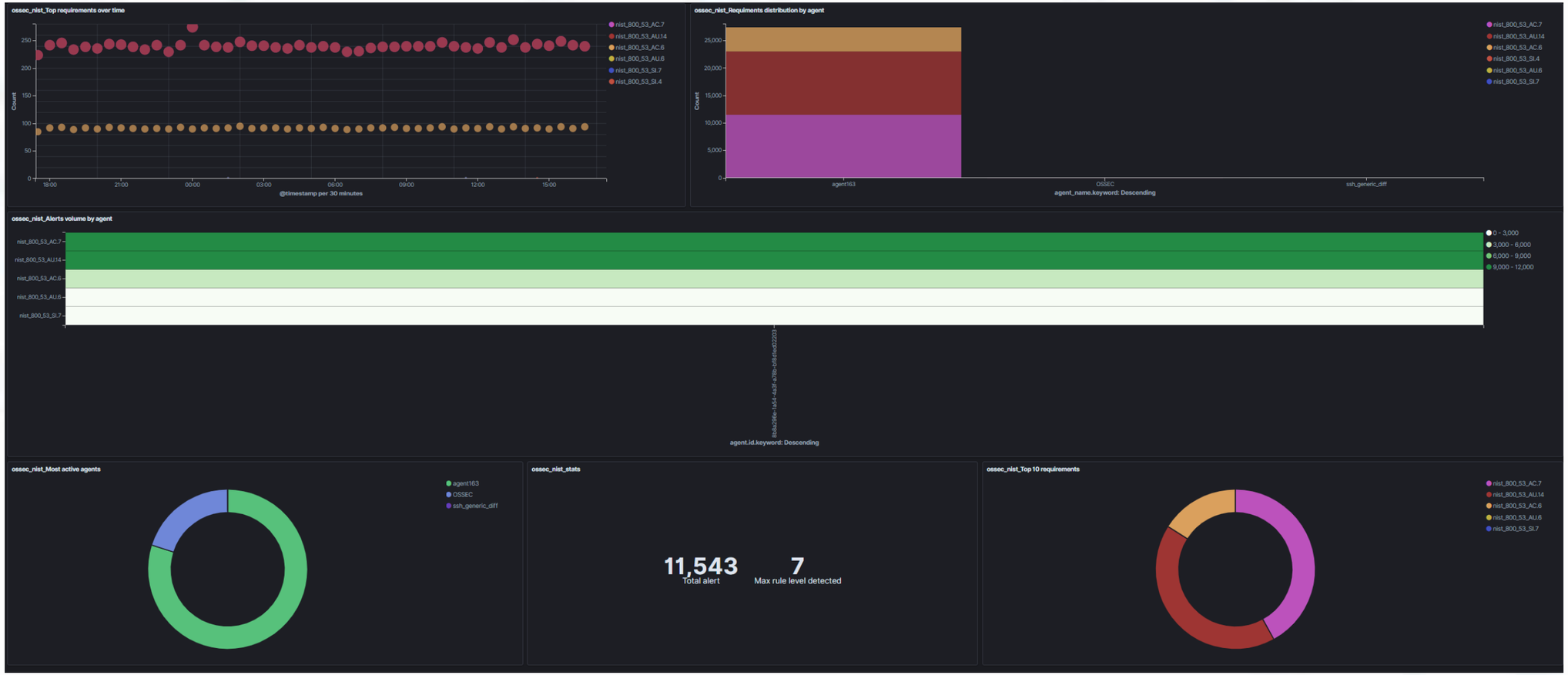
04 OSSEC產品定位及說明

- 目前我們可以利用OSSEC做到的程度是：Mitre Attack
  - 掃瞄客戶的環境，確認環境中是否有違反現有的資安規範或風險。



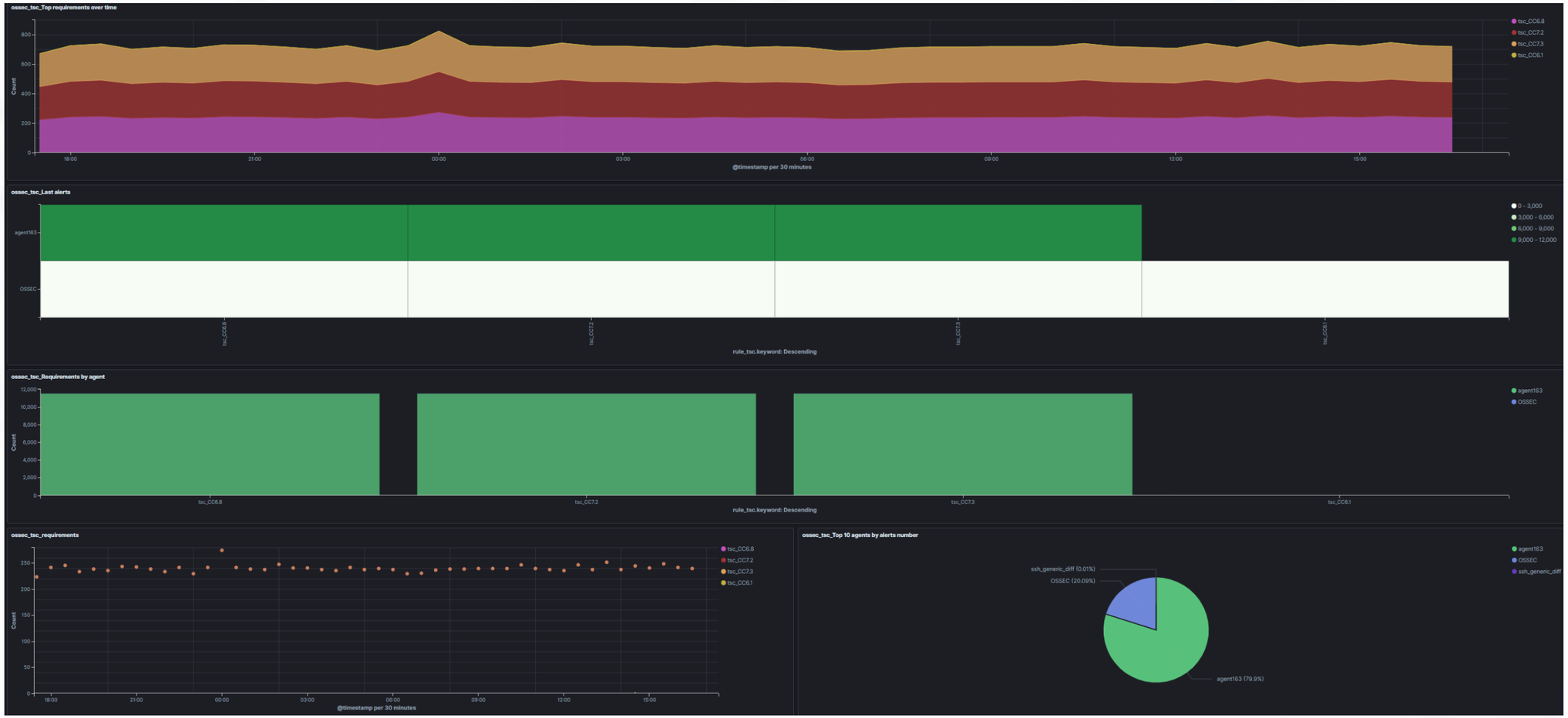
04 OSSEC產品定位及說明

- 目前我們可以利用OSSEC做到的程度是：NIST
  - 掃瞄客戶的環境，確認環境中是否有違反現有的資安規範或風險。



04 OSSEC產品定位及說明

- 目前我們可以利用OSSEC做到的程度是：TSC
  - 掃瞄客戶的環境，確認環境中是否有違反現有的資安規範或風險。



05 SOOP-CLM 優勢

台新銀行

kbro 凱擘 大寬頻

統智科技股份有限公司
PRESIDENT TECHNOLOGY CORP

FAR EASTONE 遠傳

中華民國經濟部
Ministry of Economic Affairs, R.O.C.

龍巖

Taiwan Mobile 台湾大哥大

財金資訊股份有限公司
FINANCIAL INFORMATION SERVICE CO., LTD.

JihSun Holdings 日盛金控

臺灣企銀
Taiwan Business Bank

中華郵政

陽信銀行 SUNNY BANK

Home+ 中嘉

- 百萬資料，秒級回應
- 穩定可靠的分散式架構設計
- 內建多樣視覺化模組，降低學習曲線
- 整合Hadoop，做為長期歷史資料的倉儲
- 簡易人機操作介面，可於Web UI上設定告警和日誌解析規則等日誌管理功能
- SOOP-CLM的自我監控及健檢功能
- 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
- 在地支援
- 客戶橫跨政府/金融/電信
- 高性價比的計價方式