新世代 SIEM 平台 – FortiSIEM
AI 驅動的安全營運

Kevin Yang
kmyang@fortinet.com

現今資安與網維面臨的挑戰

不僅需要防護型資安解決方案，還需要建立早期預警系統

① 滿足法規針對資通安全防護及控制措施等相關要求

② 不同品牌產品與各自獨立的管理系統，資訊統整難

③ 每天太多日誌事件產生，缺乏好工具找出關鍵問題

④ 進階威脅與勒索病毒持續成長，如何發現潛在威脅

⑤ 建立資安事故反應標準作業流程與緩解動作自動化

What is FortiSIEM

新一代 SIEM 管理平台，提供網路及用戶異常行為智能分析

資安 (SOC) 與網維 (NOC) 融合式分析

所有告警事故分類及優先處理順序一目了然

告警事故分類
- 資安事件監看
- 效能記錄監看
- 設備可用度監看
- 組態異動監看

重要告警事故排行榜

嚴重受害主機排行榜

資安 (SOC) 與網維 (NOC) 融合式分析

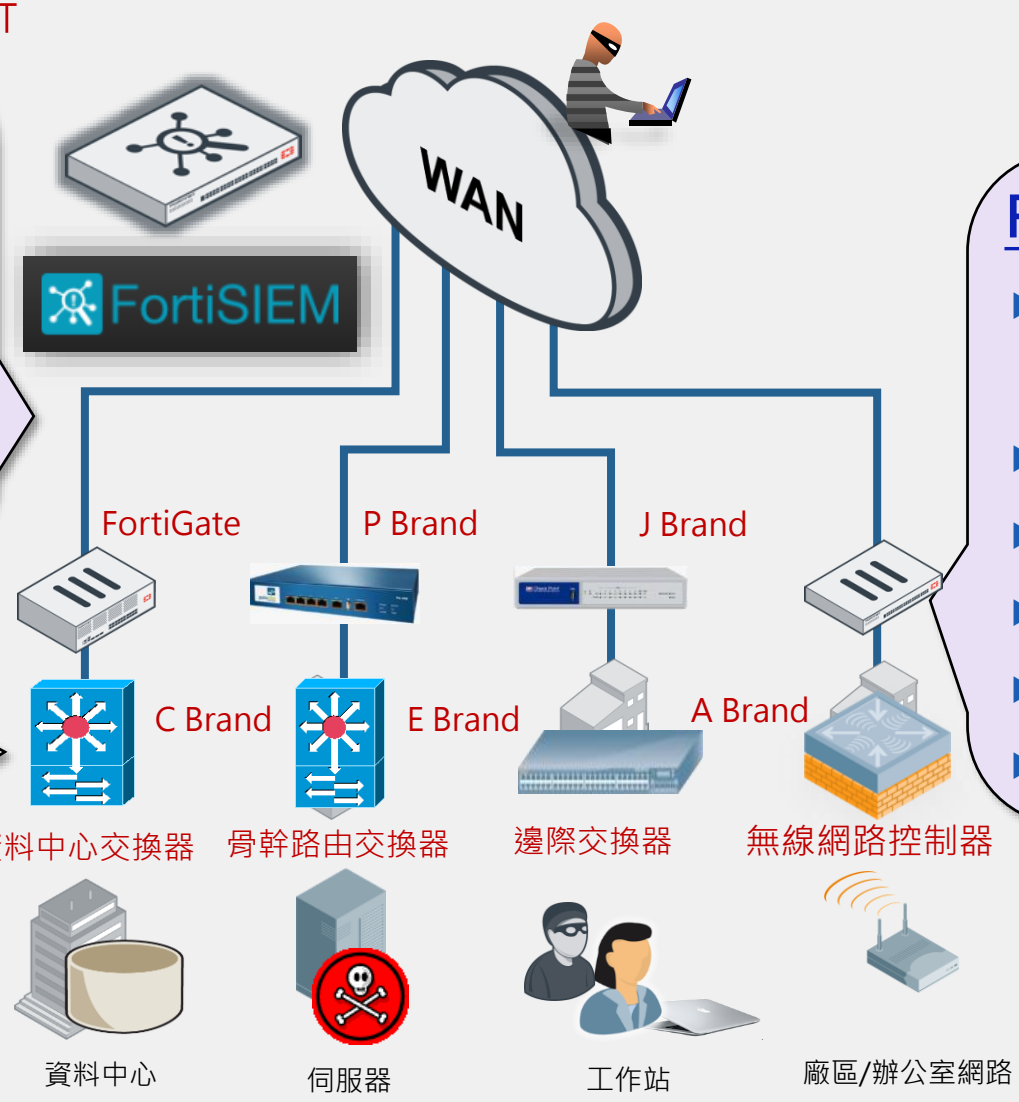
多源、多品牌日誌記錄統整與關聯分析

SNMP、CLI、API, etc.

- CMDB 資產管理
- 設備健康狀態(Up/Down)
- 效能使用率(CPU/ Memory/Bandwidth)
- 儲存空間 (Storage)
- 異常效能分析

Syslog、WMI、API, etc.

- 系統事件(Event Log)
- 資安事件(Security Log)
- 流量記錄 (Traffic Log)
- 應用系統事件 (Application Layer)
- 異常行為、事件分析



Flows

- NetFlow/Sflow /Jflow/IPFix
- 內外網路流量使用分析
- 通訊協定流量使用分析
- 點對點會談流量排行
- 網路 scan/DoS 威脅分析
- 異常行為、流量分析

自動身分識別與連網位置關聯分析

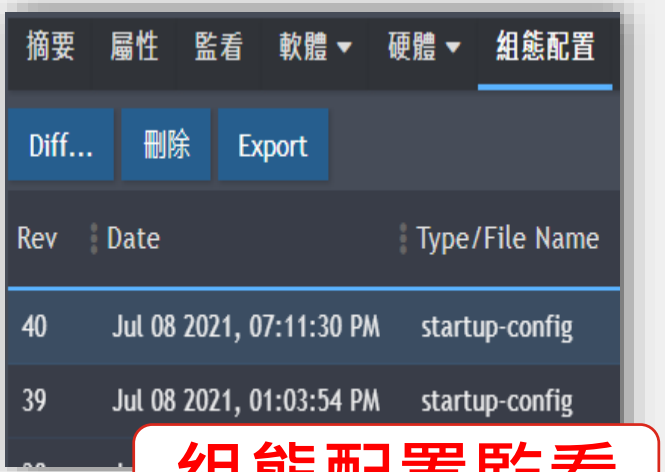
快速查找人員與設備，何時、何地以及如何連網

自動探索，設備組態管理資料庫 (CMDB)

學習了解您的網路環境並建立基準線

設備識別分類

運行效能監看



組態配置監看

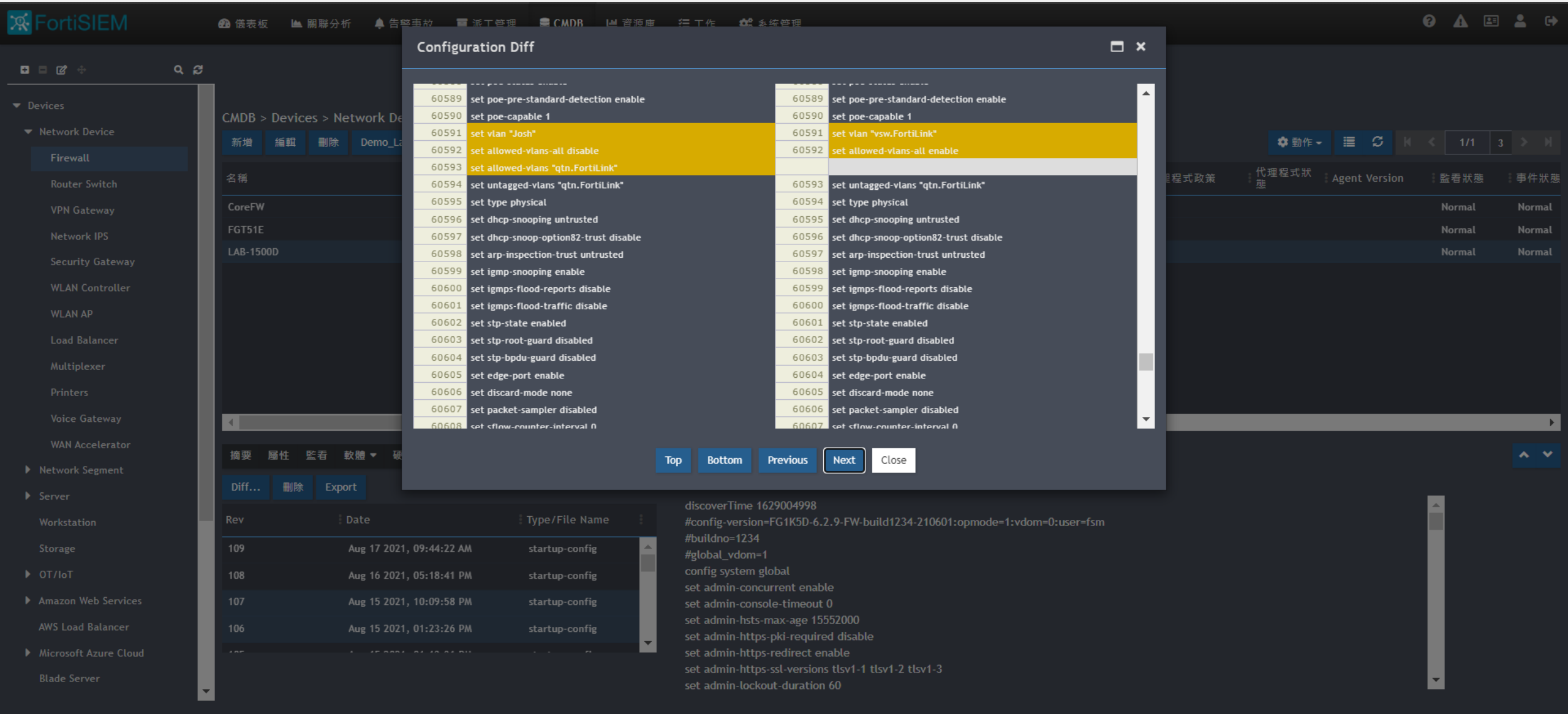
應用導向管理

威脅情資比對

設備資產統整

自動探索，設備組態管理資料庫 (CMDB)

詳細檢視設備資訊、資安態勢、效能狀況、組態異動比對



可快速擴容的高彈性架構

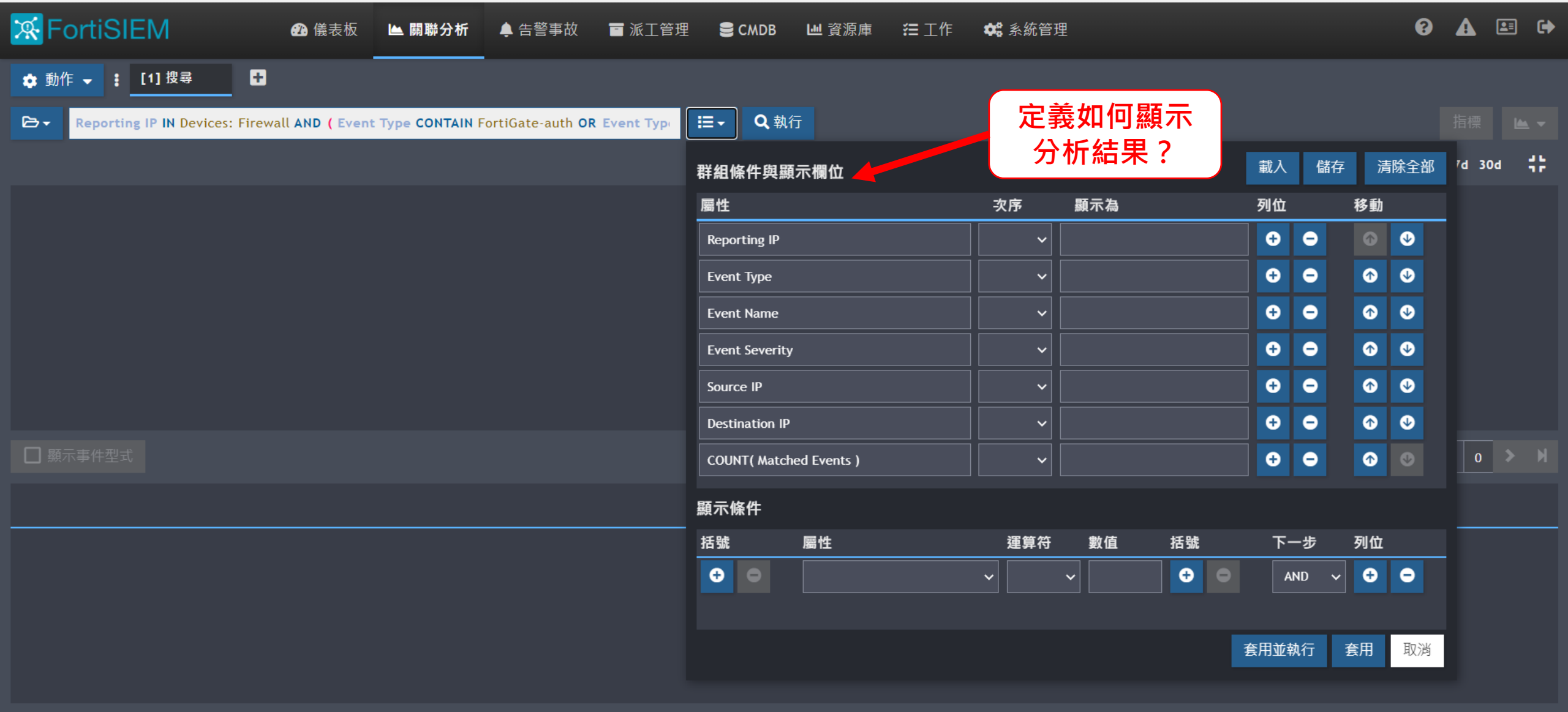
支援彈性分層管理權限與多租戶架構部署 (Multitenant Architecture)

直覺式的事件關聯分析簡單易用

以人為本的操作邏輯，過濾及顯示繁雜事件，減輕人員負擔

直覺式的事件關聯分析簡單易用

以人為本的操作邏輯，過濾及顯示繁雜事件，減輕人員負擔



直覺式的事件關聯分析簡單易用

以人為本的操作邏輯，過濾及顯示繁雜事件，減輕人員負擔

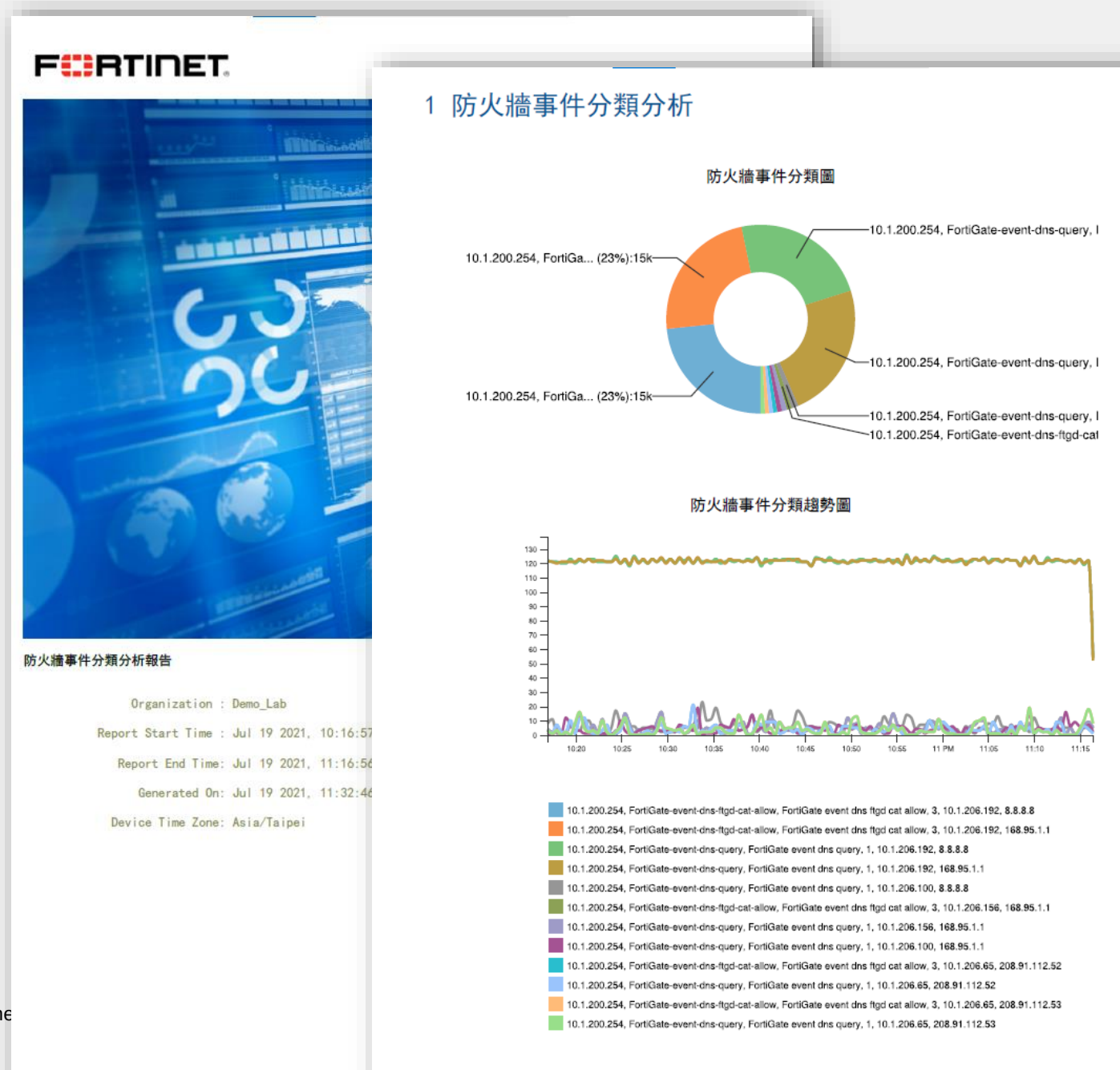
關聯分析結果可產生各式報表

手動或排程自動產生報表

豐富的內建合規性報表

提供彈性的報表客製化能力

- 數以千計的內建報表樣板可供選擇
- 合規性報表 (Compliance Reports)
  - PCI, SOX, HIPAA, FISMA
  - NERC, COBIT, ITIL, NIST
  - ISO, GLBA, GPG13, CIS
  - SANS Critical Controls
- OT 設備相關報表
- 報表客製化建構器
  - 3,000+ 可客製化欄位
  - 封面客製化能力
  - 支持多段落報表格式
  - 豐富可視性圖表，可穿插文字與附件



關聯分析結果可轉成各式監看儀表板

任何關聯分析結果都可變成您的儀表板

關聯分析結果可產生規則，觸發告警事故

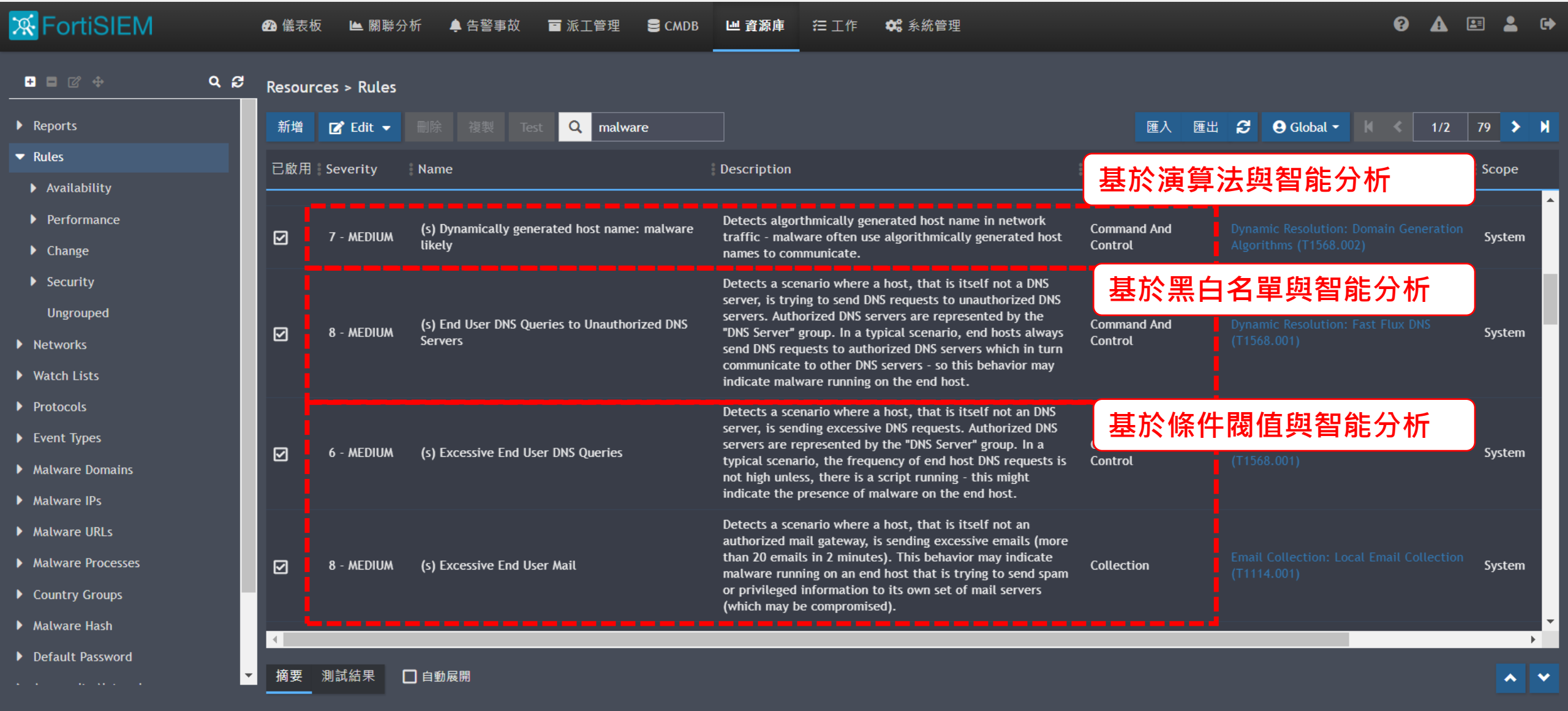
輕鬆監看及告警您關心的事件

導入智能分析 (AI)，機器學習 (ML) 分析異常行為

豐富的內建 AI / ML 告警事故規則

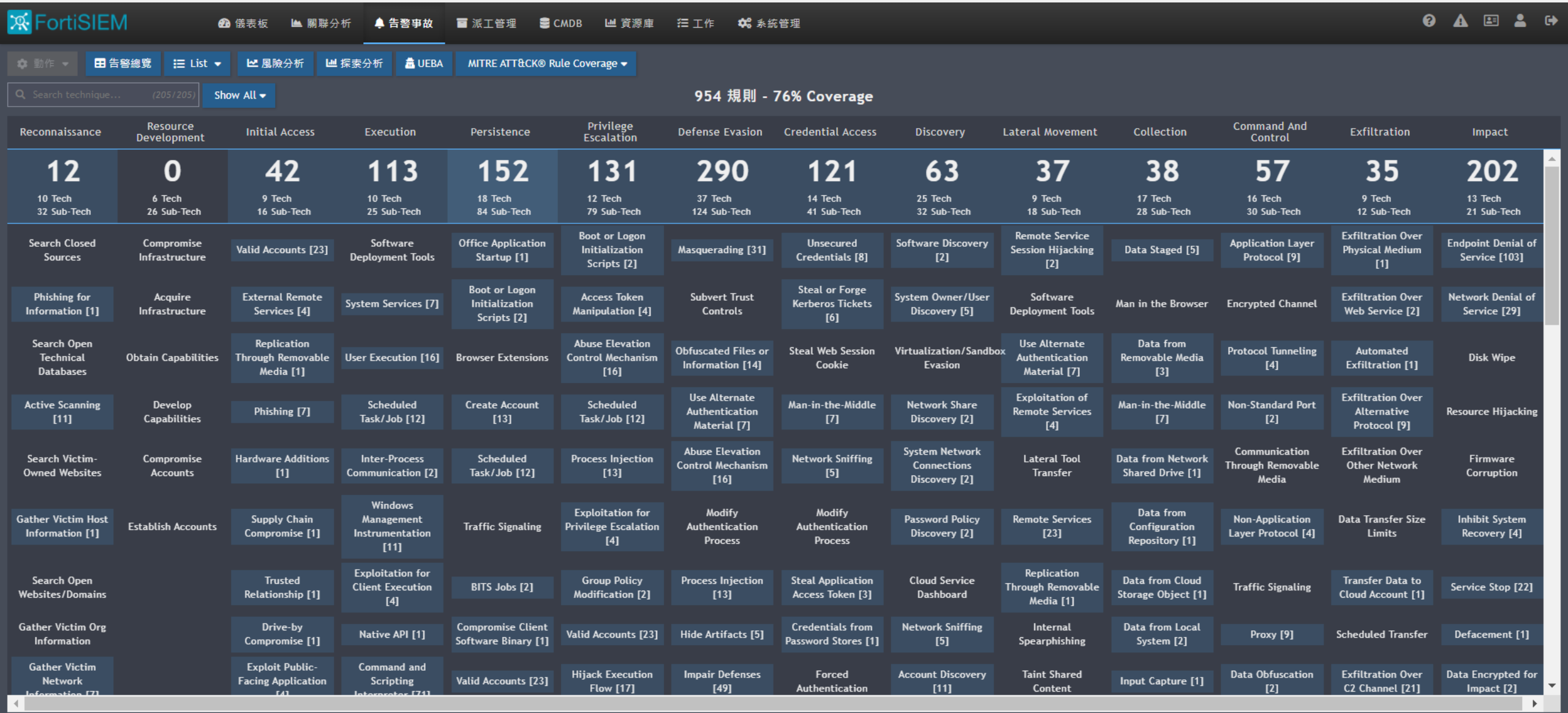
導入智能分析 (AI)，機器學習 (ML) 分析異常行為

豐富的內建 AI / ML 告警事故規則



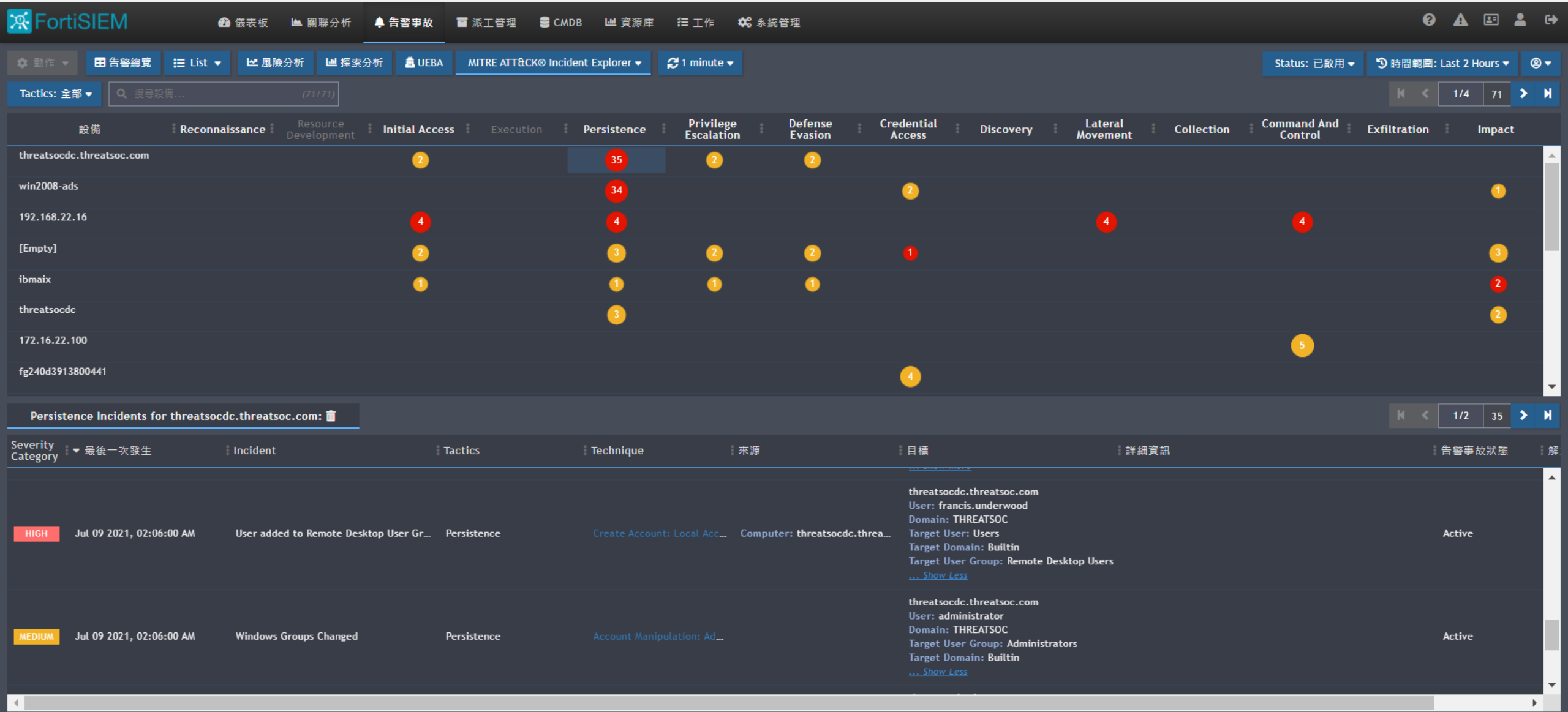
MITRE ATT&CK 資安對抗策略、手段告警圖

關聯規則對應 MITRE ATT&CK 新資安框架的覆蓋程度



MITRE ATT&CK 資安對抗策略、手段告警圖

觸發告警主機在資安攻擊鏈所處的狀態



整合並自動更新外部情資 (FortiGuard 或第三方情資)

網域、IP 地址、URL 網址、程序及雜湊碼的情資交換與分析告警

簡單建立標準化事故協作回應流程與自動化 (SOAR)

詳細檢視、追蹤告警事故

簡單建立標準化事故協作回應流程與自動化 (SOAR)

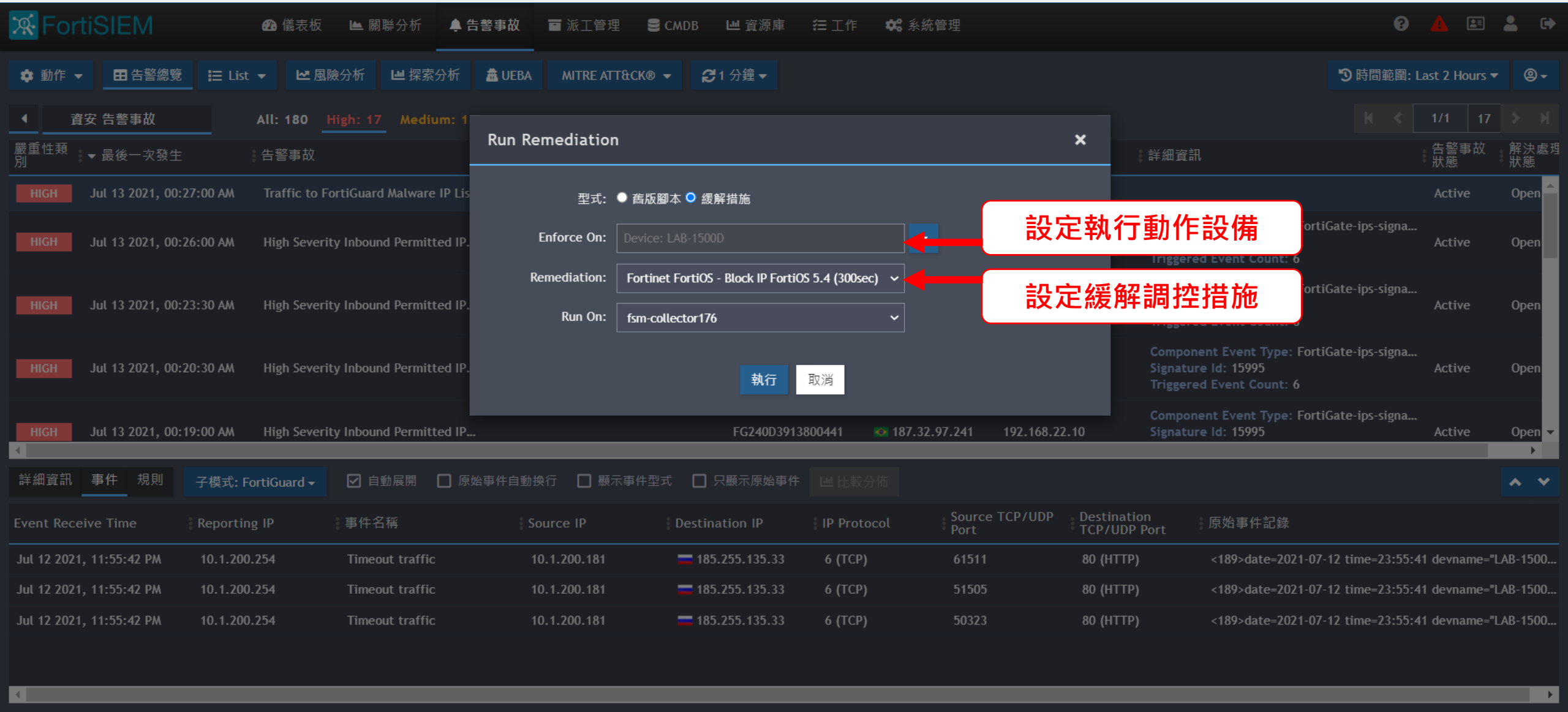
開立工單、派工協作處理

簡單建立標準化事故協作回應流程與自動化 (SOAR)

迅速反應，執行聯防緩解調控措施

簡單建立標準化事故協作回應流程與自動化 (SOAR)

迅速反應，執行聯防緩解調控措施

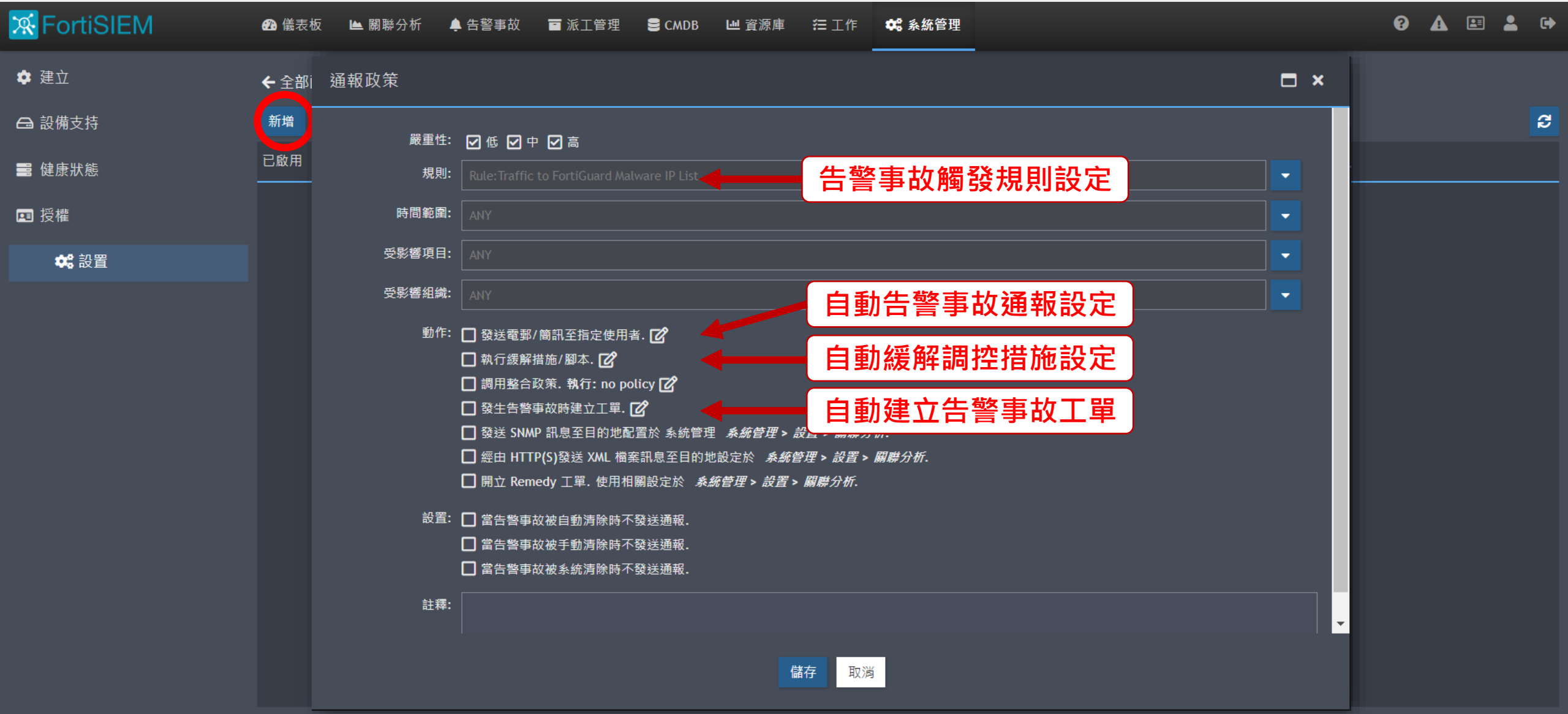


簡單建立標準化事故協作回應流程與自動化 (SOAR)

內建緩解調控措施腳本，可與多品牌設備協作聯防

簡單建立標準化事故協作回應流程與自動化 (SOAR)

全面自動化的告警事故反應流程



FortiSIEM 重要特點與價值

AI 驅動的安全營運

- 新世代的 FortiSIEM，不再只是單純的安全資訊與事件管理 (SIEM)
- 還可進一步做為企業安全/網維管理的優化工具
- 彈性的資安/網路監看儀表板提供更好的可視性
- 針對進階持續性威脅或勒索病毒的攻擊，導入 AI / ML 智能分析，對應 MITRE 資安新框架，提供先期預警能力
- 內建派工管理系統，可連動跨品牌設備，滿足自動化協作聯防的需要


FORTINET