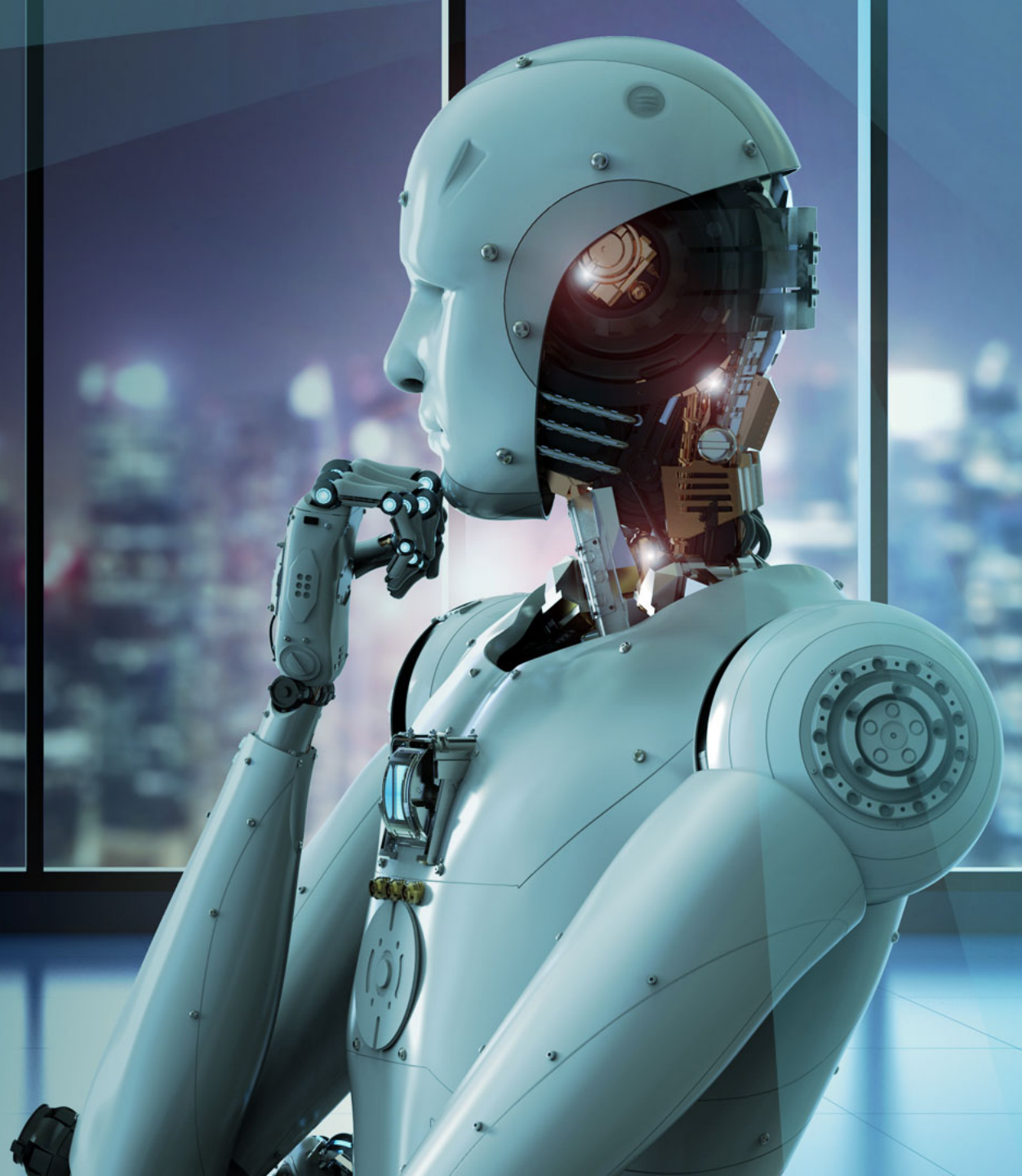
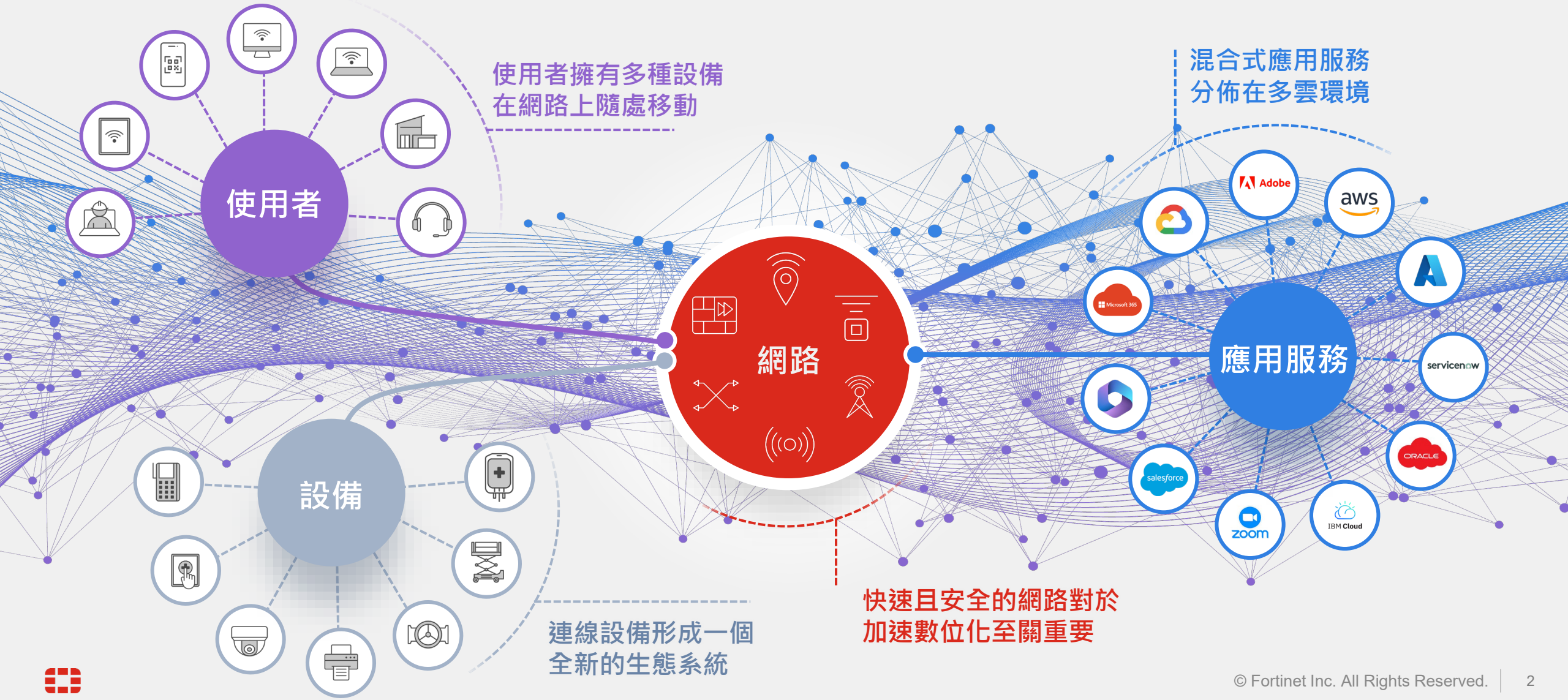
AI 驅動的安全運營



Marty Chang
Fortinet 技術顧問
mchang@fortinet.com

當網際網路變得越趨複雜...

駭客攻擊已成家常便飯



網路面臨的挑戰

微分割讓網路營運變得複雜

人工營運繁瑣

缺乏可視性

找出根本原因

企業受到的衝擊

時間的浪費

部門將時間花在繁瑣的工作上，而非戰略性計畫

失去生產力

員工花時間處理網路問題

造成金錢的損失

網路營運常面臨的挑戰

營運團隊

需要高度專業技術的
調查和耗時的修復

- 數據過多，無法監控
- 需要跨有線、無線和 SD-WAN 領域的專業知識
- 耗時的故障排除過程
- 問題的分類，在不同領域和情境下有所不同
- 效能不佳的線路服務

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。

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

FortiAIOps 效益

AIOps + Ops Team

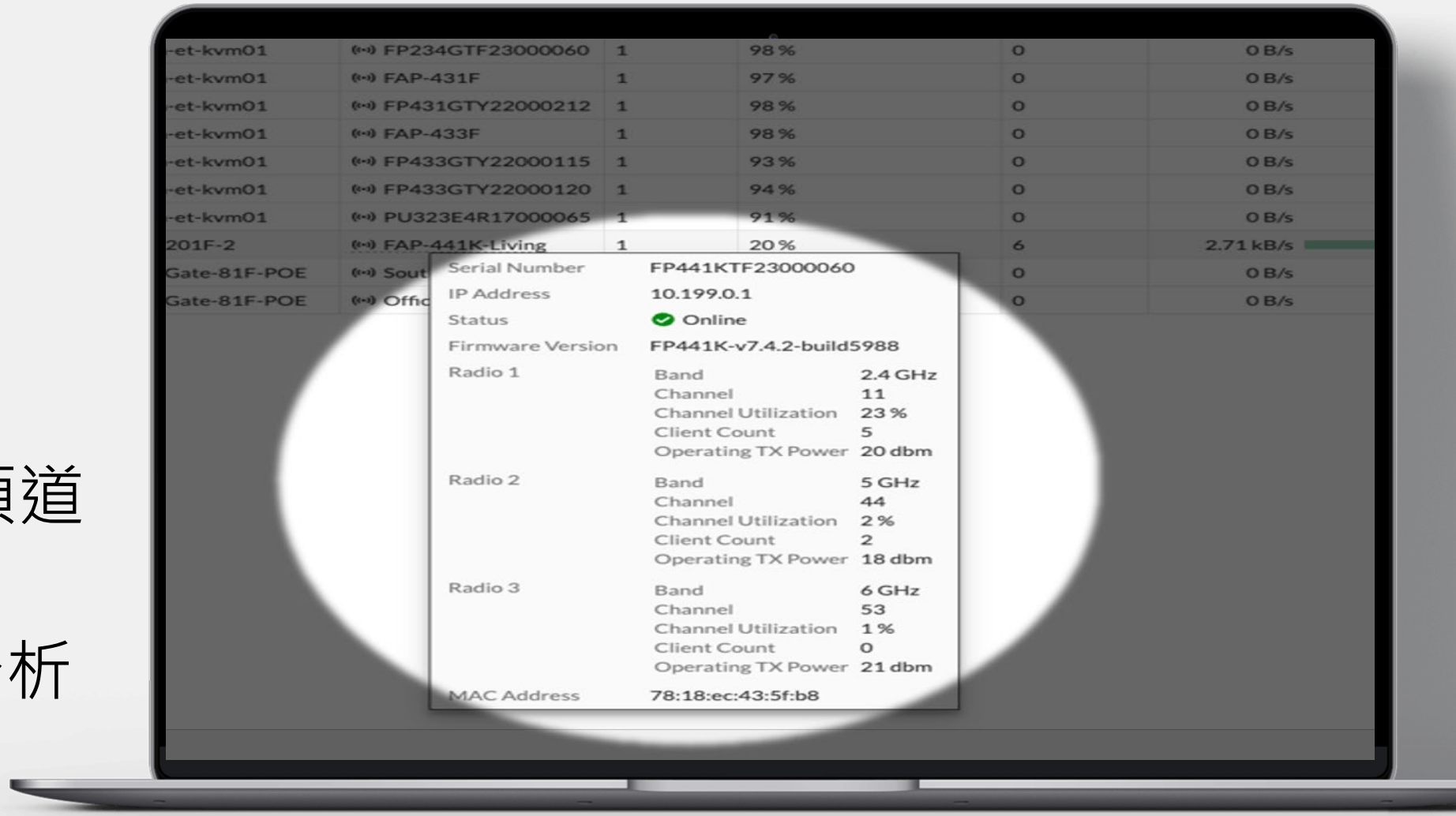
輕鬆的分析各個網路節點資料
建立網路流量基準線
提供最佳的改善方案

- 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

FortiAIOps

無線訊號統計資料

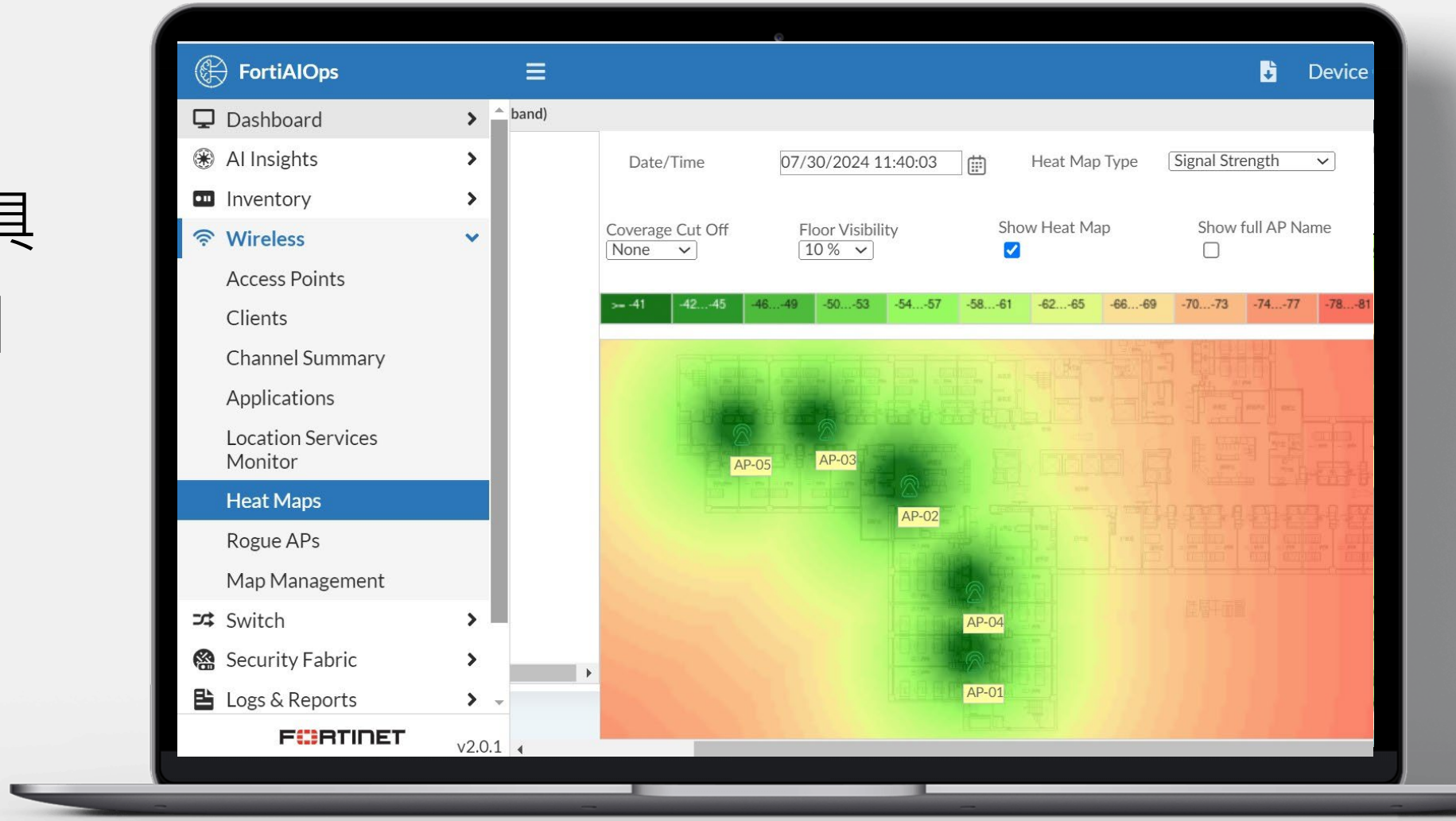
- 無線趨勢分析
  - 頻道使用率
  - 雜訊程度
  - 流量統計
- 整體無線網路頻道使用率
- 單一 AP 深入分析



FortiAIOps

Map Management – RF Planner

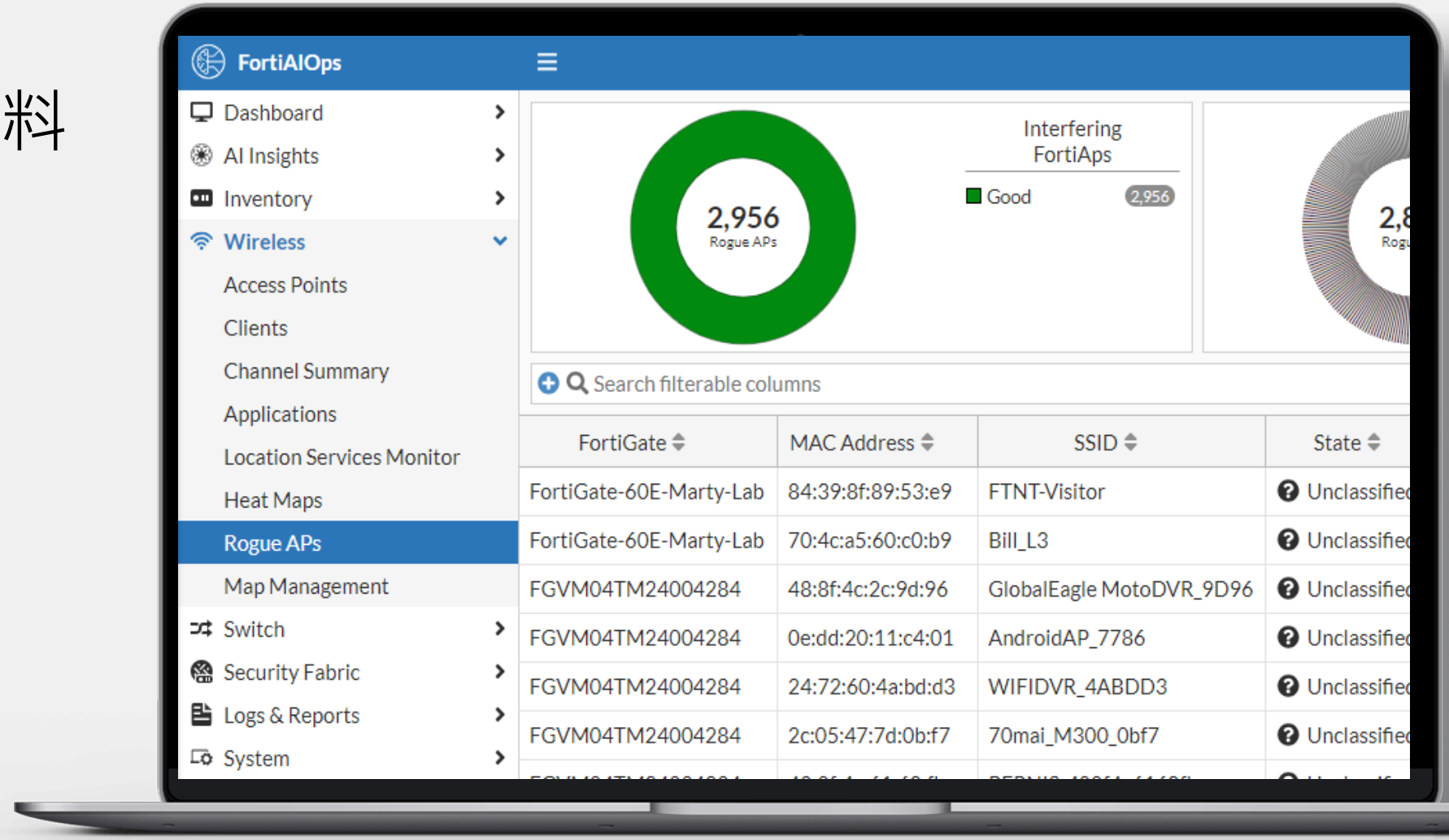
- 無線網路 Site-Survey 工具
- 無線網路熱感圖

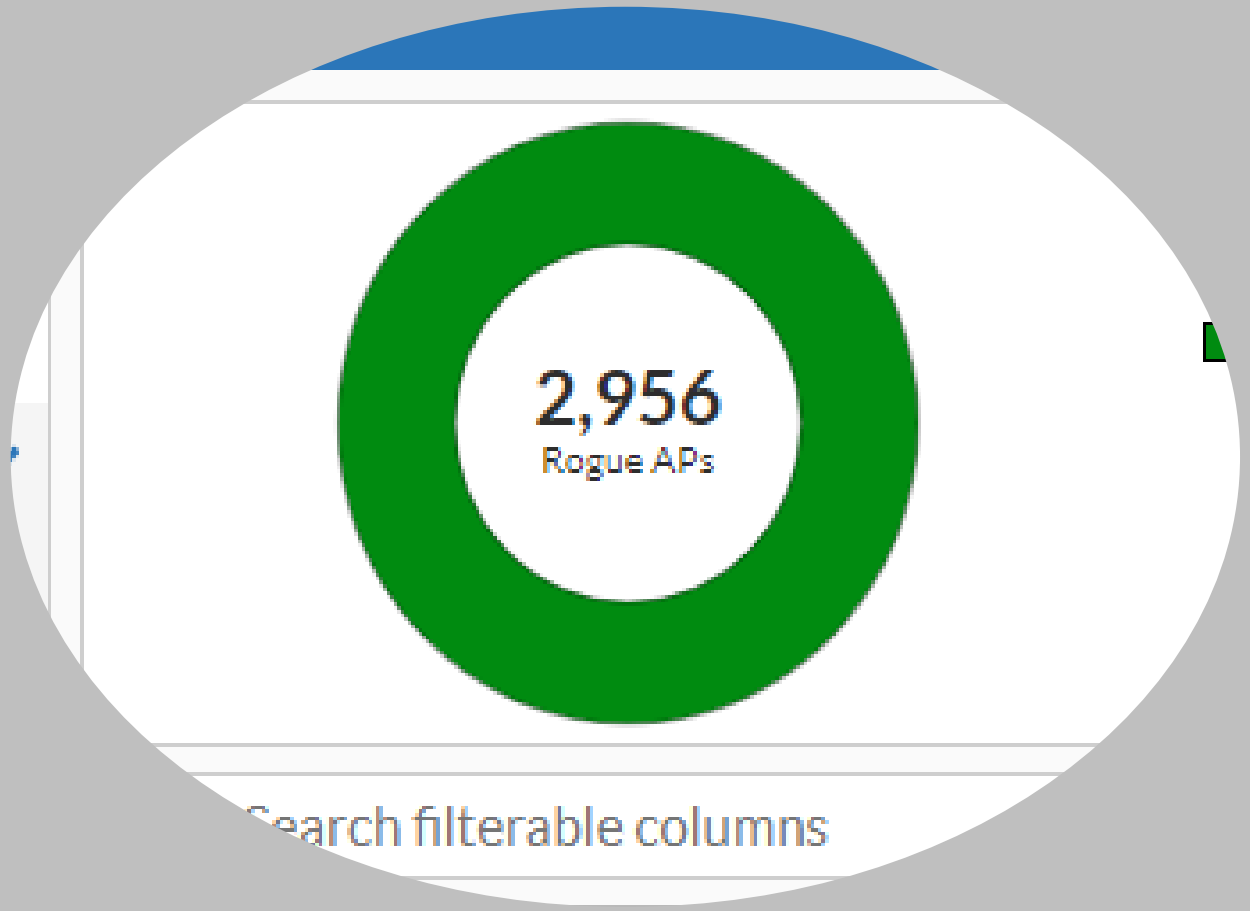


FortiAIOps

Monitoring – Rouge APs

- 干擾 AP 統計資料





附近干擾 AP 高達 2900 多個

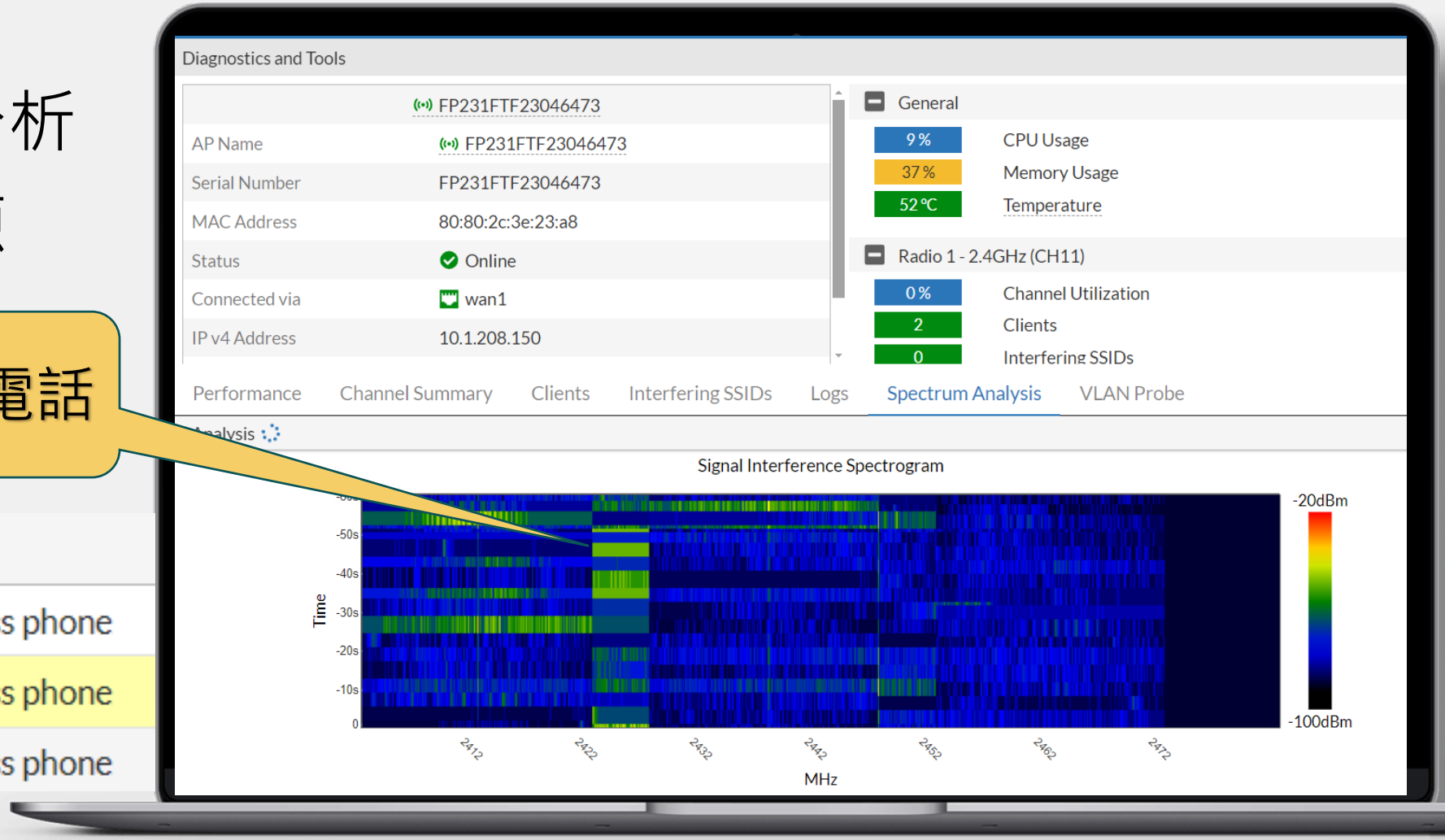
FortiAIOps

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

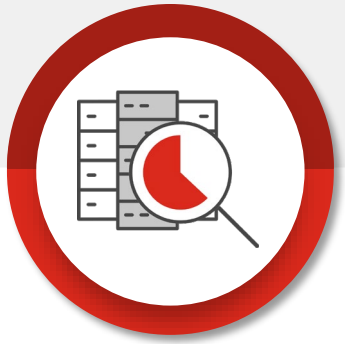
Frequency	Type
2402	WiFi, DSSS cordless phone
2427	WiFi, DSSS cordless phone
2452	WiFi, DSSS cordless phone



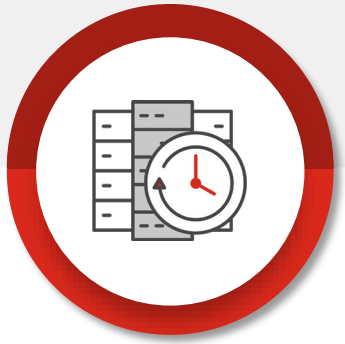
FortiAIOps

AI / 機器學習基準線的建立

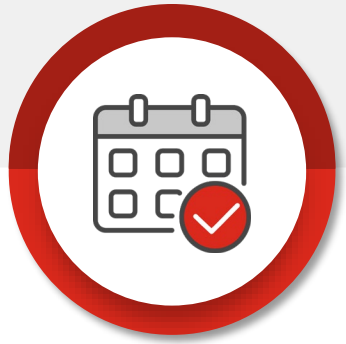
自動收集
FortiGate
FortiSwitch
FortiAP
SD-WAN
使用資訊



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

AI / 機器學習

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

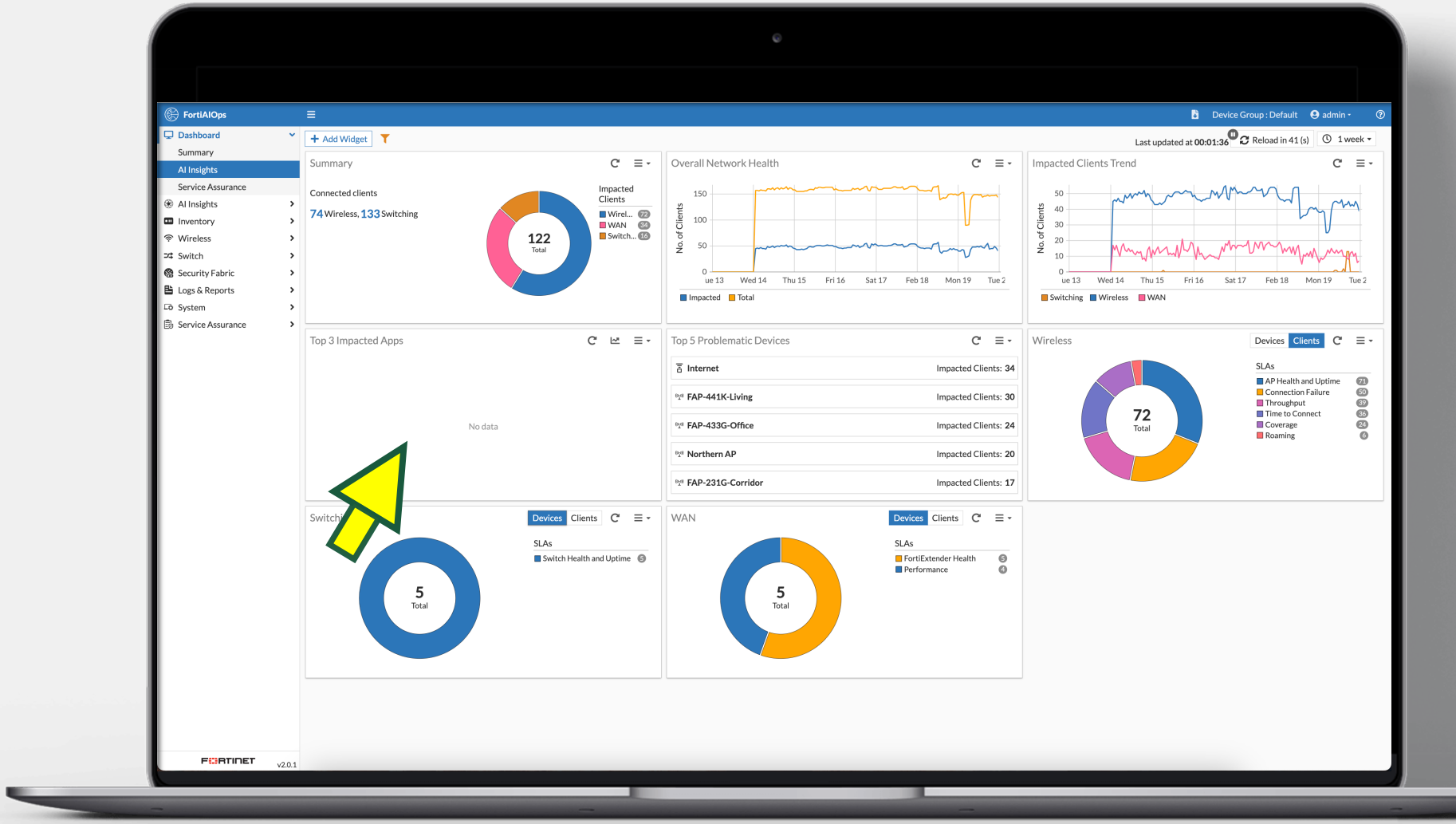
傳統方式解決問題

費時又費力，需要跨有線、無線和 SD-WAN 領域的專業知識

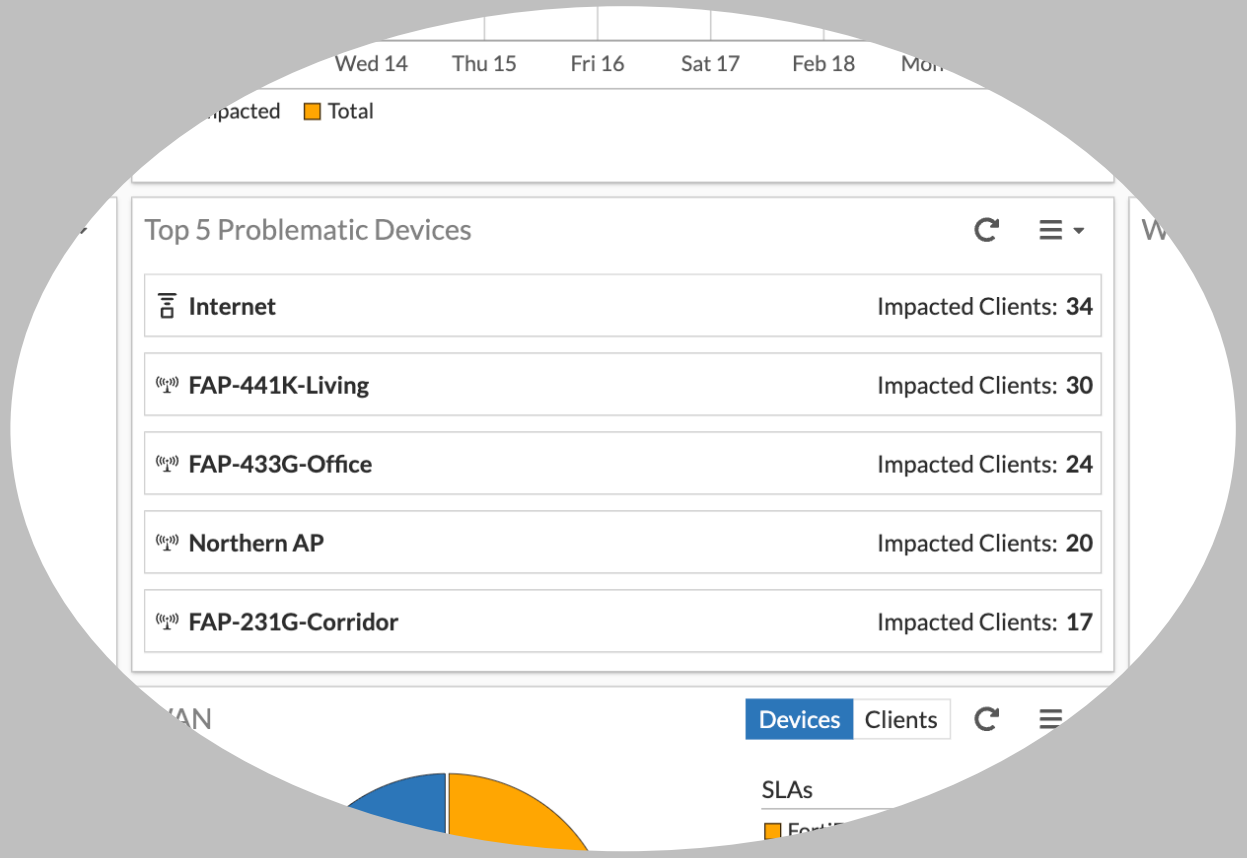
透過 AI 解決問題

省時又省力，AI 直擊問題核心

- 透過點擊滑鼠
- 快速找到問題



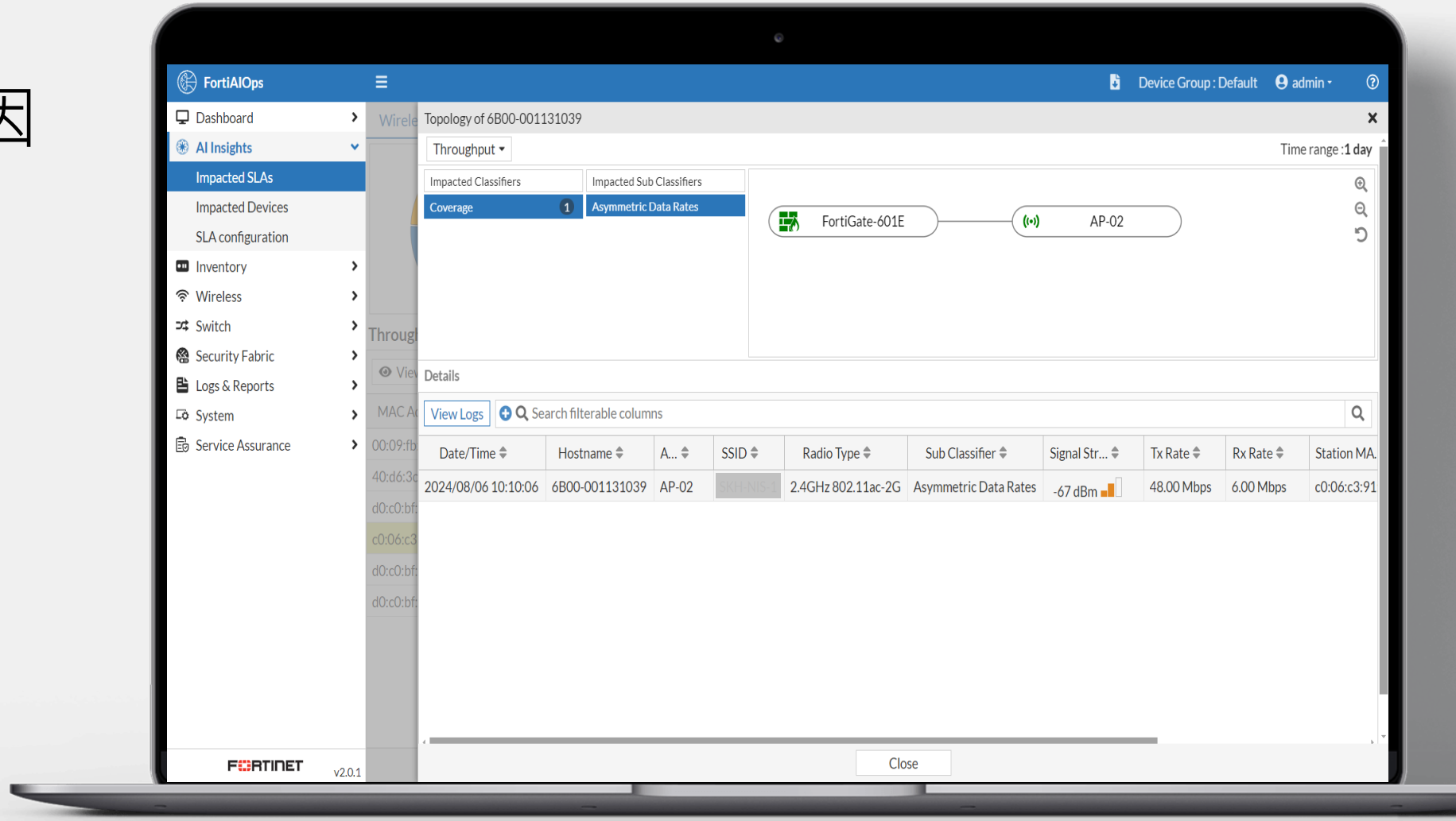
找出受影響的使用者


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

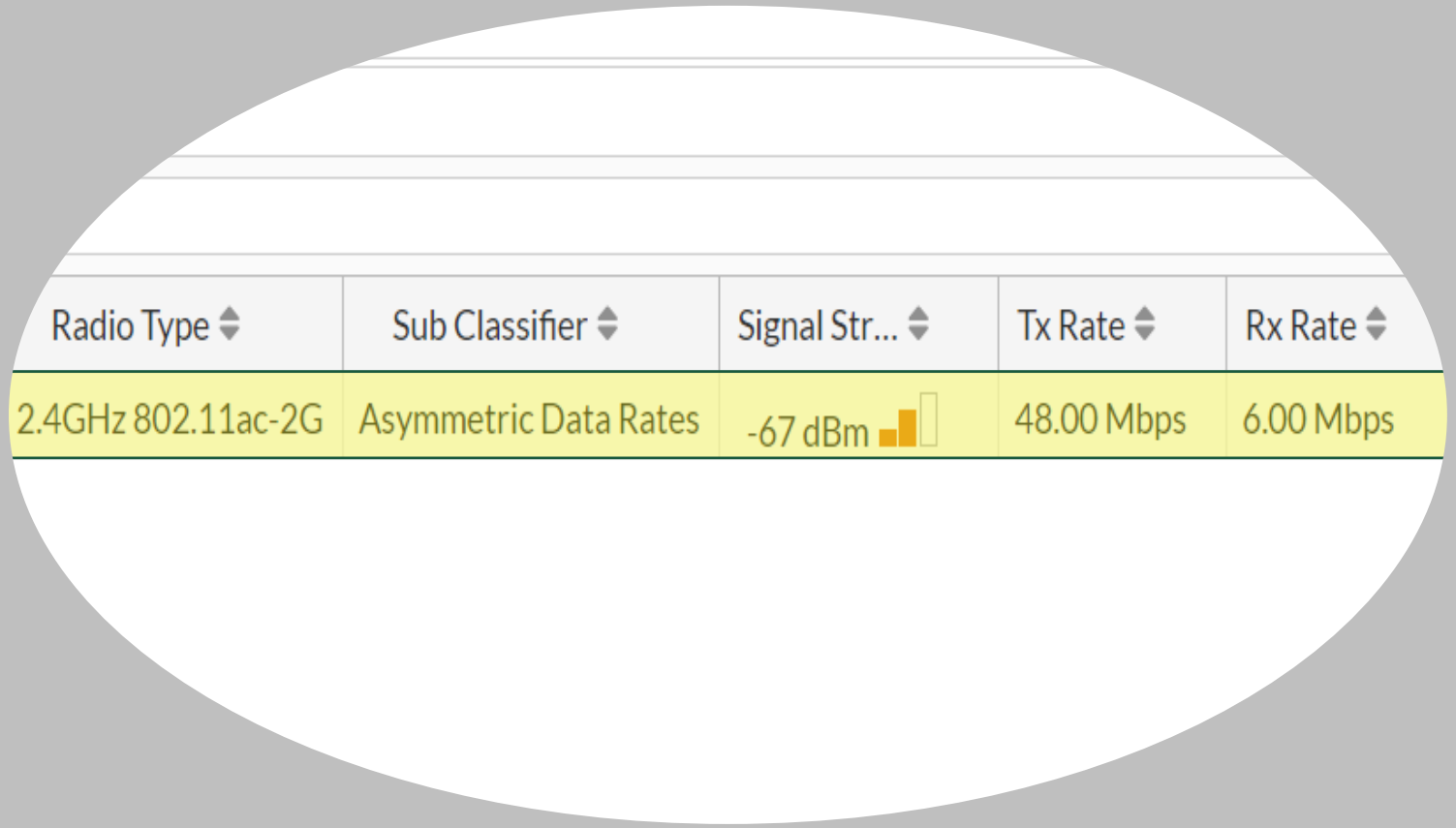
FortiAIOps

找出連線速度慢的問題

- 透過 AI 判斷原因



AI 自動判斷：無線訊號傳送速率不對等

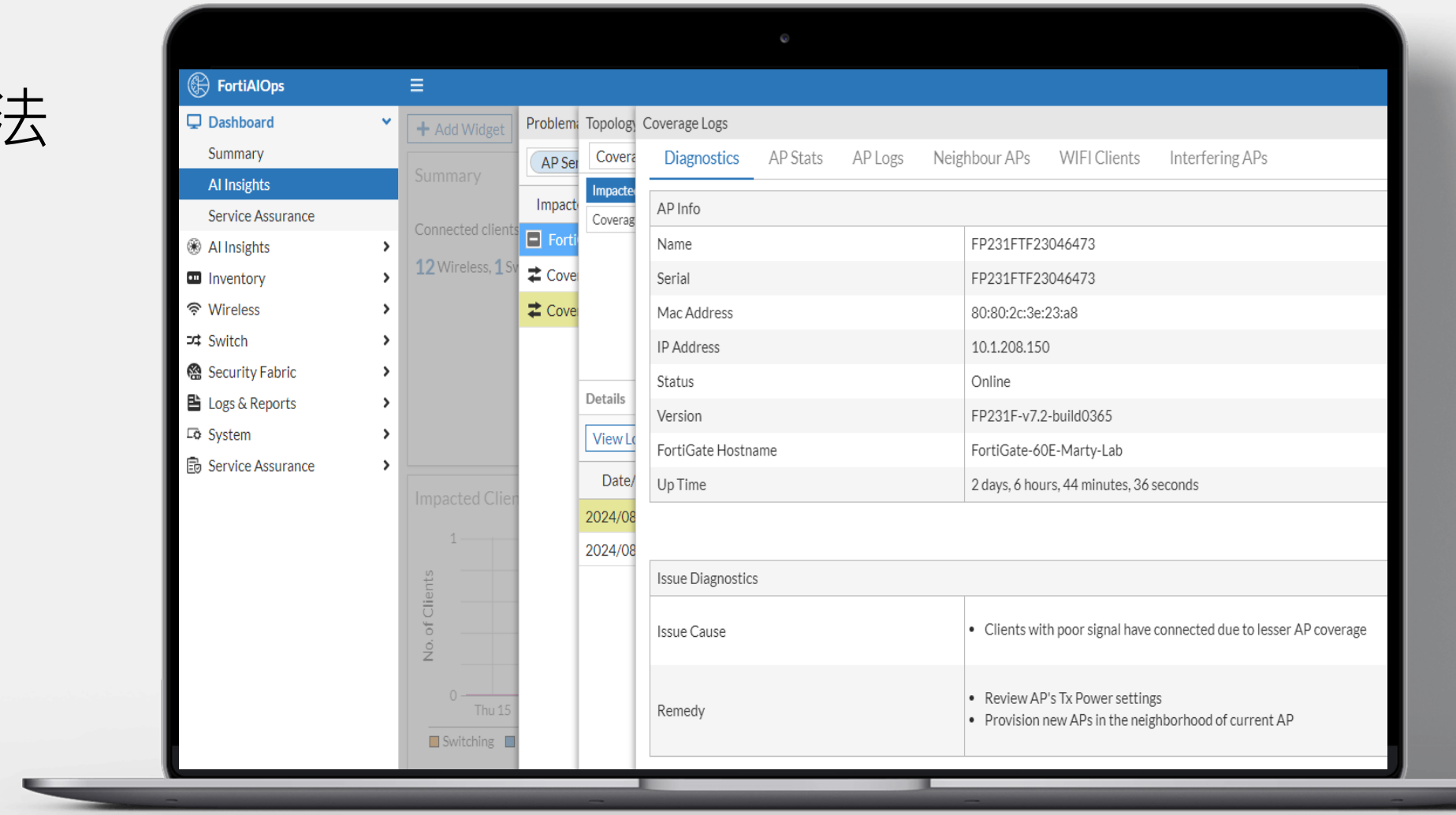


Radio Type	Sub Classifier	Signal Str...	Tx Rate	Rx Rate
2.4GHz 802.11ac-2G	Asymmetric Data Rates	-67 dBm	48.00 Mbps	6.00 Mbps

FortiAIOps

找出連線速度慢的問題

- 利用 AI 提供解法



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

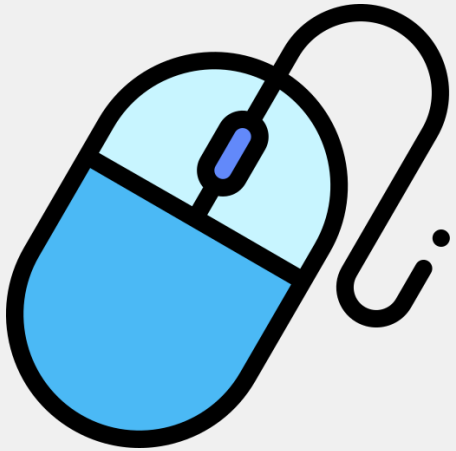
Ella：今天無線卡卡的耶!

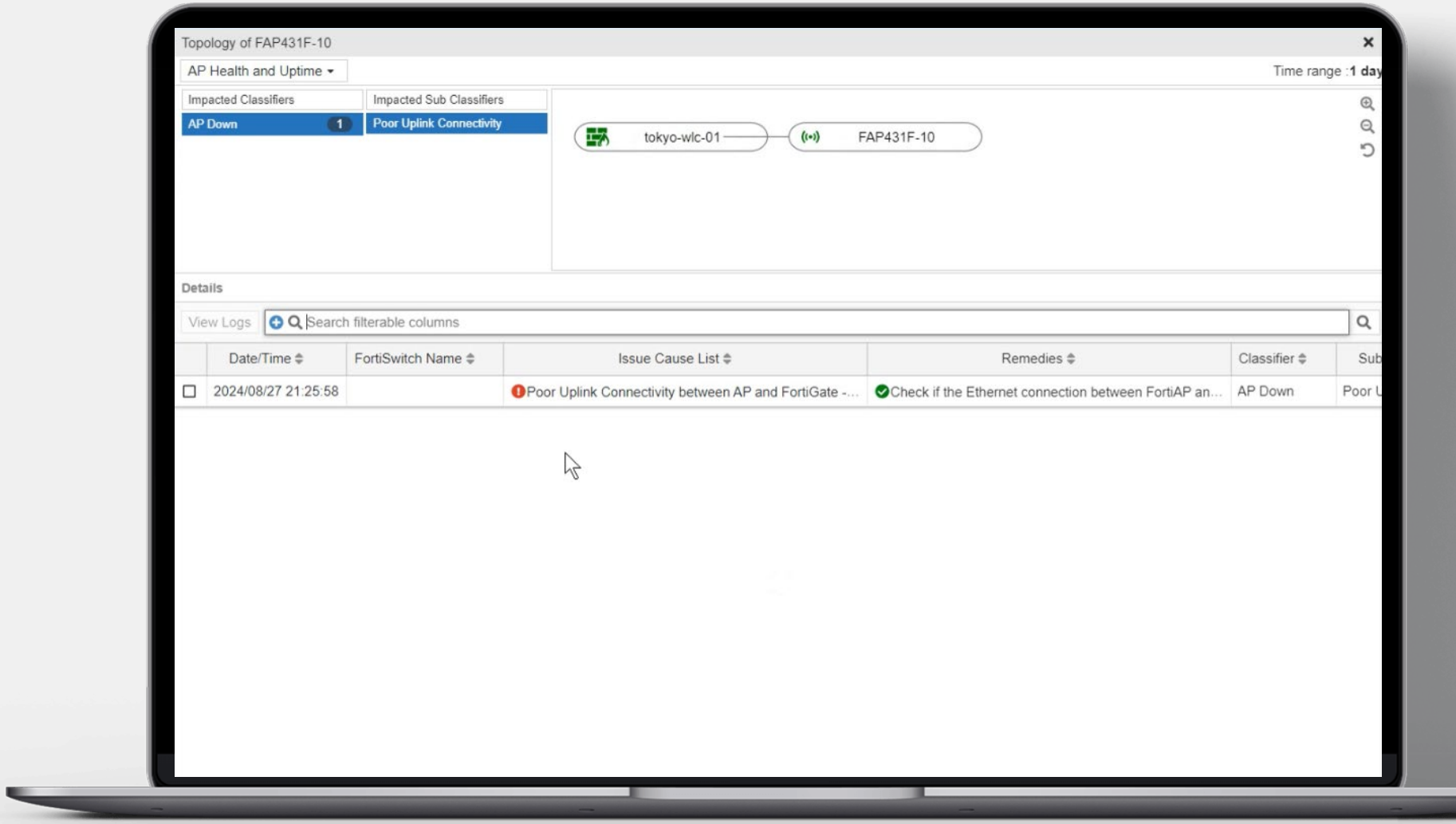
您好，這裡是控八控控–控控控

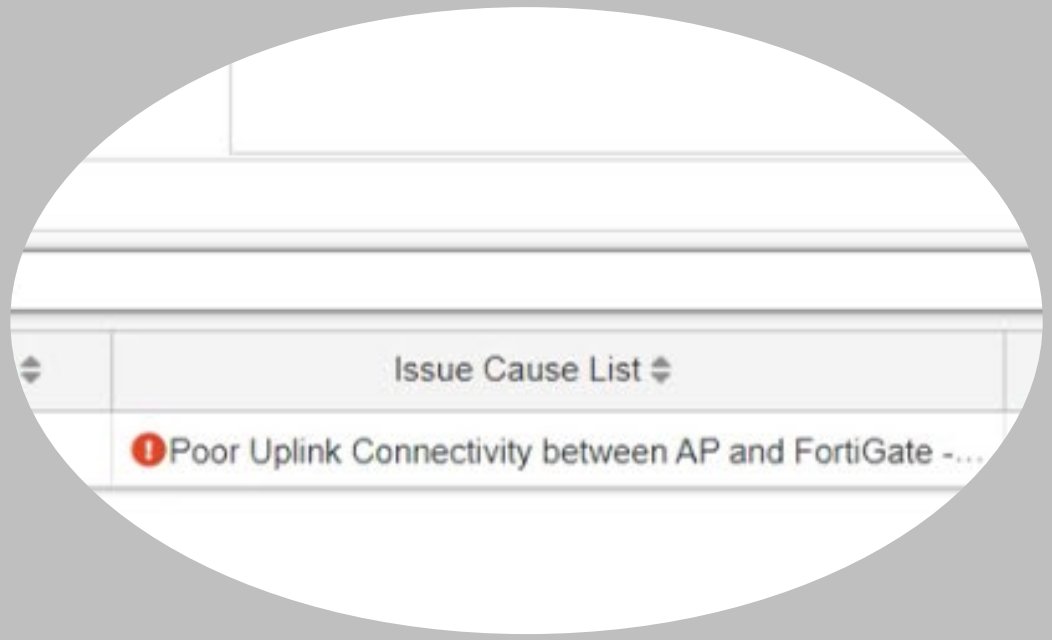
FortiAIOps

找出有線網路問題

- 透過 AI 判斷原因





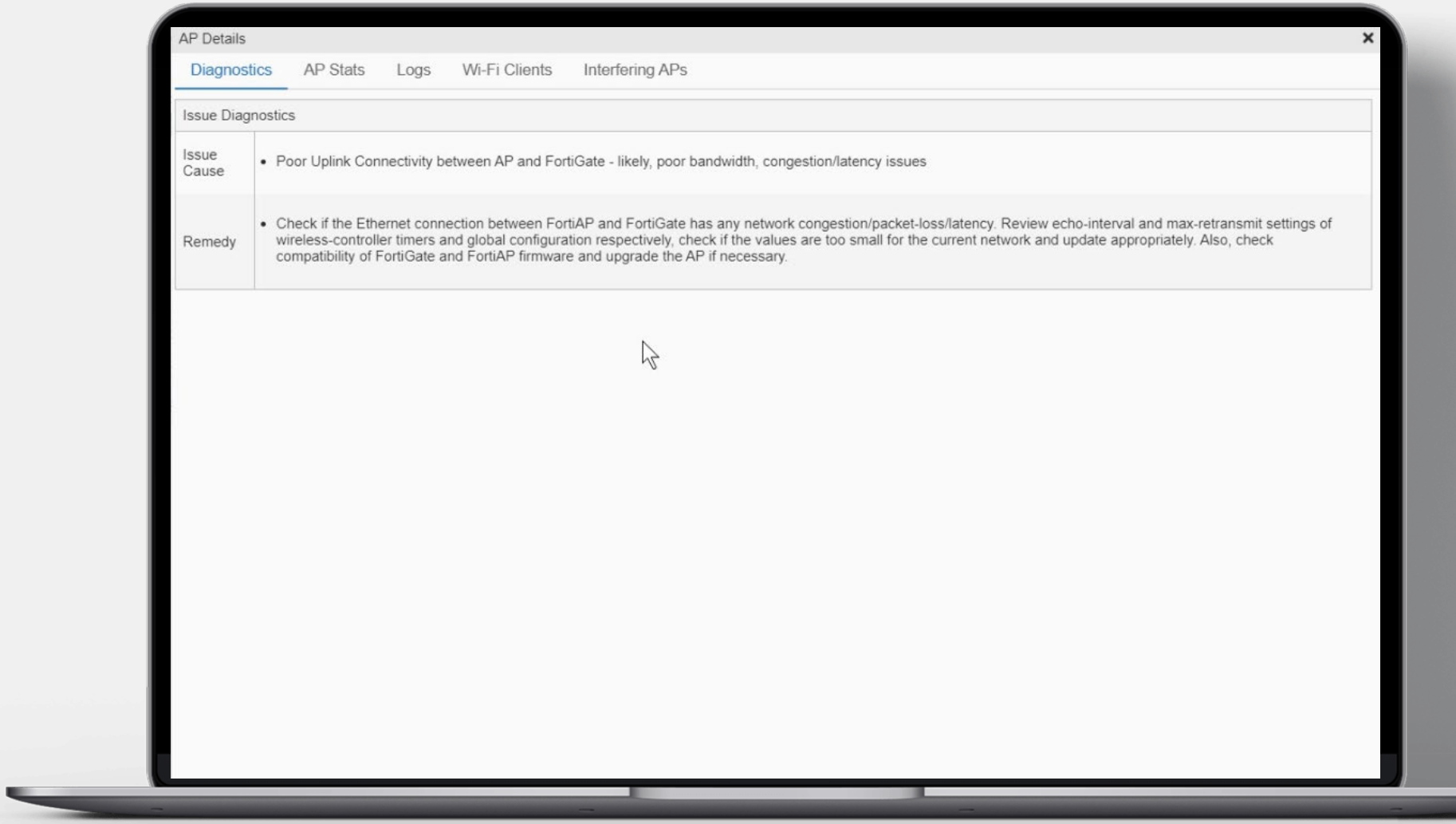


AI 自動判斷：AP 與控制器中間的線路不良

FortiAIOps

找出有線網路問題

- 利用 AI 提供解法



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

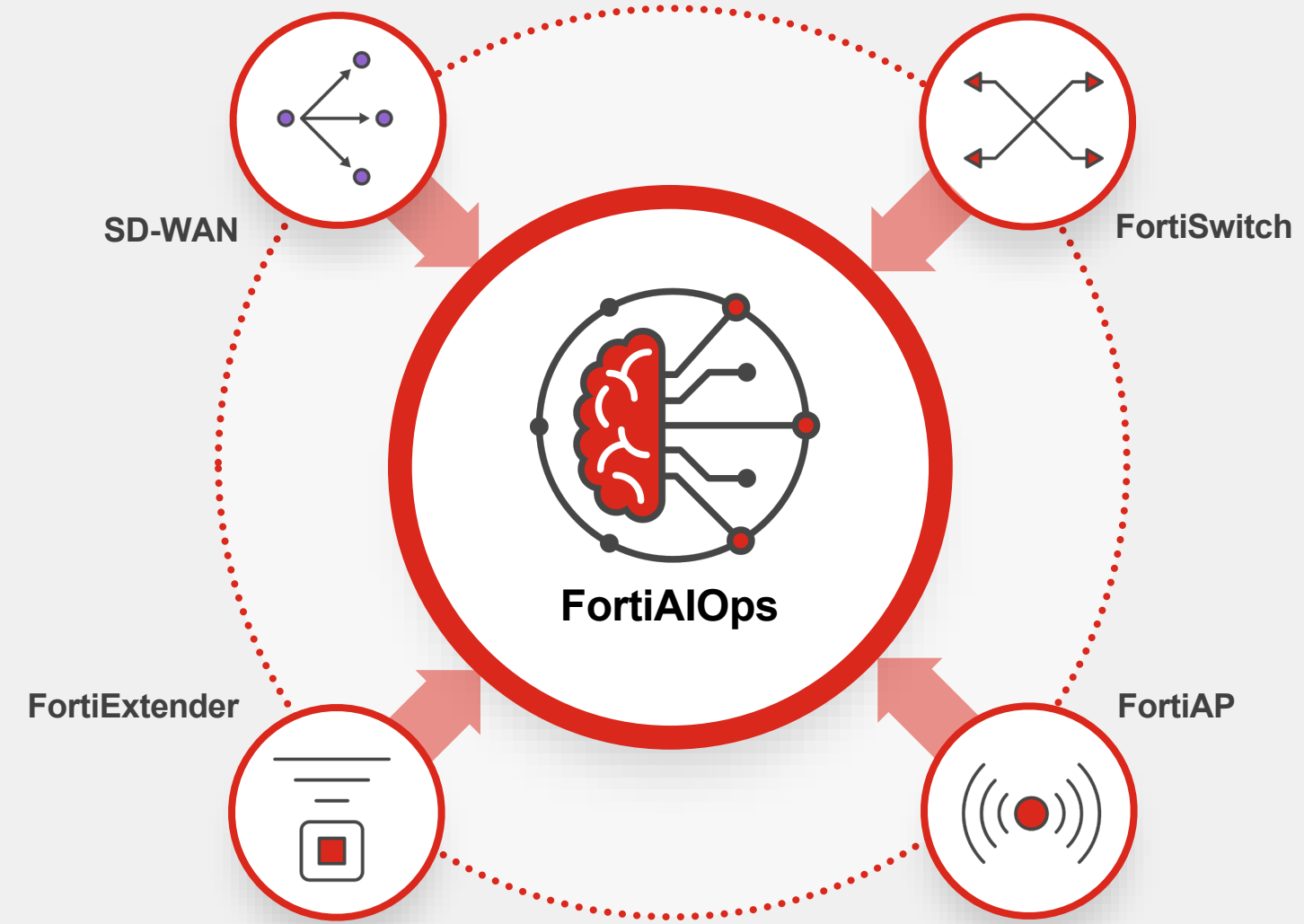
- 趨勢分析 / 歷史基準線
- 網路流量可視化

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

這樣就夠了嗎？

各行業都有害怕遇到的情況

醫生驚治嗽

總鋪驚呷午

做土水驚抓漏

做 IT 驚抓慢

FortiAI Demo

INVESTIGATE ACTION

Retrieve incident for slow server

Hi there, please retrieve the incident for the slow server.

FortiAI, 幫我個忙，請協助分析導致 Server 運行緩慢的事件

FortiAnalyzer 7.6

Hello! I found an incident related to the issue you mentioned.

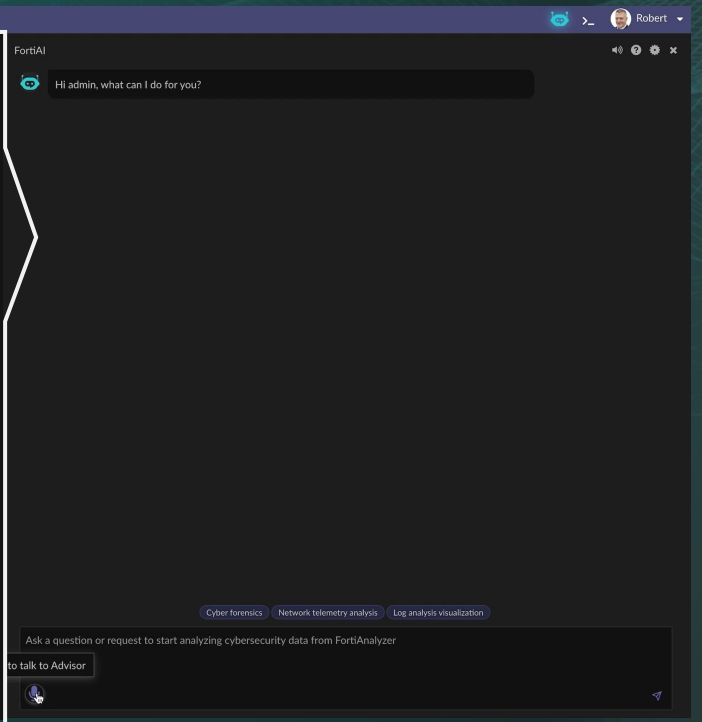
This incident IN00000011 involves the file backup server at IP address 172.16.88.23, categorized as "Malicious Code" with a high severity level. The reported issue is that the server is running slow.

Would you like to check more details about this particular endpoint? I can provide additional information and offer a FortiAnalyzer playbook via FortiClient EMS connector for further investigation.

Note: Ensure that the FortiClient EMS connector is properly configured for seamless integration.

您好！我找到了一個與此問題相關的 Server 事件

- 這個事件 (編號IN00000011) **涉及 IP=172.16.88.23 的文件備份 Server，分類為「惡意代碼 Mailicous Code」，嚴重等級為高嚴重性。**
- **此事件報告指出，這個 Backup Server 運行緩慢。**
- 您是否想查看此 Server 的更多詳細信息?
- 我可以提供更多信息，並通過 FortiClient EMS 連接器提供 FortiAnalyzer 聯動運作以進一步調查此事件。



FortiAI Demo

INVESTIGATE | ACTION

- Retrieve incident for slow server
- Run FortiClient playbook

Yes, please run the FortiClient playbook.

好的，那你幫我執行該 Server 上的 FortiClient 自動化腳本

FortiAnalyzer 7.6

➢ Server 效能概覽:

Server IP	Process	CPU Usage
172.16.88.23	qcloud	98%

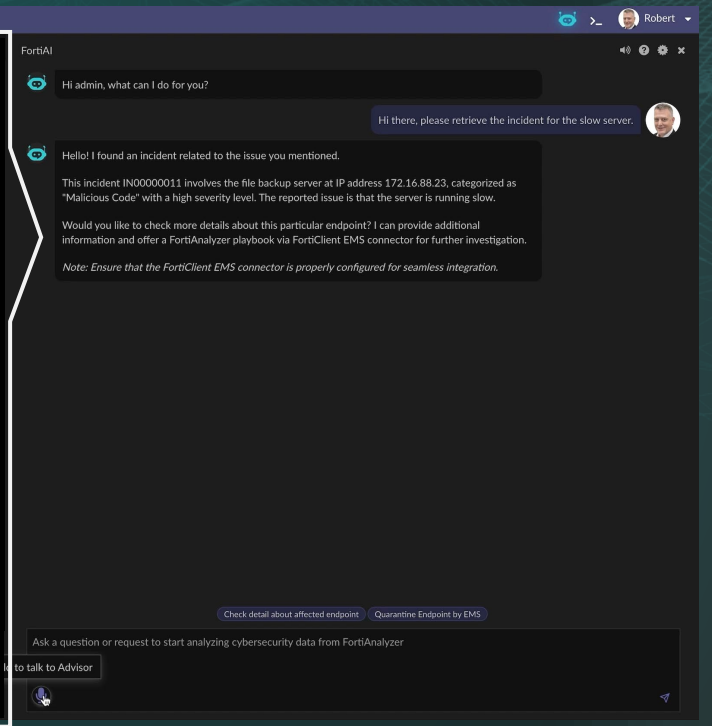
➢ 文件備份 Server (172.16.88.23) 正在經歷運行緩慢的問題，主要是由於 qcloud 進程佔用了 98% 的 CPU 資源

➢ Process Details:

PID	進程名稱	CPU 使用率	使用者	運行時間	命令路徑	連接 IP
1234	qcloud	98%	admin	2小時30分	/usr/local/bin/qcloud	136.243.90.99
5678	apache	12%	www-data	1小時45分	/usr/sbin/apache2	-
9876	sshd	5%	root	4小時15分	/usr/sbin/sshd	-

➢ 除了 qcloud 之外，其他進程如 apache、sshd 等也在此 Server 上運行

➢ **建議使用 FortiGuard 和 VirusTotal 對 IP=136.243.90.99 進行進一步檢查**



FortiAI Demo

INVESTIGATE | ACTION

- Retrieve incident for slow server
- Run FortiClient playbook
- Investigate public IP address

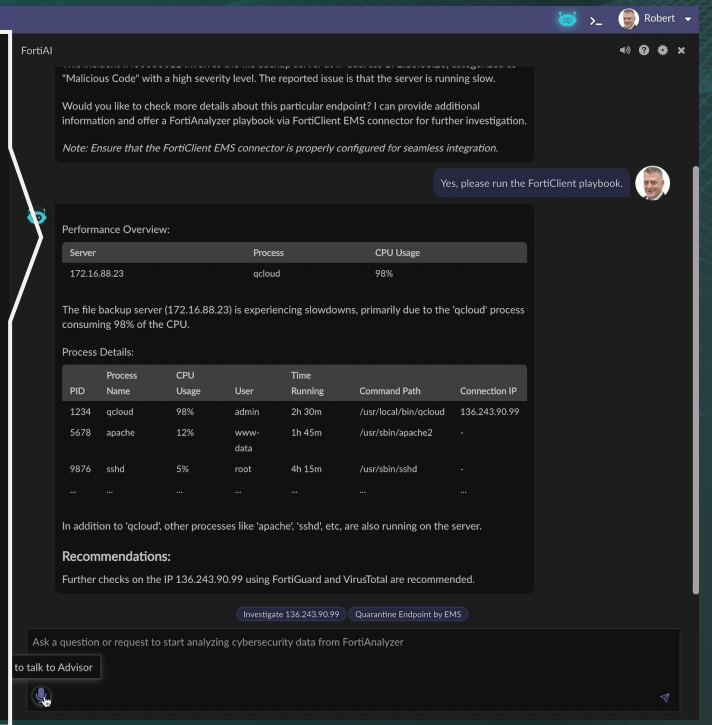
Sounds good, please Investigate this public IP address.
好主意，請調查一下這個公有 IP 位址 (136.243.90.99)

FortiAnalyzer 7.6

FortiGuard Alert:

- **威脅： 門羅幣(Monero), 加密貨幣, 挖礦程式**
- **影響：消耗主機與網路資源**
- **涉及的技術：** 基於瀏覽器、網路協議、客戶端-伺服器、點對點、雲端服務、移動設備 … 等等。
- 觀察到的行為： 在預設的 TCP/80 和 TCP/443 端口上使用過多的頻寬。
- **潛在後果：文件備份 Server 172.16.88.23 上的運作緩慢可能是由於門羅幣(Monero) 加密貨幣挖礦程式所導致。**

強烈建議立即採取修復措施，以解決這一潛在的安全威脅。



FortiAI Demo

INVESTIGATE | ACTION

- Retrieve incident for slow server
- Run FortiClient playbook
- Investigate public IP address
- Search for IP addresses connecting to malicious IP

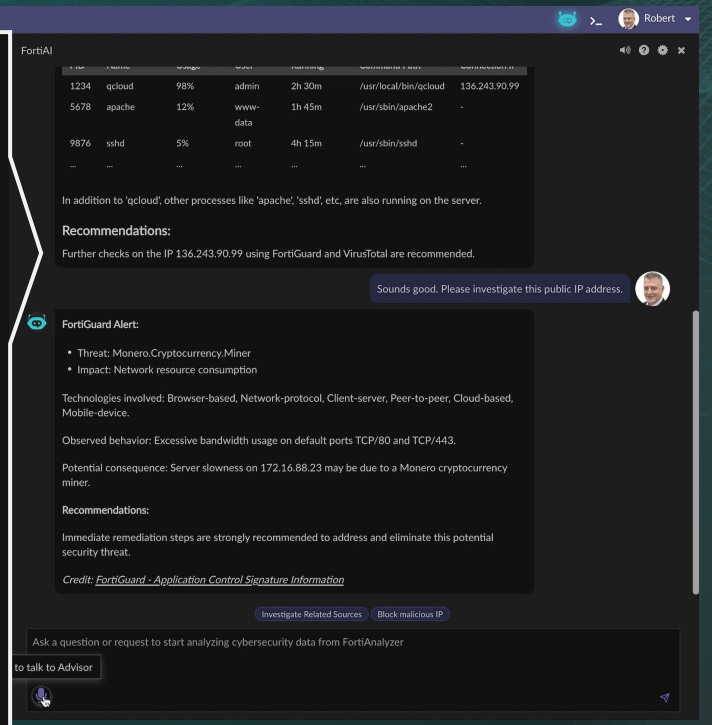
Please search for any other IP addresses connecting to the same malicious IP.
請搜尋連接到惡意 IP(136.243.90.99)的任何內網 IP 位址

調查結果：

- 三筆內網 IP 嘗試連接到該外部惡意 IP (136.243.90.99):

來源 IP	連線持續時間
10.3.15.254	25秒
172.16.88.23	2分8秒
172.16.115.11	46秒

- FortiAnalyzer 查詢已識別出三筆內網 IP 嘗試連接到該惡意 IP，其中包括當前正在經歷運作緩慢問題的 172.16.88.23 (檔案 Backup Server.)。
- **建議調查以上三筆內網 IP 以確認潛在威脅**
- **檢查 FortiAnalyzer Threat Hunting (威脅狩獵)以獲取有關惡意 IP=136.243.90.99 的更多訊息。**



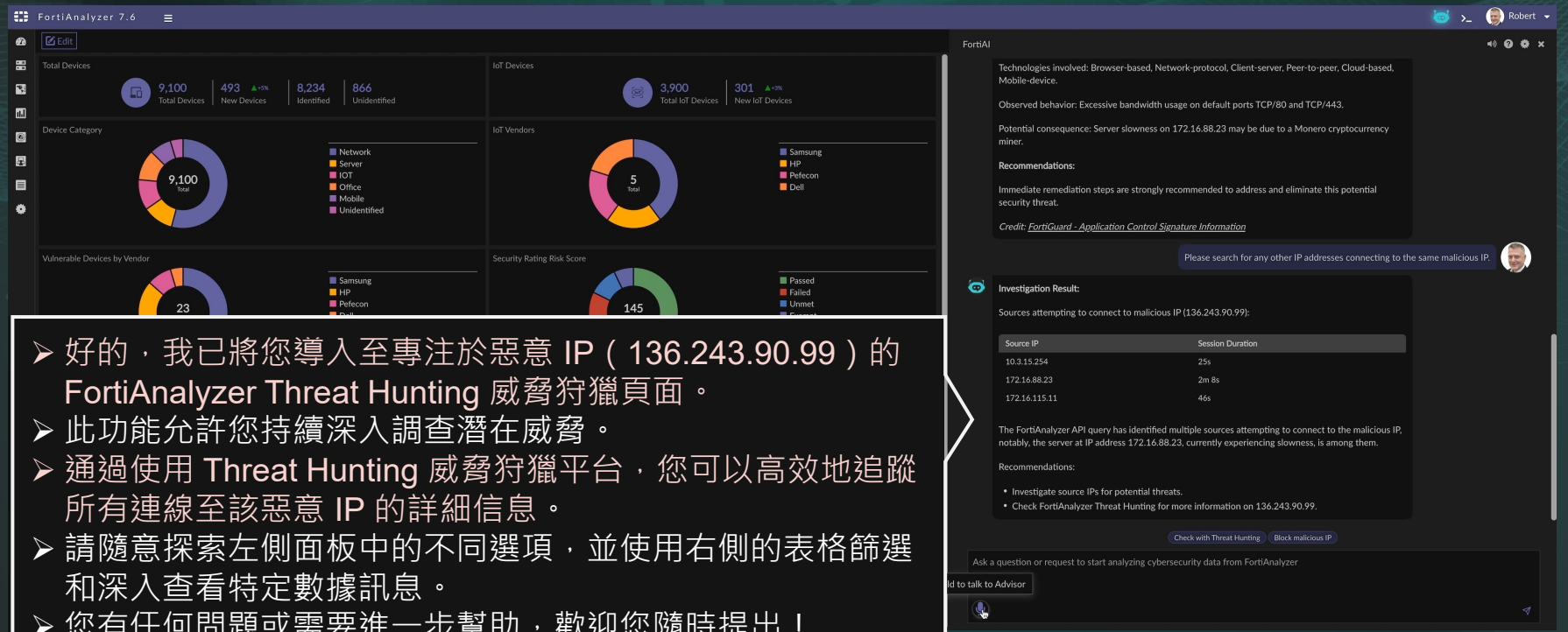
FortiAI Demo

INVESTIGATE | ACTION

- Retrieve incident for slow server
- Run FortiClient playbook
- Investigate public IP address
- Search for IP addresses connecting to malicious IP
- Load Threat Hunting Page

Please load the Threat Hunting page so I can take a look.

好，請載入Threat Hunting 威脅狩獵搜尋頁面，以便我查看



- 好的，我已將您導入至專注於惡意 IP（136.243.90.99）的 FortiAnalyzer Threat Hunting 威脅狩獵頁面。
- 此功能允許您持續深入調查潛在威脅。
- 通過使用 Threat Hunting 威脅狩獵平台，您可以高效地追蹤所有連線至該惡意 IP 的詳細信息。
- 請隨意探索左側面板中的不同選項，並使用右側的表格篩選和深入查看特定數據訊息。
- 您有任何問題或需要進一步幫助，歡迎您隨時提出！

FortiAI Demo

INVESTIGATE | ACTION

- Retrieve incident for slow server
- Run FortiClient playbook
- Investigate public IP address
- Search for IP addresses connecting to malicious IP
- Load Threat Hunting Page
- Search for abnormal login activity

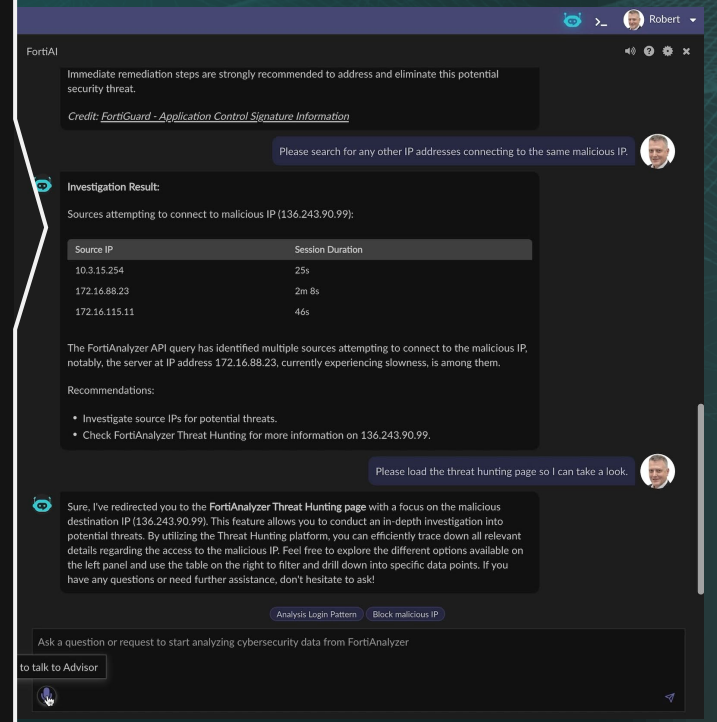
Thank you, please search for abnormal login activity related to the source IP addresses.
謝謝你，請尋找與備份 Server 172.16.88.23 相關的異常登入活動

2024年3月7日：
- 23:15:39, 10.100.55.254 使用 SSH 登入，透過用戶 “root” 帳密嘗試登入，並且登入成功。

2024年3月5日：
- 16:24:55, 10.100.55.254 多次 “root” 嘗試登入失敗。
- 發生多次密碼驗證失敗，可能存在暴力破解嘗試。
- 後續嘗試登入均顯示密碼驗證失敗。

2024年2月2日：
- 18:12:22, 10.100.55.254 透過用戶 “root” 的密碼嘗試登入失敗。

- **以上針對 “root” 帳戶的暴力破解攻擊事件**
- **建議先實施帳戶鎖定策略，並進一步調查。**
- **如果需要更進一步的資訊，我可以帶您前往 Logview 進行深入檢查，您是否願意繼續？**



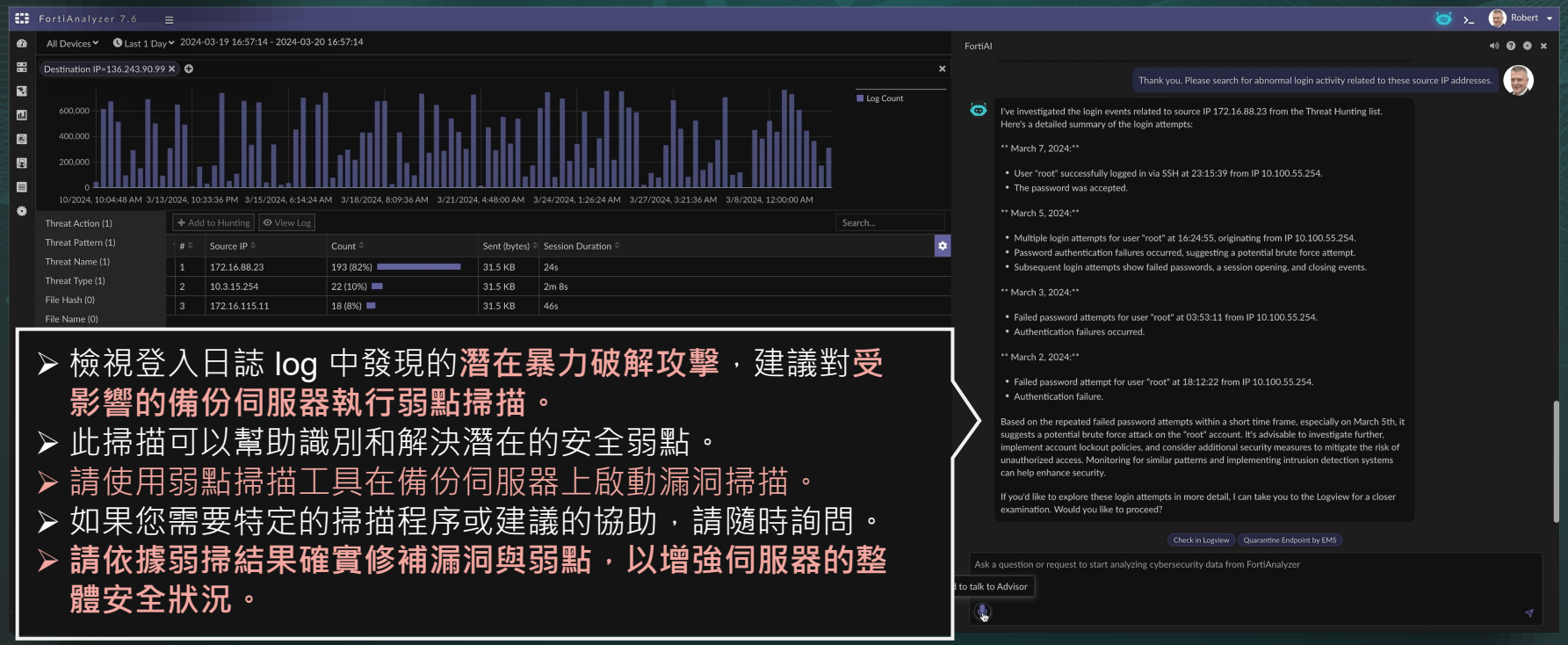
FortiAI Demo

INVESTIGATE | ACTION

- Retrieve incident for slow server
- Run FortiClient playbook
- Investigate public IP address
- Search for IP addresses connecting to malicious IP
- Load Threat Hunting Page
- Search for abnormal login activity
- Display log view

Sure, please proceed.

當然，讓我們繼續調查



- 檢視登入日誌 log 中發現的**潛在暴力破解攻擊**，建議對**受影響的備份伺服器執行弱點掃描**。
- 此掃描可以幫助識別和解決潛在的安全弱點。
- 請使用弱點掃描工具在備份伺服器上啟動漏洞掃描。
- 如果您需要特定的掃描程序或建議的協助，請隨時詢問。
- **請依據弱掃結果確實修補漏洞與弱點，以增強伺服器的整體安全狀況。**

FortiAI Demo

INVESTIGATE | ACTION

Reassign incident to forensics team

Please reassign the incident to the forensics team.

請將此事件分配給資安鑑識小組

FortiAI Demo

INVESTIGATE | ACTION

- Reassign incident to forensics team
- Block malicious IP address

Good idea, please go ahead.

好主意，請繼續

我已成功執行以下作業：

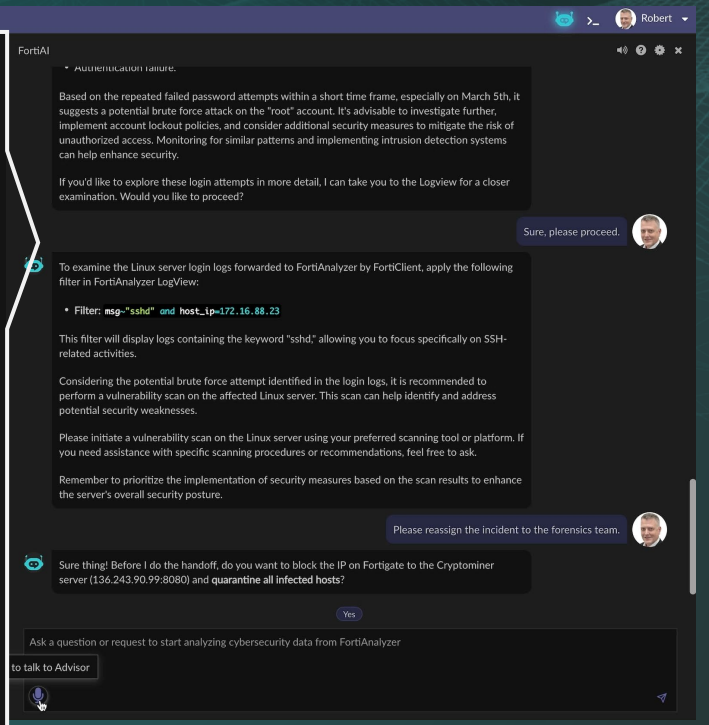
1、封鎖外部惡意 IP 連線行為：

- 執行自動化腳本「Block_IP」以阻止與可疑「qcloud」進程關聯的惡意 IP 位址 136.243.90.99 (挖礦主機)。

2. 隔離內網受感染主機：

- 執行自動化腳本「Quarantine_Hosts」以隔離受可疑活動影響的端點。
- 以下為受隔離的感染主機 IP：
  - 10.3.15.254
  - 172.16.88.23 (文件備份主機)
  - 172.16.1.11

這些措施目的在增強資安防護態勢並處理調查期間發現的資安威脅。



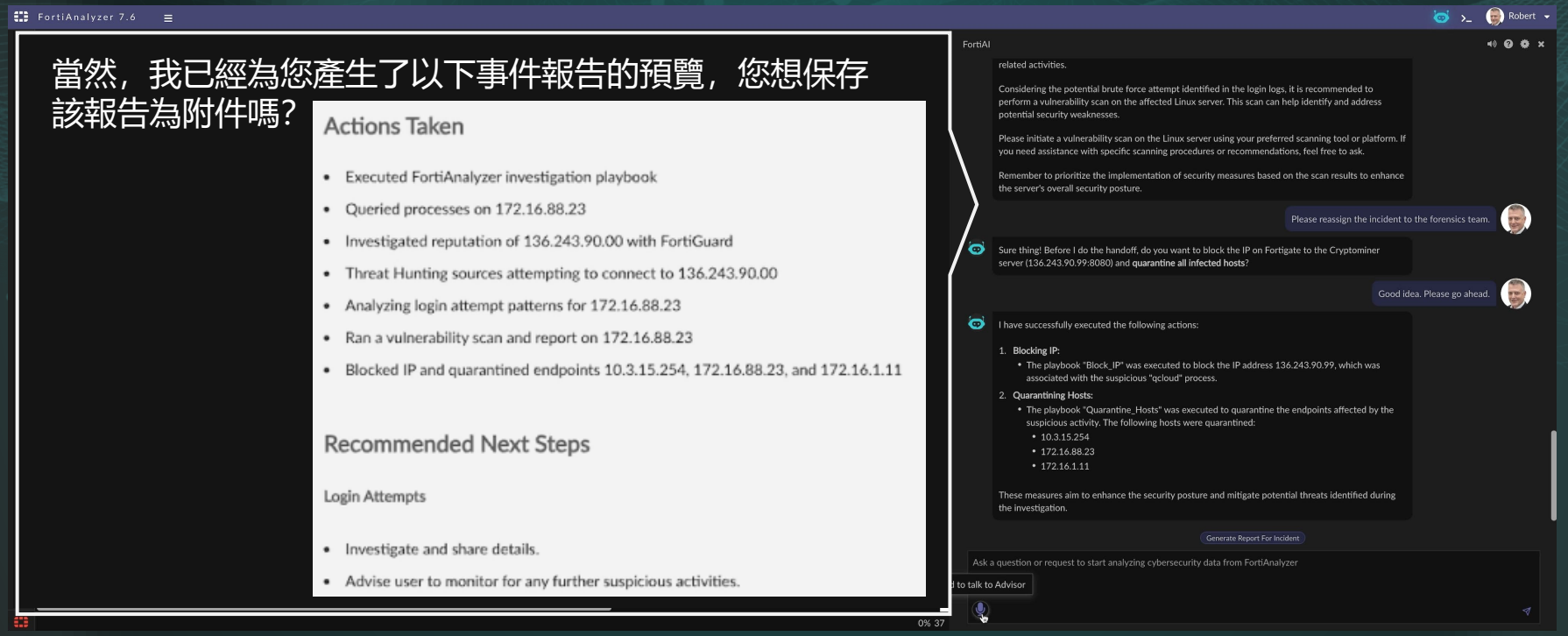
FortiAI Demo

INVESTIGATE | ACTION

- Reassign incident to forensics team
- Block malicious IP address
- Generate a report for the incident

Please generate a report for this incident.

請為此事件產出一份報告



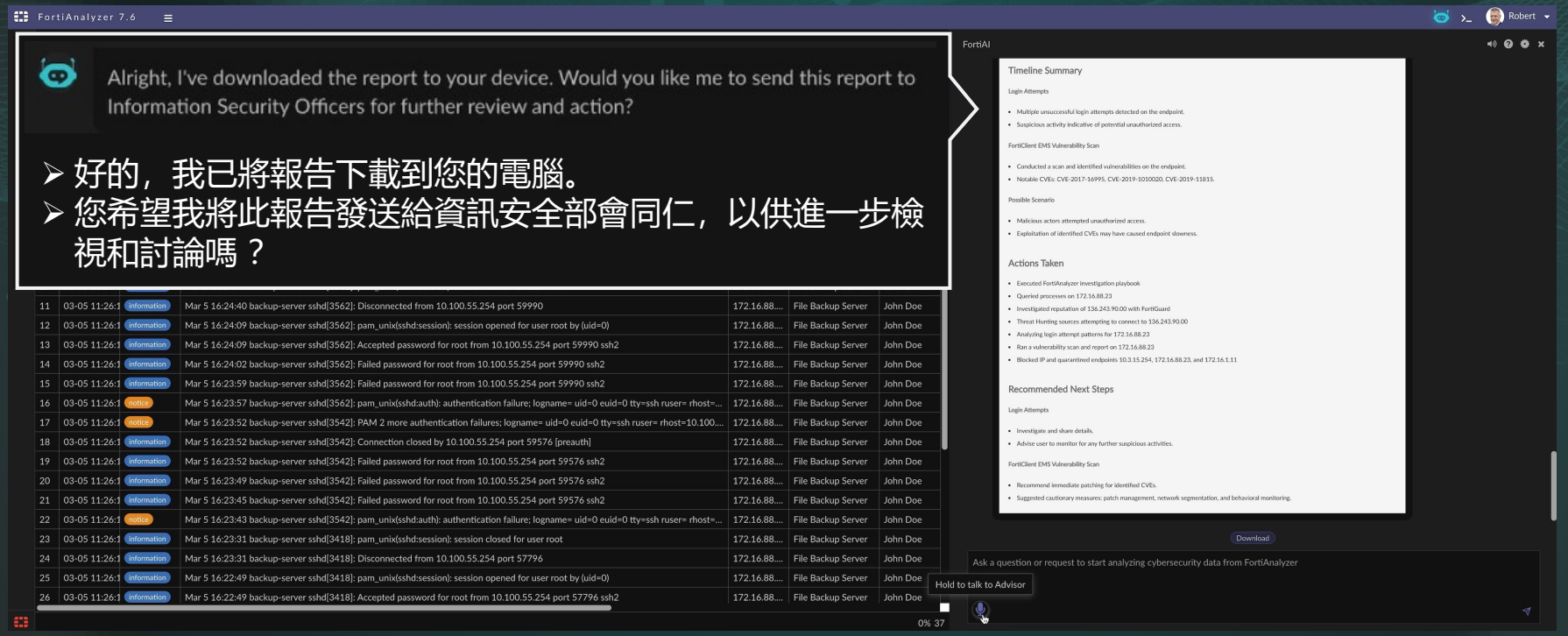
FortiAI Demo

INVESTIGATE | ACTION

- Reassign incident to forensics team
- Block malicious IP address
- Generate a report for the incident
- Download a copy of the report to computer

Yes, please download it to my computer.

好，請下載到我的電腦



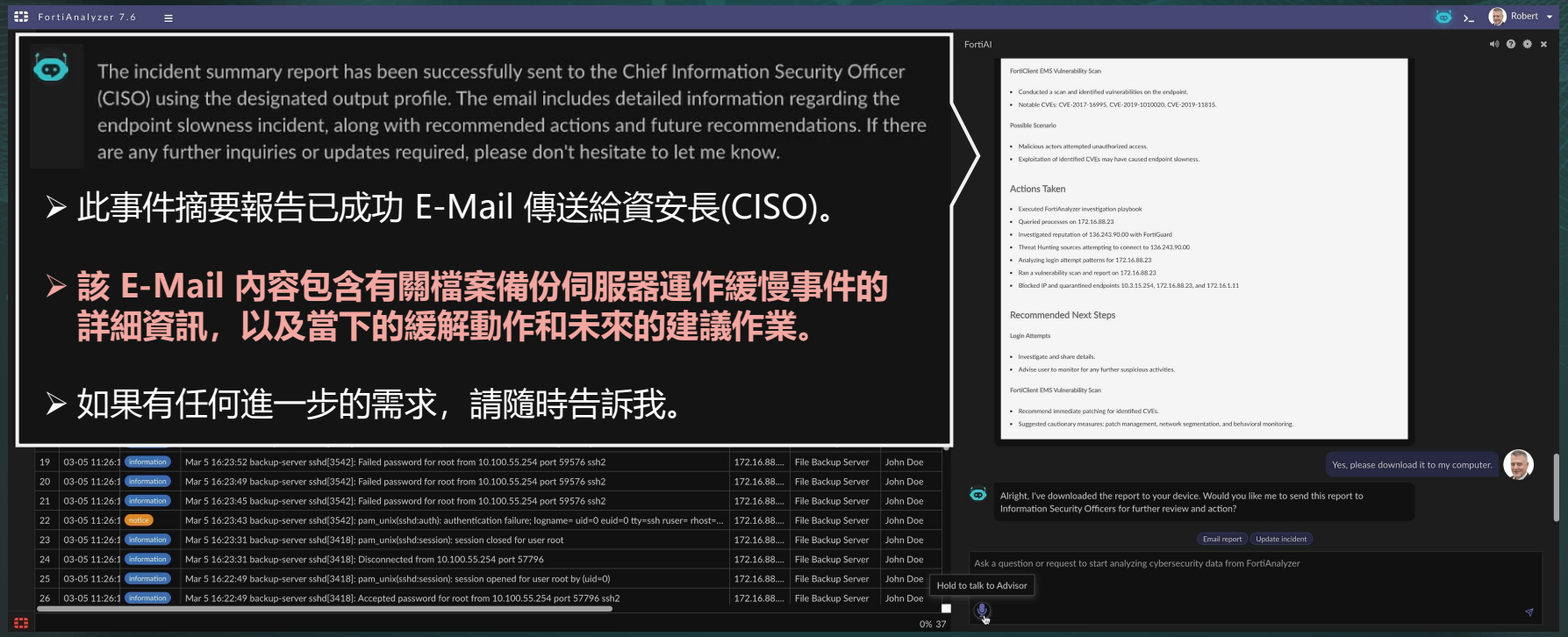
FortiAI Demo

INVESTIGATE | ACTION

- Reassign incident to forensics team
- Block malicious IP address
- Generate a report for the incident
- Download a copy of the report to computer
- Email a copy of the report to the CISO

Please also email a copy of the report to the CISO.

請透過電子郵件將報告副本發送一份給資安長 (CISO)

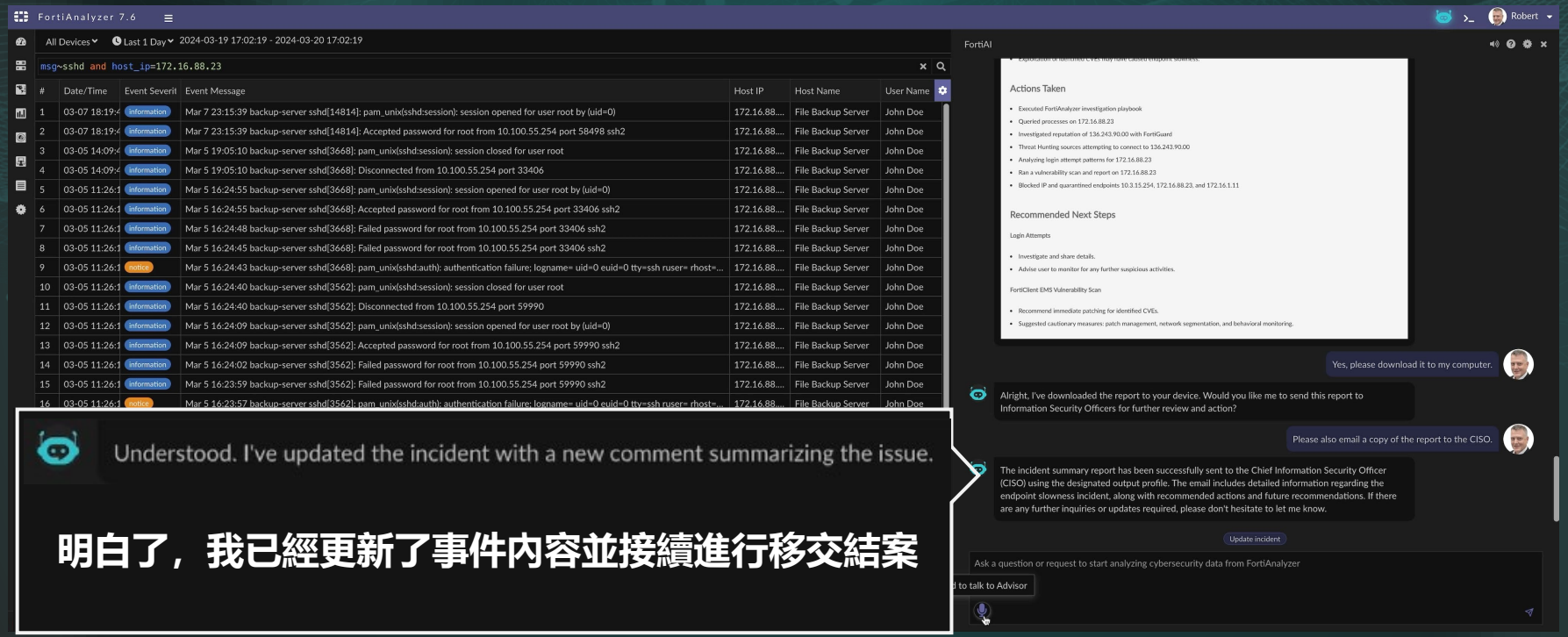


FortiAI Demo

INVESTIGATE | ACTION

- Reassign incident to forensics team
- Block malicious IP address
- Generate a report for the incident
- Download a copy of the report to computer
- Email a copy of the report to the CISO
- Update incident details. Handoff to forensics team.

Great, please update the incident details and handoff to the forensics team.
太好了，請更新事件詳細資訊並將其移交給資安鑑識小組




FORTINET