FORTINET

資安防禦的基本功 - 如何透過 AI 強化戰力

Teddy Chuang

FORTINET 業務副總

資安/網路 維運中心

- **FortiAnalyzer** — Central Log & report
- **FortiNAC** — IoT Access Control
- **FortiSandbox** — File Analysis
- **FortiAI** — Virtual Security Analyst ™
- **FortiSIEM** — SIEM / UEBA
- **FortiXDR** — XDR
- **FortiManager** — Central Device Mgmt.
- **FortiAuthenticator** — User Access Mgmt.
- **FortiTester** — Network Tester
- **FortiDeceptor** — Honeypot
- **FortiSOAR** — SOAR
- **FortiPAM** — PAM

雲端服務 / 雲端託管

Cloud mgmt.

FortiGate Cloud | FortiLAN Cloud | FortiExtender Cloud | FortiManager Cloud | FortiAnalyzer Cloud | FortiClient EMS Cloud | FortiToken Cloud | FortiSOAR Cloud

Cloud services

FortiPresence | FortiMail Cloud | FortiPhish | FortiGSLB | FortiConverter | Fortinet SOCaaS | FortiSASE | FortiPenTest | FortiWeb Cloud | FortiSandbox Cloud | FortiVoice Cloud | FortiMonitor

終端行動用戶

- **FortiToken** — 2 Factor OTP Token
- **FortiClient / FortiEDR** — VPN, ZTNA, EPP, and SASE Client

SaaS

- **FortiCASB**
- **FortiCWP**

- Secure SD-WAN
- IPsec / SSL VPN
- SASE

- **FortiGate** — Security Gateway
- ZTNA

- **FortiDDoS** — L7 D/DOS Mitigator
- **FortiADC** — Load Balancer
- **FortiMail** — Mail Sec. Gateway
- **FortiWeb** — Web App. Firewall
- **FortiIsolator** — Browser Isolation
- **FortiProxy** — Secure Web Gateway

外點/分公司

- **FortiWiFi** — Secure WiFi Access
- **FortiExtender** — 3G/4G/5G WAN

區域內網

- **FortiSwitch** — Switch
- **FortiAP** — Wireless Access Point
- **FortiRecorder** — Surveillance Manager
- **FortiVoice** — IP PBX
- **FortiCamera**
- **FortiFone**

資料中心

業界最完整且全面的資安佈局

AI、5G普及 資安攻擊急速加劇

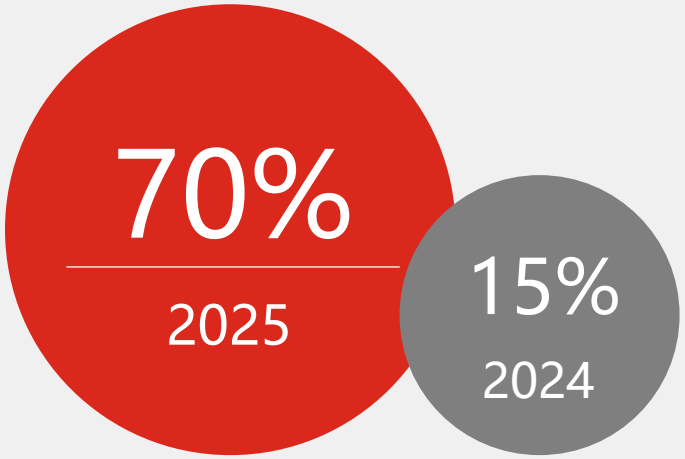
【資安週報】0303~0307，彰基醫院遭勒索軟體CrazyHunter攻擊，預期可能出現系統化攻擊狀況，全臺關鍵CI醫院拉警報

二二八年假後3月初的資安新聞中，彰化基督教醫院也和不久前的馬偕醫院，一樣遭遇CrazyHunter這支勒索軟體攻擊，引發全國關注，衛生福利部指出這已是系統性攻擊情形；在網路威脅態勢方面，我們最新一期封面故事解析網路威脅態勢日益複雜的現況，並從資安經濟學與AI資安角度，幫助大家展望2025年網路安全態勢

全方位整合與自動化網路資安領導廠商 Fortinet®（NASDAQ：FTNT）旗下FortiGuard Labs威脅情資中心今（14）日公布 《2024 全球資安威脅預測》報告顯示，透過「網路犯罪即服務（Cybercrime-as-a-Service，CaaS）」的攻擊案例增加，加上生成式人工智慧的出現，威脅者比過往任何時候都更容易發動攻擊。同時，攻擊者各自仰賴的工具不斷演進，更一再提升攻擊行動的複雜性，目前已經可以發動更具針對性且更隱匿的攻擊，並且有能力規避一些強大的安全防護，其攻擊週期中每個戰術循環也變得更加靈活。

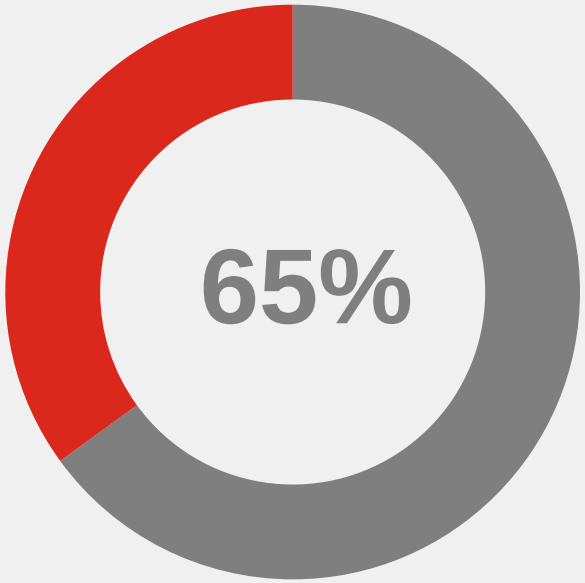
網路維運的變革已經展開了 …

Gartner: 生成式 AI 在提高營運效率和競爭優勢方面發揮變革性力量



供應商 (Vendors)

- 網路供應商透過生成式 AI，與機器人對話互動，來增強網路運營能力
- 根據 Gartner 數據，使用新一代 AI 工具的供應商將從今年的 15% 增加到明年的 70%



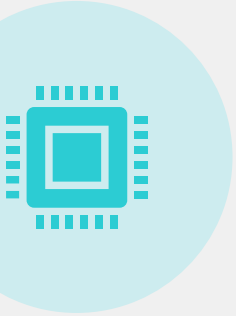
管理者 (Customers)

- 設定配置和故障排除等維運作業仍然有 65% 透過人工手動執行，這凸顯了透過 GenAI 實現自動化來提升效率的龐大契機。

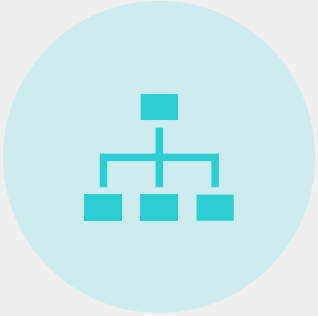
© Fortinet Inc. All Rights Reserved.

GenAI 的 iPhone 時刻已經來臨，將成為網路維運的基石

Gartner: 生成式 AI 的目標，提高營運效率，提升 IT 團隊技能水平，並改善用戶體驗



到 2025 年時，**20%** 的**初始設定配置將使用 GenAI 協助**，而在 2023 年時，這個比例趨近於 0%。



到 2026 年時，**60%** 的網路營運人員將**依賴 GenAI 進行持續性網維管理**，而在 2024 年初時，這個比例還不到 5%。

GenAI 可以減少多達 **25%** 的**故障排除時間、安裝時間和到場檢視時間。**

網路效能和可用性的改進可以將最終用戶的工作效率提高達 **25%**。

© Fortinet Inc. All Rights Reserved.

FortiAI 能為我們做些甚麼?

提升洞察力

建構整個維運環境的知識庫，從網路、用戶、傳輸數據的應用以及資安態勢

協助決策制定

依據洞察後狀態推薦管理者接續的行動制定，以上是基於維運環境的分析並執行最佳實踐執行

自動化腳本執行

通過管理者同意後的自動化腳本來執行決策後的推薦行動

© Fortinet Inc. All Rights Reserved.

網路營運大趨勢

網路營運中心
自動化流程處理

網路供應商的領導者正被要求提供安全的網路並實現自動化，以支持組織的數位轉型。

Gartner Hype Cycle for Enterprise Networking, 2022

應用服務
識別管控

到 2026 年，至少 **60%** 的領導者將使用 DEM (數位化體驗管理) 從用戶的角度來評估應用服務和終端性能，而 2021 年這個比例不足 20%。

Gartner, Market Guide for Digital Experience Monitoring, 28 March 2022

AIOps
人工智能導入

IDC 預測，到 2027 年，AI 驅動的自動化將可確保數位基礎設施配置、性能、成本和安全的一致性，透過減少 **70%** 的人為操作來提高服務水平目標。

© Fortinet Inc. All Rights Reserved.

人工智能帶給我們怎樣的幫助?

網路營運中的人工智能與機器學習 (AI / ML)

記錄分析

機器學習建立
營運基準線

狀態監控

發現網路異常態勢
與問題癥結點

危機預警

關聯性分析，識別問題
確定根本原因 (RCA)

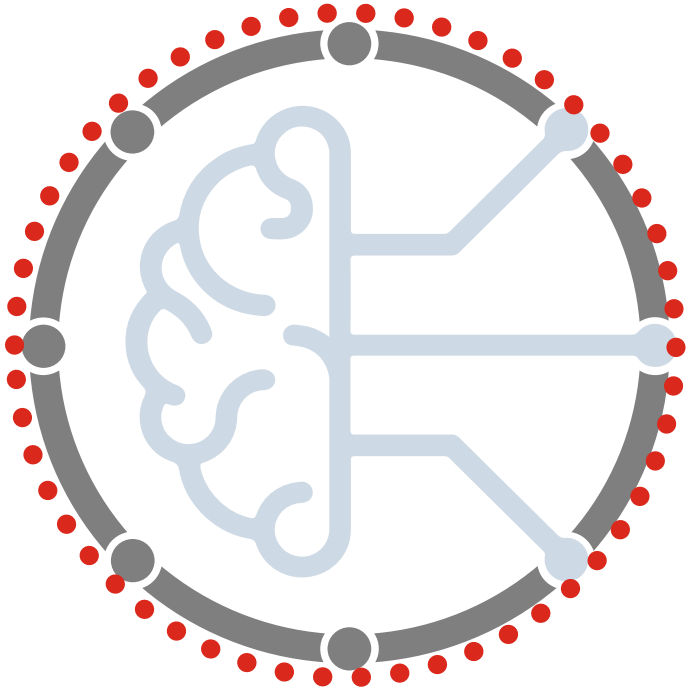
提供對策

AI 提供專業建議
快速解決問題

© Fortinet Inc. All Rights Reserved.

FortiAIOps 概觀

AI / 機器學習在安全織網的應用



Workflow
Dashboard / GUI

Incident API

Stats API

FortiOS

FortiExtender

FortiAP

SD-WAN

FortiSwitch

FortiAIOps 是一種人工智能與機器學習 (AI / ML) 解決方案，提升可視性、識別異常行為、發現問題根本原因，執行網路營運中心 (NOC) 優化。

© Fortinet Inc. All Rights Reserved.

FortiAIOps 效益

AIOps

+

Ops Team

輕鬆的分析各個網路節點資料
建立網路流量基準線
提供最佳的改善方案

- 減輕網路技術的依賴
- 快速找到問題癥結點
- 減少復原所需時間
- 增進網路與應用服務可靠度
- 提升使用者體驗

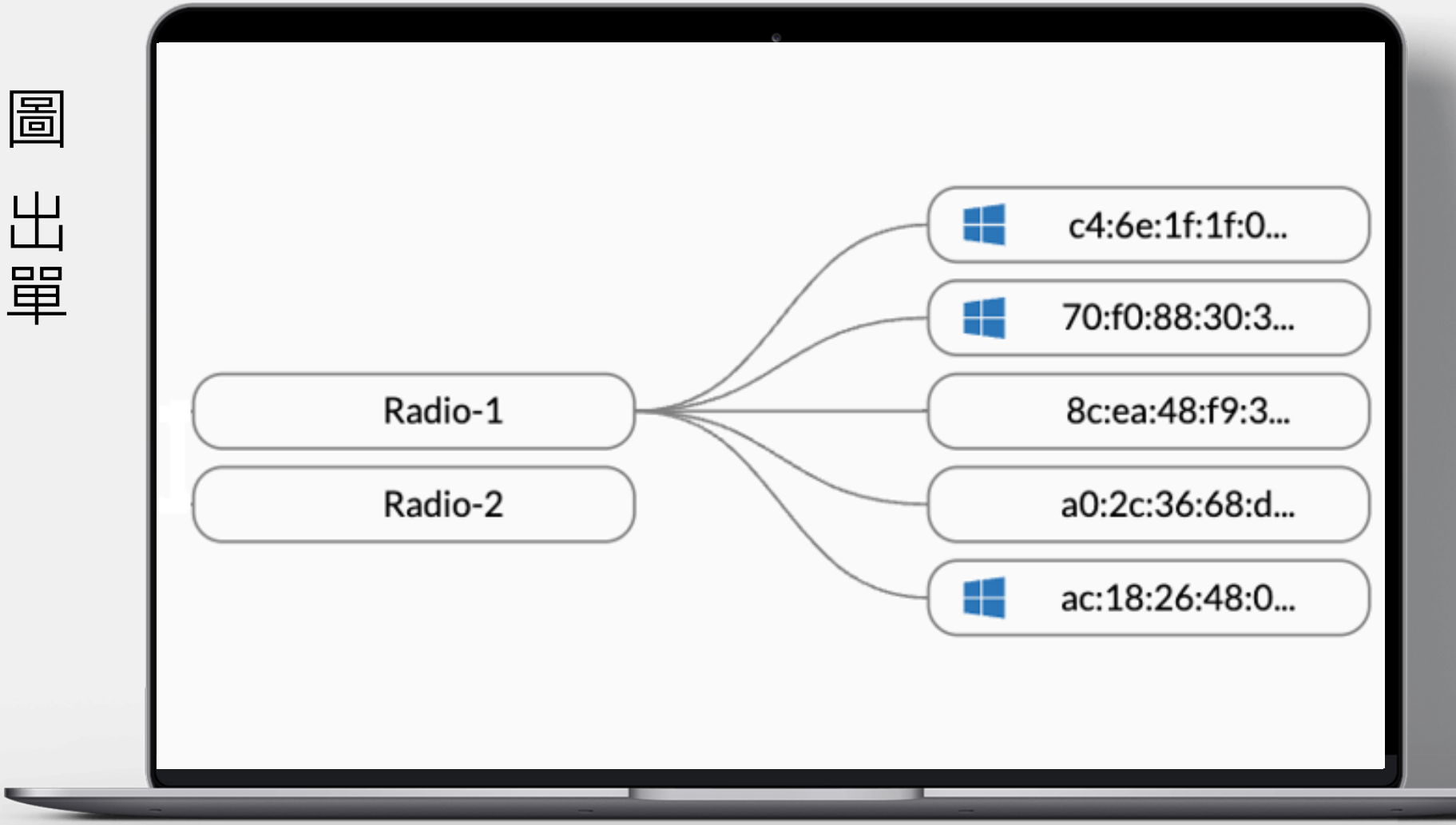
© Fortinet Inc. All Rights Reserved.

直覺化的操作介面

CONFIDENTIAL
Access Limited to Authorized Personnel

FortiAIOps

- 簡單易懂的拓譜圖
- 依據無線頻段列出無線網路用戶清單



© Fortinet Inc. All Rights Reserved.

FortiAIOps

無線訊號統計資料

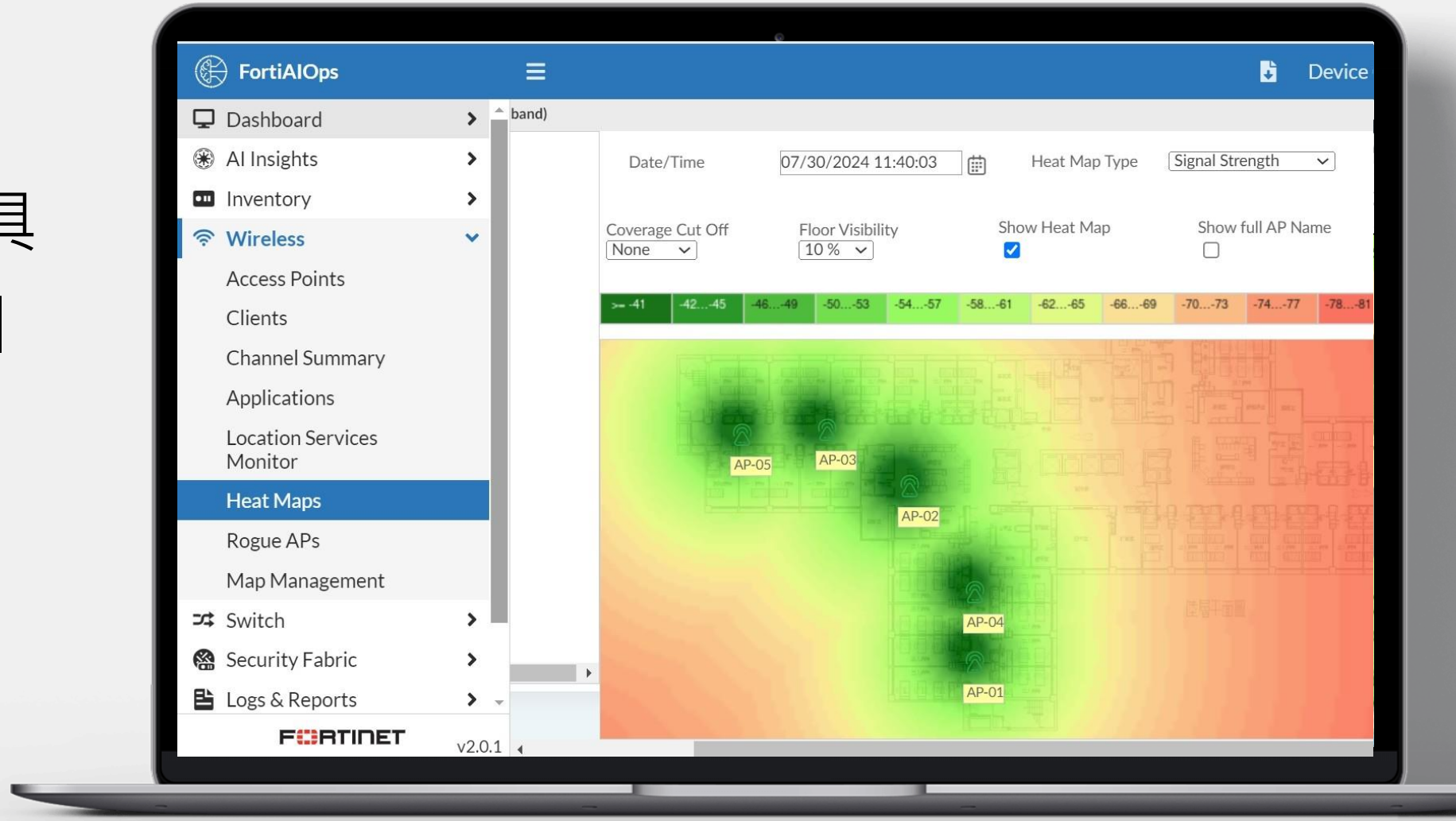
- 無線趨勢分析
  - 頻道使用率
  - 雜訊程度
  - 流量統計
- 整體無線網路頻道使用率
- 單一 AP 深入分析

© Fortinet Inc. All Rights Reserved.

FortiAIOps

Map Management – RF Planner

- 無線網路 Site-Survey 工具
- 無線網路熱感圖

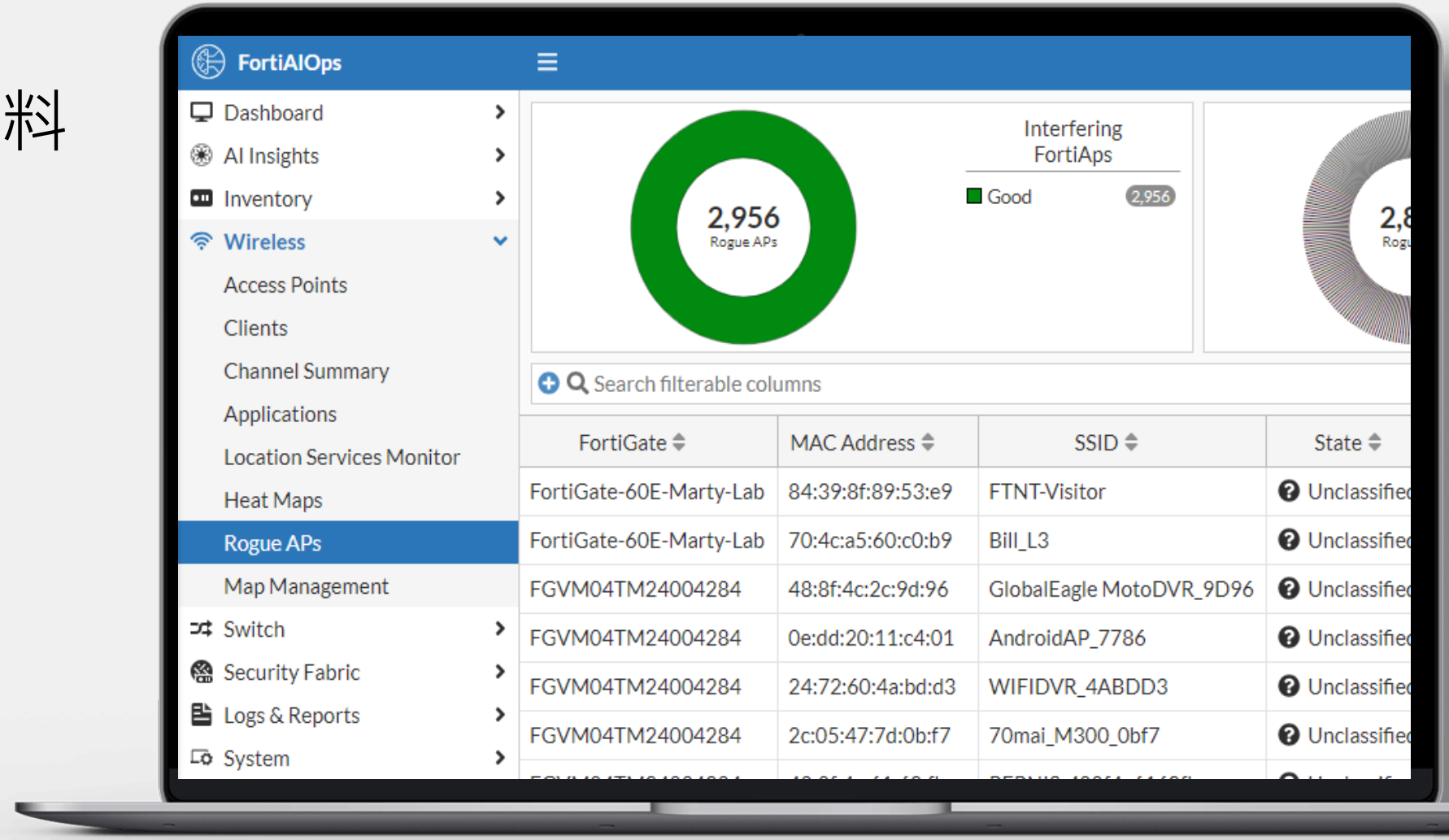


© Fortinet Inc. All Rights Reserved.

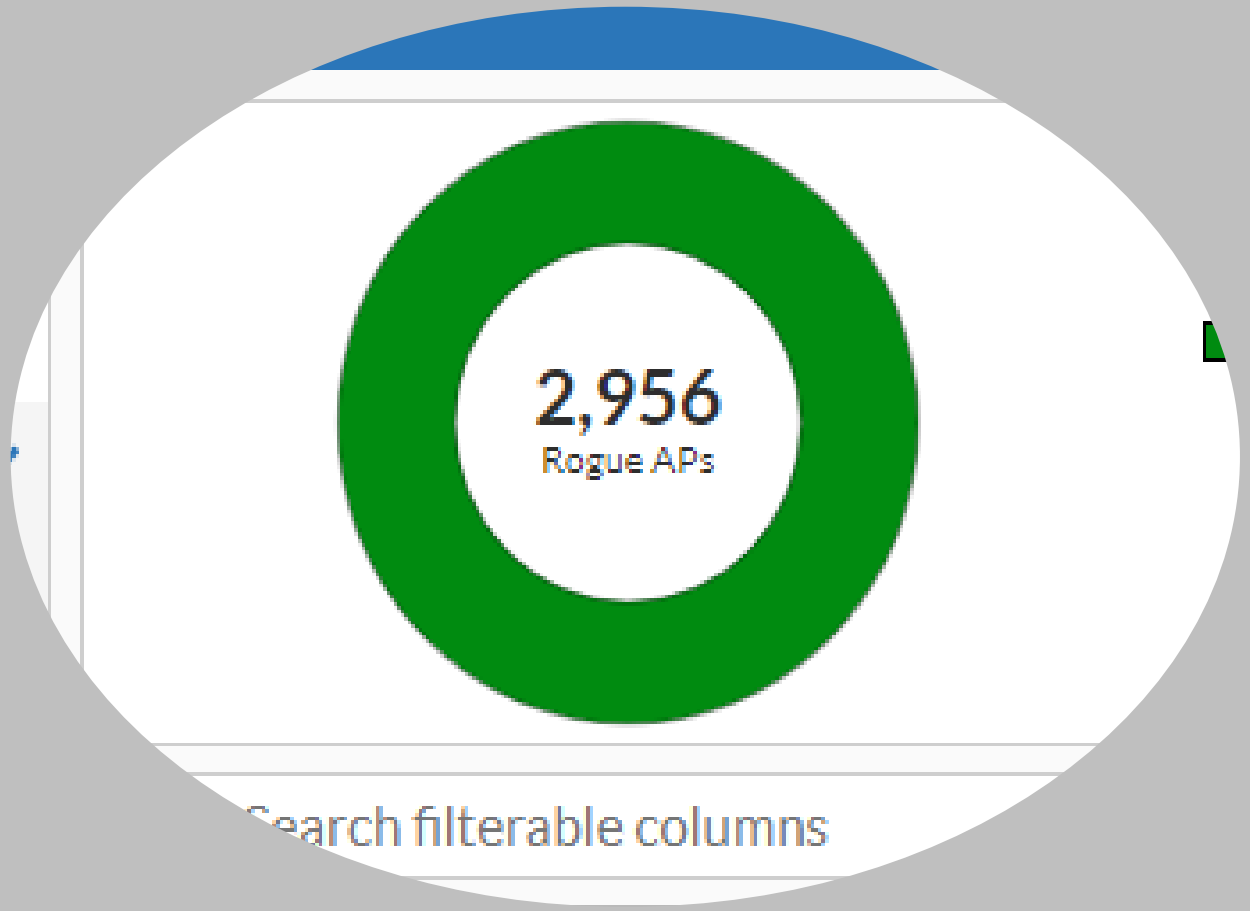
FortiAIOps

Monitoring – Rouge APs

- 干擾 AP 統計資料



© Fortinet Inc. All Rights Reserved.



附近干擾 AP 高達 2900 多個

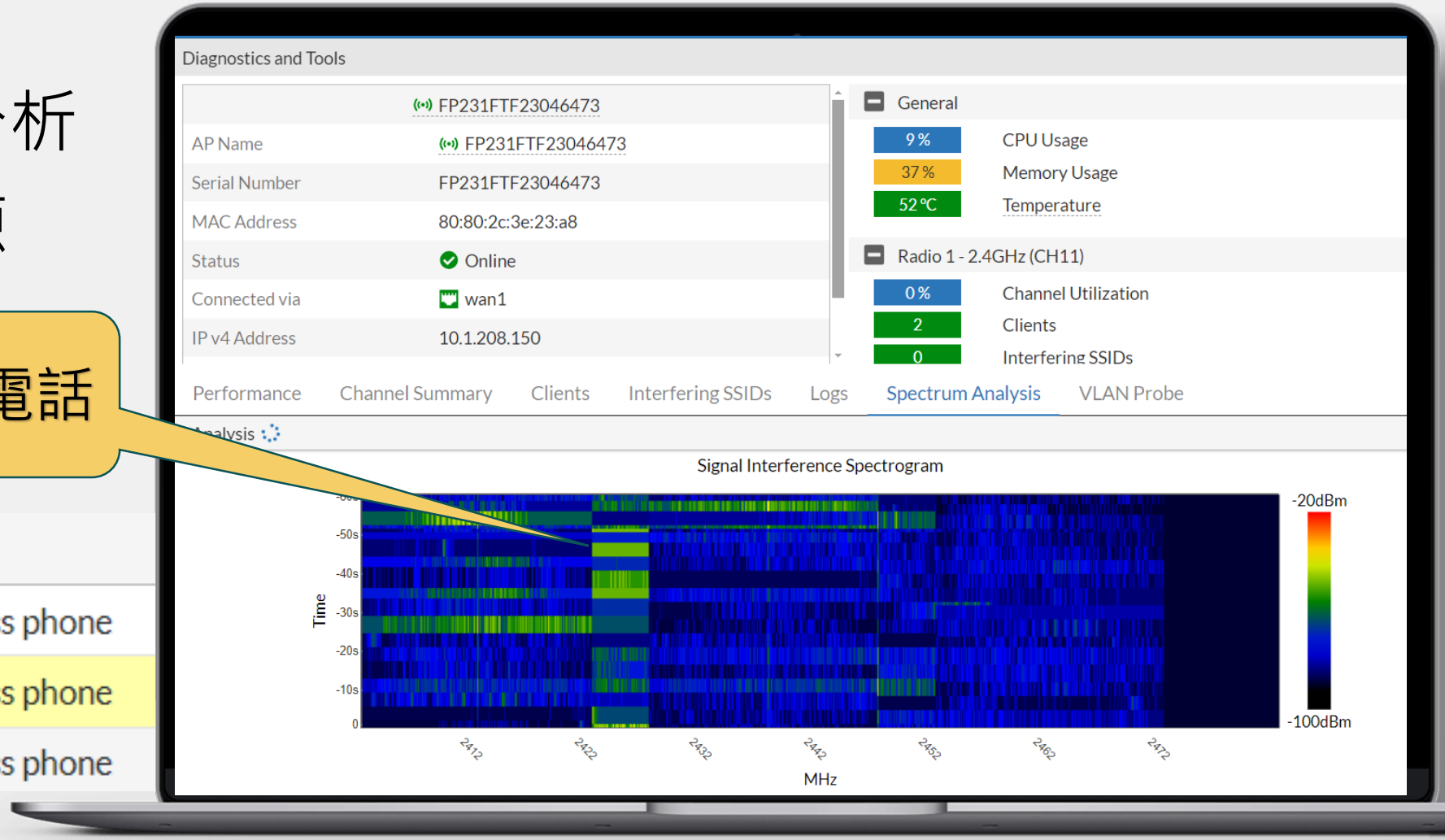
FortiAIOps

Monitoring – Spectrum Analysis

- 無線網路頻譜分析
- 一眼找出干擾源

2.4GHz 家用無線電話

Frequency	Type
2402	WiFi, DSSS cordless phone
2427	WiFi, DSSS cordless phone
2452	WiFi, DSSS cordless phone



© Fortinet Inc. All Rights Reserved.

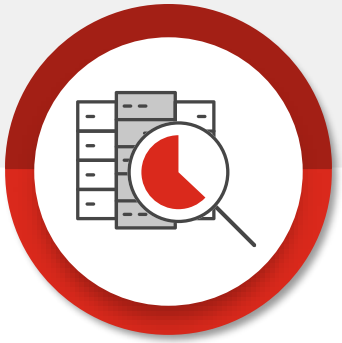
AI / 機器學習

CONFIDENTIAL
Access Limited to Authorized Personnel

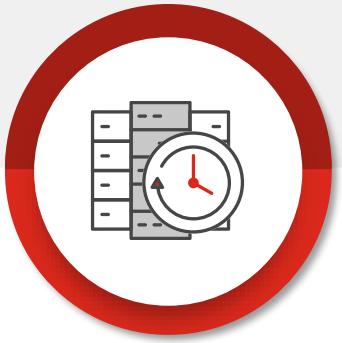
FortiAIOps

AI / 機器學習基準線的建立

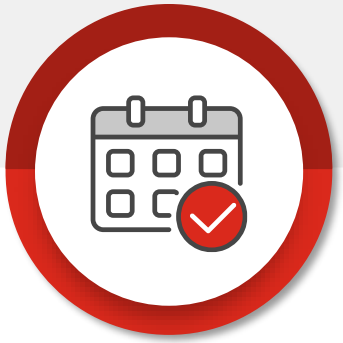
自動收集
FortiGate
FortiSwitch
FortiAP
SD-WAN
使用資訊



收集資料，以七天為基礎，建立各項基準線



比對目前資料與過去七天歷史資料差異處



透過 AI 運算找出受影響的設備與受影響的應用服務

AI 提供專業的建議快速解決問題

© Fortinet Inc. All Rights Reserved.

如何利用 AI 解決問題

Emma：今天無線網路很慢耶!

您好，這裡是控八控控–控控控

© Fortinet Inc. All Rights Reserved.

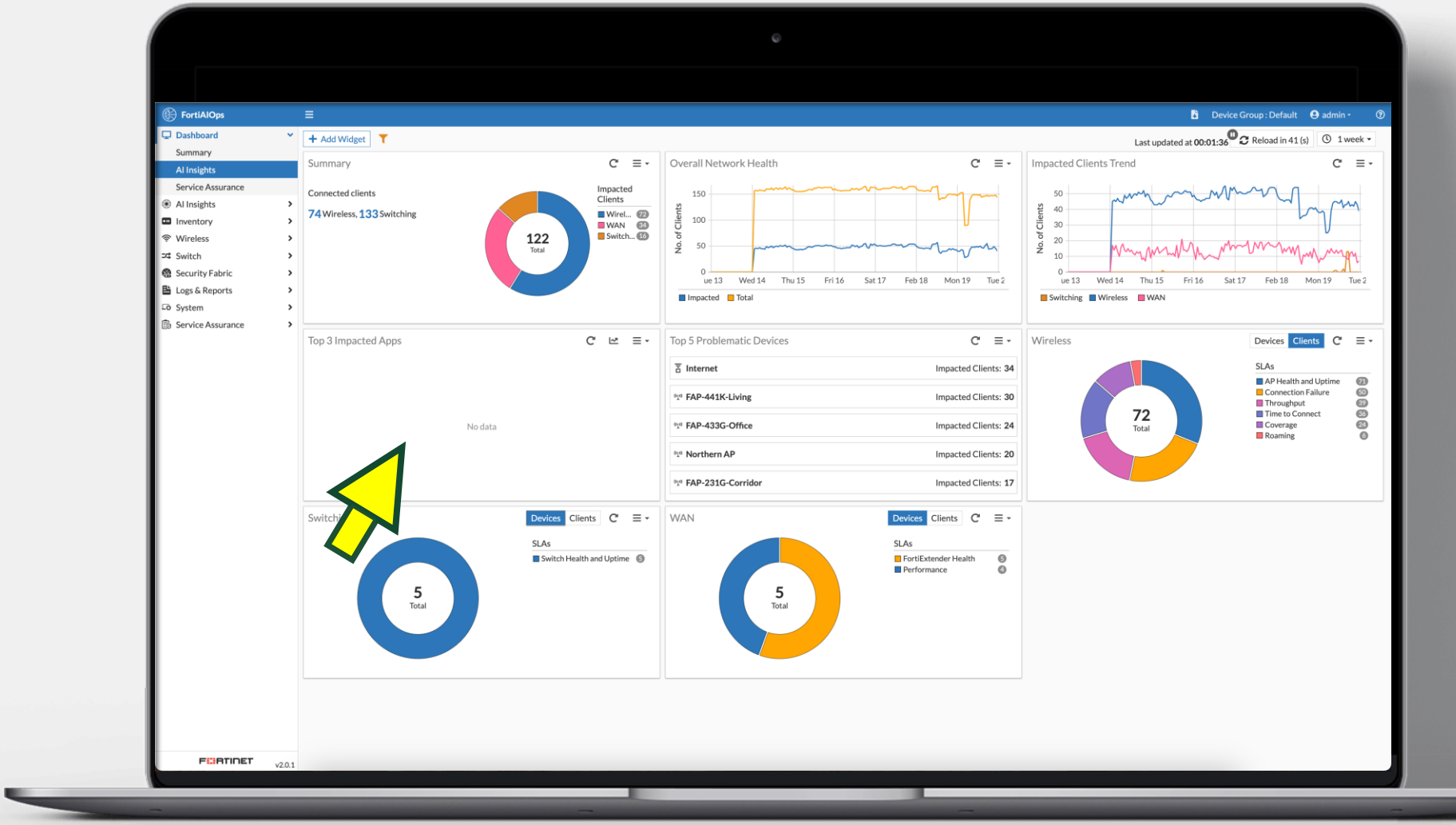
傳統方式解決問題

費時又費力，需要跨有線、無線和 SD-WAN 領域的專業知識

透過 AI 解決問題

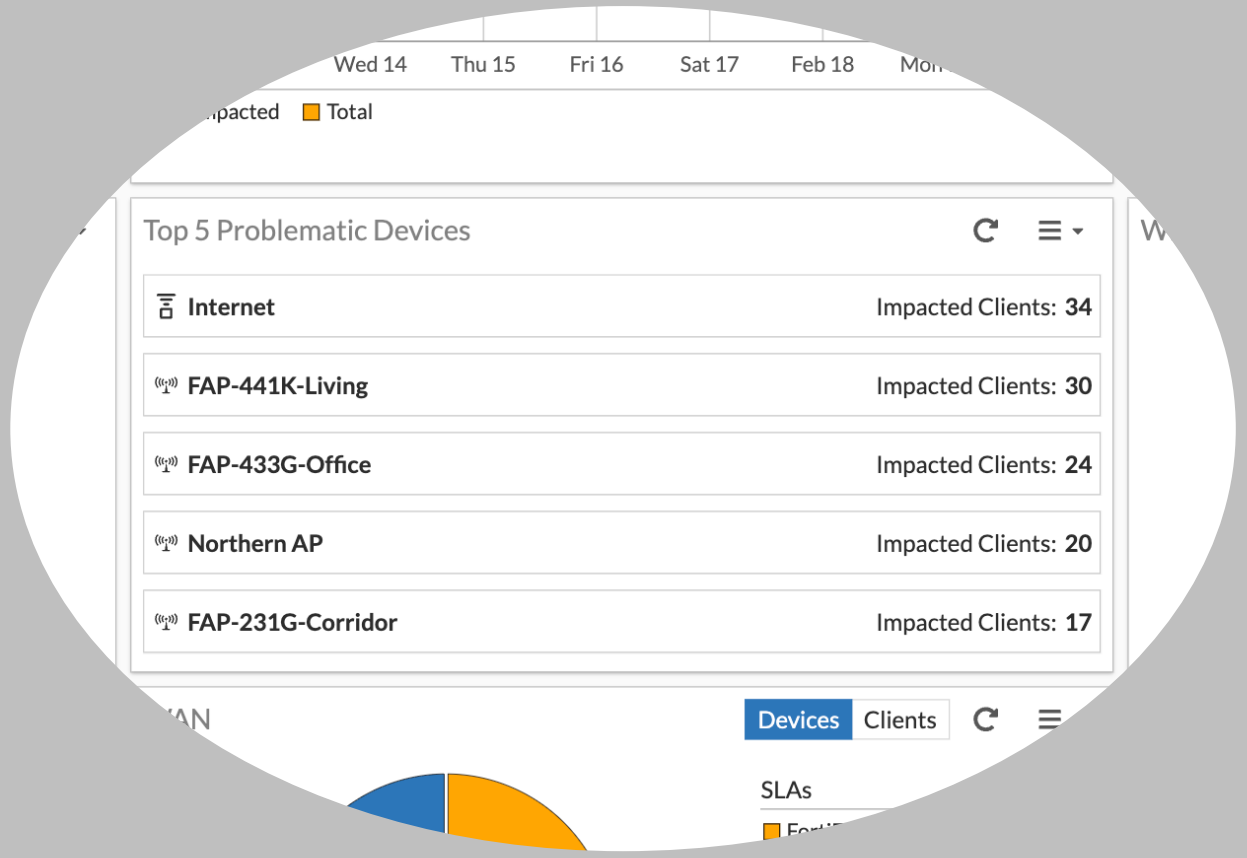
省時又省力，AI 直擊問題核心

- 透過點擊滑鼠
- 快速找到問題



© Fortinet Inc. All Rights Reserved.

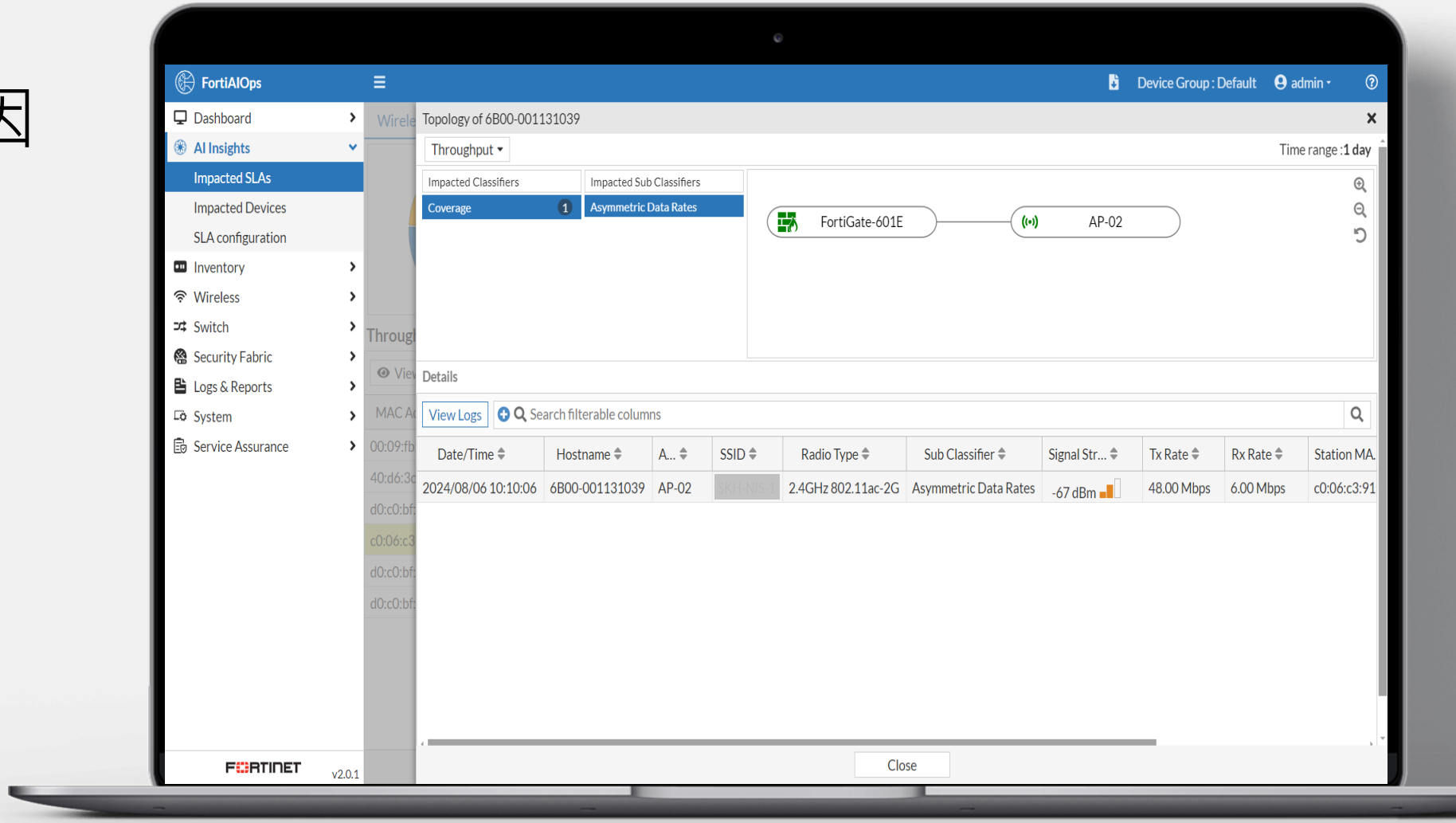
找出受影響的使用者


Wed 14
Thu 15
Fri 16
Sat 17
Feb 18
Total
Top 5 Problematic Devices
Internet
Impacted Clients: 34
FAP-441K-Living
Impacted Clients: 30
FAP-433G-Office
Impacted Clients: 24
Northern AP
Impacted Clients: 20
FAP-231G-Corridor
Impacted Clients: 17
Devices
Clients
SLAs

FortiAIOps

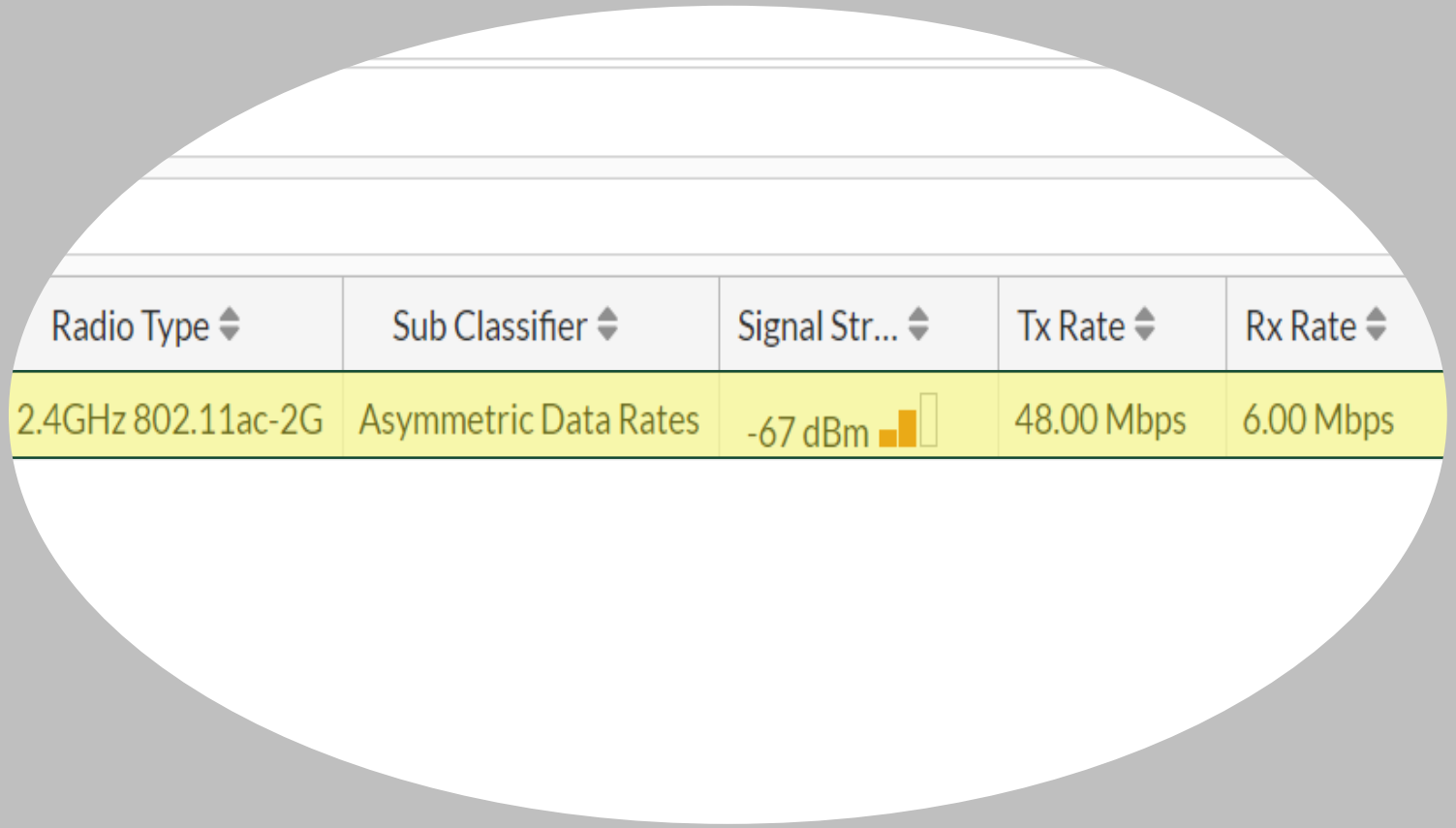
找出連線速度慢的問題

- 透過 AI 判斷原因



© Fortinet Inc. All Rights Reserved.

AI 自動判斷：無線訊號傳送速率不對等

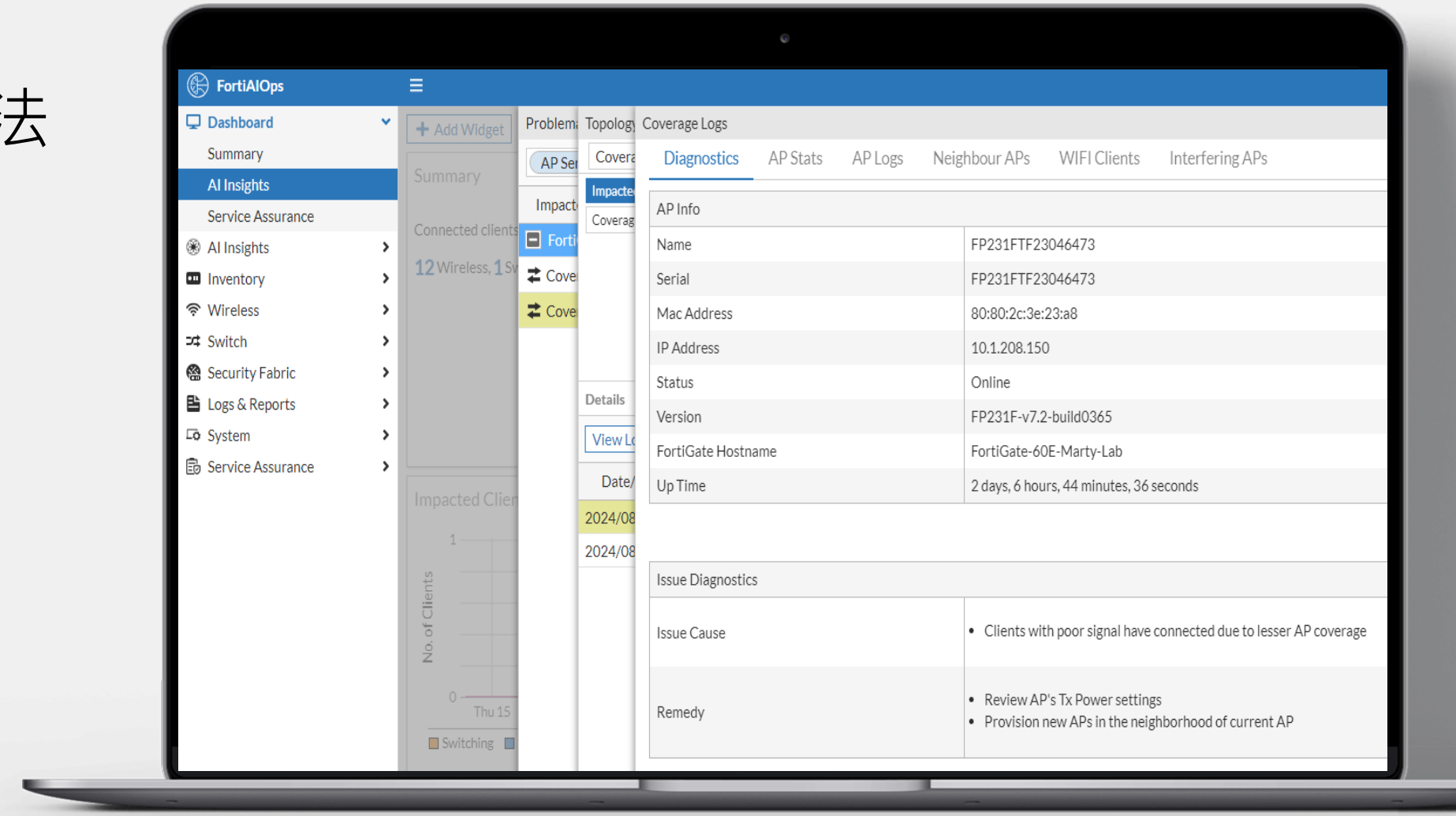


Radio Type	Sub Classifier	Signal Str...	Tx Rate	Rx Rate
2.4GHz 802.11ac-2G	Asymmetric Data Rates	-67 dBm	48.00 Mbps	6.00 Mbps

FortiAIOps

找出連線速度慢的問題

- 利用 AI 提供解法



© Fortinet Inc. All Rights Reserved.

AI 建議：調整 AP 傳送功率或增建新 AP

- Review AP's Tx Power settings
- Provision new APs in the neighborhood of current AP

如何利用 AI 解決問題

Lucy：有無線網路但上不了網耶!

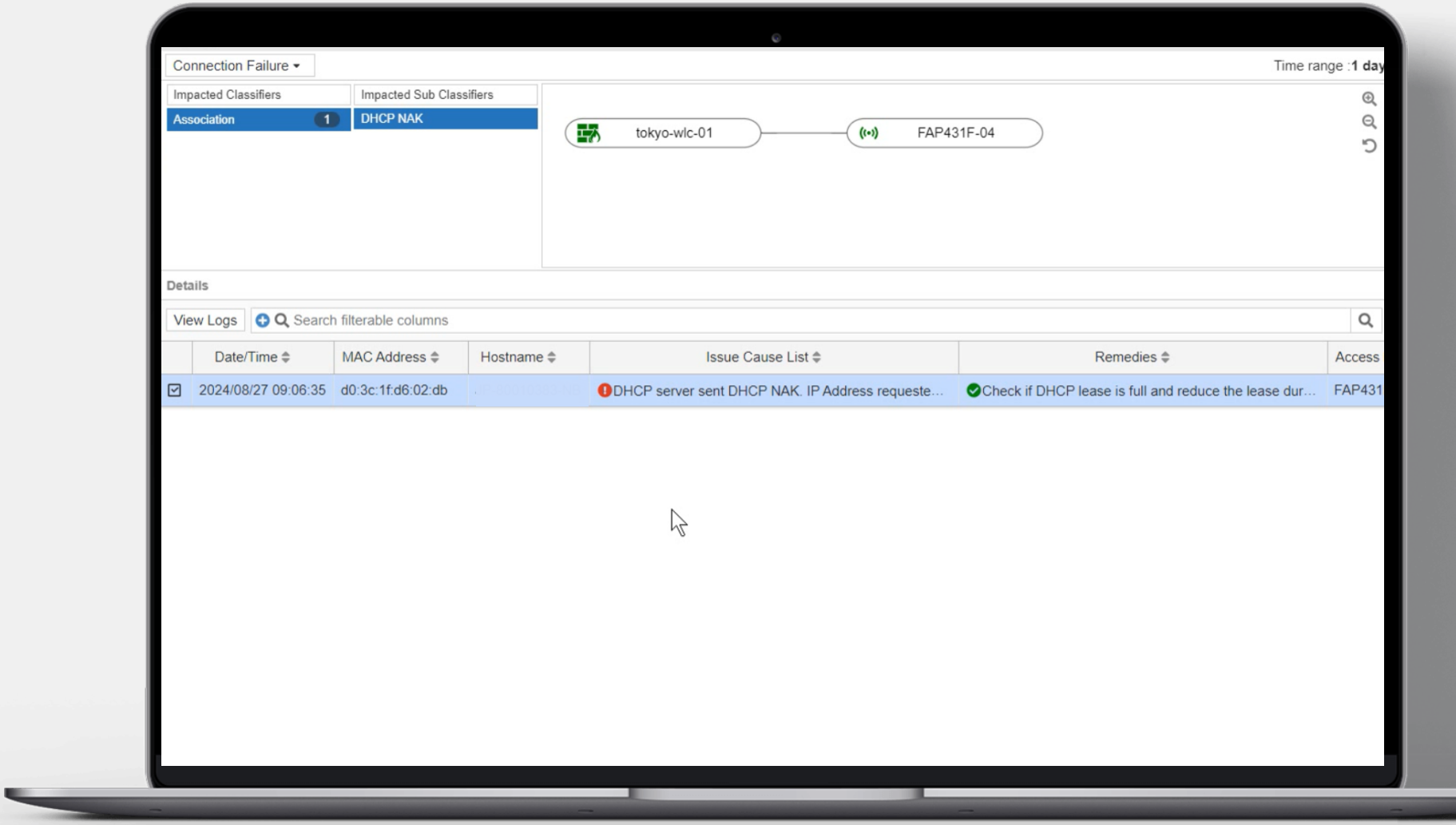
您好，這裡是控八控控–控控控

© Fortinet Inc. All Rights Reserved.

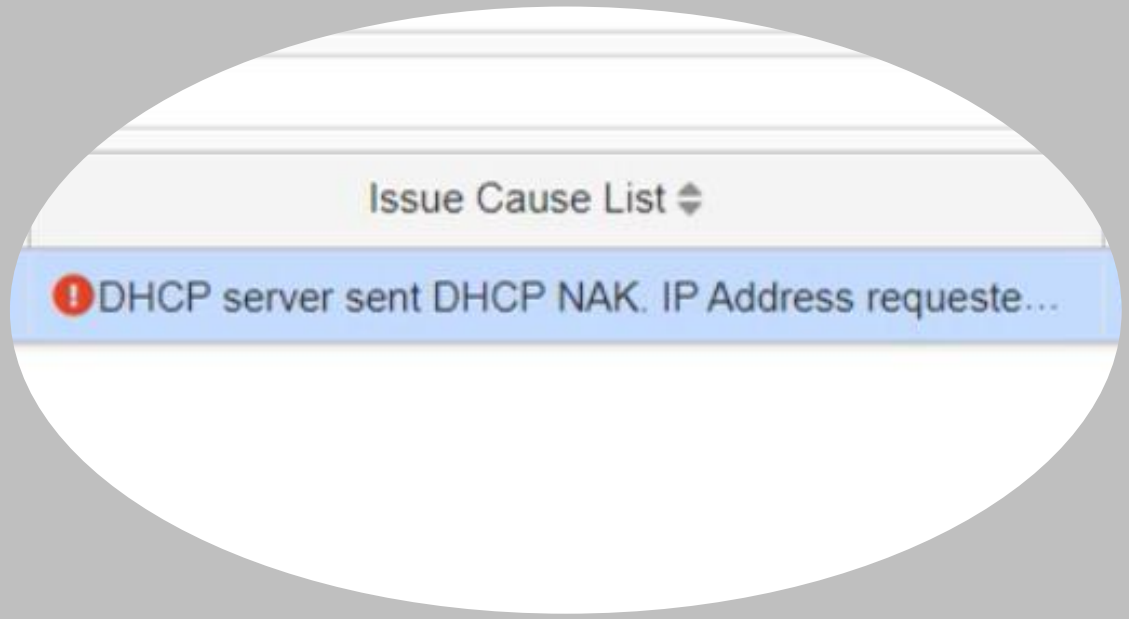
FortiAIOps

找出無法上網問題

- 透過 AI 判斷原因



© Fortinet Inc. All Rights Reserved.

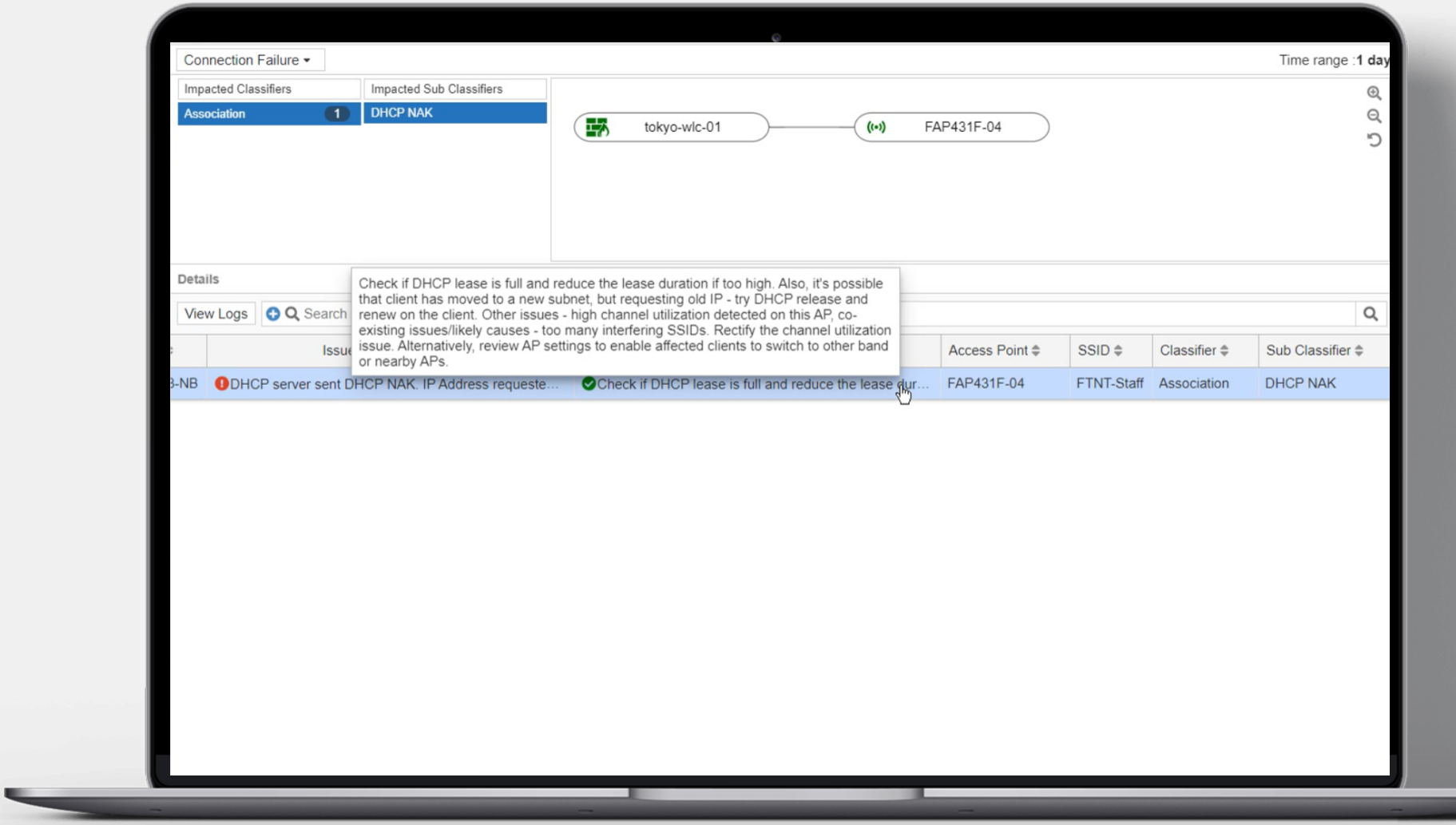


AI 自動判斷：DHCP 伺服器拒絕請求

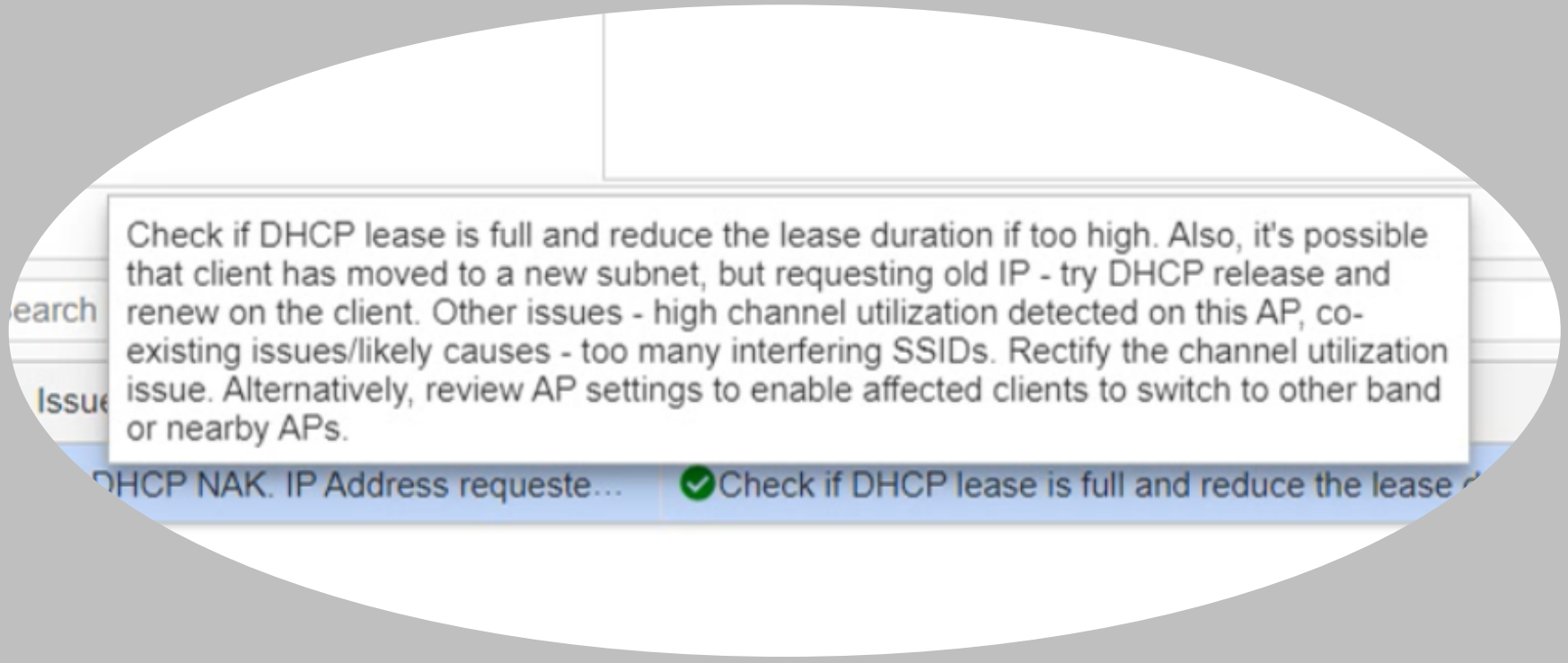
FortiAIOps

解決無法上網問題

- 利用 AI 提供解法



© Fortinet Inc. All Rights Reserved.



AI 自動判斷：檢查 DHCP 使用狀況，
增加可配發的 IP 或調整 DHCP 租約期

如何利用 AI 解決問題

Marty：今天無線網路怪怪的!

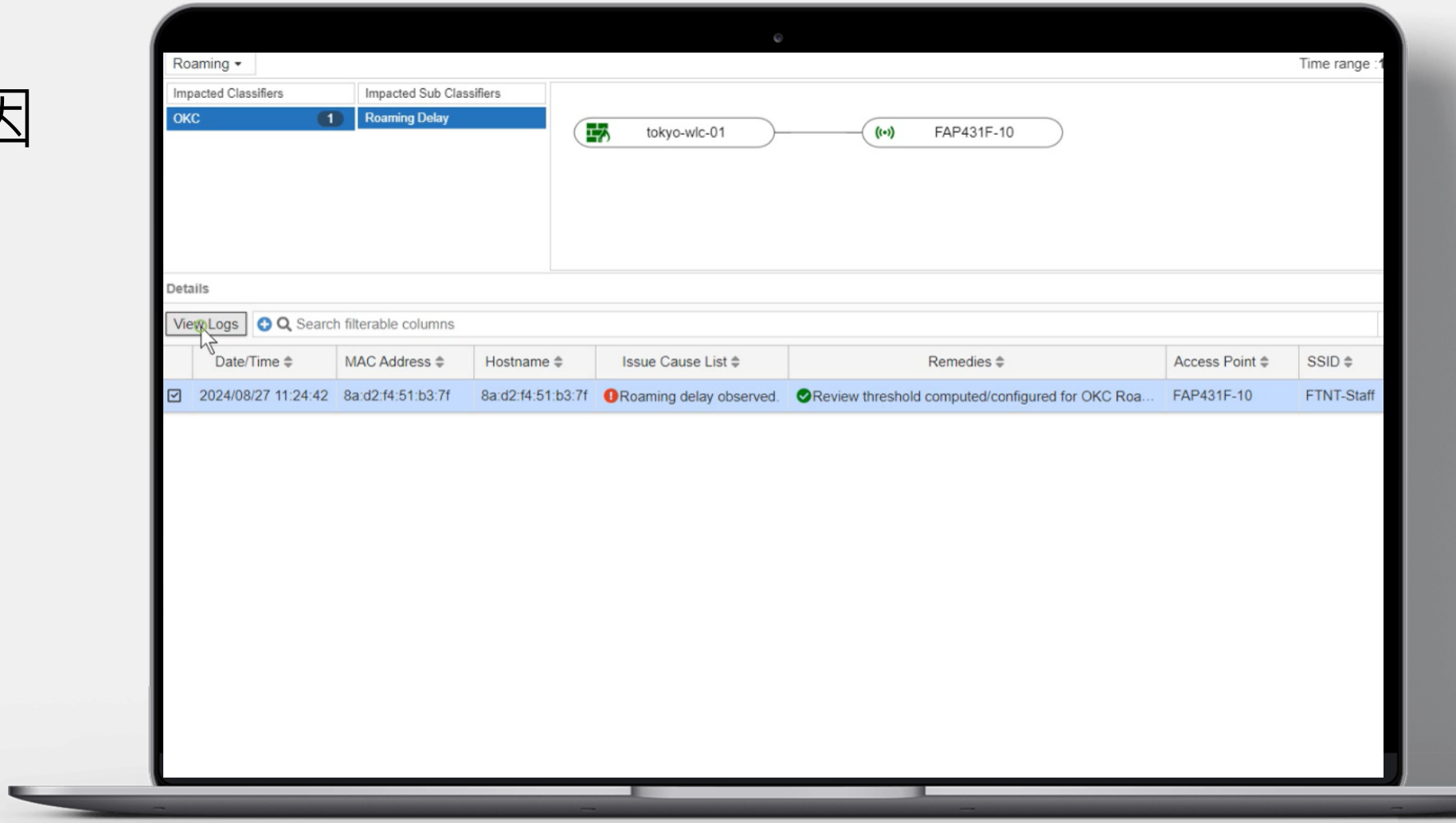
您好，這裡是控八控控–控控控

© Fortinet Inc. All Rights Reserved.

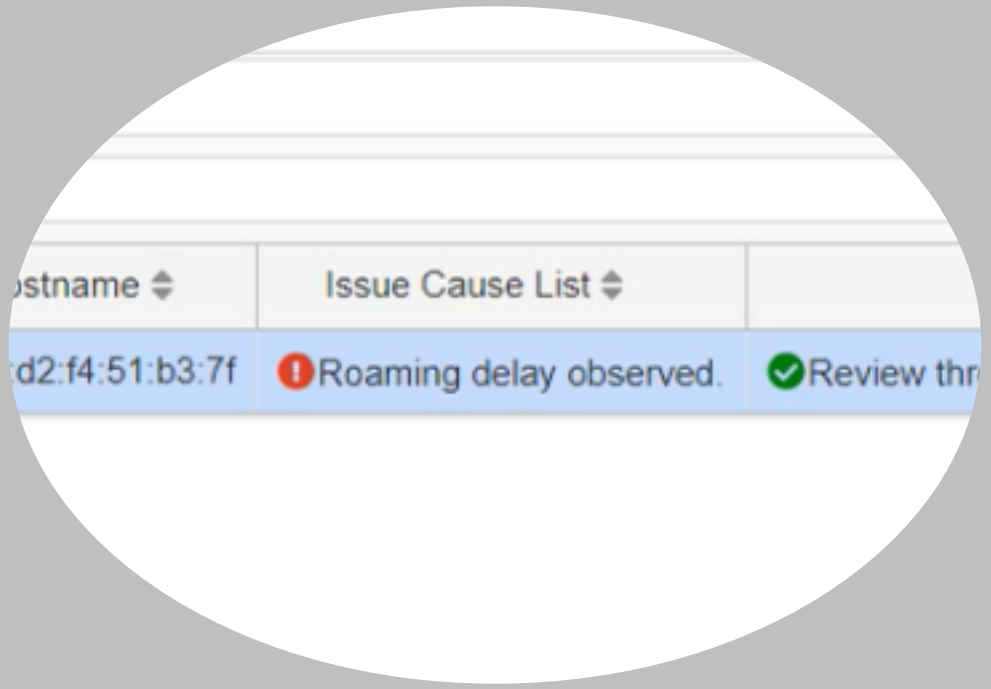
FortiAIOps

找出無線網路漫遊問題

- 透過 AI 判斷原因



© Fortinet Inc. All Rights Reserved.

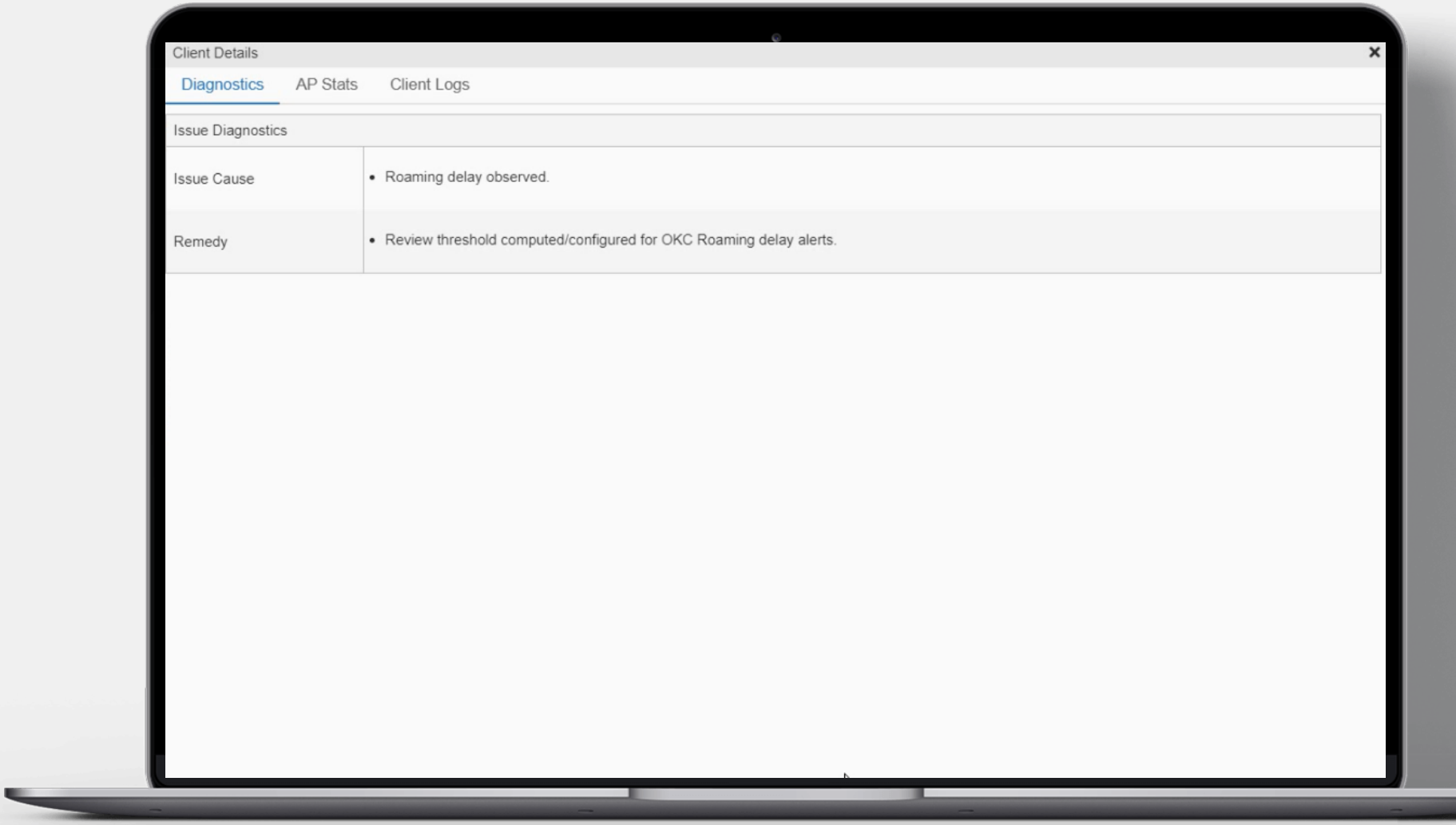


AI 自動判斷：無線漫遊發現異常

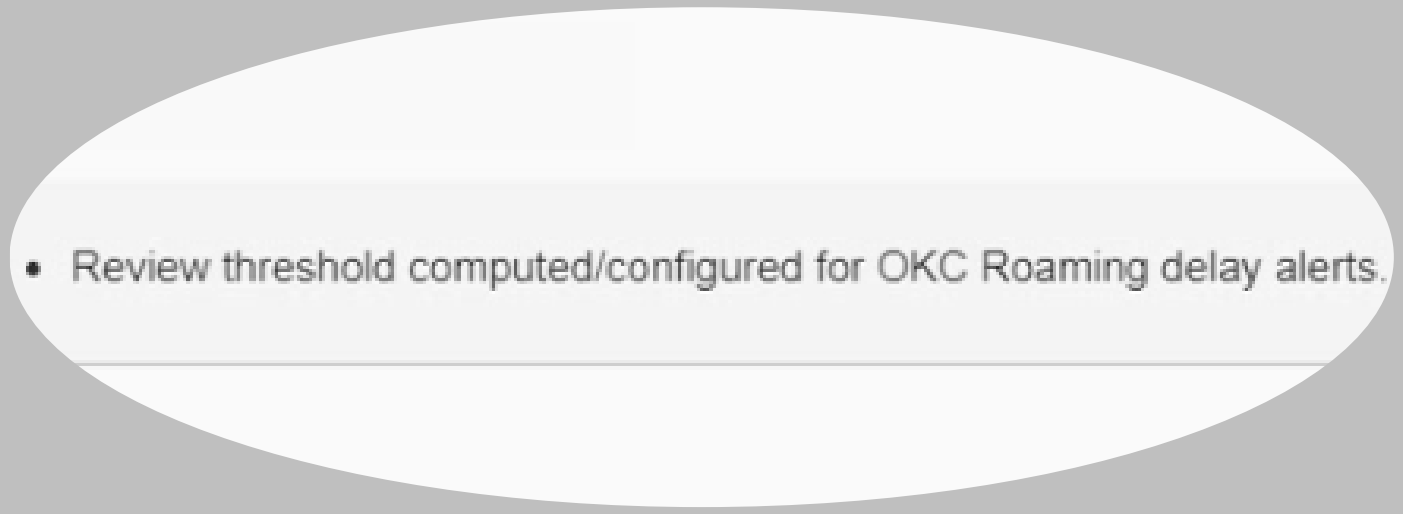
FortiAIOps

找出無線網路漫遊問題

- 利用 AI 提供解法



© Fortinet Inc. All Rights Reserved.



AI 建議：檢查無線漫遊積極度設定

如何利用 AI 解決問題

Ella：今天無線卡卡的耶!

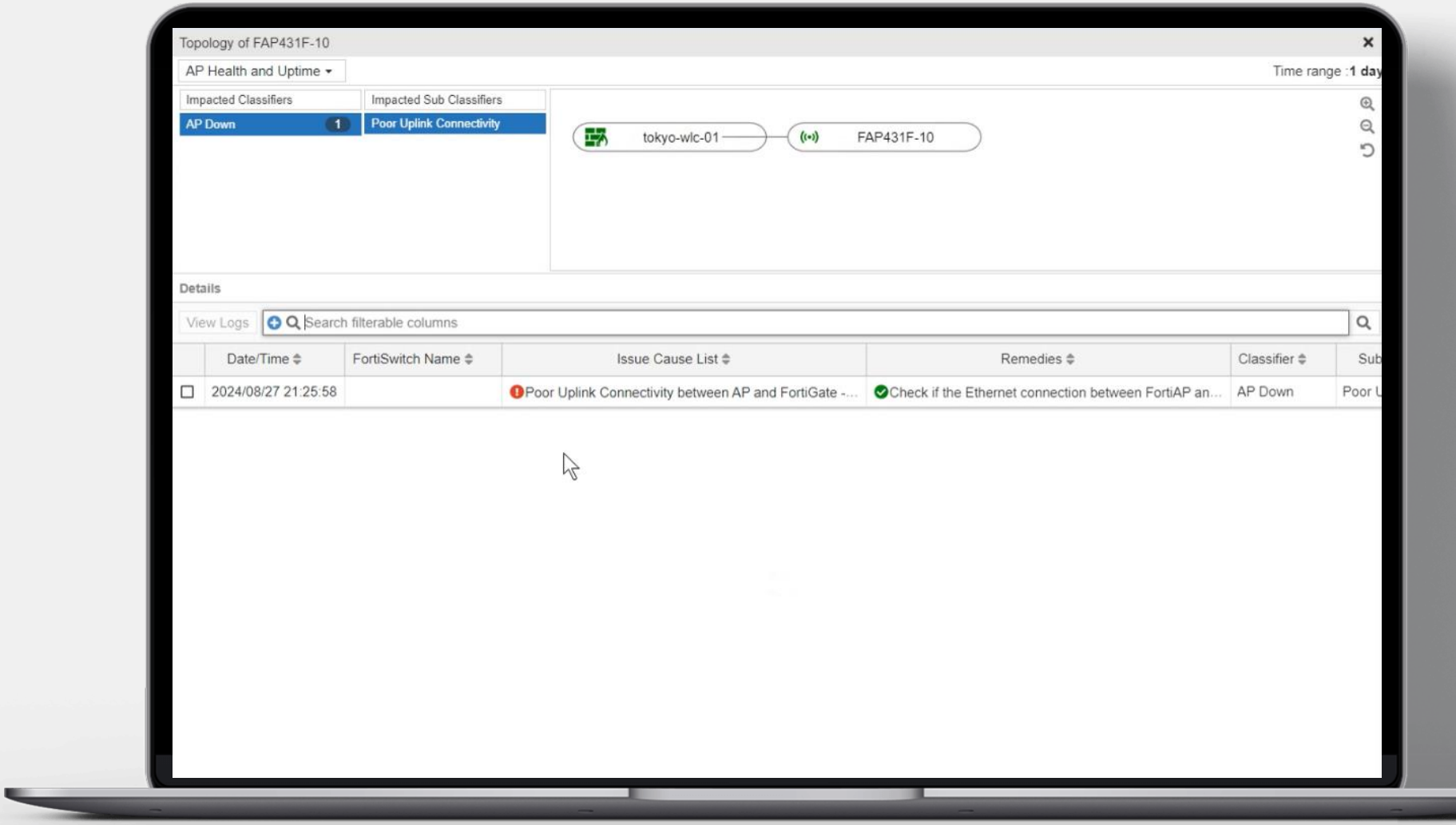
您好，這裡是控八控控–控控控

© Fortinet Inc. All Rights Reserved.

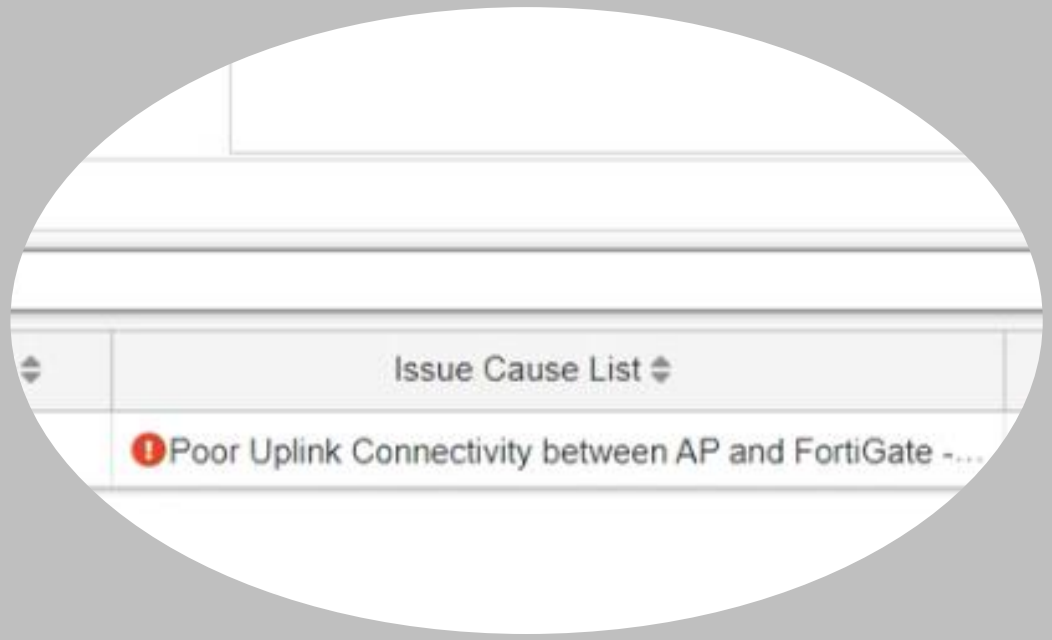
FortiAIOps

找出有線網路問題

- 透過 AI 判斷原因



© Fortinet Inc. All Rights Reserved.

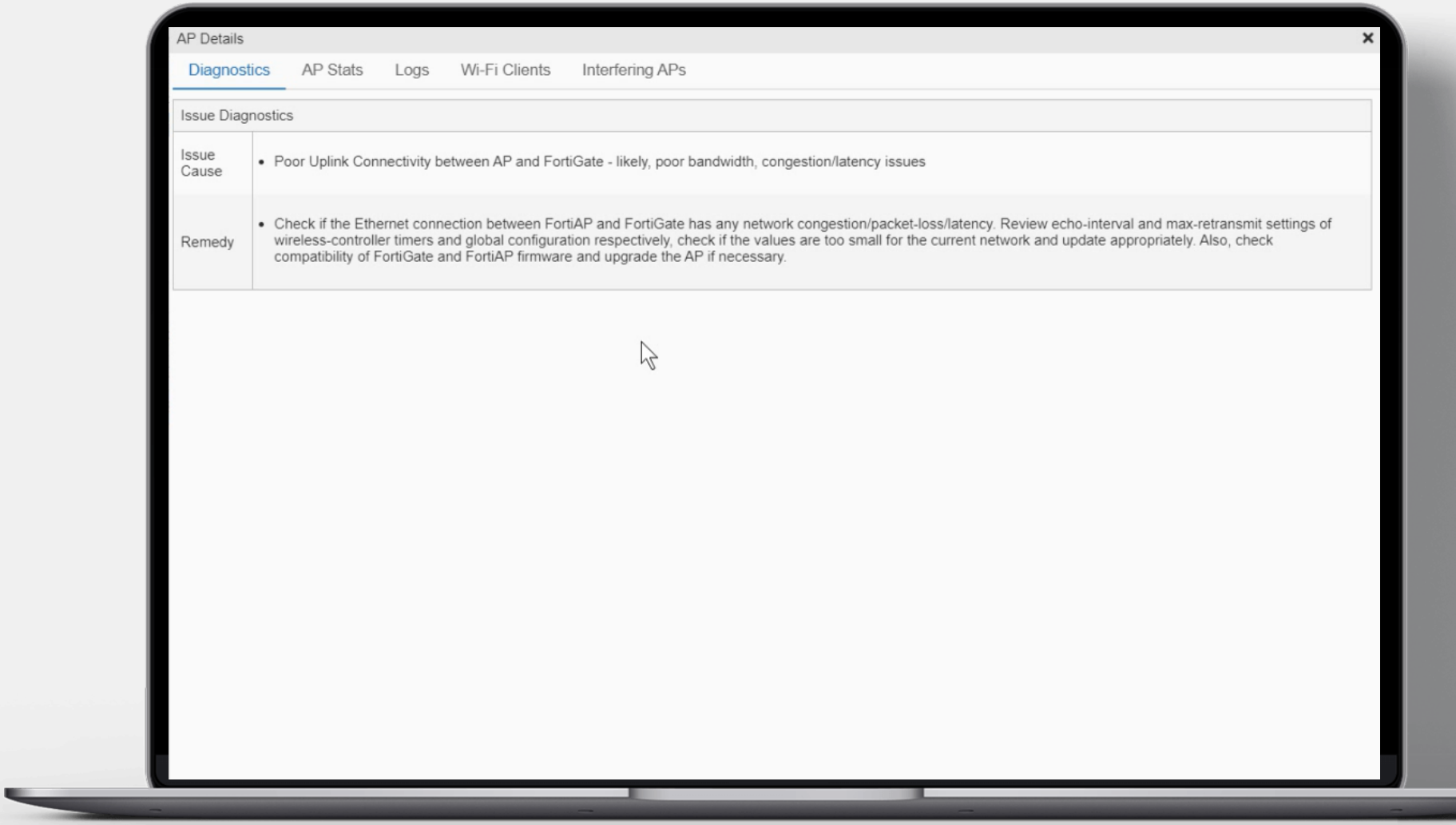


AI 自動判斷：AP 與控制器中間的線路不良

FortiAIOps

找出有線網路問題

- 利用 AI 提供解法



© Fortinet Inc. All Rights Reserved.

Issue Diagnostics	
Issue Cause	• Poor Uplink Connectivity between AP and FortiGate - likely, poor bandwidth, congestion/latency issues
Remedy	• Check if the Ethernet connection between FortiAP and FortiGate has any network congestion/packet-loss/latency. Review echo-interval and max-retransmit settings of wireless-controller timers and global configuration respectively, check if the values are too small for the current network and update appropriately. Also, check compatibility of FortiGate and FortiAP firmware and upgrade the AP if necessary.

AI 建議：

檢查 AP 與控制器之間的交換器連線速率是否正常，有沒有封包遺失，AP 與控制器間的韌體是否匹配。

FortiAIOps

將 AI / 機器學習融入安全織網中

持續監控

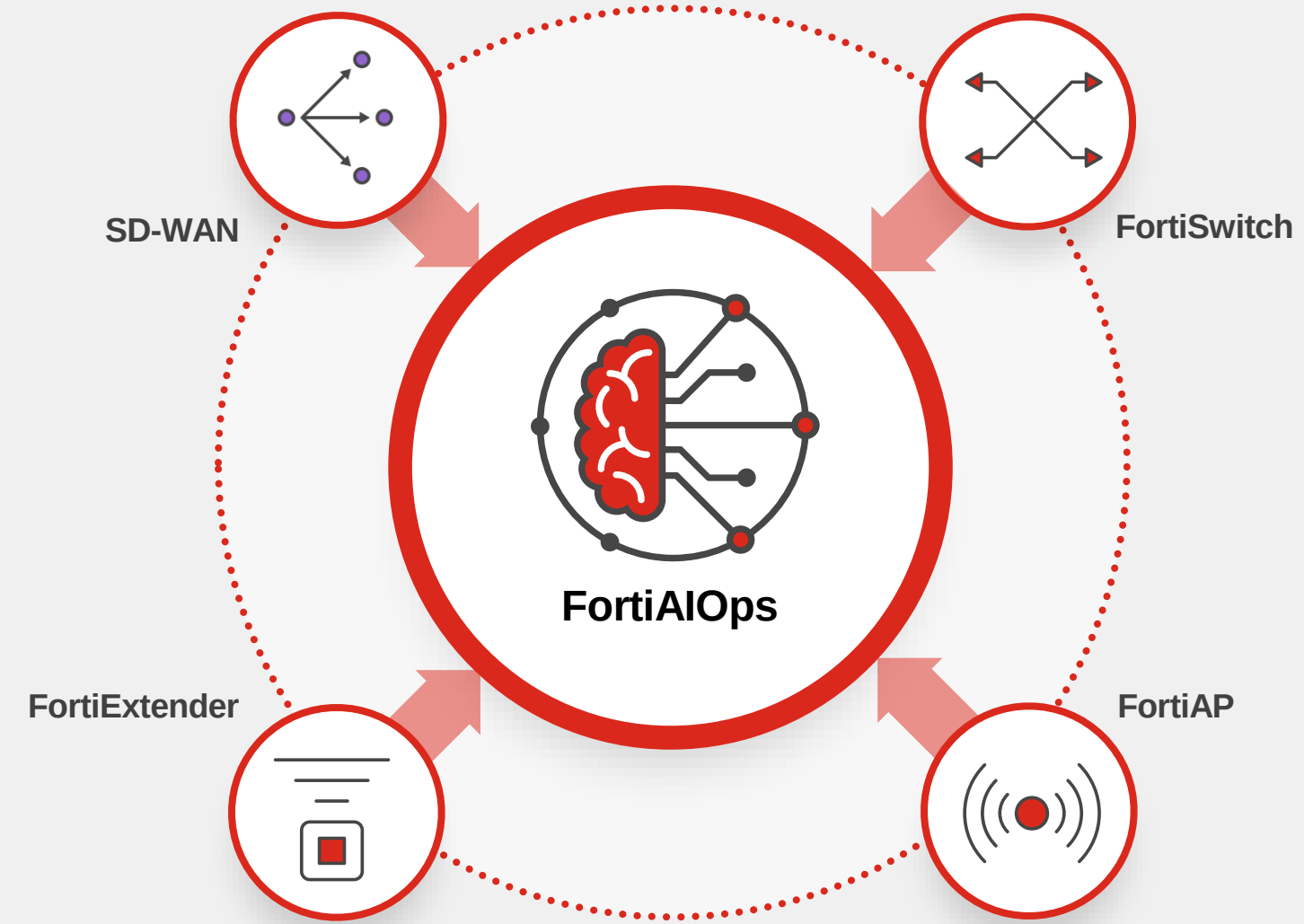
- 趨勢分析 / 歷史基準線
- 網路流量可視化

智能除錯

- 無線網路服務不中斷
- 無線網路頻譜分析
- 無線網路熱感圖
- 網路線品質測試
- 視訊軟體品質監控

AI / 機器學習

- 動態學習網路品質曲線
- 問題判斷與分類
- 建議改善措施



© Fortinet Inc. All Rights Reserved.

FortiAI for
FortiSIEM

AI 驅動的安全營運 (SecOps)

四大面向導入 AI 與機器學習，對抗新型態與未知的資安威脅

基於網路資訊流
Network-Based

Sandbox

NDR

基於日誌與記錄
Log-Based

SIEM

SOAR

基於端點行為模式
Endpoint-Based

EDR

Deception

基於資安情資服務
TIS-Based

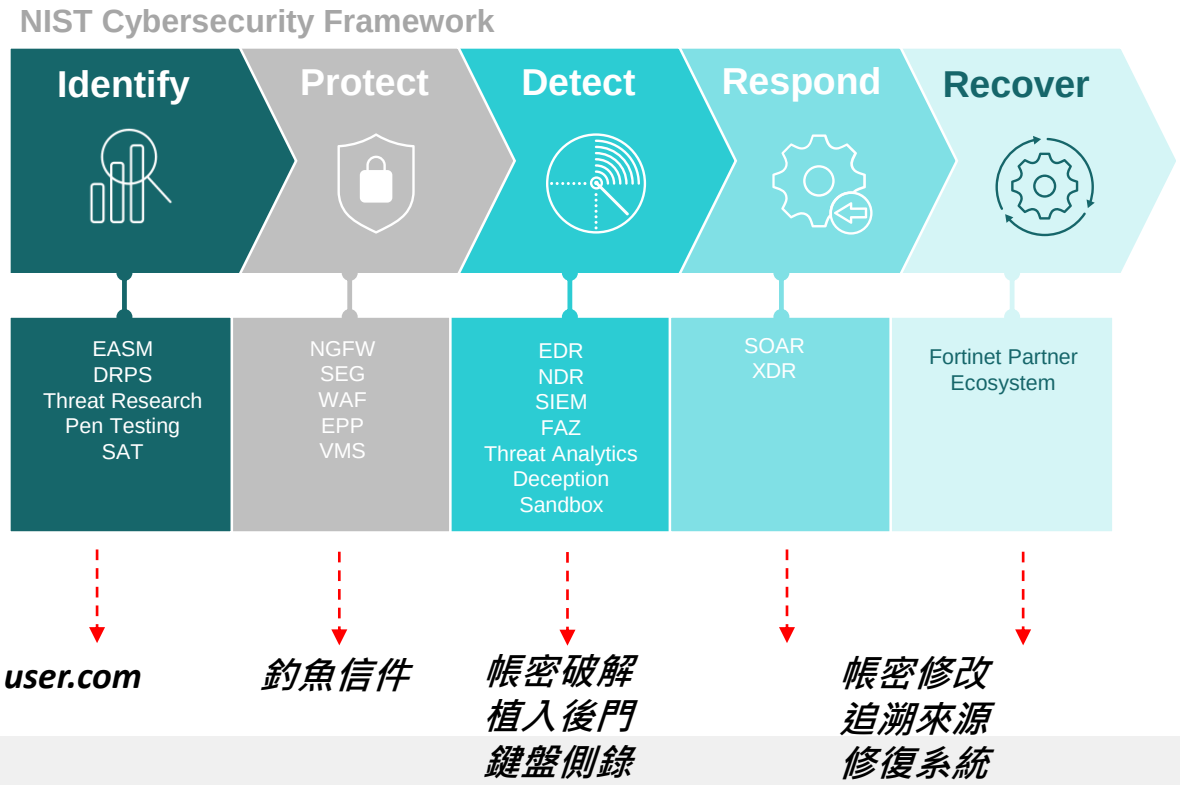
FortiGuard Lab.

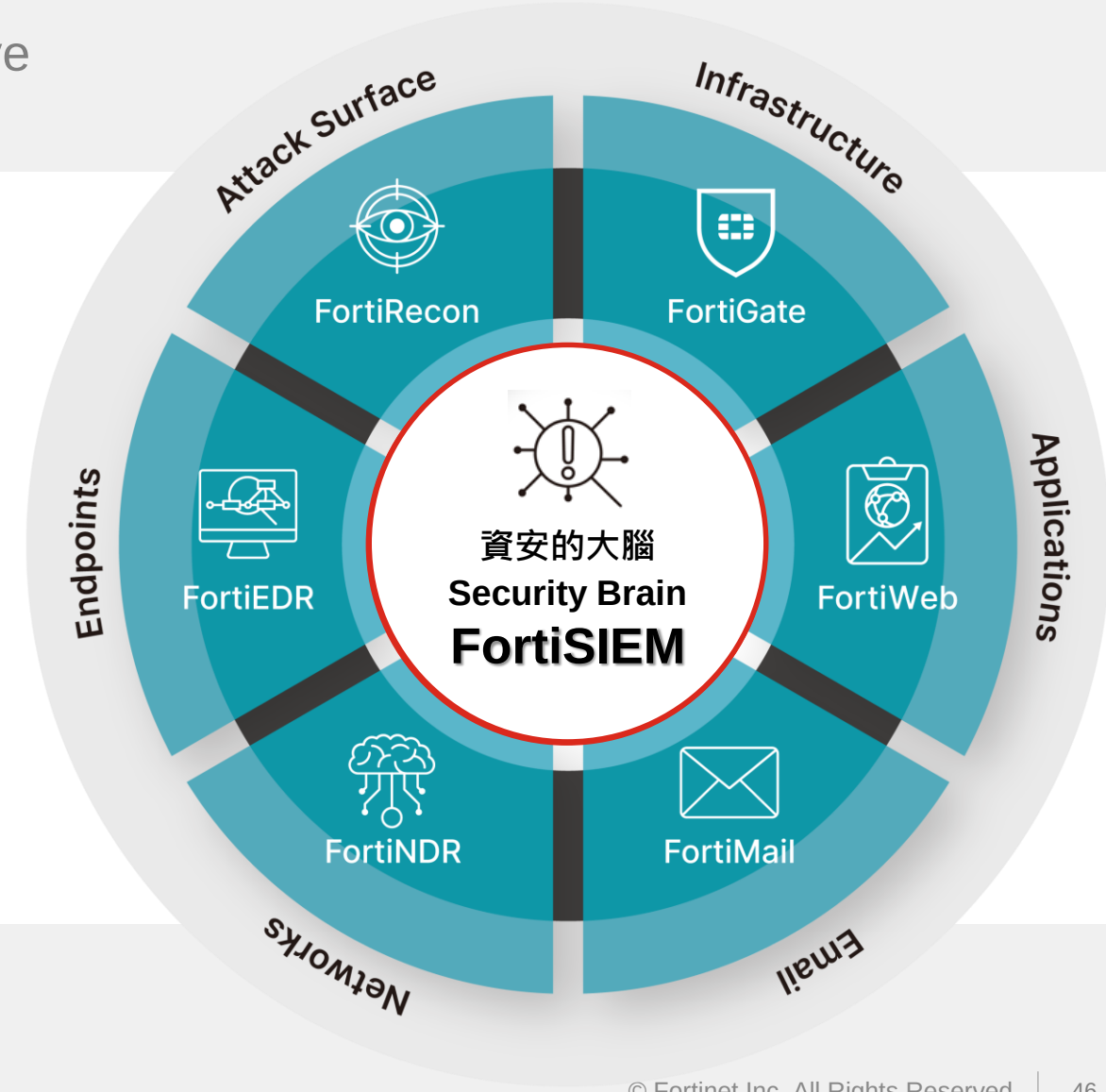
DRPS

© Fortinet Inc. All Rights Reserved.

Fortinet SecOps 資安智能營運
Detects and Responds to Threats Faster

Alignment to NIST cybersecurity framework to improve risk management





© Fortinet Inc. All Rights Reserved.

資安 (SOC) 與網維 (NOC) 融合式分析

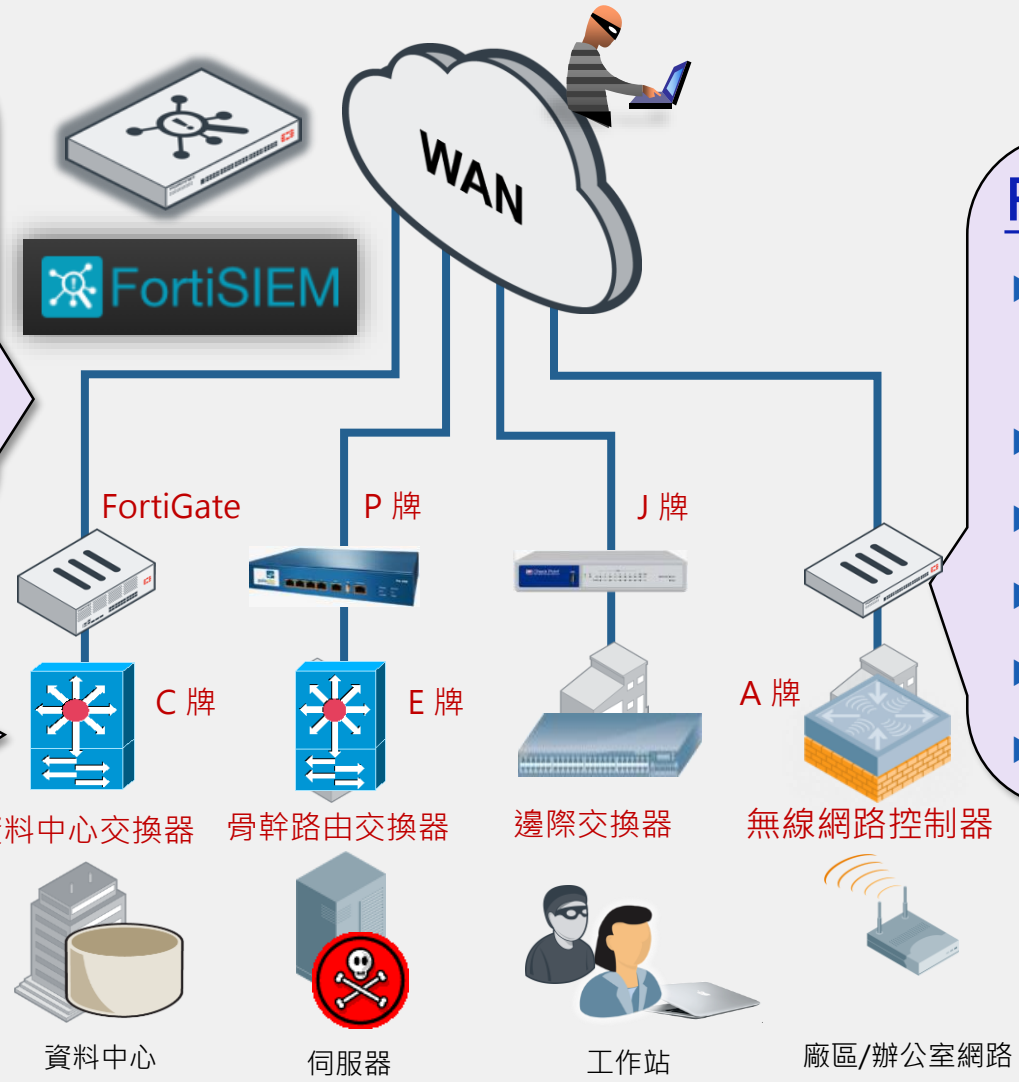
多來源、多品牌日誌記錄統整與關聯分析

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.

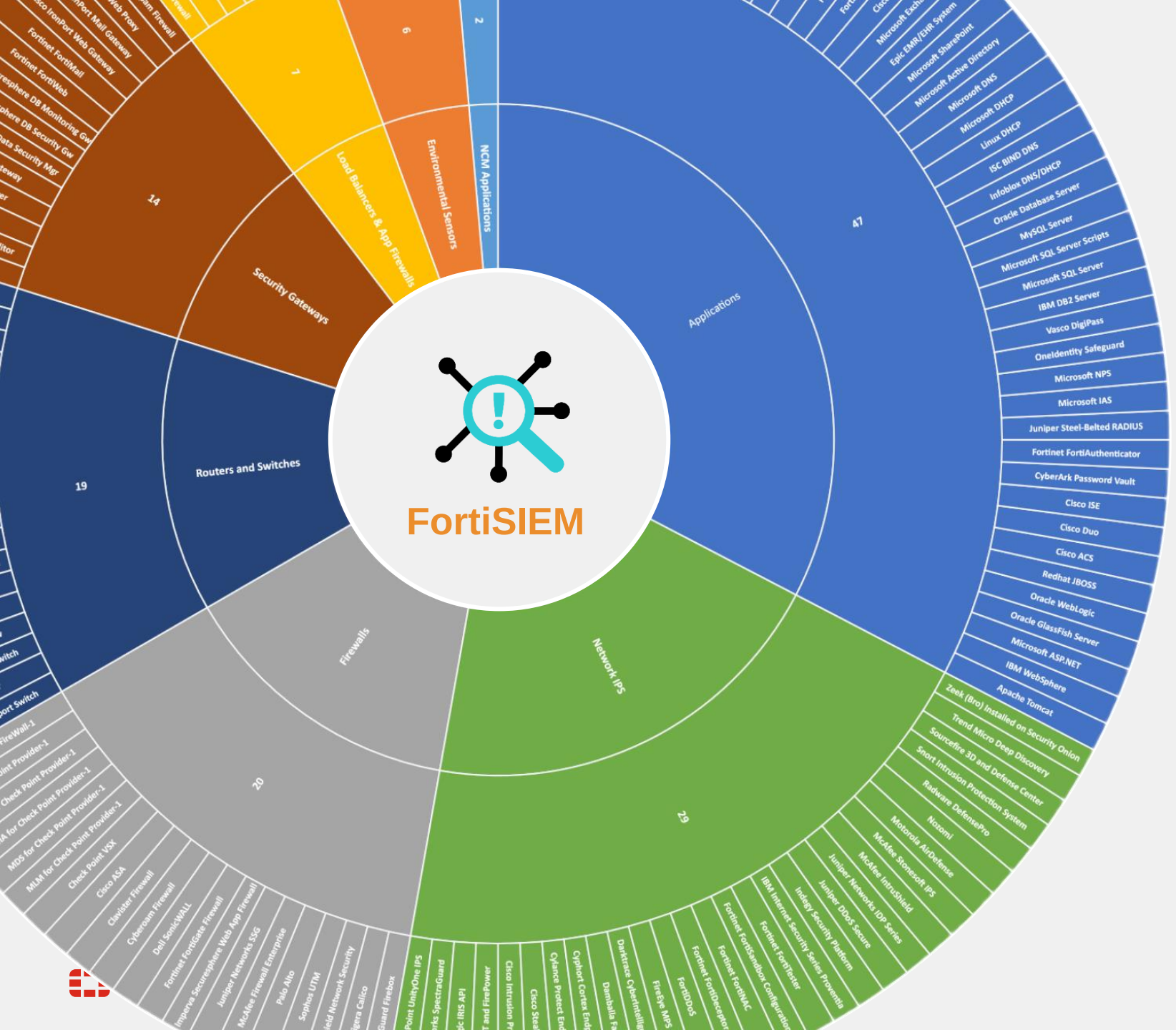
- 系統事件(Event Log)
- 資安事件(Security Log)
- 流量記錄 (Traffic Log)
- 應用系統事件 (Application Layer)
- 異常行為、事件分析



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

© Fortinet Inc. All Rights Reserved.



廣泛的設備與應用服務支援

FortiSIEM 預設支援超過 400+ 種以上各式設備與應用服務

內建日誌解譯編輯器 (Parser Editor) 可支援更多的設備與應用

© Fortinet Inc. All Rights Reserved.

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

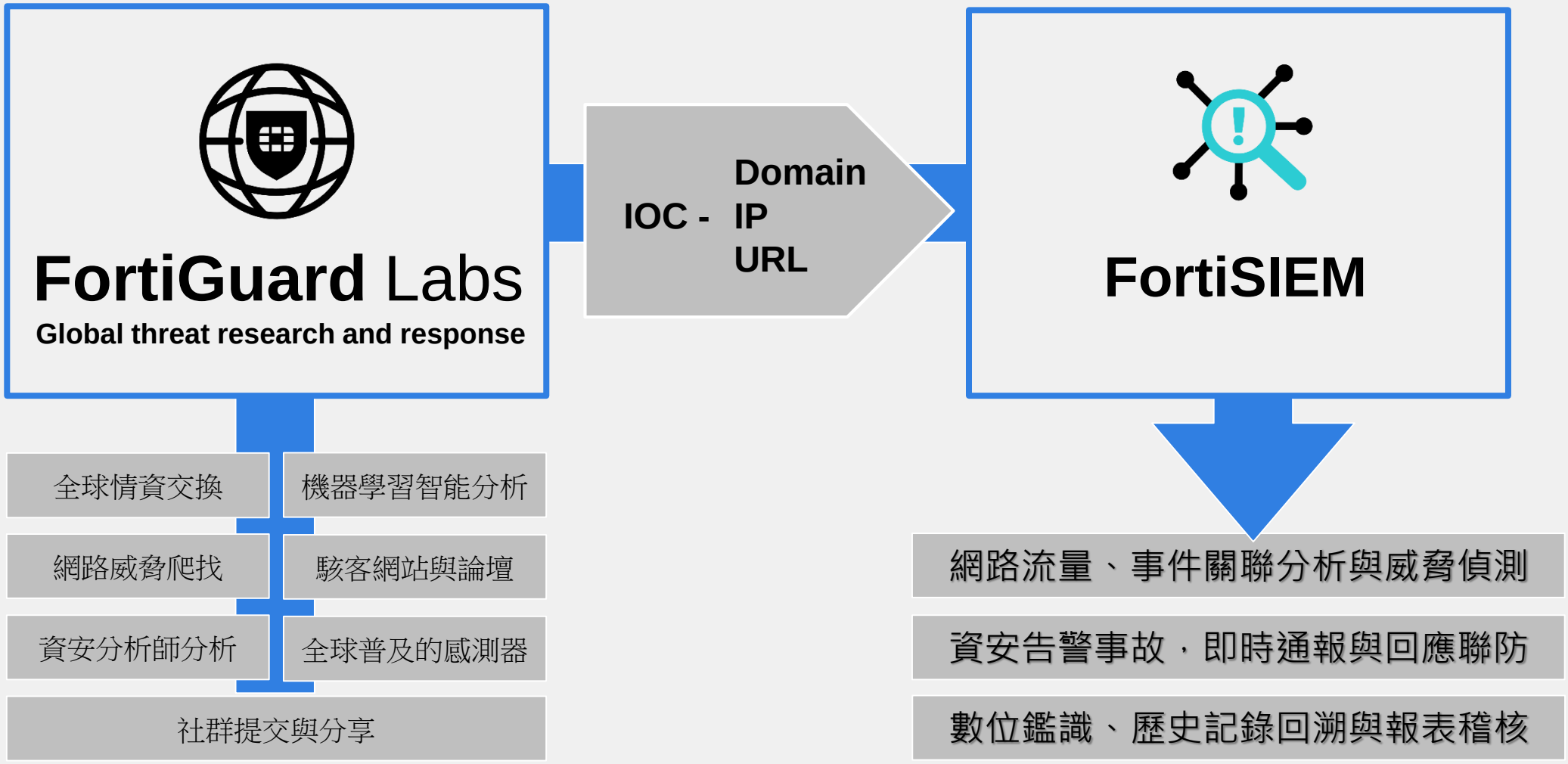
嚴重受害主機排行榜

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

自動更新情資，分析、告警與聯防

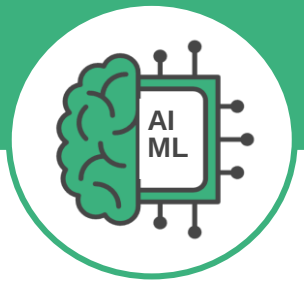
整合並自動更新外部情資 (FortiGuard、第三方情資或用戶自行定義)



© Fortinet Inc. All Rights Reserved.

FortiSIEM AI 與機器學習功能

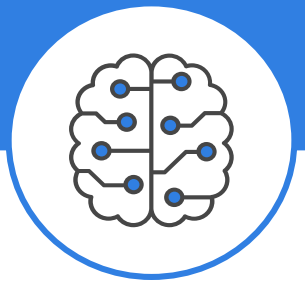
用戶/端點行為分析
AI for UEBA



AI for UEBA 行為分析

- ✓ 基於日誌的關聯分析，包括：
  登入/登出行為模式、系統開/關機、程序建立/終止、檔案刪除等等

機器學習工作台
AI for ML Workbench



AI for 機器學習工作台

- ✓ 導入 20+ 多種機器學習演算法模型與應用案例
- ✓ 實現靈活，可自定義演算法與應用案例能力
- ✓ 圖形化使用者介面，方便配置

與生成式 AI 整合
AI for Operation

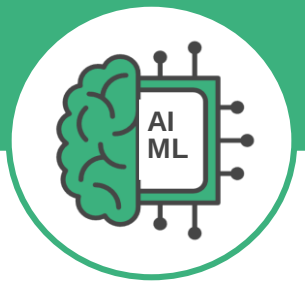
AI for 日常智能維運

- ✓ 整合 OpenAI (ChartGPT in FortiSIEM)
- ✓ 互動式問答，分析師日常維運輕鬆尋求 AI 助理協助
- ✓ 查詢會遮蓋敏感資料，保護重要資訊不外洩

© Fortinet Inc. All Rights Reserved.

FortiSIEM AI 與機器學習功能

用戶/端點行為分析
AI for UEBA



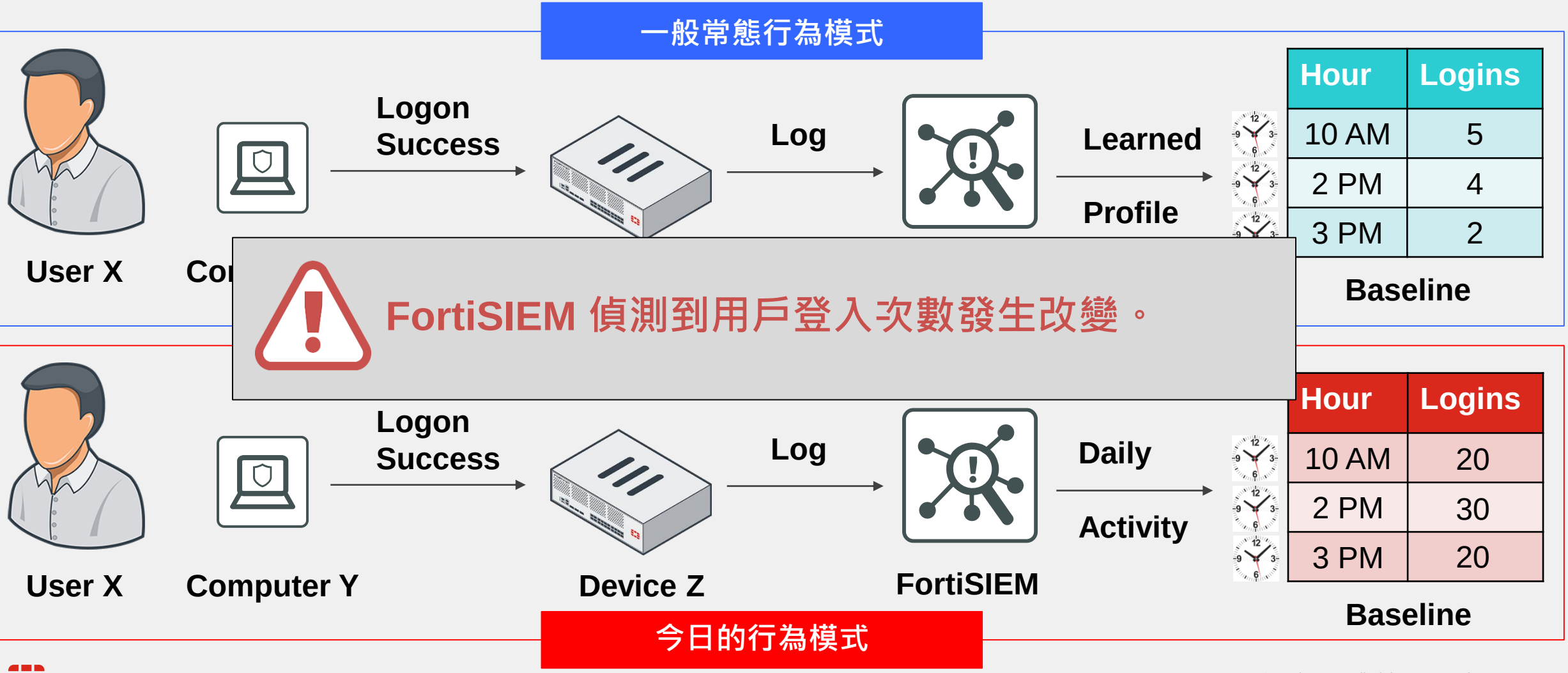
AI for UEBA 行為分析

✓ 基於日誌的關聯分析，包括：
登入/登出行為模式、系統開/關機、程序建立/終止、檔案刪除等等

© Fortinet Inc. All Rights Reserved.

基礎 UEBA 行為分析：追蹤分析用戶登入模式 (次數)

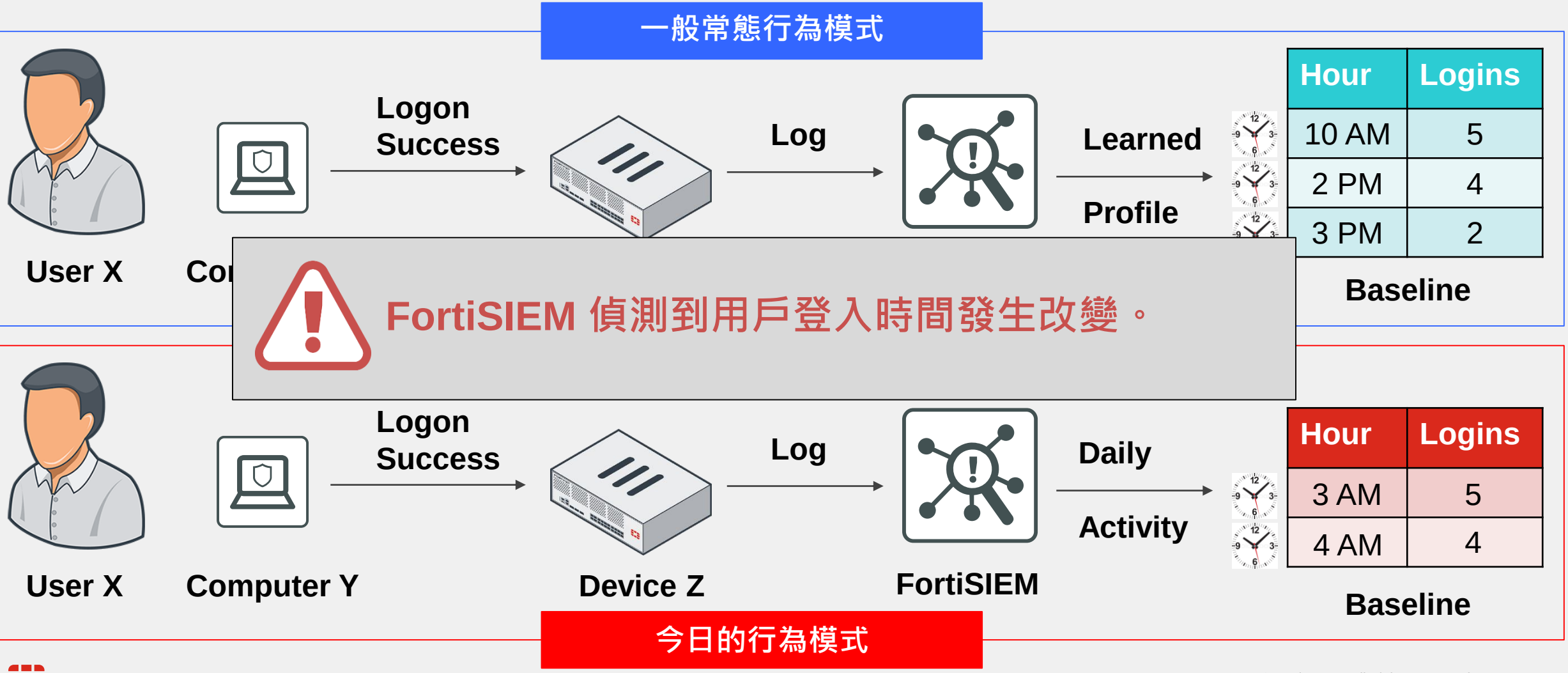
Rule：Sudden Increase in User Login Volume



© Fortinet Inc. All Rights Reserved.

基礎 UEBA 行為分析：追蹤分析用戶登入模式 (時段)

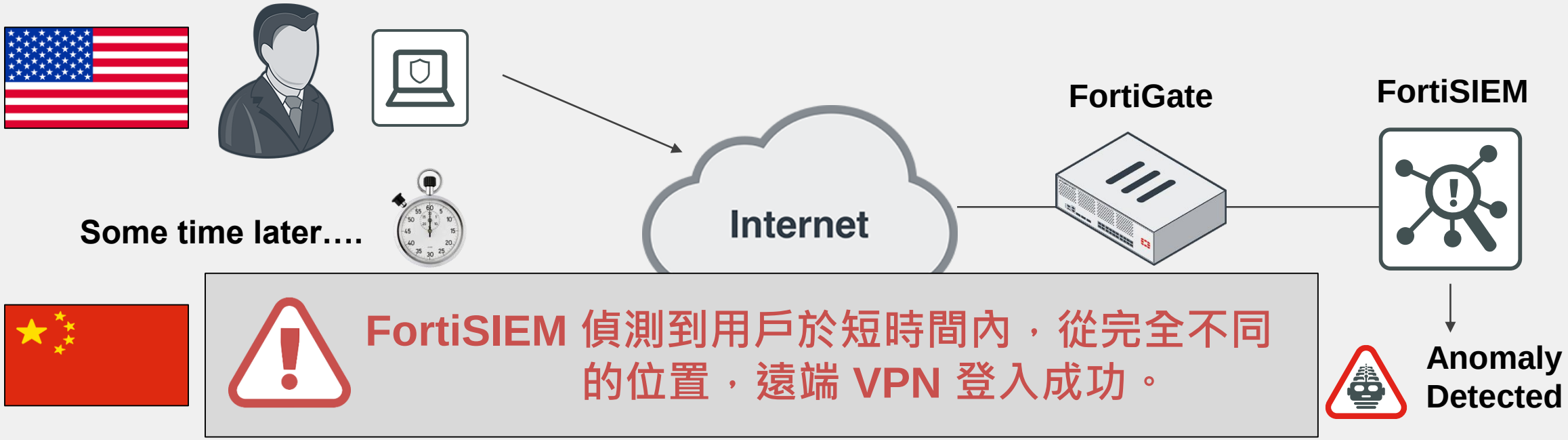
Rule：Sudden User Login Pattern Change

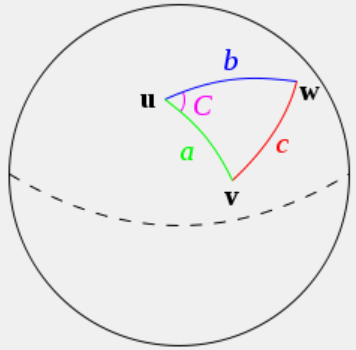


© Fortinet Inc. All Rights Reserved.

基礎 UEBA 行為分析：追蹤分析用戶登入模式 (位置)

Rule：Sudden User Location Change





$$\mathrm{hav}(\theta) = \sin^2\left(\frac{\theta}{2}\right) = \frac{1-\cos(\theta)}{2}$$

Haversine Formula

© Fortinet Inc. All Rights Reserved.

FortiSIEM AI 與機器學習功能

機器學習工作台
AI for ML Workbench

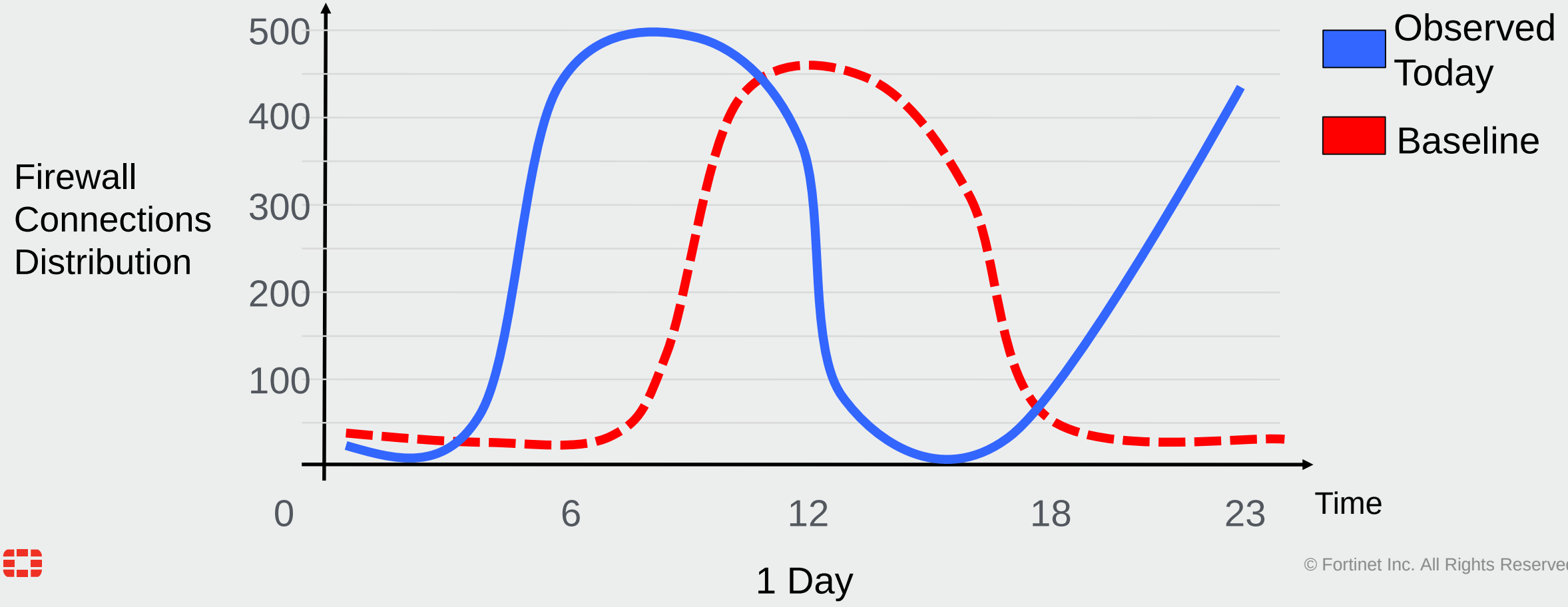
AI for 機器學習工作台

- ✓ 導入 20+ 多種機器學習演算法模型與應用案例
- ✓ 實現靈活，可自定義演算法與應用案例能力
- ✓ 圖形化使用者介面，方便配置

© Fortinet Inc. All Rights Reserved.

機器學習基準線關聯分析 (ML Baseline Rules)

機器學習建立動態維運基準線 (Kullback-Leibler Divergence)



© Fortinet Inc. All Rights Reserved.

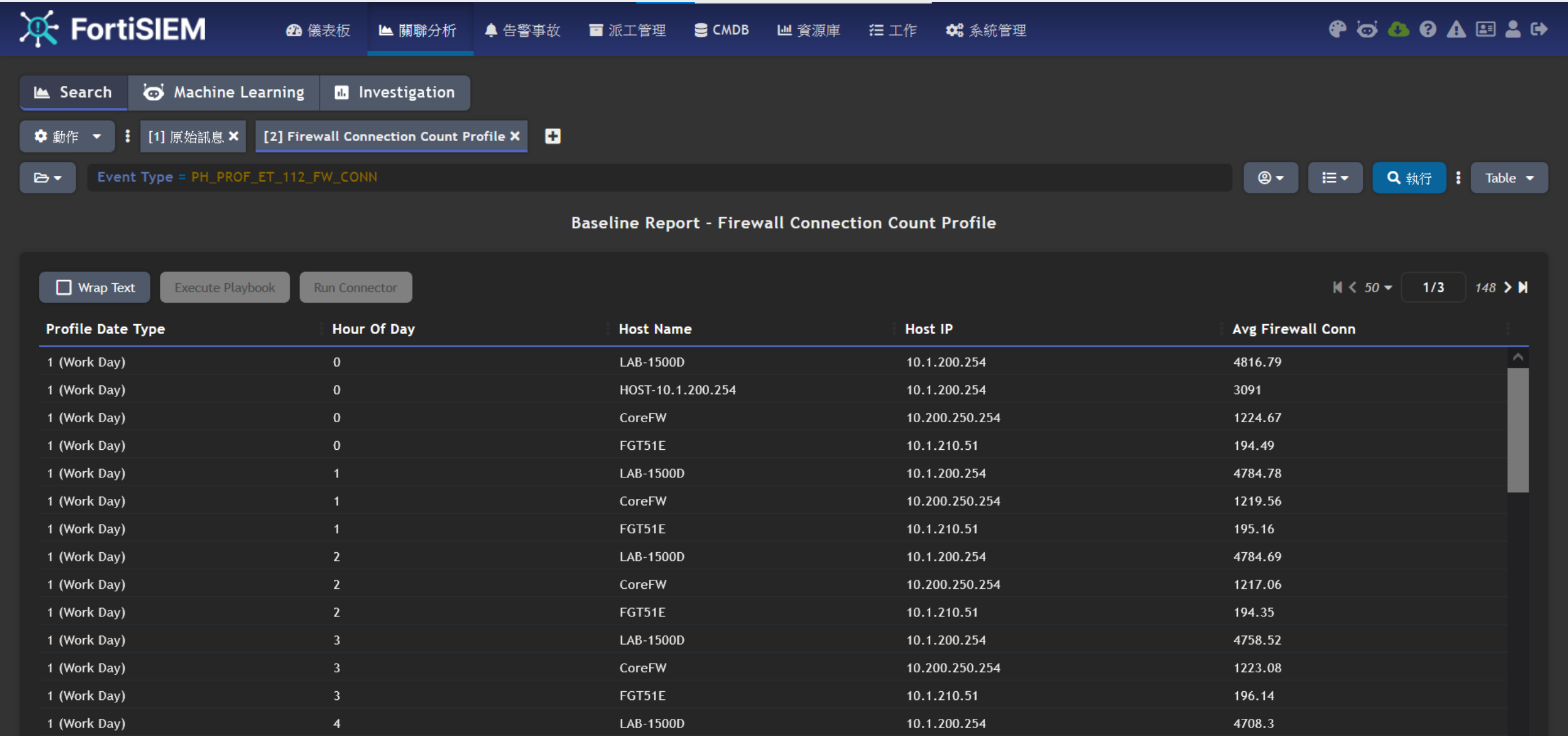
機器學習基準線關聯分析 (ML Baseline Rules)

基準線預設報表

Name	Description	Scope	Data Source	Report Design Template
Device CPU, Memory Usage Profile	This report provides baselines cpu, memory usage profile	System	All devices via SNMP Monitoring	Global System Reports Root Template
Device Disk I/O Profile	This report provides baselines disk I/O usage for servers, VMs and ESX	System	VCenter Via VM_SDK	Global System Reports Root Template
DNS Request Profile	This report baselines DNS requests on a per client basis: the number of requests and distinct destinations it attempted to resolve.	System	Microsoft DNS via FortiSIEM Agent, BIND DNS via Syslog,InfoBlox NiOS via Syslog, Cisco Umbrella via AWS_S3,HTTPS_ADVANCED	Global System Reports Root Template
DNS Traffic Profile	This report baselines DNS traffic characteristics on a per client basis: sent and receive bytes and packets.	System	Traffic log from network devices and firewalls via syslog/netflow - FortiGate, Cisco IOS, Cisco ASA, Checkpoint FW-1, Palo Alto PAN-OS, Sonicwall etc.	Global System Reports Root Template
Failed User Logon Profile	This report baselines failed user logons at a host	System	Windows Security Log via OMI or FortiSIEM Agent, Linux via Syslog, FortiGate via Syslog, All other devices via Syslog	Global System Reports Root Template
Firewall Connection Count Profile	This report provides baseline of permitted firewall connection count	System	FortiGate via SNMP Monitoring, Cisco ASA Via SNMP Monitoring	Global System Reports Root Template
Firewall Denied Aggregate	This profile captures the amount of denied traffic and the		Traffic log from network devices and firewalls via	Global System Reports Root

機器學習基準線關聯分析 (ML Baseline Rules)

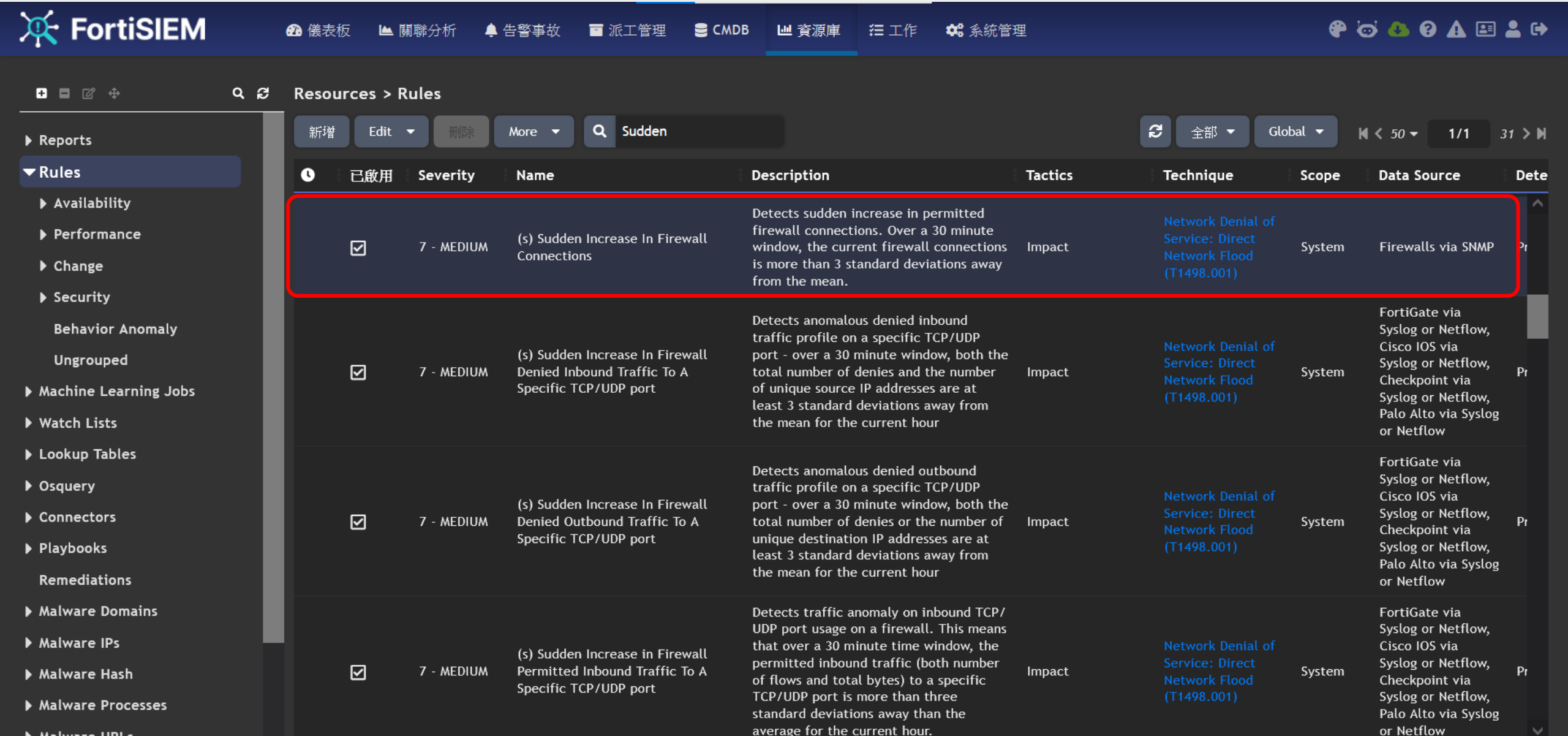
基準線統計偏差值資料



Profile Date Type	Hour Of Day	Host Name	Host IP	Avg Firewall Conn
1 (Work Day)	0	LAB-1500D	10.1.200.254	4816.79
1 (Work Day)	0	HOST-10.1.200.254	10.1.200.254	3091
1 (Work Day)	0	CoreFW	10.200.250.254	1224.67
1 (Work Day)	0	FGT51E	10.1.210.51	194.49
1 (Work Day)	1	LAB-1500D	10.1.200.254	4784.78
1 (Work Day)	1	CoreFW	10.200.250.254	1219.56
1 (Work Day)	1	FGT51E	10.1.210.51	195.16
1 (Work Day)	2	LAB-1500D	10.1.200.254	4784.69
1 (Work Day)	2	CoreFW	10.200.250.254	1217.06
1 (Work Day)	2	FGT51E	10.1.210.51	194.35
1 (Work Day)	3	LAB-1500D	10.1.200.254	4758.52
1 (Work Day)	3	CoreFW	10.200.250.254	1223.08
1 (Work Day)	3	FGT51E	10.1.210.51	196.14
1 (Work Day)	4	LAB-1500D	10.1.200.254	4708.3

機器學習基準線關聯分析 (ML Baseline Rules)

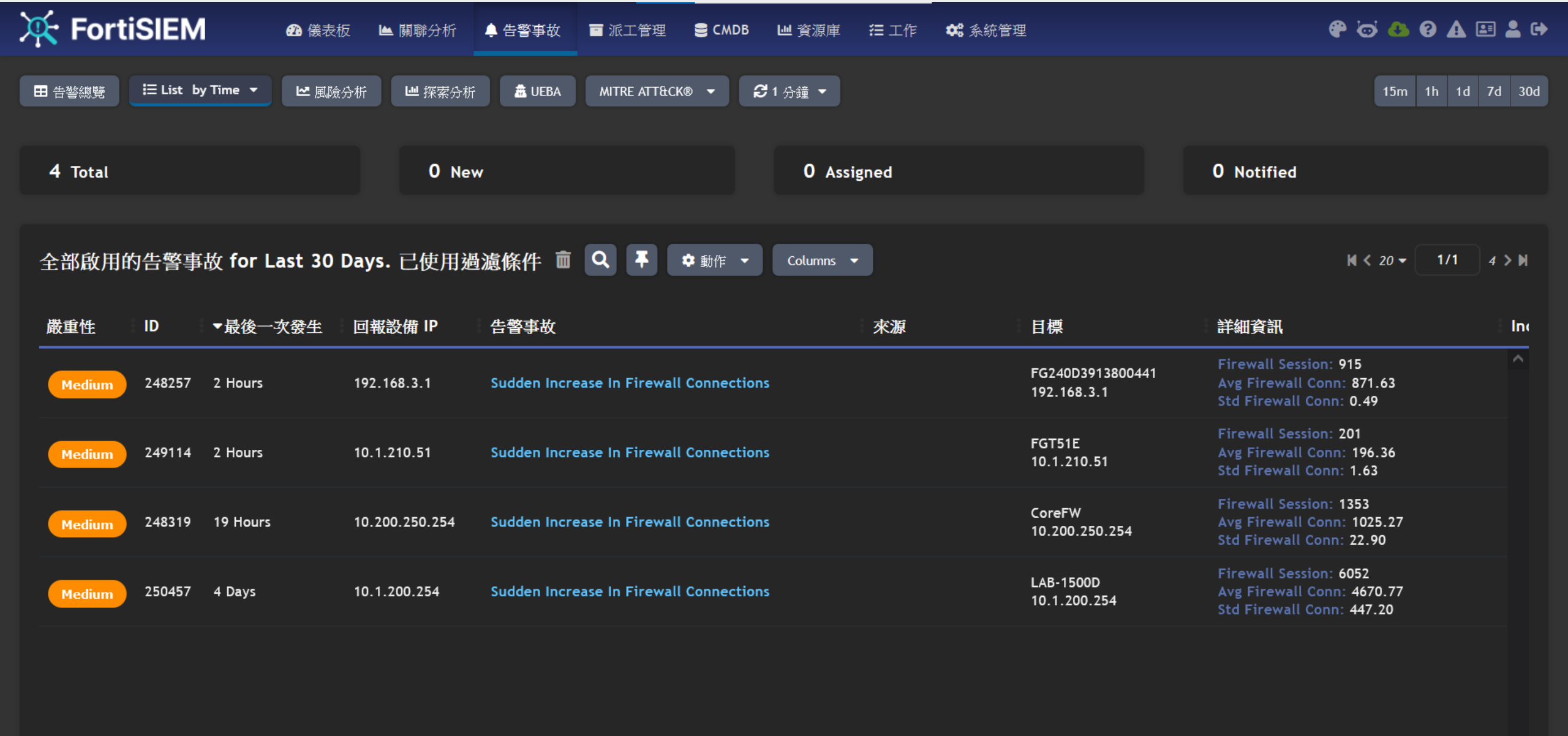
基準線關聯分析規則



已啟用	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Dete
☑	7 - MEDIUM	(s) Sudden Increase In Firewall Connections	Detects sudden increase in permitted firewall connections. Over a 30 minute window, the current firewall connections is more than 3 standard deviations away from the mean.	Impact	Network Denial of Service: Direct Network Flood (T1498.001)	System	Firewalls via SNMP	Pr
☑	7 - MEDIUM	(s) Sudden Increase In Firewall Denied Inbound Traffic To A Specific TCP/UDP port	Detects anomalous denied inbound traffic profile on a specific TCP/UDP port - over a 30 minute window, both the total number of denies and the number of unique source IP addresses are at least 3 standard deviations away from the mean for the current hour	Impact	Network Denial of Service: Direct Network Flood (T1498.001)	System	FortiGate via Syslog or Netflow, Cisco IOS via Syslog or Netflow, Checkpoint via Syslog or Netflow, Palo Alto via Syslog or Netflow	Pr
☑	7 - MEDIUM	(s) Sudden Increase In Firewall Denied Outbound Traffic To A Specific TCP/UDP port	Detects anomalous denied outbound traffic profile on a specific TCP/UDP port - over a 30 minute window, both the total number of denies or the number of unique destination IP addresses are at least 3 standard deviations away from the mean for the current hour	Impact	Network Denial of Service: Direct Network Flood (T1498.001)	System	FortiGate via Syslog or Netflow, Cisco IOS via Syslog or Netflow, Checkpoint via Syslog or Netflow, Palo Alto via Syslog or Netflow	Pr
☑	7 - MEDIUM	(s) Sudden Increase in Firewall Permitted Inbound Traffic To A Specific TCP/UDP port	Detects traffic anomaly on inbound TCP/UDP port usage on a firewall. This means that over a 30 minute time window, the permitted inbound traffic (both number of flows and total bytes) to a specific TCP/UDP port is more than three standard deviations away than the average for the current hour.	Impact	Network Denial of Service: Direct Network Flood (T1498.001)	System	FortiGate via Syslog or Netflow, Cisco IOS via Syslog or Netflow, Checkpoint via Syslog or Netflow, Palo Alto via Syslog or Netflow	Pr

機器學習基準線關聯分析 (ML Baseline Rules)

基準線關聯分析產生告警



FortiSIEM AI 與機器學習功能

與生成式 AI 整合
AI for Operation

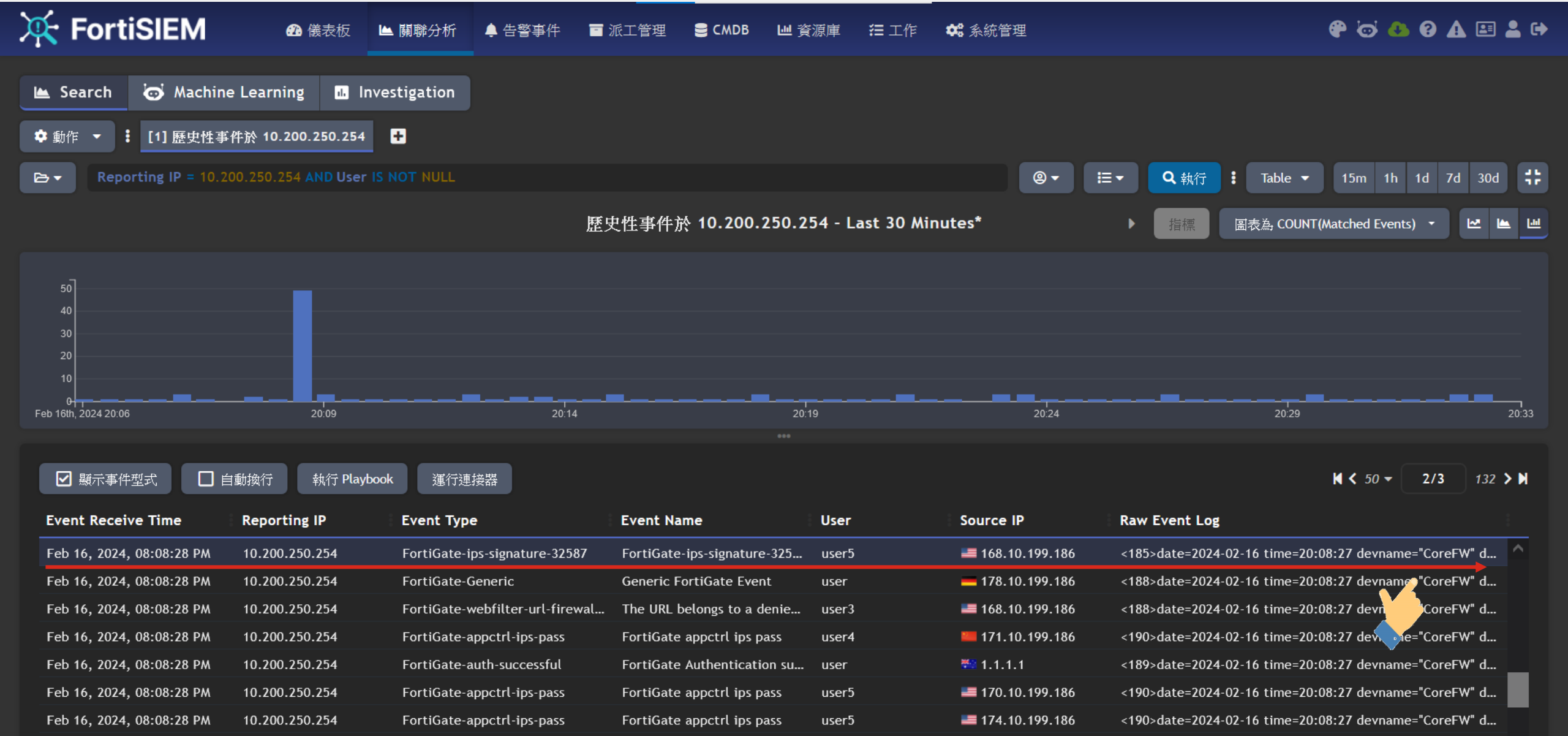
AI for 日常智能維運

- ✓ 整合 OpenAI (ChartGPT in FortiSIEM)
- ✓ 互動式問答，分析師日常維運輕鬆尋求 AI 助理協助
- ✓ 查詢會遮蓋敏感資料，保護重要資訊不外洩

© Fortinet Inc. All Rights Reserved.

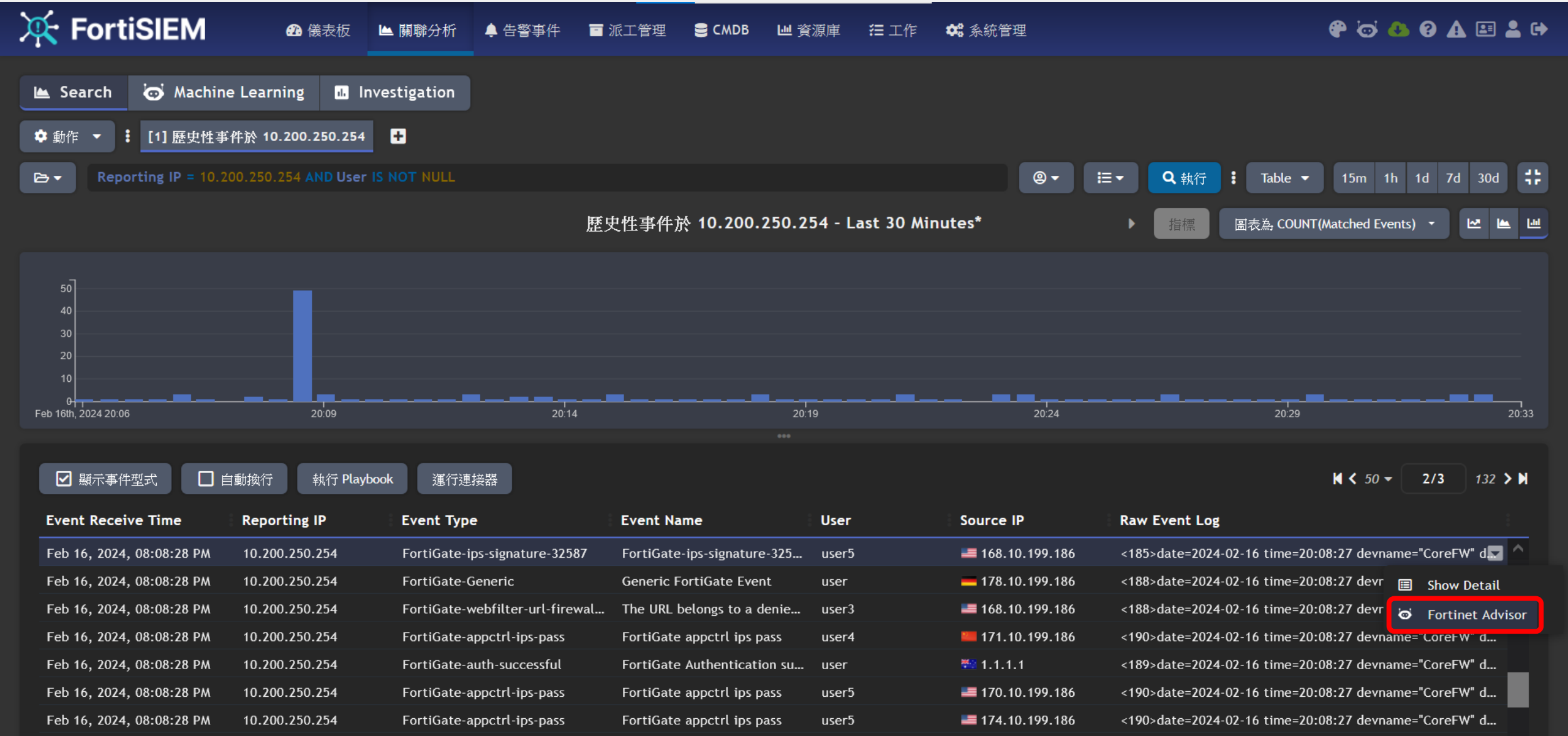
FortiSIEM 結合 FortiAI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？



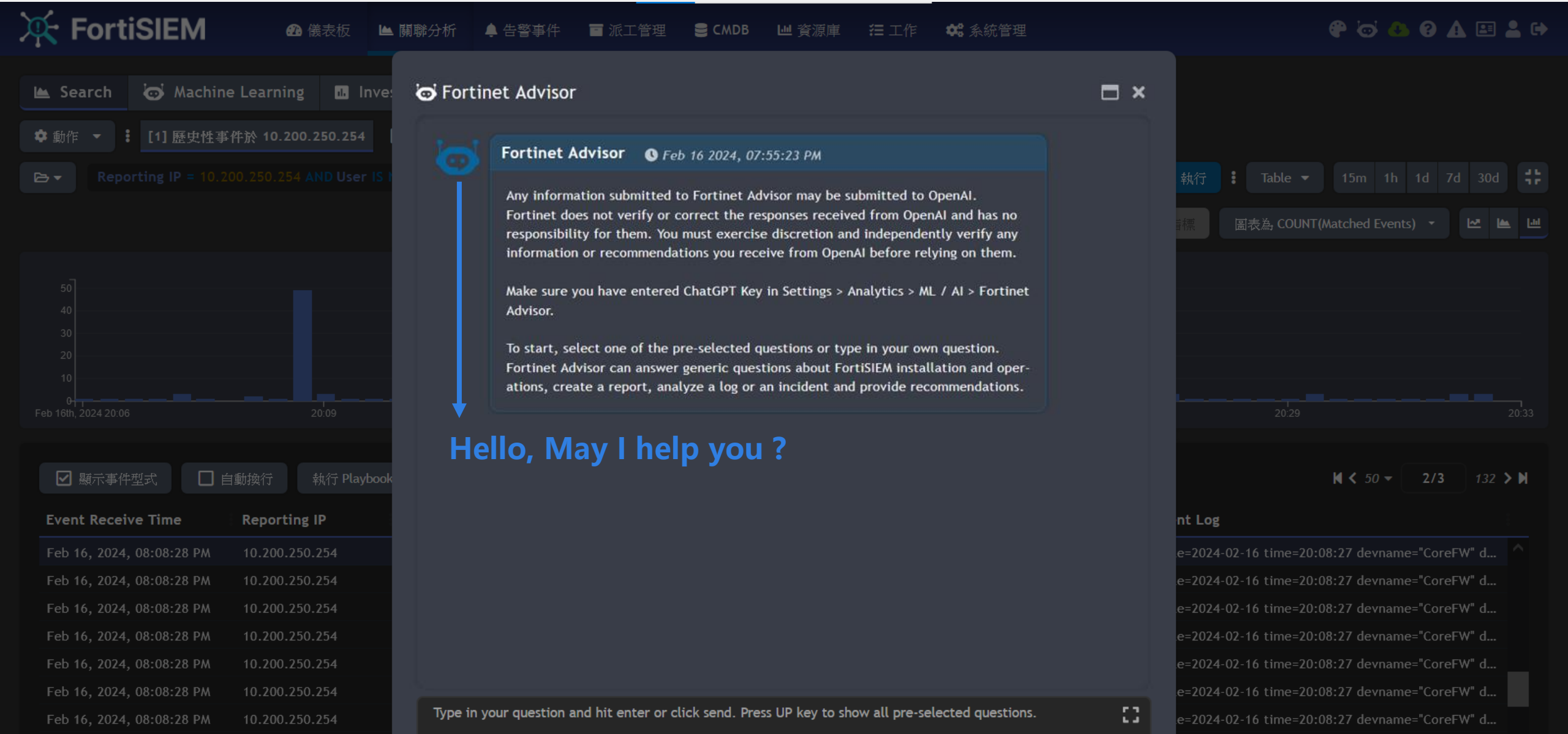
FortiSIEM 結合 FortiAI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？



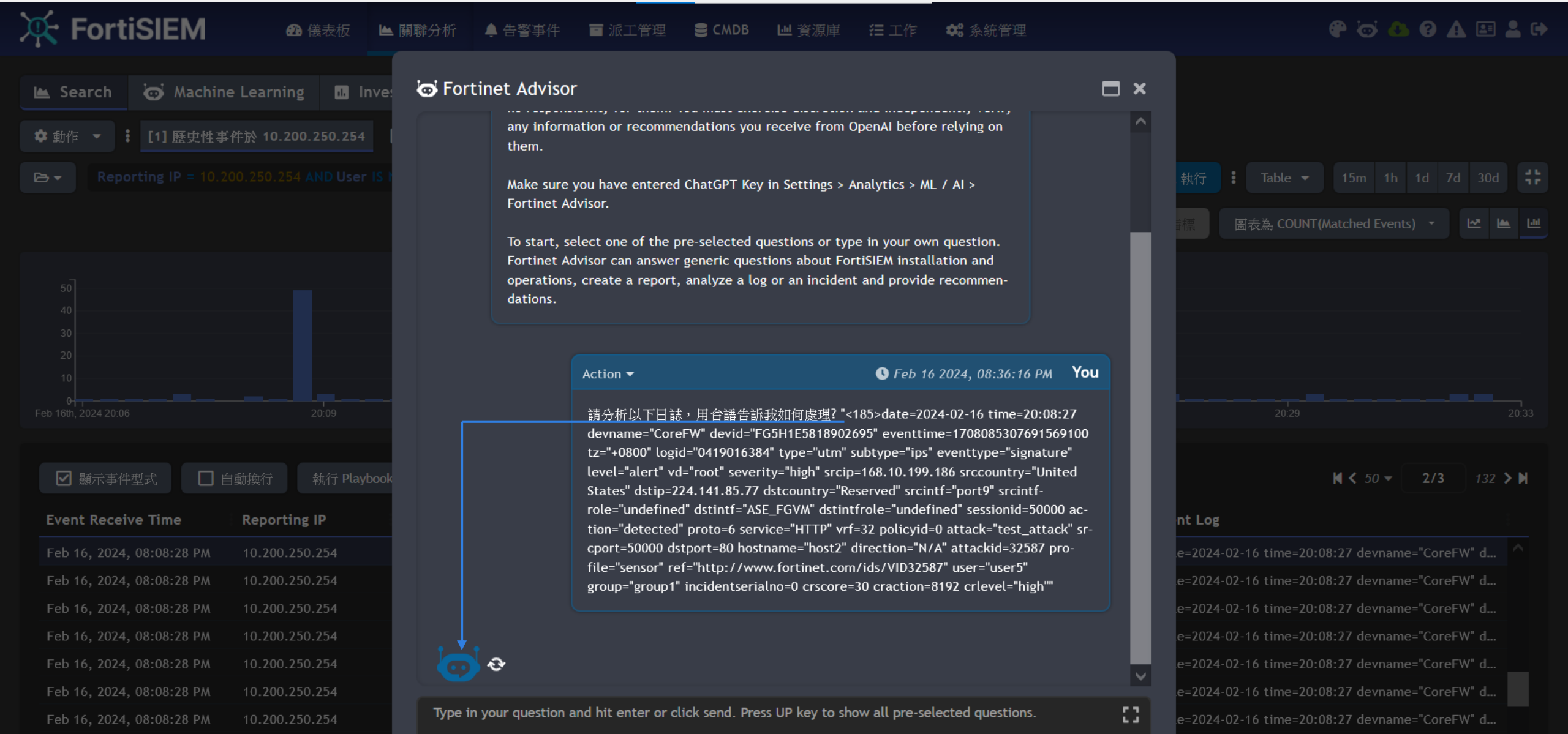
FortiSIEM 結合 FortiAI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？



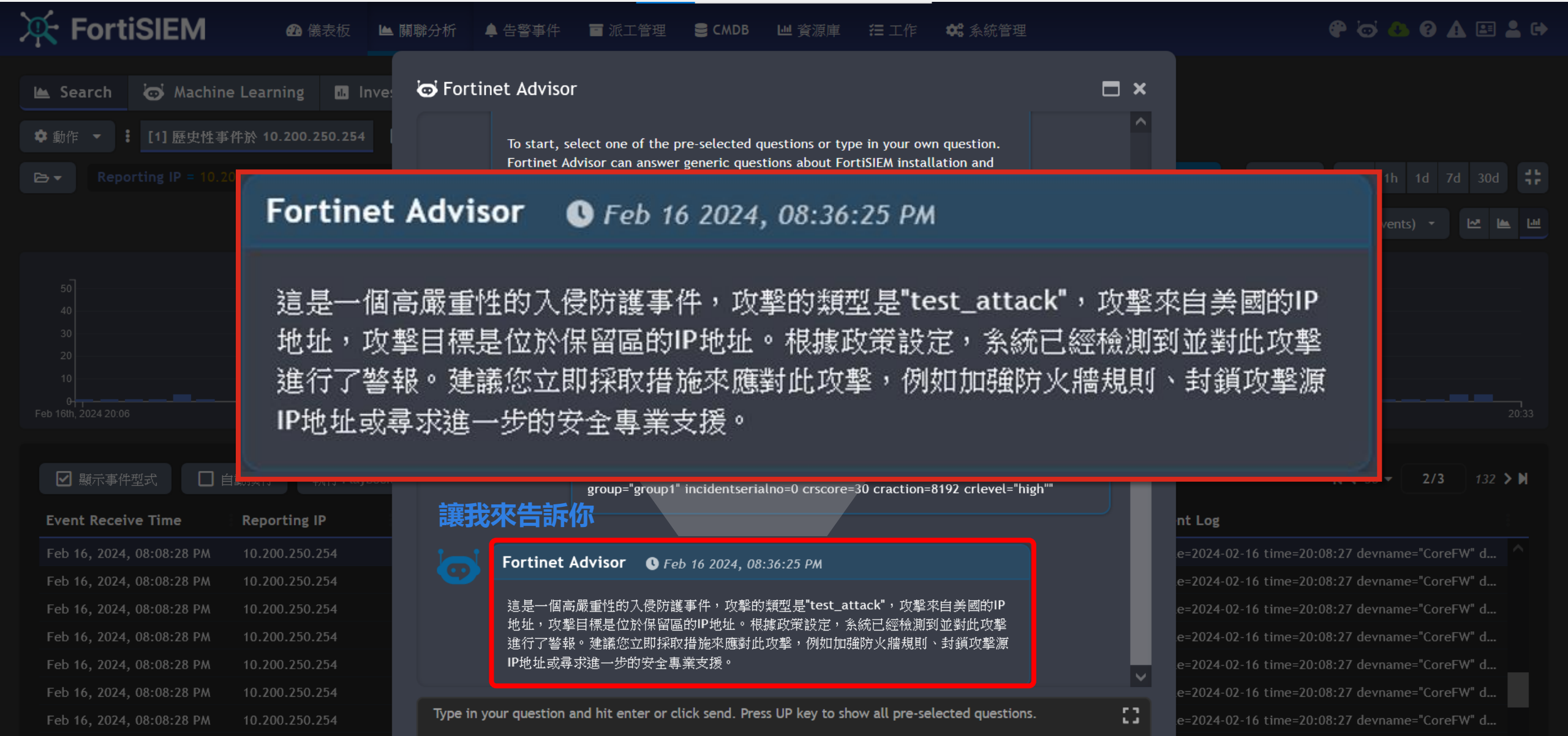
FortiSIEM 結合 FortiAI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？



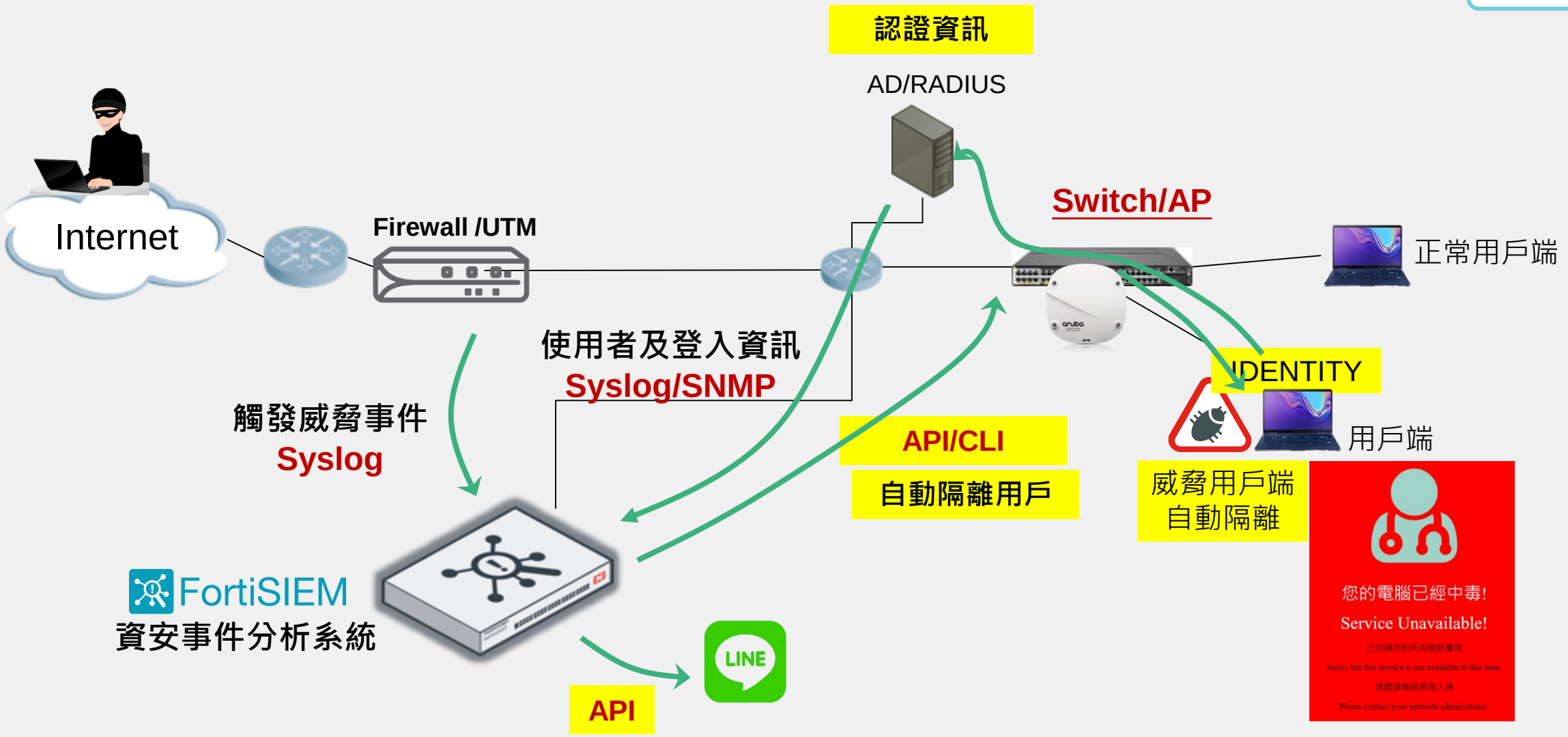
FortiSIEM 結合 FortiAI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？



協作聯防與回應自動化 (SOAR)

FortiSIEM 資安聯防協作自動回應處理示意圖



© Fortinet Inc. All Rights Reserved.

FortiSIEM 重要特點與價值

資料統整、威脅偵測、維運監看、事故回應一氣呵成

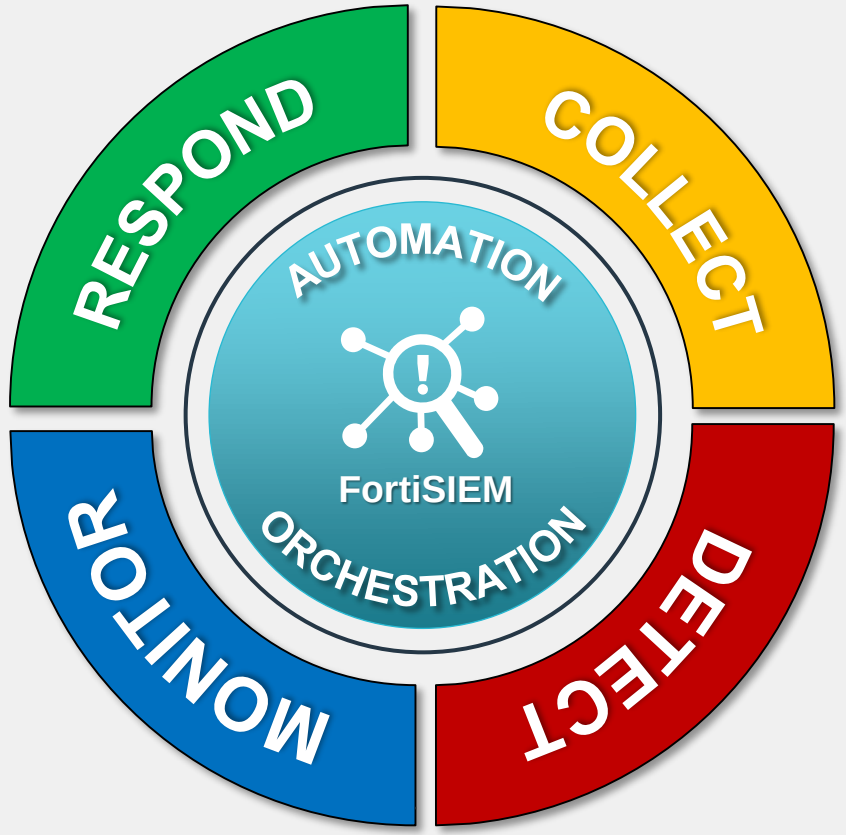
各種資訊匯集統整，日誌稽核，合規報表，安全資訊與事件管理 (SIEM)

還可作為資安/網維管理的優化工具

AI / ML 智能關聯分析，對應 MITRE 資安框架，提供威脅先期預警能力

資安/網維戰情室儀表板提供更好的可視性

內建派工管理，連動跨品牌的設備，滿足自動化回應、協作聯防 (SOAR) 需求



© Fortinet Inc. All Rights Reserved.

FORTINET