

BiMAP

FiH 全域戰情中心

即時監控 + 彈性模組 + 多維分析 + 趨勢預警

ITOps 維運戰情中心

SecOps 資安戰情中心

DevOps 應用戰情中心

BT 營運戰情中心

FiH 全域戰情中心

應用場景及功能模組

網路流量分析

透過網路設備所採集到的流量資訊，如：Netflow，並搭配專業分析模型，透過 UI 直覺的示警顏色，以及事件回報機制，方便用戶一眼辨識出異常狀況。

硬體效能分析

透過 SNMP 資訊，取得硬體內部運作狀況，例如設備溫度、轉速、電源狀況、風扇運轉等，有效監控目前硬體健康度。

Infrastructure 效能分析

企業伺服器上運行多項服務，透過採集 metrics (cpu/mem/diskio)，並將伺服器進行分群，利用 N-7-1 分析模型，簡單找出系統瓶頸，以利進一步優化。

資安事件分析與情資管理

透過資安設備與情資管理的相互搭配，並整合資產管理，如：IP/網段資訊，讓資安分析數據更具有可讀性，一眼即可知曉目前資安防護現況。

API 效能與異常分析

針對企業內的 AP Log、檔案、資料庫，以及其他所有資料源進行收集、業務分析、資料分析、正規化，並進行客製視覺化，以利進行庫分析、檔案異常檢核等應用。

戰情中心管理模組

依據不同的設備模組，可以組合為 ITOps 維運戰情中心、SecOps 資安戰情中心、DevOps 應用戰情中心和 BT 營運戰情中心等不同類型的戰情中心。

自動化報表模組

透過指定資料源，排序的方式，以圖表或是表格方式，進行資料報表呈現，並定期將報表透過 Email 寄送負責人員。

智能告警模組

基於 ELK 企業級資料庫，儲存海量資料，透過告警模組，定時進行資料檢核、設定 TTL，觸發閾值即透過 Line、Email 告警，也可透過 Kibana 即時監控告警狀況。

高速集群架構且無容量使用限制

原生支援 cluster 模式，足以確保系統穩定性及保有資料不遺失的特性。根據資料週期進一步劃分 Hot/Warm/Cold 節點，且無處理資料的容量和流量限制。

儀表板彈性設計

依據實際的需求，自行定義分析儀表板，並根據不同的儀表板進行權限劃分，給管理團隊、系統維運團隊、開發團隊等不同的群組，進行不同的監控分析儀表板。

FiH 全域戰情中心架構圖

FiH 可以整合任意資料來源，利用大數據中台高度彈性的架構，尤其面臨到資安事件時，資訊量可能在短時間內，瞬間飆升。因 FiH 具有 Cluster 水平擴充的優勢，不論是資料的收集、儲存與正規化，都可以輕易完成，再利用 Grafana/Kibana 的客製視覺化優勢，透過 FiH 戰情中心整合所有資料於一體。



資安戰情中心管理模組

FiH 全域戰情中心，可水平整合不同類型儀表板於一身，並透過權限管理，讓不同人員、角色可以專注於不同域領之儀表板，不需在不同的網頁不斷切換。依據不同的設備模組，可以組合為 ITOps 維運戰情中心、SecOps 資安維運戰情中心、DevOps 應用戰情中心和 BT 營運中心等不同的類型的戰情中心。



Infrastructure 效能分析模組

- 出現異常後，才被動開始處理異常現象
- 頭痛醫頭、腳痛醫腳，無法事先防治
- 舊系統問題不斷，影響新系統開發進度

- 單一系統中資料交換複雜，維護困難
- 應用系統之間關聯性高，相互影響
- 一旦發生異常問題，處理週期過長，尤其是效能問題。

■ 被動救火的維運模式

■ 系統之間的關聯性複雜

■ 現有的監控手段無法滿足需求

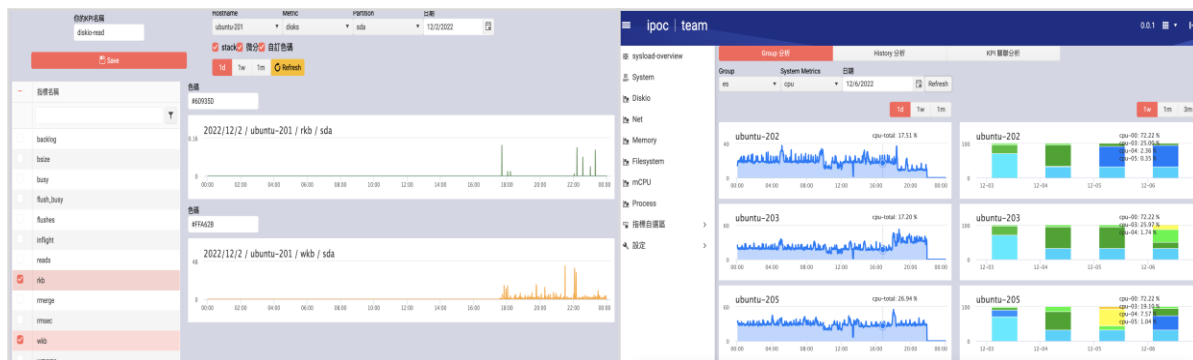
■ 資料增長和業務需求的變更

- 監控手段單一，無法有效定位問題
- 監控工具過於複雜，技術培養不易
- 部署多種監控工具，難以匯總統一

- 資料持續增長，造成高峰期持續變慢
- 軟體版本更新，衍生新的效能問題
- 業務量增加後，系統支撐力無法預測

效能分析模組特點

分析效能模組採用群組概念，將系統指標進行交叉比對，關聯式分析的方式，找出系統可能的瓶頸。透過即時數據與長期資料模型，比對出異常的時間，抓出異常點。



自選 KPI 模式	挑選想要觀察的指標，並自由地進行組合，搭配出最適用分析儀表板
伺服器分群	同時觀察相近性質的伺服器各項指標，並透過短、長期分析圖，進一步分析營運狀況，或是否具有異常
Process 資源分析	系統會自動帶出時間段內，佔用資源 TopN 的處理程序，查看是否異常
N-7-1 分析模型	以群組的方式同時監控多台 Server，並比較過去 7 天之歷史數據，以及多項關鍵指標的關聯分析。

智能告警模組

- 清楚簡易的規則管理介面
- TTL 告警機制，告警不重覆
- 變數定義功能，查詢組合更多元
- 自定義告警類型，方便統計報告

Rule Engine | 規則管理

名稱	規則區域	群組	類型	狀態	command
資安事件觸發	外部網路	1.人侵攻擊類	WAF	啟動	[編輯] [刪除] [詳情]
流量異常	外部網路	4.政策規則類	Traffic	啟動	[編輯] [刪除] [詳情]
多國家重複登入	內部網路	1.人侵攻擊類	Firewall	啟動	[編輯] [刪除] [詳情]
設備失聯	內部網路	1.人侵攻擊類	Firewall	啟動	[編輯] [刪除] [詳情]
Link	內部網路	6.系統調查類	Router	關閉	[編輯] [刪除] [詳情]
成功登入	內部網路	6.系統調查類	Router	啟動	[編輯] [刪除] [詳情]
指令修改	內部網路	6.系統調查類	Router	關閉	[編輯] [刪除] [詳情]
路由變更	內部網路	6.系統調查類	Router	關閉	[編輯] [刪除] [詳情]
EEM	內部網路	6.系統調查類	Router	啟動	[編輯] [刪除] [詳情]
其他異常	內部網路	6.系統調查類	Router	啟動	[編輯] [刪除] [詳情]

1 - 10 of 10 items

異常觸發即時通報

儲存

返回

是否啟動 ☒

規則名稱: 多國家重複登入

規則區域: 內部網路

規則類型: Firewall

規則群組: 1.人侵攻擊類

條件 彙總 動作

☒ Line 通知 測試

Line Token: *****

Line 單次最大告警量: 10

Line 訊息: \$(username) 三分鐘內登入失敗超過 \$(count) 次，請確認是否異常。

☐ Email 通知 測試

TO: example@bimap.co

CC: service@bimap.co

BCC:

Email 單次最大告警量: 1,000

Email 訊息:

資安群

[Alert Notify] 帳號: Andy002, 三分鐘內登入失敗 > 10 次, 請確認是否異常

1. 提供 WEB 自定義告警規則，將所有記錄與事件等內容資訊 (例如身分識別、角色、存取) 進行整合，並找出組織所定義出的風險。
2. 即時追蹤與警示，當特定使用者、應用程式、伺服器或網路設備受到威脅時即可接收通知，包含電子郵件、和通訊平台等。
3. 設定告警事件說明和分析結果，與建議解決措施說明。
4. 可以設定告警的規則群組，將各類的告警規則進行分類。
5. 提供設定 TTL (Time To Live) 的告警存活時間(分/時/日)。



集先鋒科技有限公司

<https://bimap.com.tw>

新北市板橋區文化路二段 500 號 4 樓

授權經銷商