當SOC遇見NOC

原來SIEM的使用也可以很簡單

Kevin Yang

kmyang@fortinet.com

Gartner says:

NOC/SOC TODAY

從積極預防的角度來面對網路資訊安全

Shift Cybersecurity Investment to Detection and Response

FOUNDATIONAL **Refreshed:** 03 May 2017 | **Published:** 07 January 2016 **ID:** G00292536

Analyst(s): *Ayal Tirosh | Paul E. Proctor*

"Organizations need to detect and respond to malicious behaviors and incidents, because even the best preventative controls will not prevent all incidents."

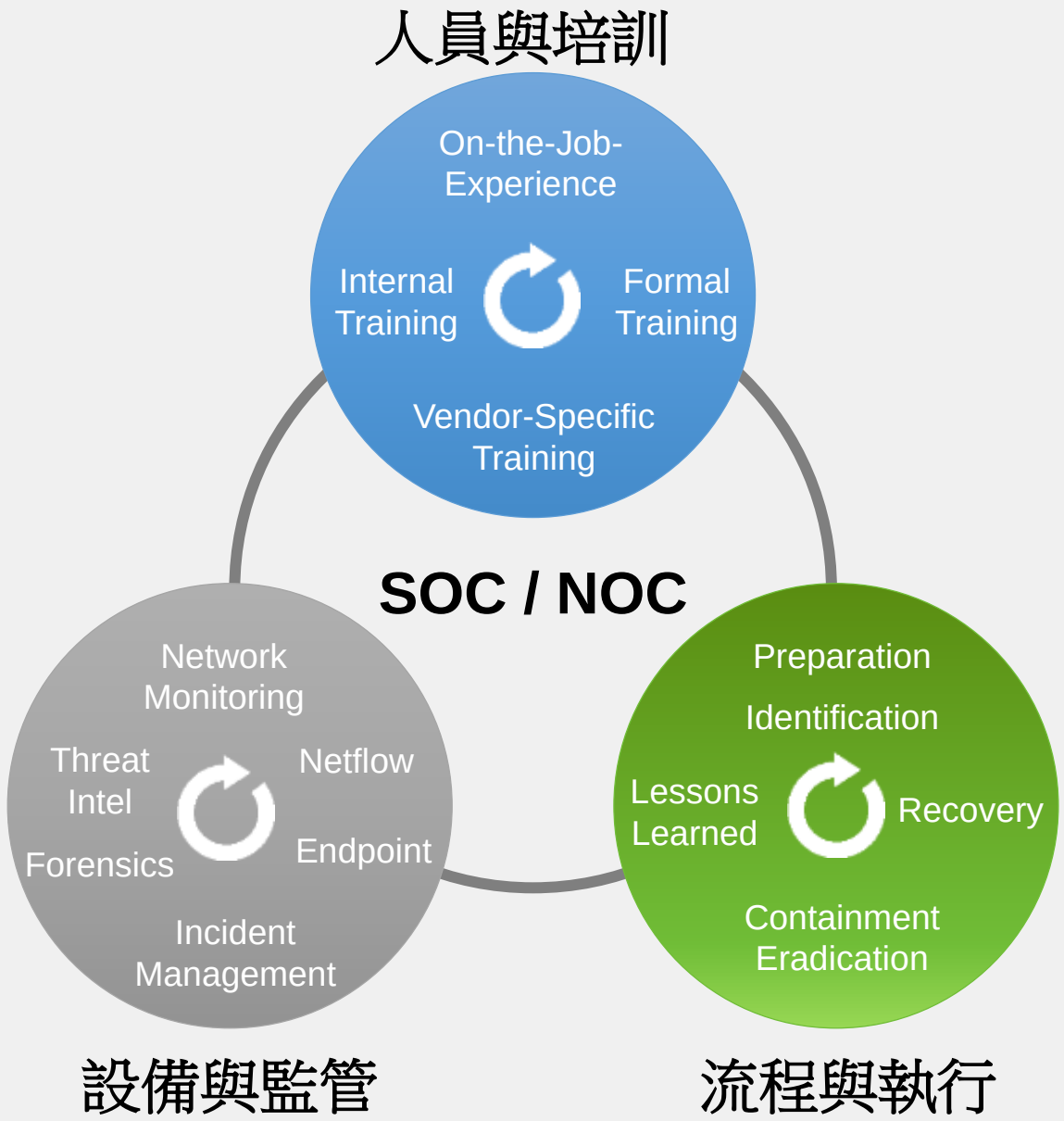
Application Performance Monitoring and Application Security Monitoring Are Converging

Published: 25 April 2017 **ID:** G00324828

Analyst(s): *Cameron Haight | Neil MacDonald*

"...an end user doesn't care if their application service problems are performance or security-related.
In other words, high CPU utilization, a SQL injection attack or a denial of service (DoS) attack can result in service degradation."

資安維運控管三重奏


人員與培訓
On-the-Job-Experience
Internal Training
Formal Training
Vendor-Specific Training
SOC / NOC
Network Monitoring
Threat Intel
Netflow
Forensics
Endpoint
Incident Management
Preparation
Identification
Lessons Learned
Recovery
Containment Eradication
設備與監管
流程與執行

傳統的 SIEM vs. 新一代的 SIEM

NOC/SOC TODAY

Skilled Personnel

- Collect Logs
- Reduce the Size if Possible
- Transport to Central Location
- Normalize / Enrich / Correlate
- Enhanced Search Capabilities
- Alert / Take Actions in Real-Time
- Data Storage
- Produce Reports

Traditional **SIEM** Capabilities

- 資安 (SOC) 與網維 (NOC) 融合式分析
- 設備資產、配置與效能管理 (CMDB)
- 可快速擴容的高彈性架構
- 支持多租戶管理環境
- 直覺式事件分析簡單易用
- 整合眾多設備與既有環境
- 單一的統合性介面管理平台

新一代的 SIEM 平台
更好的可視性 (**Visibility**) 與擴容性 (**Scalability**)
降低使用維運的複雜度 (**Less Complexity**)

資安 (SOC) 與網維 (NOC) 融合式分析

NOC/SOC TODAY

資安 SOC 分析	網維 NOC 分析
Log Ingestion, Parsing and Storage	***Real-Time Infrastructure Discovery CMDB***
File Integrity Monitoring	***Network and Interface Utilization***
Patented Log Analytics	***CPU, Memory, Disk Performance Monitoring***
Incident Management, Ticketing and Response	***Availability Monitoring***
Dynamic Identity and Location Report	***Storage Monitoring***
External Threat Feed Intelligence Integration	***Change monitoring – config., installed software***
Reporting and Compliance – Built in/Custom	***Infrastructure and User Application Monitoring***
Rule and Statistical Anomaly Based Reporting	***Synthetic Transaction Monitoring***

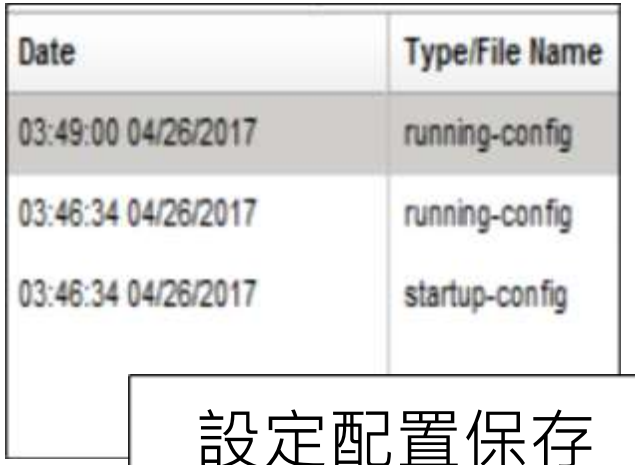
Cross Correlated in Real-Time

設備資產、配置管理資料庫 (CMDB)

NOC/SOC TODAY

設備識別分類

運行效能監控



設定配置保存

應用導向管理

威脅交查比對

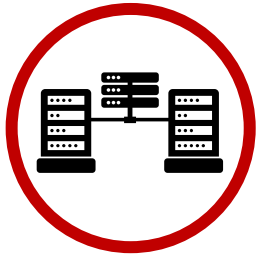
設備資產統整

新一代 SIEM 分散式架構主要構成元件

NOC/SOC TODAY

SUPERVISOR → SIEM 系統核心功能，單一使用者介面、CMDB 資料庫與報表管理

WORKERS → 分散式運算協作節點，可橫向擴充 SIEM 系統，提升資料關聯分析效能



COLLECTORS → 分散式資料收集節點，設備探索與分類，資料解譯、正規化、壓縮與加密傳輸

WINDOWS AGENTS → 針對 WINDOWS 系統提供更方便有效的日誌收集代理程式

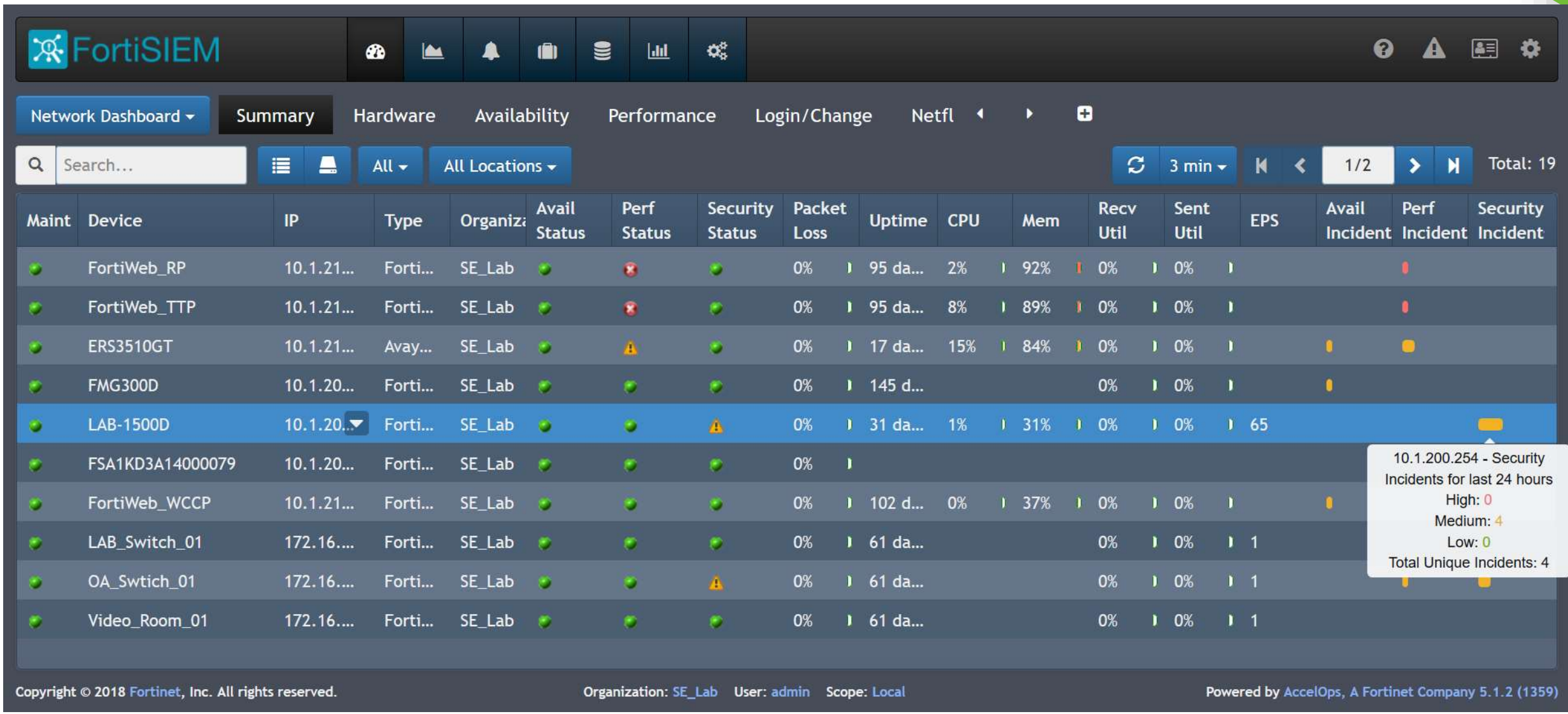
可快速擴容的高彈性架構 Rapid Scale Architecture

NOC/SOC TODAY

- 支援多租戶資安服務管理部署 (Managed Security Service Provider)

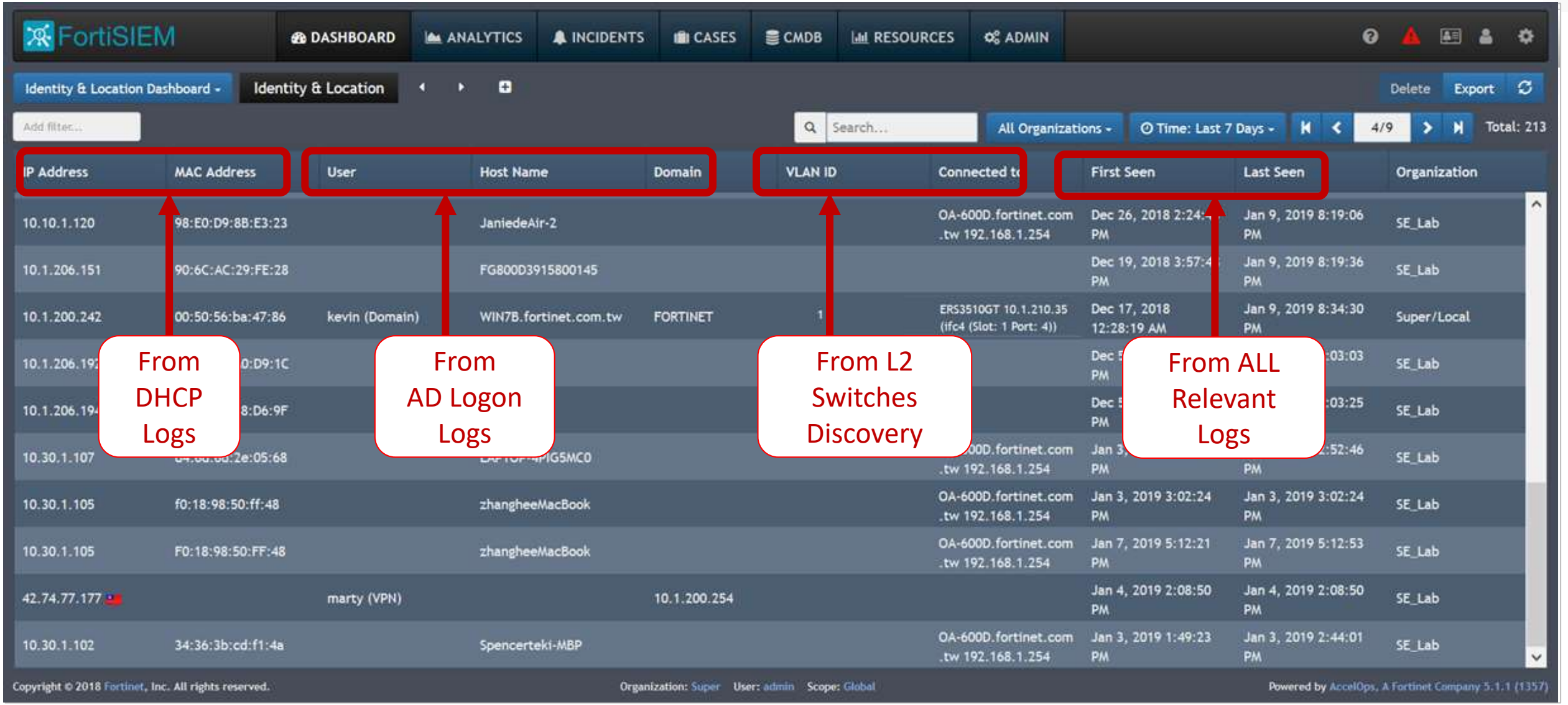
SOC 與 NOC 的融合分析：
設備資安、效能狀態彙總表 (Network Summary Dashboard)

NOC/SOC TODAY



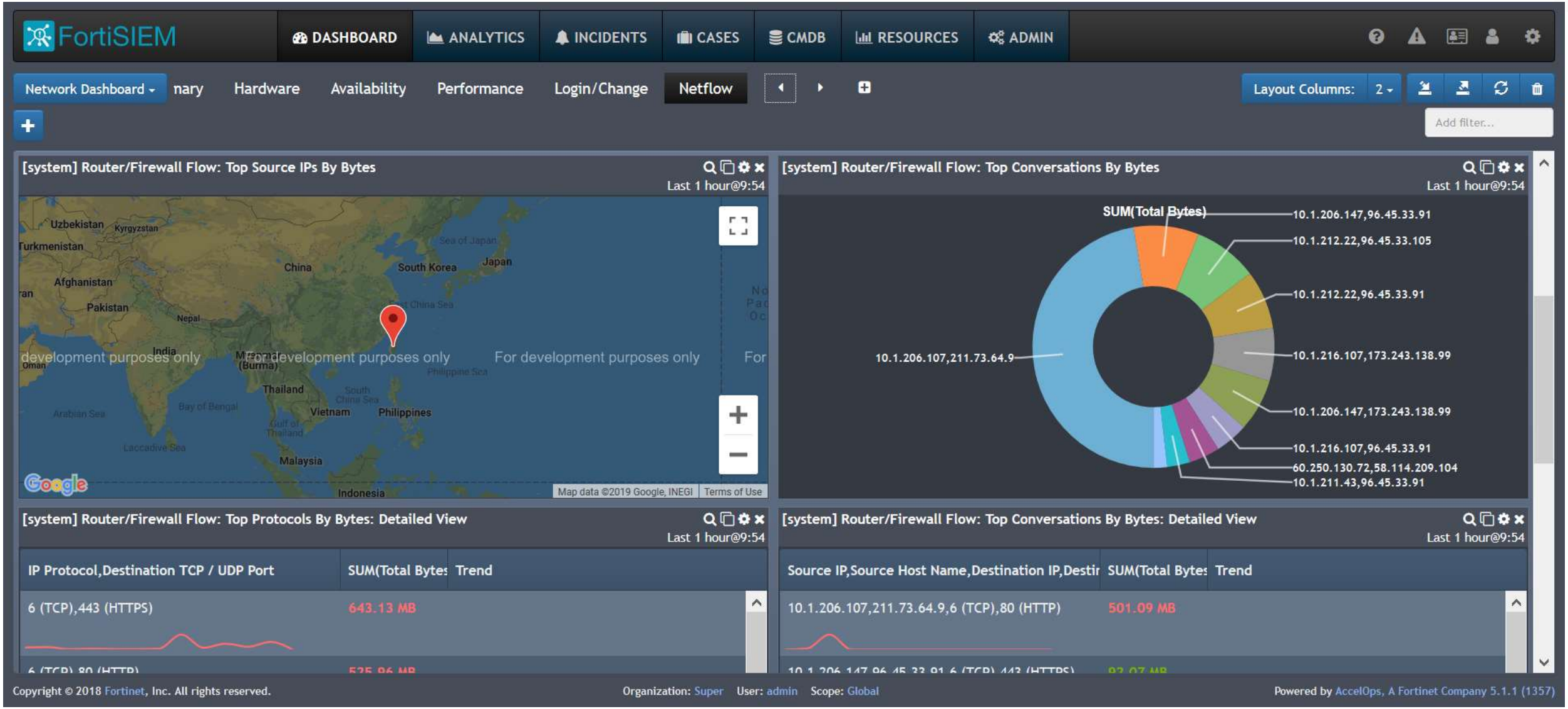
SOC 與 NOC 的融合分析：
自動 IP、MAC、User、Location 關聯分析

NOC/SOC TODAY



SOC 與 NOC 的融合分析：
支持 Netflow / Sflow 流量統計

NOC/SOC TODAY

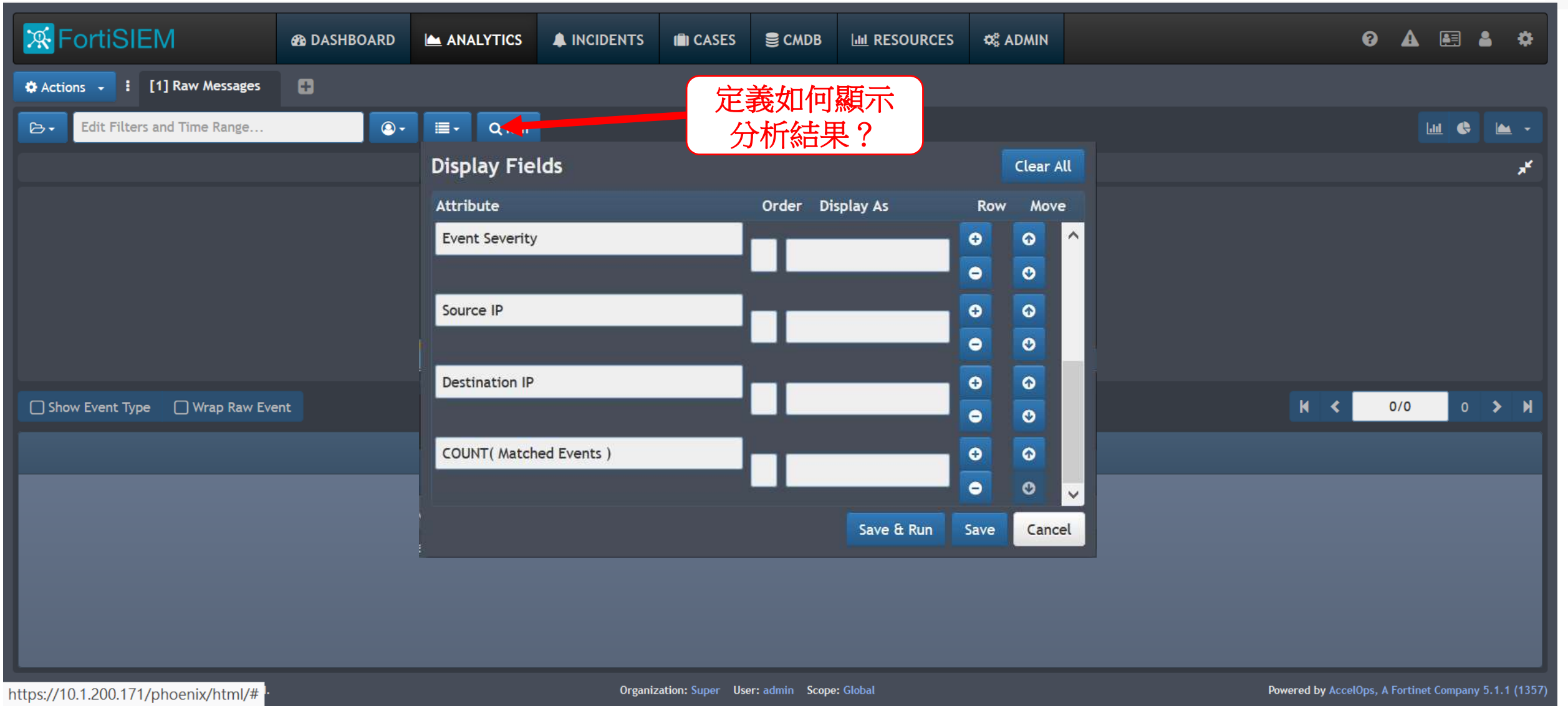


直覺式的事件關聯分析處理：
以人為本的操作邏輯，簡單易用，減輕人員負擔

NOC/SOC TODAY

直覺式的事件關聯分析處理：
以人為本的操作邏輯，簡單易用，減輕人員負擔

NOC/SOC TODAY



直覺式的事件關聯分析處理：
以人為本的操作邏輯，簡單易用，減輕人員負擔

NOC/SOC TODAY

Reporting IP	Event Name	Severity	Source IP	Destination IP	COUNT(Matched Events)
10.1.200.254	The URL belongs to an allowed category in the firewall policy	3	10.1.210.100	96.45.36.31	494
10.1.200.254	FortiGate event dns resolv error	7	10.1.210.51	208.91.112.53	56
10.1.200.254	FortiGate event dns resolv error	7	10.1.210.51	208.91.112.52	29
10.1.200.254	Admin logoff	1	10.1.200.175	10.1.200.254	26
10.1.200.254	Failed admin logon	10	10.1.200.175	10.1.200.254	26
10.1.200.254	Successful admin logon	1	10.1.200.175	10.1.200.254	26

Organization: Super User: admin Scope: Global
Powered by AccelOps, A Fortinet Company 5.1.1 (1357)

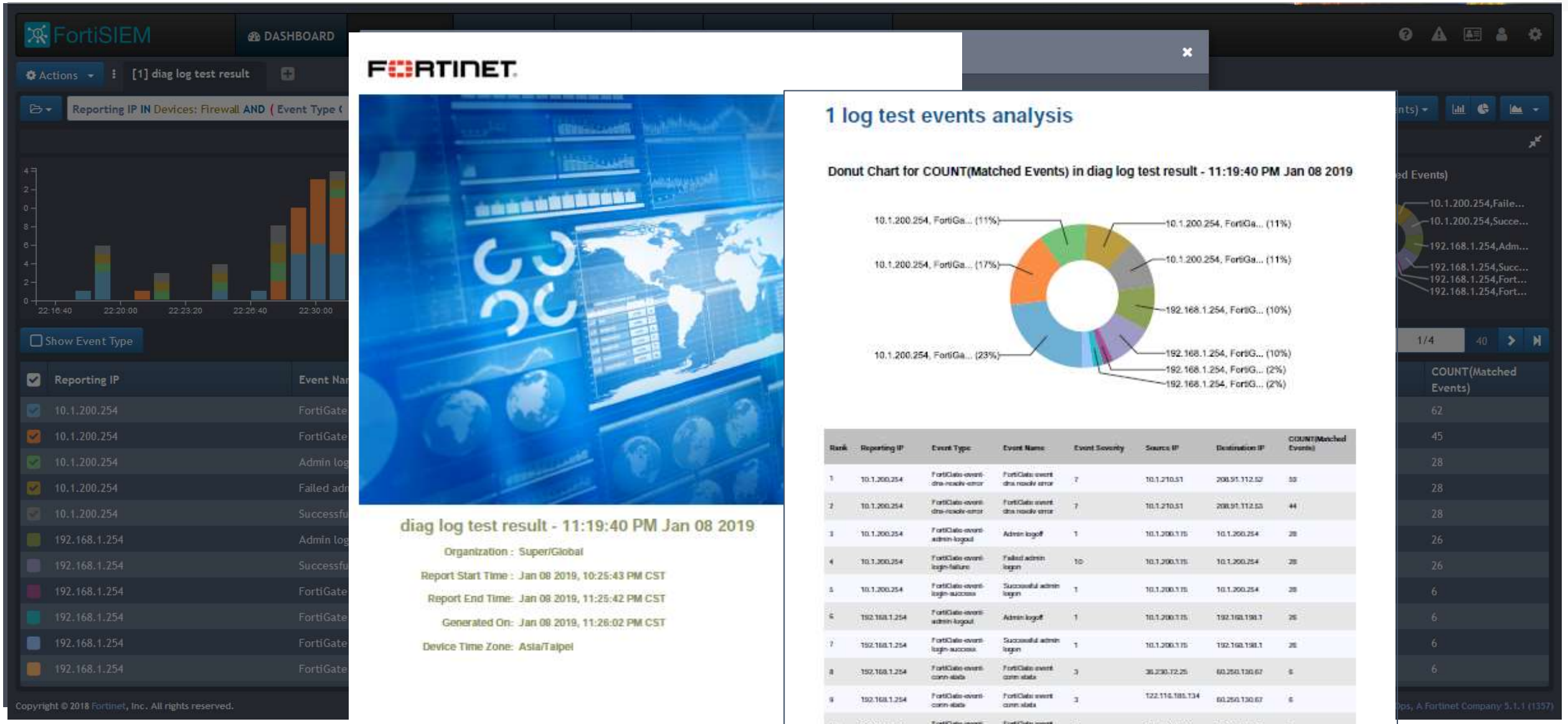
直覺式的事件關聯分析處理：
分析結果可輸出報表 (手動或排程)

NOC/SOC TODAY

Reporting IP	Event Name	Severity	Source IP	Destination IP	COUNT(Matched Events)
10.1.200.254	The URL belongs to an allowed category in the firewall policy	3	10.1.210.100	96.45.36.31	494
10.1.200.254	FortiGate event dns resolv error	7	10.1.210.51	208.91.112.53	56
10.1.200.254	FortiGate event dns resolv error	7	10.1.210.51	208.91.112.52	29
10.1.200.254	Admin logoff	1	10.1.200.175	10.1.200.254	26
10.1.200.254	Failed admin logon	10	10.1.200.175	10.1.200.254	26
10.1.200.254	Successful admin logon	1	10.1.200.175	10.1.200.254	26

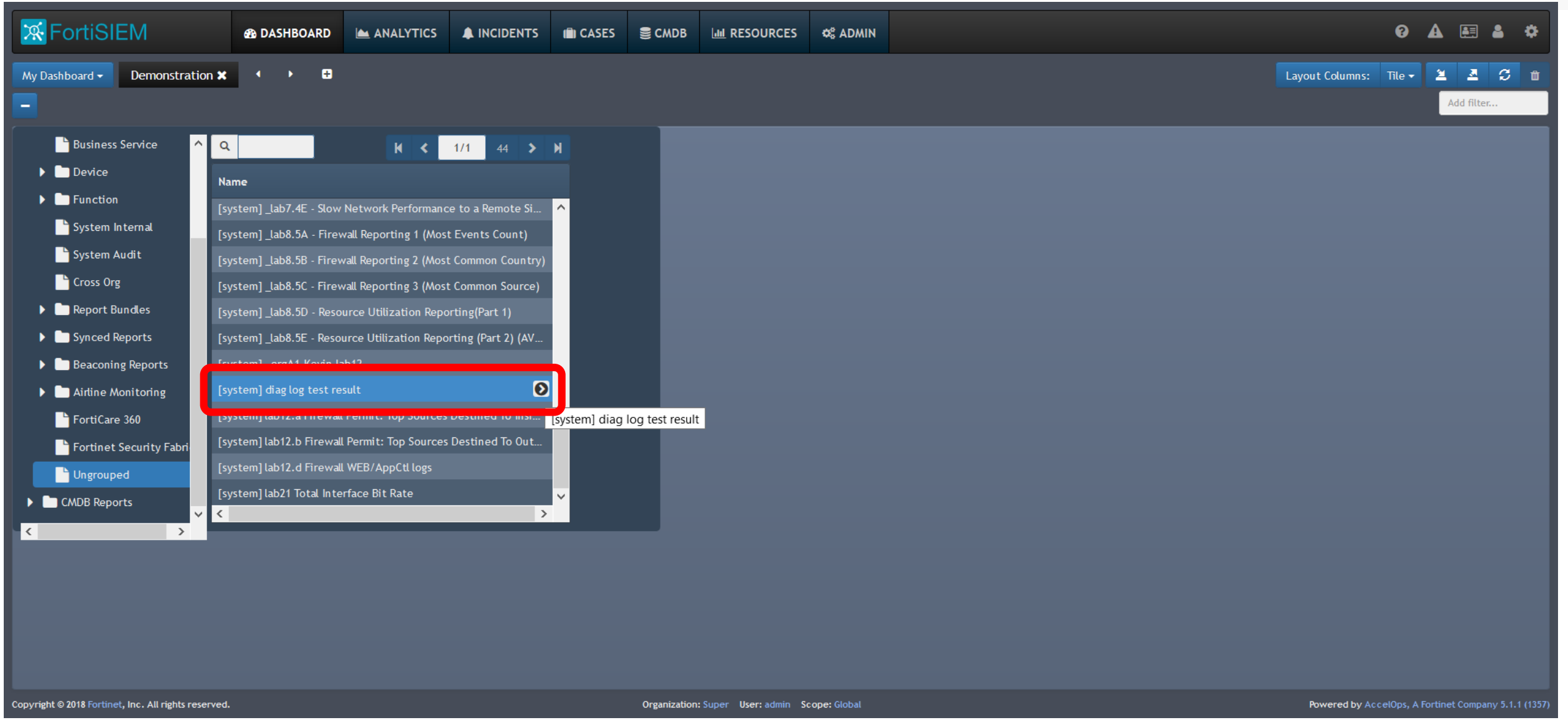
直覺式的事件關聯分析處理：
分析結果可輸出報表 (手動或排程)

NOC/SOC TODAY



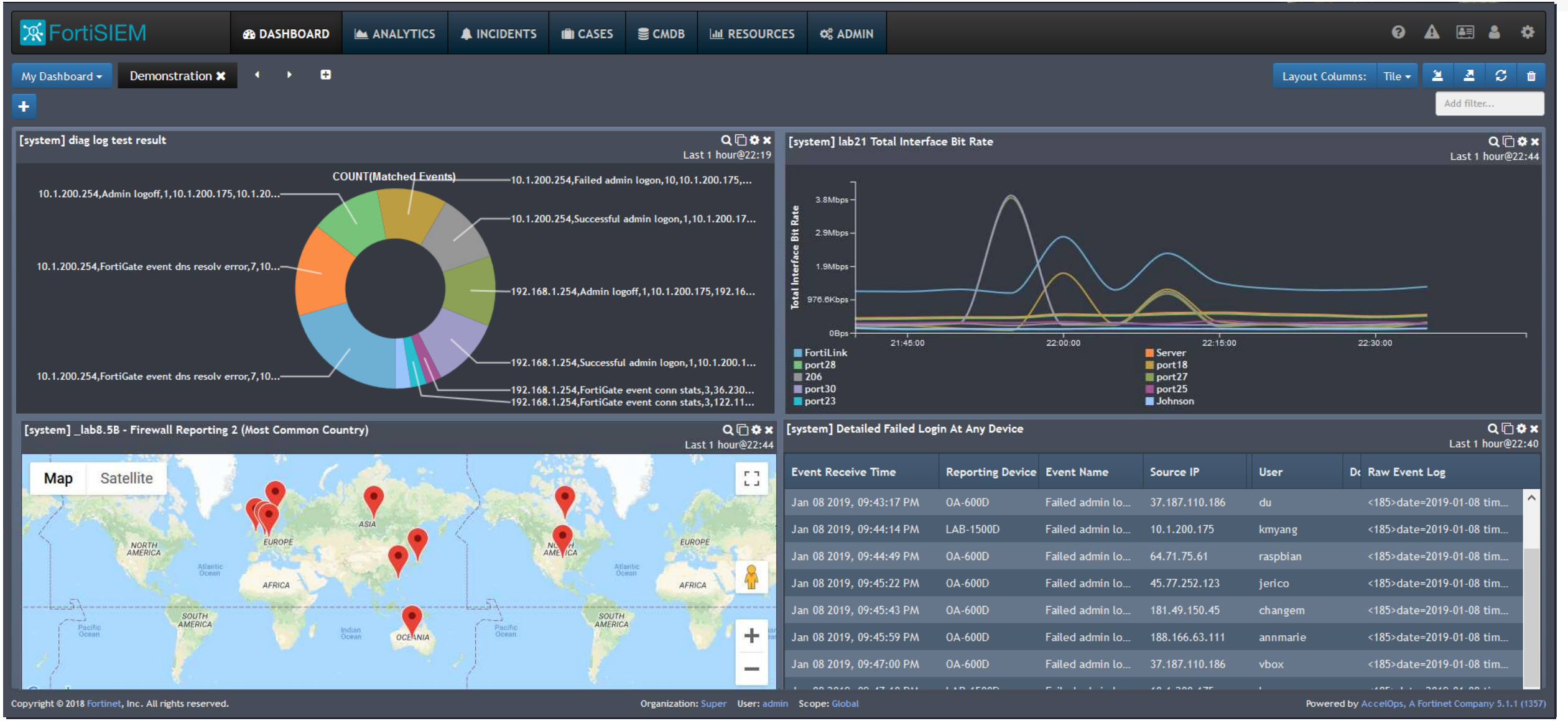
直覺式的事件關聯分析處理：
分析結果可轉成各式監看儀表板

NOC/SOC TODAY



直覺式的事件關聯分析處理：
分析結果可轉成各式監看儀表板

NOC/SOC TODAY

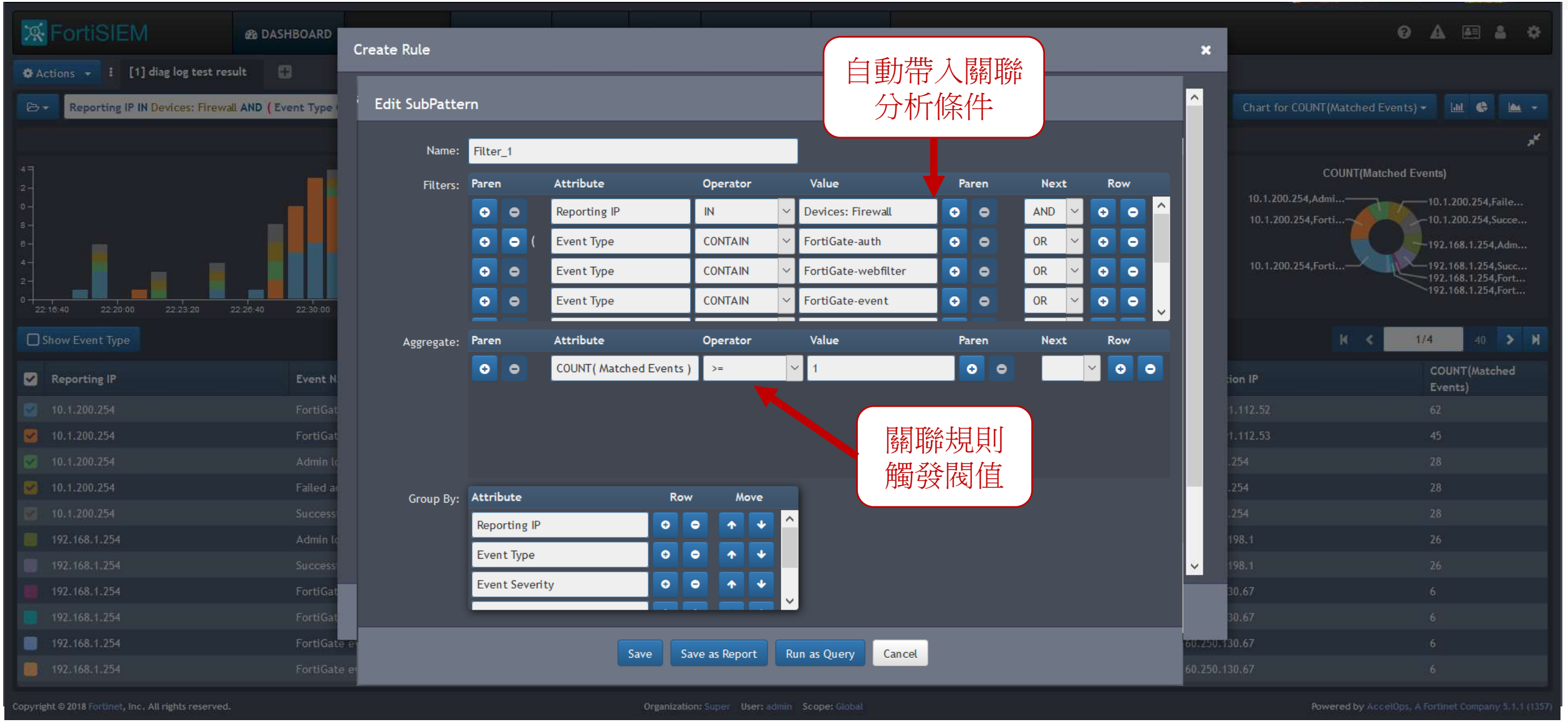


直覺式的事件關聯分析處理：
分析結果可產生規則，觸發事故告警

NOC/SOC TODAY

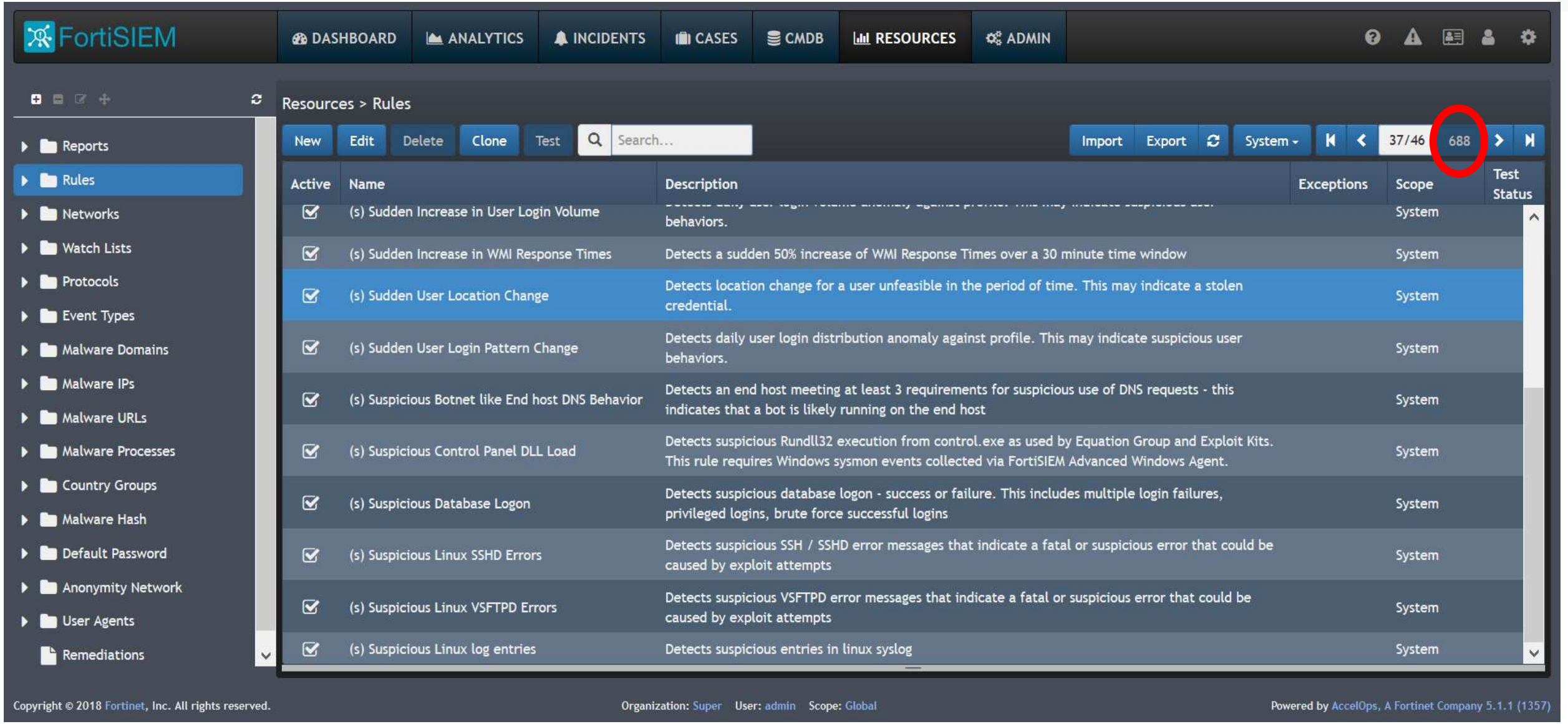
直覺式的事件關聯分析處理：
分析結果可產生規則，觸發事故告警

NOC/SOC TODAY



內建豐富的關聯規則與用戶終端行為分析 (UEBA)
以用戶登入模式異常為例 (Sudden User Login Pattern Change)

NOC/SOC TODAY



內建支援眾多廠牌設備

NOC/SOC TODAY

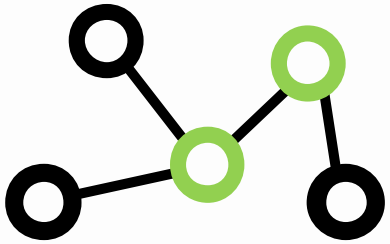
快速與彈性的整合

NOC/SOC TODAY

與外部威脅情資整合

- Malware Domain, IP, File hash, User Agent, URL
- Real-time/Historical query
- Out-of-the-box support

與報修派工系統和作業流程整合



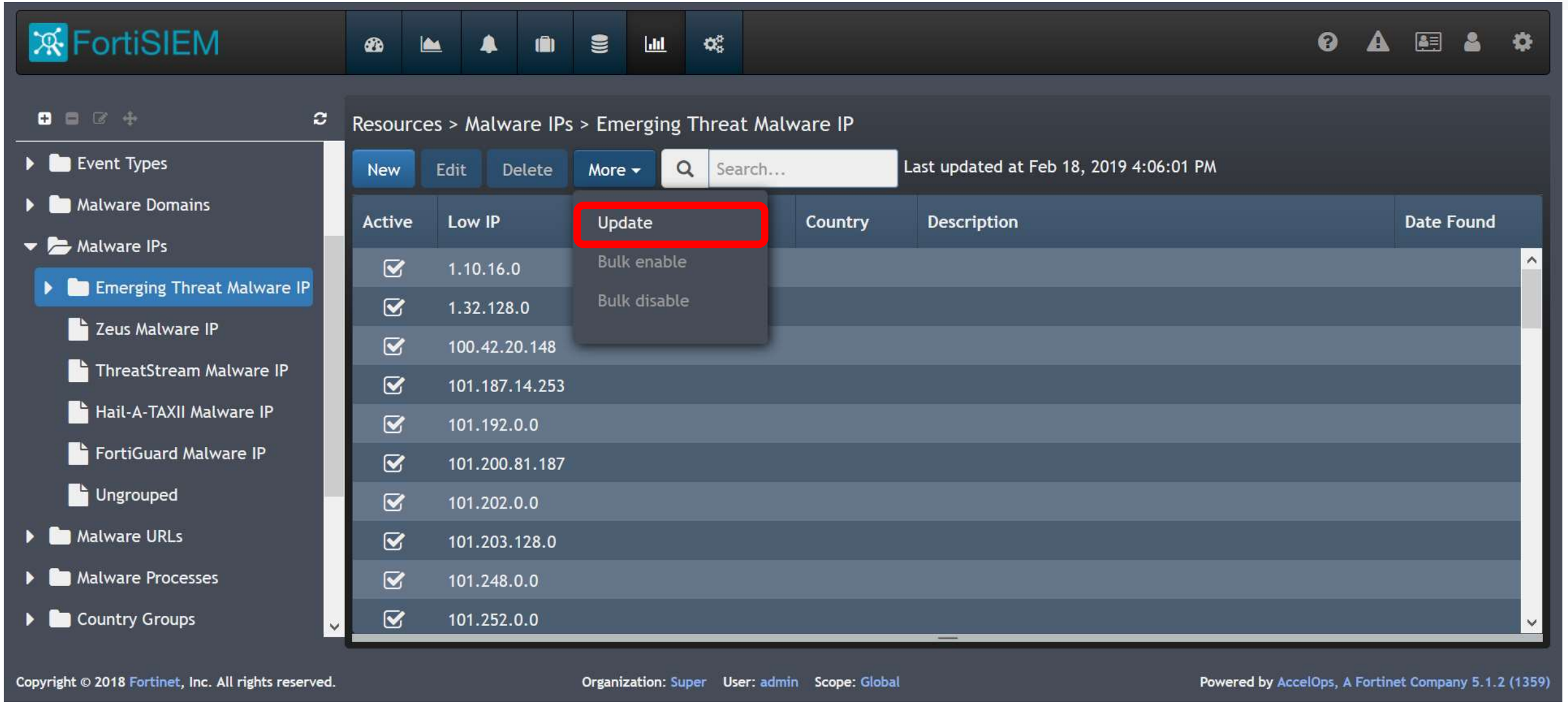
- Build-in or Integrate with External Ticket System
- 2-way integration
- API / GUI based integration

與雲端應用系統整合

- Okta – SSO
- Kafka – Big Data
- Box – Document sharing
- Salesforce – CRM Activity

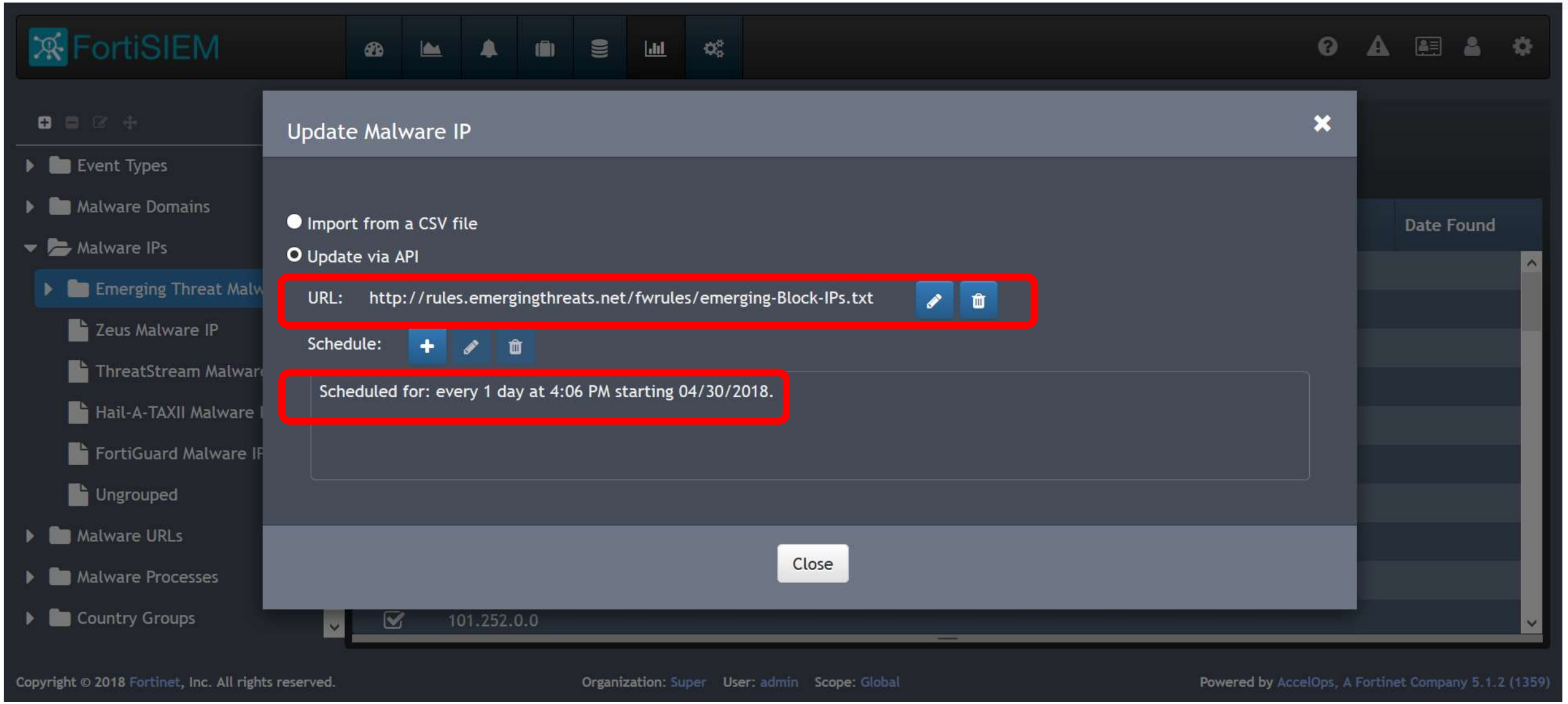
與外部威脅情資整合

NOC/SOC TODAY



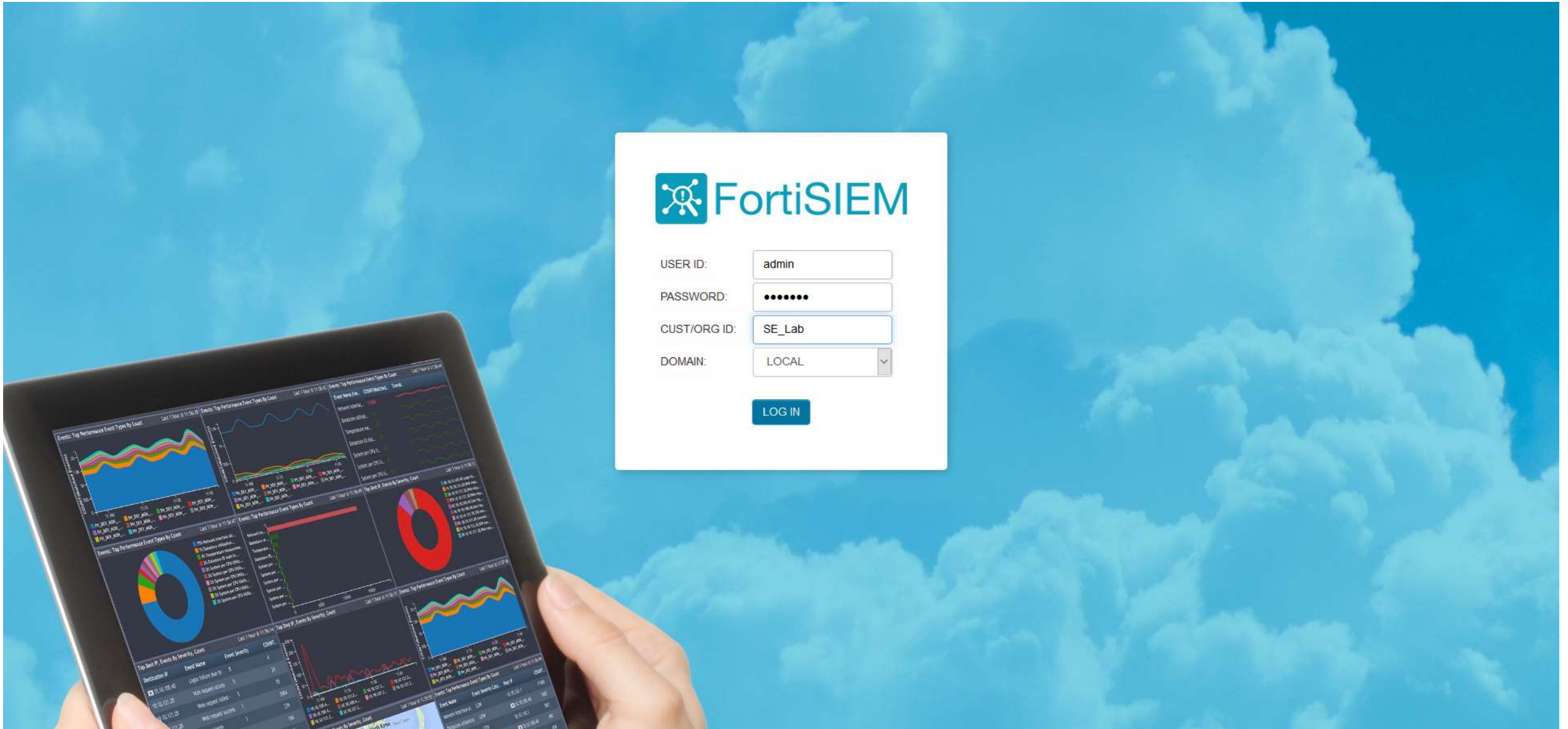
與外部威脅情資整合

NOC/SOC TODAY



即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例
登入系統

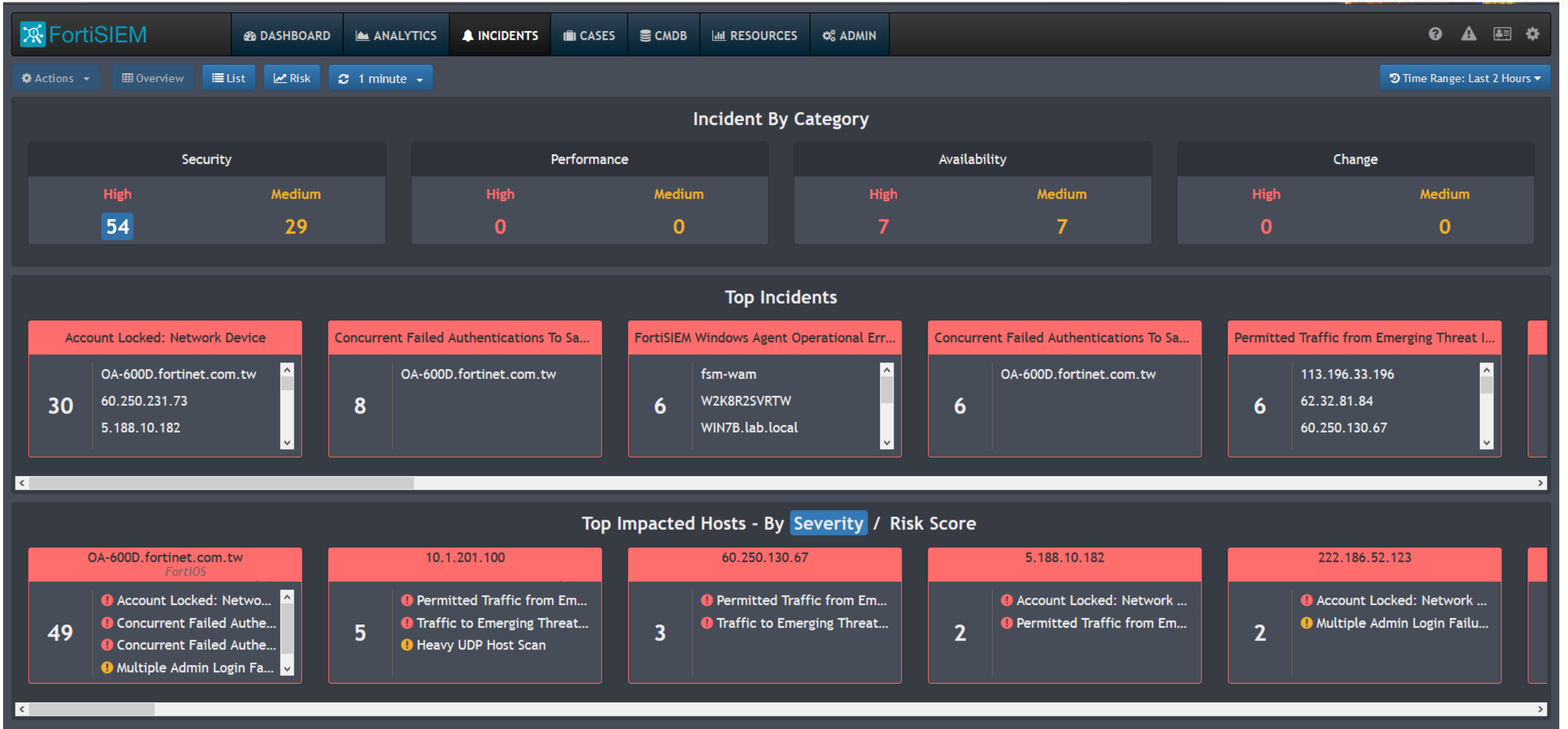
NOC/SOC TODAY



即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例

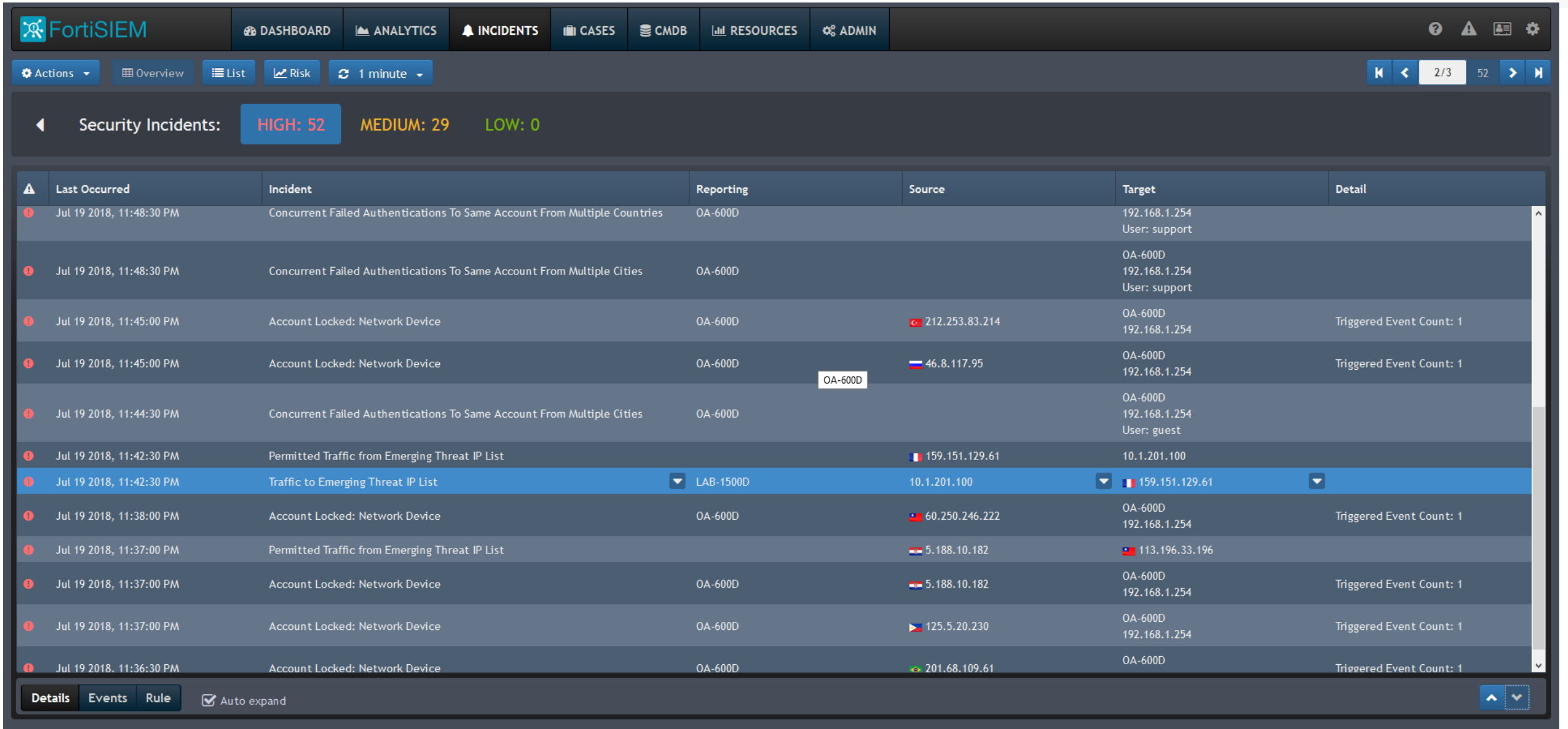
事故彙整儀表板 (Incidents Overview Dashboard)

NOC/SOC TODAY



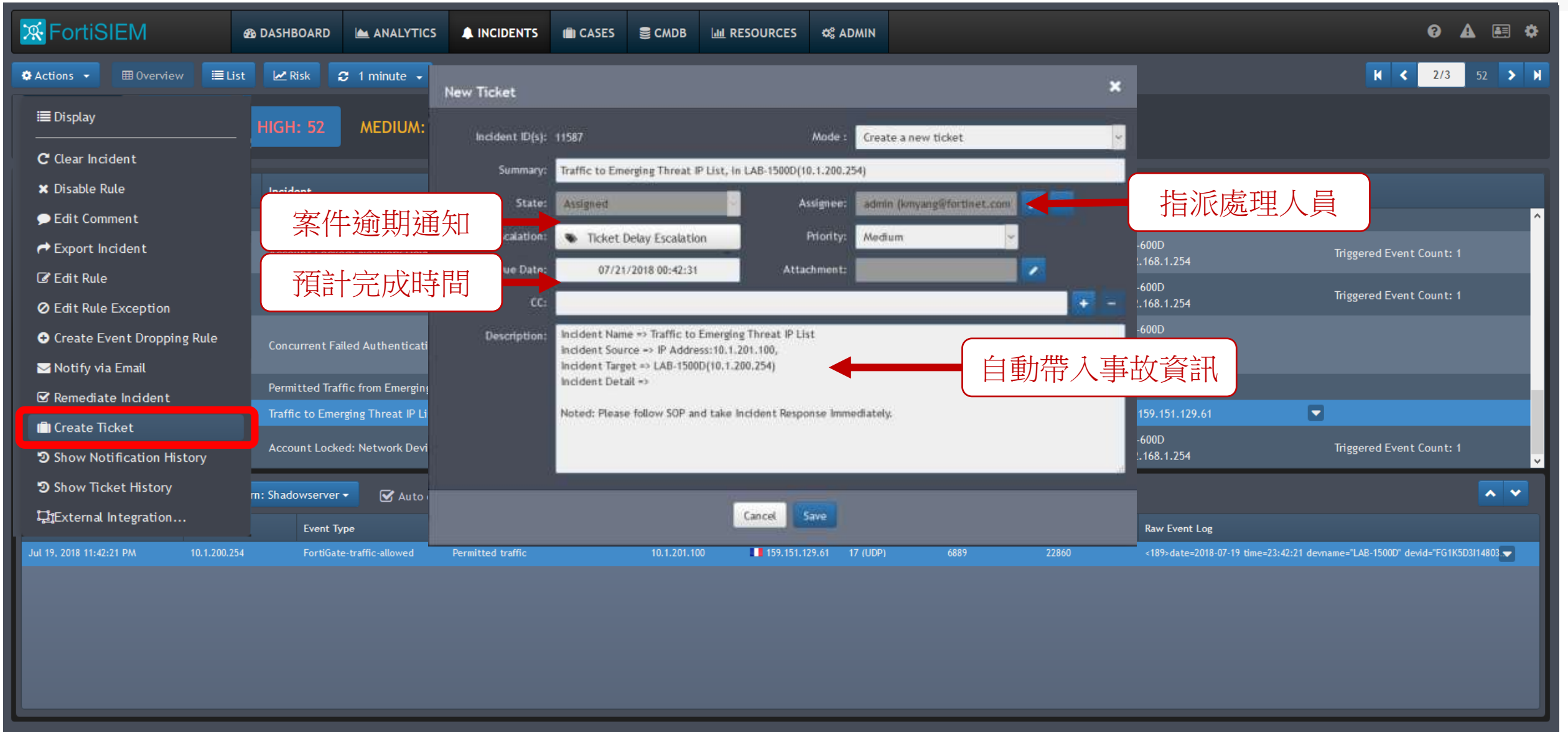
即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例
點擊進入查看事故詳情

NOC/SOC TODAY



即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例
可開事故處理單進行處理

NOC/SOC TODAY



即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例
系統內建派工處理系統，可追蹤事故處理進度

NOC/SOC TODAY

FortiSIEM | DASHBOARD | ANALYTICS | INCIDENTS | CASES | CMDB | RESOURCES | ADMIN

New | Edit | Add filter... | Time Range *LAST* 30 Days | Export

Elapsed	State	Priority	Ticket ID	Summary	Assignee	Creator	Creation Date
Overdue	Assigned	Medium	4780051	Permitted Traffic from Emerging Threat IP List, in (1...	admin	admin <kmyang@fortinet.com>	Jul 11 2018, 08:20:58 PM
54 %	Assigned	High	4780052	Permitted Traffic from Emerging Threat IP List,destI...	admin	admin <kmyang@fortinet.com>	Jul 19 2018, 11:26:52 AM
0 %	Assigned	Medium	6156150	Traffic to Emerging Threat IP List, in LAB-1500D(10.1...	admin	admin <kmyang@fortinet.com>	Jul 20 2018, 12:46:12 AM

Detail

Incident ID: 11587
Organization: SE_Lab
Due Date: Jul 21 2018, 12:42:31 AM
Escalation Policy: Ticket Delay Escalation
CC:
Attachment:

Action History

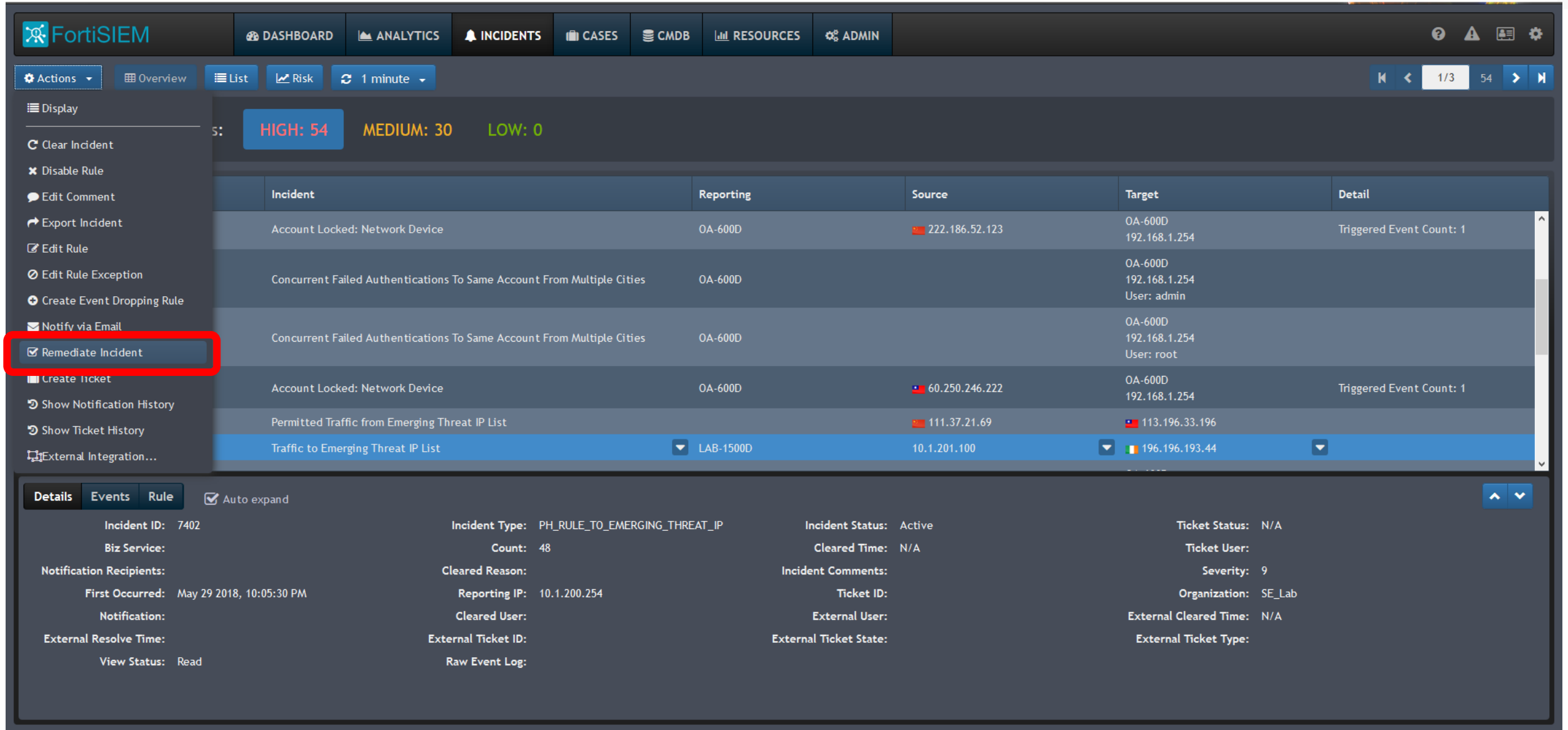
SE_Lab/admin Jul 20 2018, 12:46:12 AM

Add notes: Incident Name => Traffic to Emerging Threat IP List
Incident Source => IP Address:10.1.201.100,
Incident Target => LAB-1500D(10.1.200.254)
Incident Detail =>

Noted: Please follow SOP and take Incident Response Immediately.

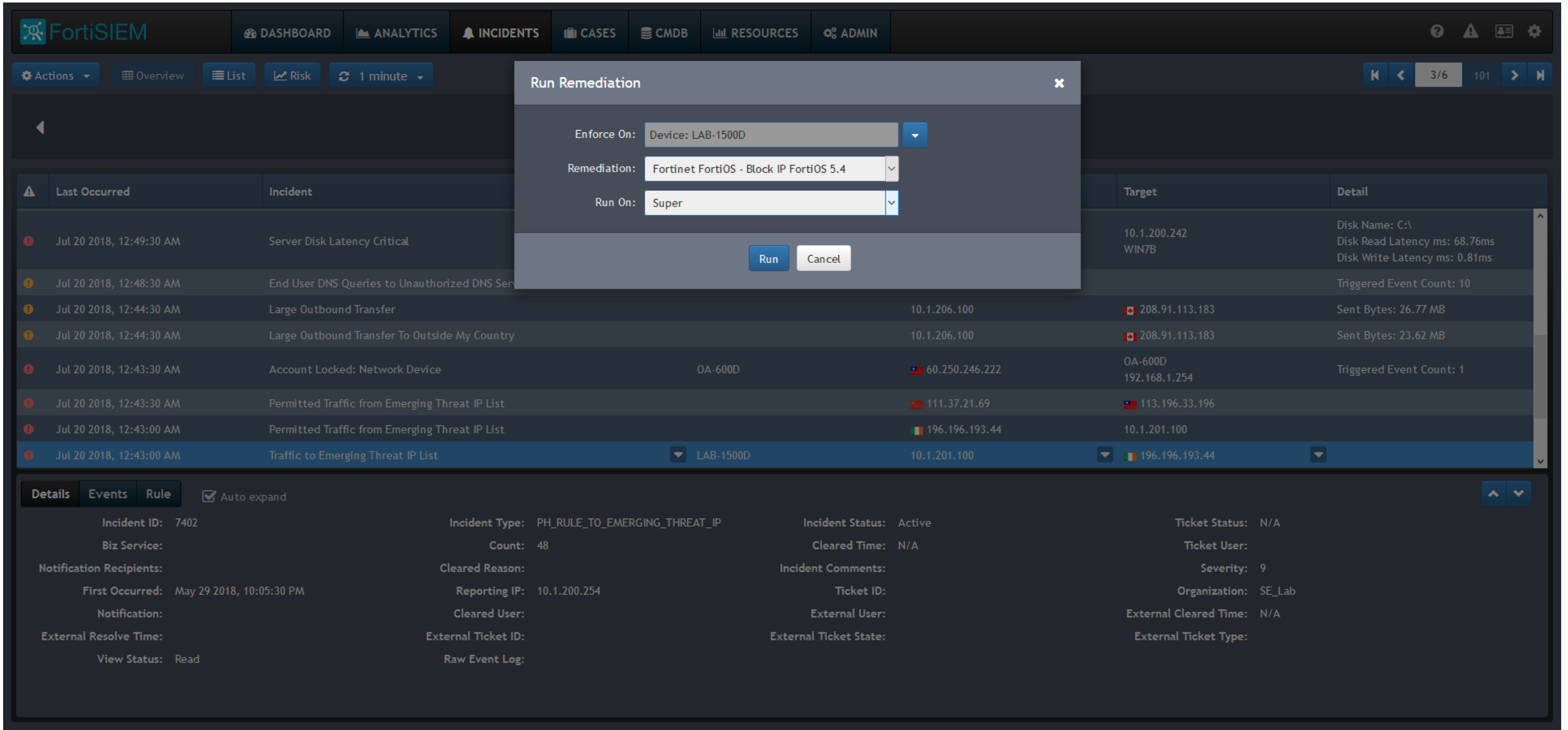
即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例
被指派人員可迅速反應處理

NOC/SOC TODAY

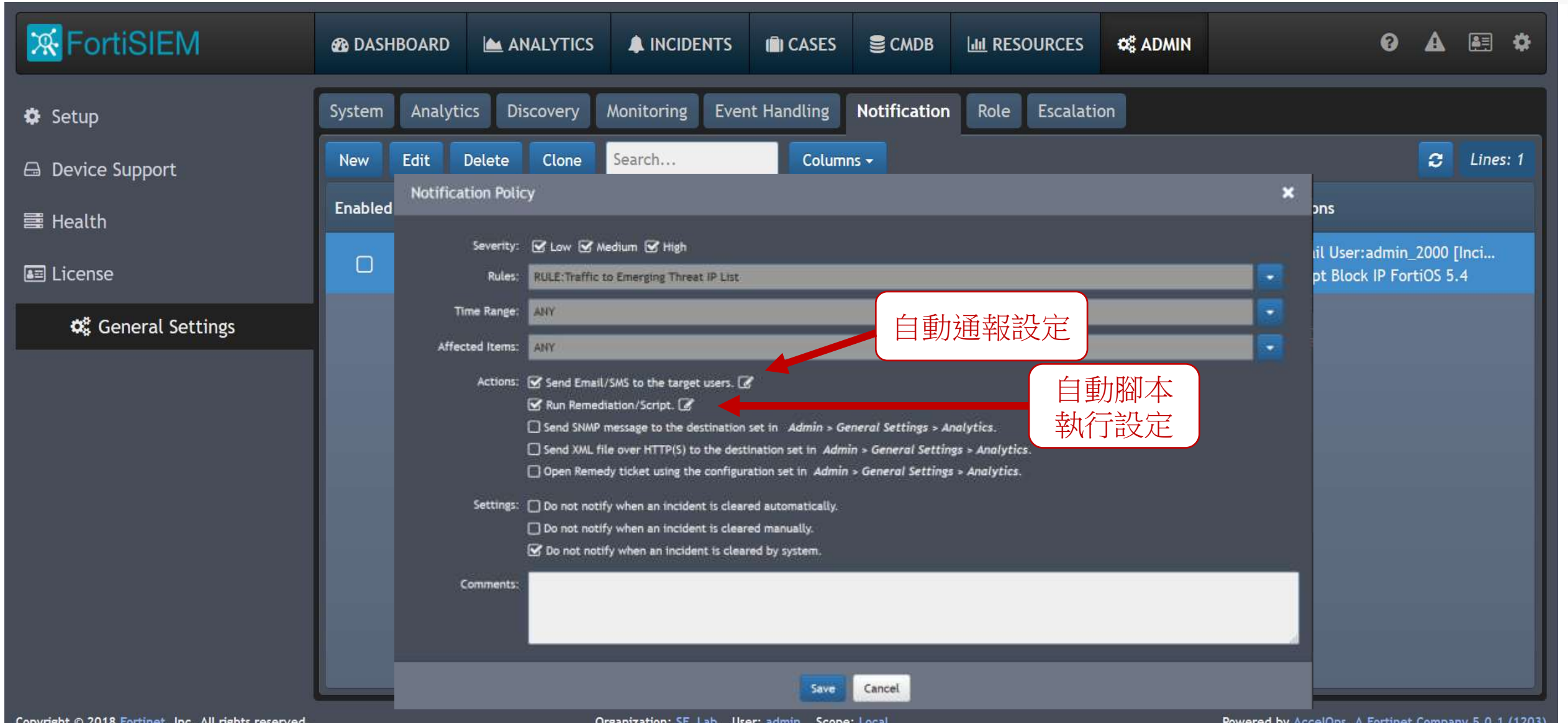


即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例
被指派人員可迅速反應處理

NOC/SOC TODAY



即時事故反應與處理：以內網連線外部高風險 IP 地址告警為例
自動通報與設備自動聯防處理流程



新世代 SIEM 重點整理

NOC/SOC TODAY

1. 資安(SOC)與網維(NOC)融合式分析
2. 設備資產、配置與效能管理(CMDB)
3. 可快速擴容的高彈性架構
4. 直覺式事件分析簡單易用
5. 支持多租戶管理環境
6. 整合眾多設備與既有環境

7. 單一的統合性介面管理平台


FORTINET