N-Partner

運用AI技術
優化您的校園維運管理

Data Analyst
王聖雄 Sherman
Sherman@npartner.com
0926-834979

• 工欲善其事必先利其器

N-Partner的數據儲存與智慧分析技術

N-Partner的核心技術

快篩確認詳細狀況

發覺體溫異常或有其他症狀後，
透過更詳細的檢查確認問題

監控身體狀況

到各大場所都要隨時量體溫，
確定是否有發燒的狀況

收集不同類型數據

SIEM

Log

Network Management

Flow Analysis

N-Partner

- Big Data Collection
- Correlation
- Learning

掃描QR Code

最有效的預防擴散就是將潛伏期期間的
親密接觸者一併找出確認狀況

N-Partner 智慧維運方案

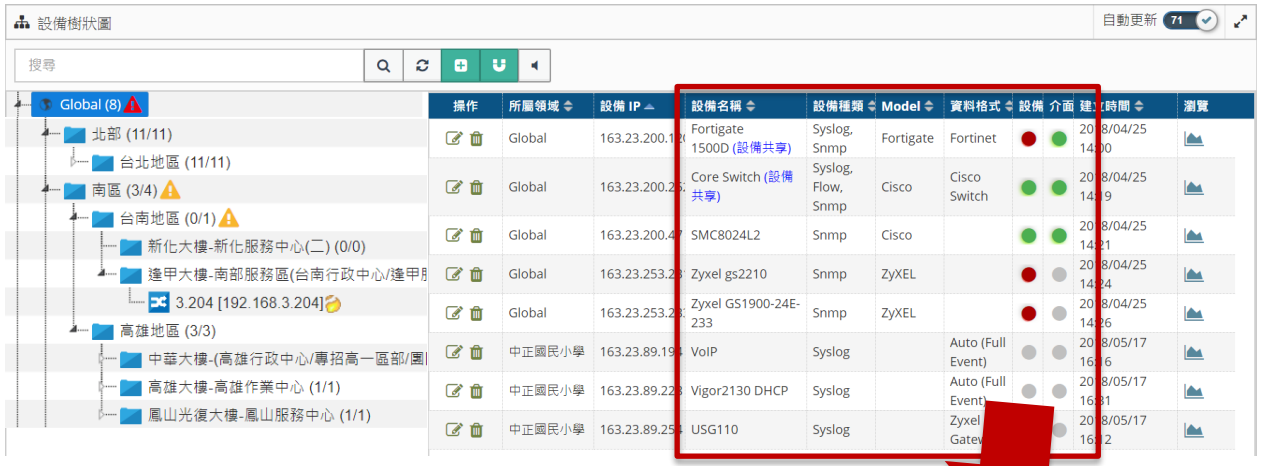
維運方案加以整合，輕鬆面對日益複雜的網路架構與維運難題

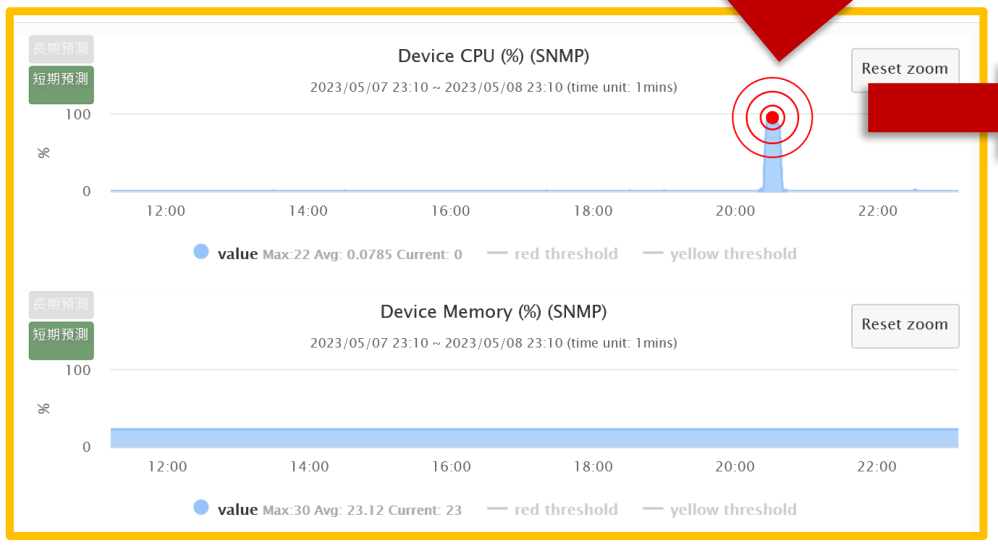
1. 跨品牌設備健康狀態監控與告警
   建立資產清單,點擊就知障礙根源
2. 網路與網頁服務效能監測功能
   (Performance Monitoring, PM)
3. CPU/Disk/Traffic/Round Trip Time
   未來2-3個月的走勢預測
4. 市場上最佳CP值日誌收集系統
   內建數百種知名日誌正規化功能
5. 網路實名制，把IP對應成使用者名稱
   還能定位所在Switch-Interface
6. 內建更強大的網路流量數據分析能力
   手握即時發覺爆發型病毒的利器
7. 資安強化與聯合防禦
8. 與威脅情資庫結合
   清除內網遭駭客潛伏設備
9. 更美觀的自定義Dashboard
   創造專屬戰情中心

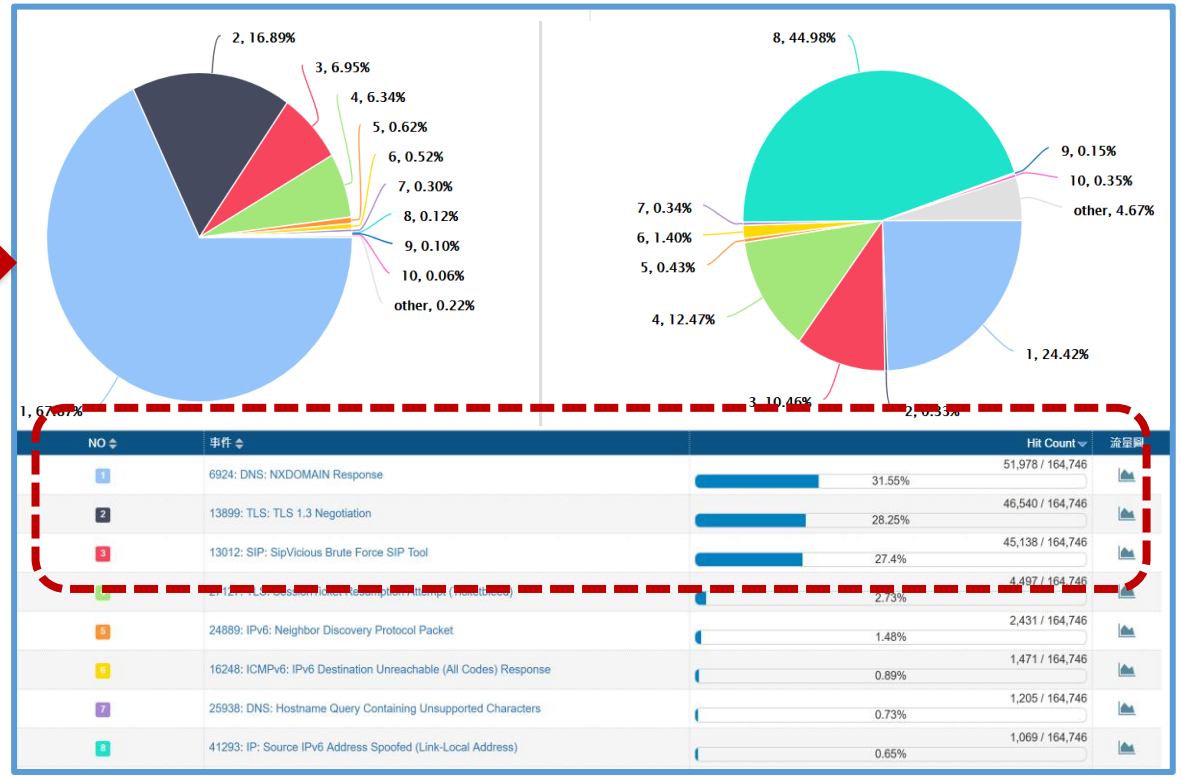
跨品牌設備健康狀態監控與告警

建立資產清單，點擊就知道障礙根源

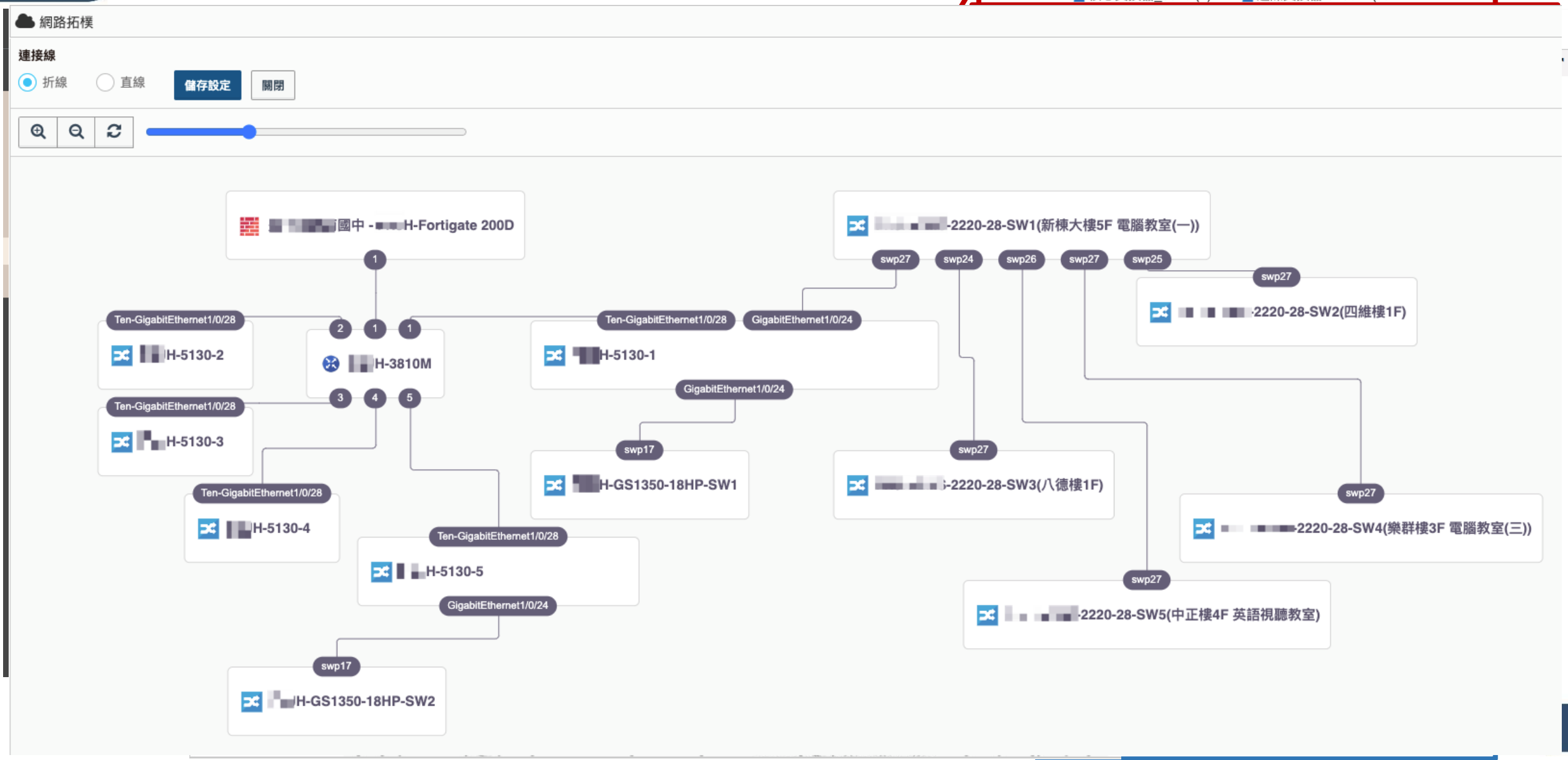
跨品牌設備資產及健康狀態監控自動關聯日誌與流量







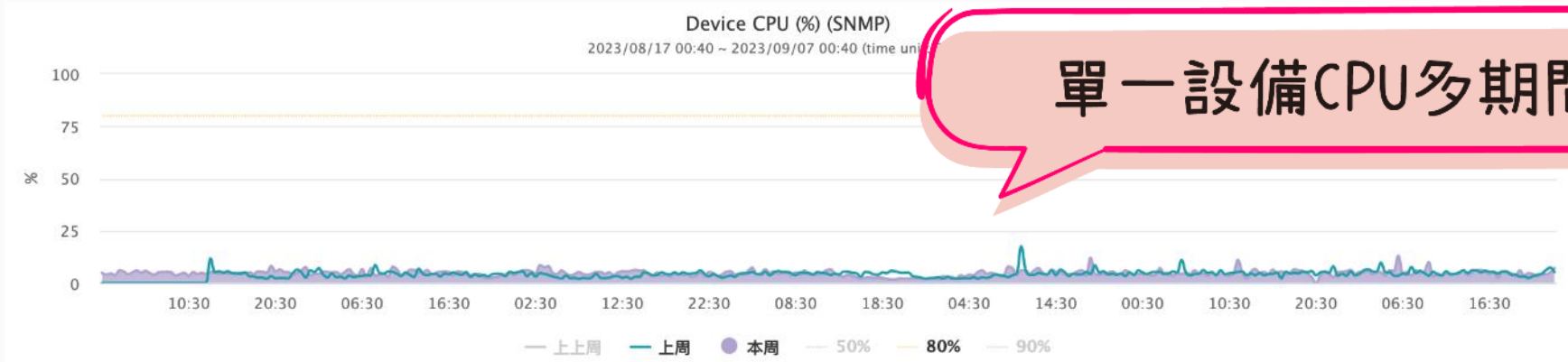
自動繪製拓樸圖


核心交換器_3810 (2) <-> 邊際交換器-5130-2 (Ten-
網路拓樸
連接線
折線
直線
儲存設定
關閉
國中 -H-Fortigate 200D
1
Ten-GigabitEthernet1/0/28
H-5130-2
2
1
1
H-3810M
Ten-GigabitEthernet1/0/28
GigabitEthernet1/0/24
H-5130-1
3
4
5
Ten-GigabitEthernet1/0/28
H-5130-3
GigabitEthernet1/0/24
swp17
H-GS1350-18HP-SW1
Ten-GigabitEthernet1/0/28
H-5130-4
Ten-GigabitEthernet1/0/28
H-5130-5
GigabitEthernet1/0/24
swp17
H-GS1350-18HP-SW2
-2220-28-SW1(新棟大樓5F 電腦教室(一))
swp27
swp24
swp26
swp27
swp25
swp27
2220-28-SW2(四維樓1F)
swp27
-2220-28-SW3(八德樓1F)
swp27
swp27
2220-28-SW4(樂群樓3F 電腦教室(三))
swp27
2220-28-SW5(中正樓4F 英語視聽教室)

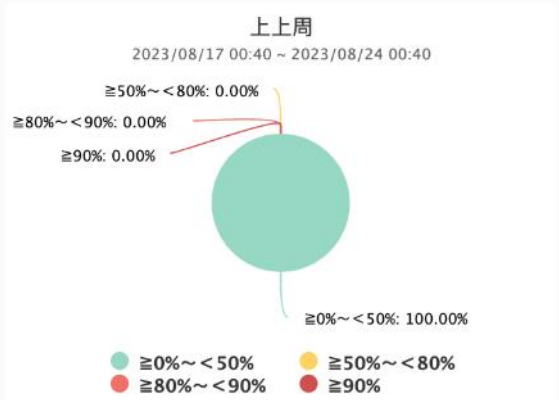
服務級別協定 (Service-Level Agreement, SLA)

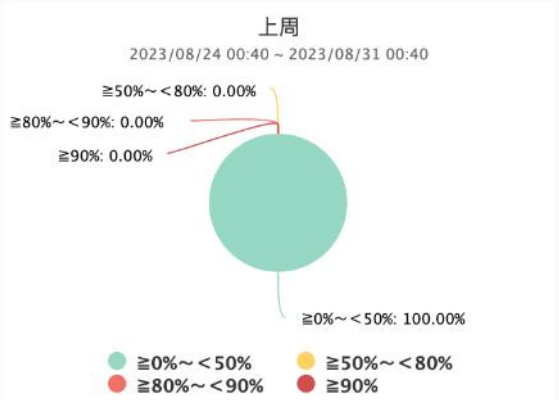
時間週期

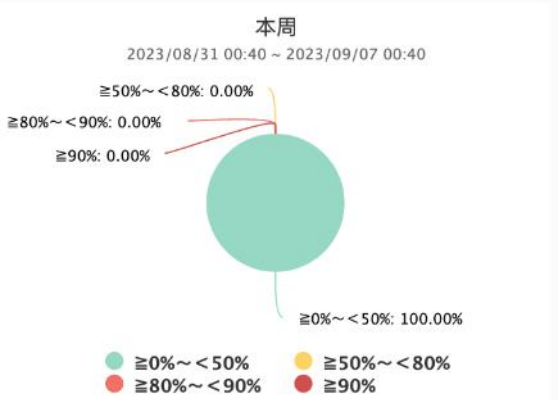
1 天　1 周　1 個月　啟動查詢

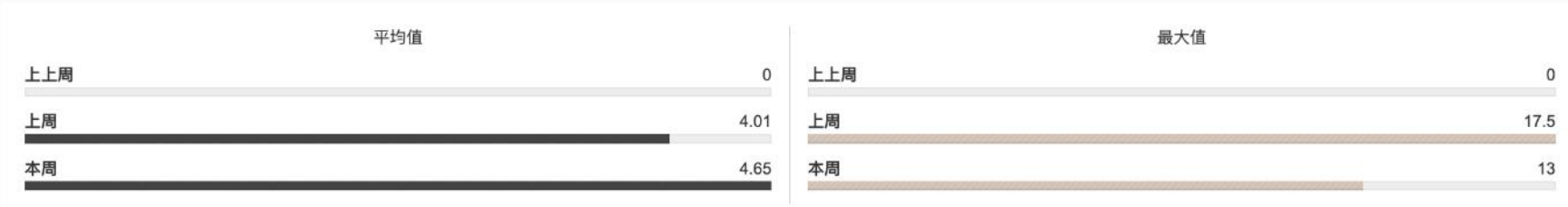


單一設備CPU多期間比較





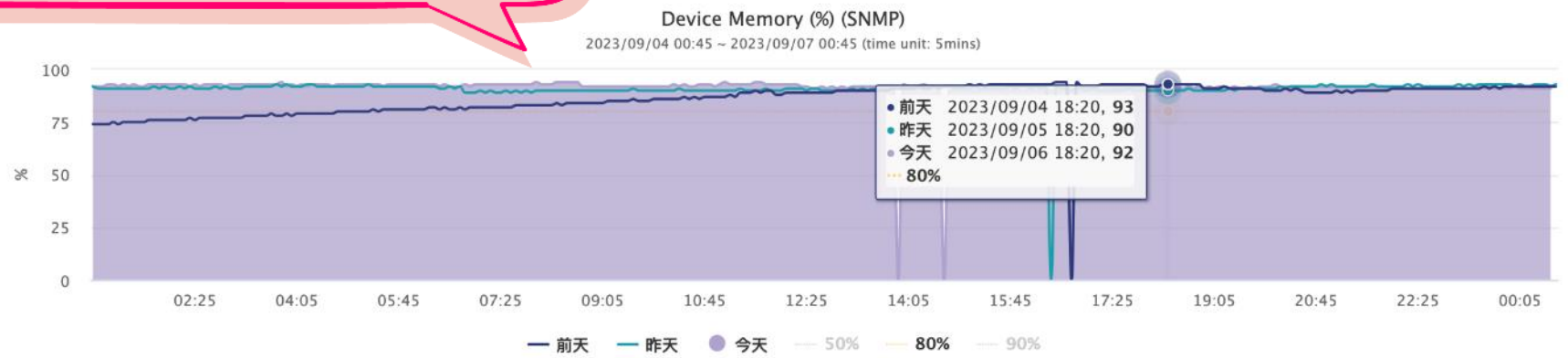


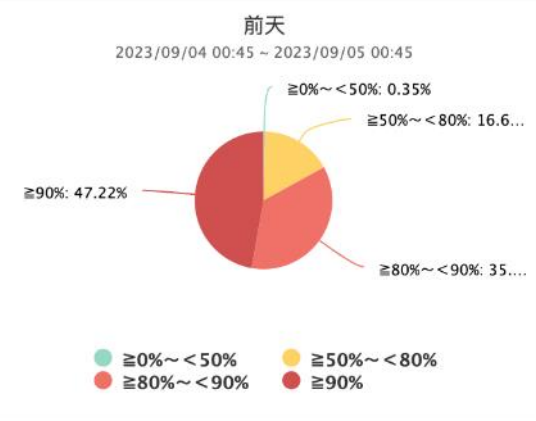


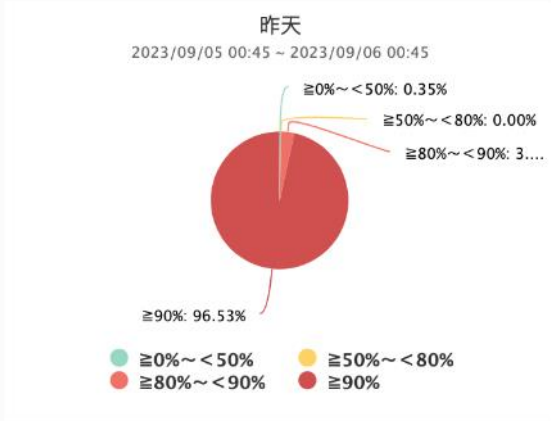
單一設備記憶體多期間比較

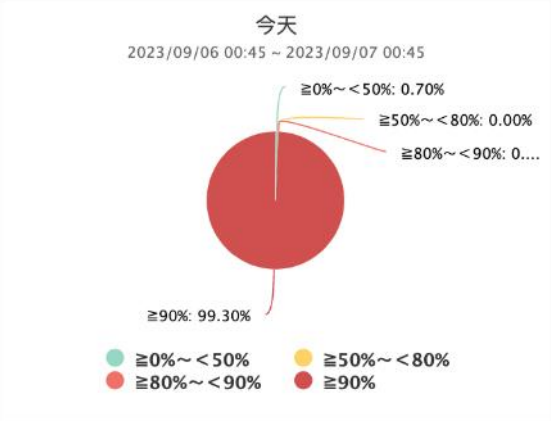
服務級別協定 (Service-Level Agreement, SLA)

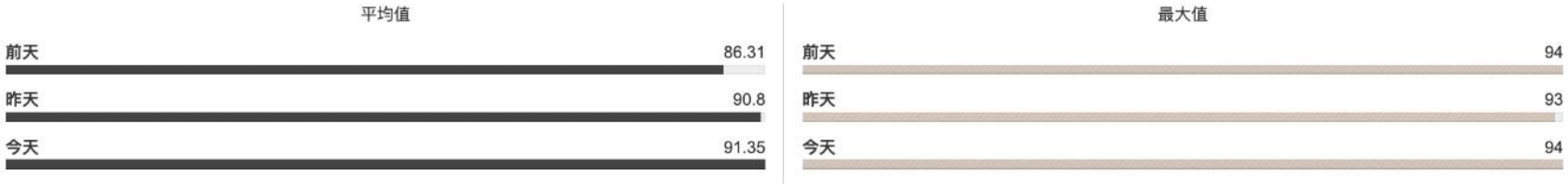
時間週期











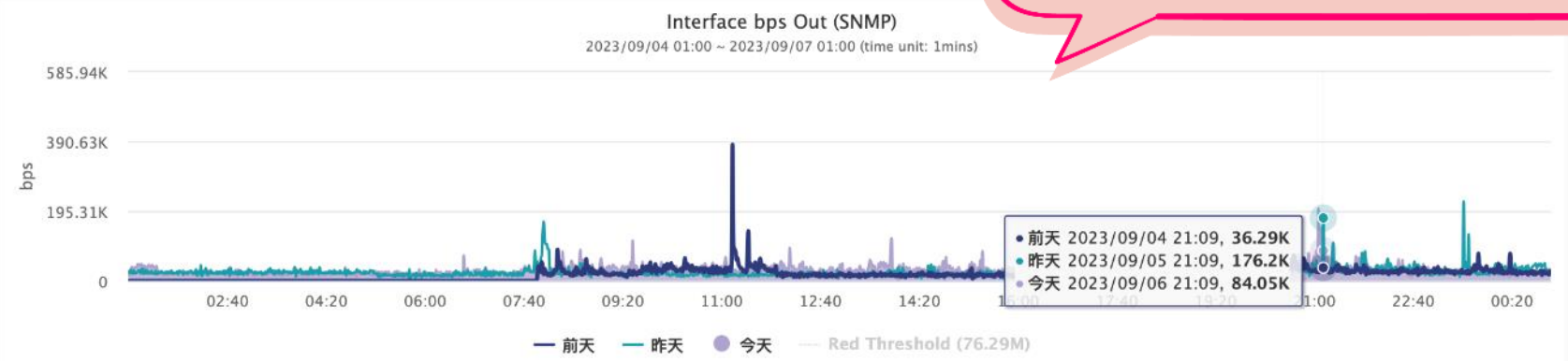
Interf

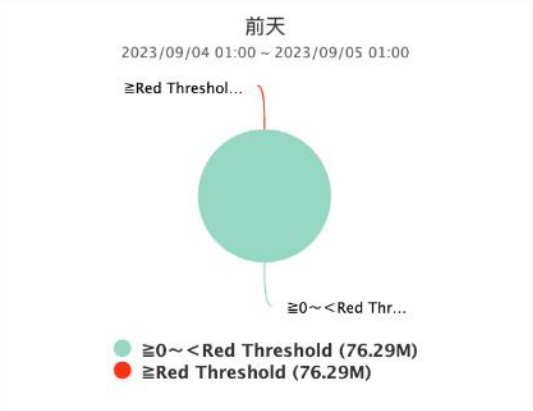
Interface bps Out (SNMP)

服務級別協定 (Service-Level Agreement, SLA)

時間週期

1 天 1 周 1 個月 啟動查詢





平均值

前天	18K
昨天	25.89K
今天	30.55K

最大值

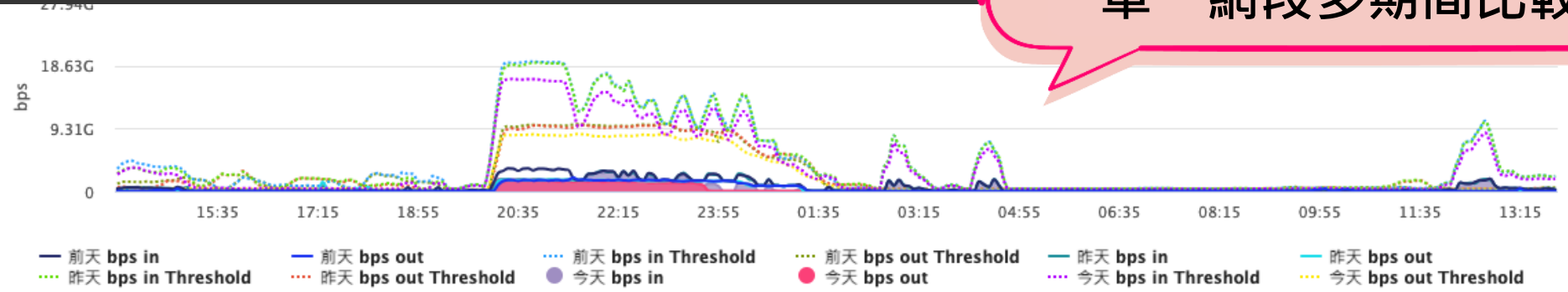
前天	381.63K
昨天	223.05K
今天	202.17K

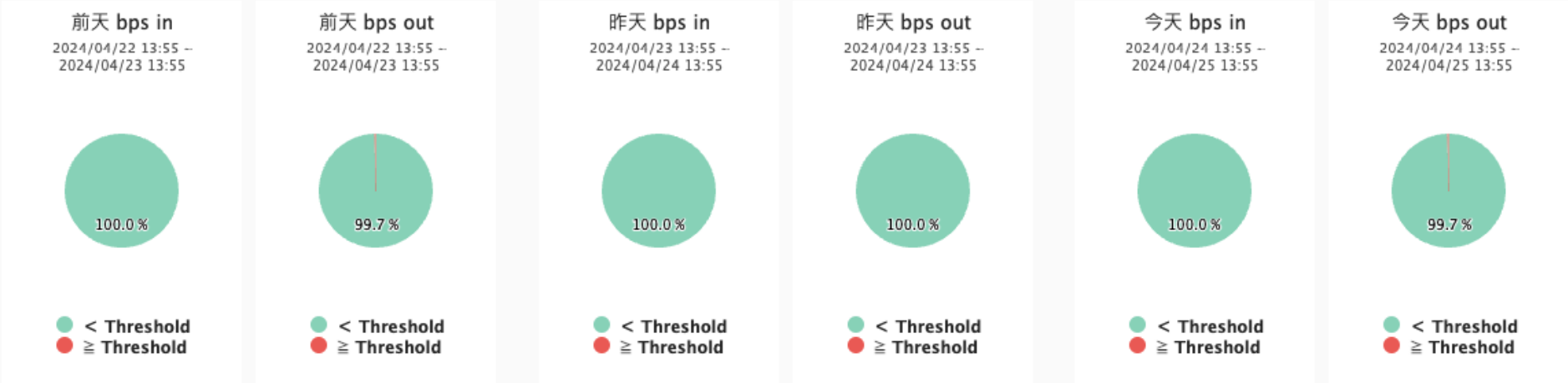
單一設備介面多期間比較總覽

時間週期	Ifspeed	平均頻寬使用率 (%)		尖峰頻寬使用率 (%)		流量異常告警次數		封包錯誤次數		封包丟棄次數	
		流入	流出	流入	流出	流入	流出	流入	流出	流入	流出
本周 2023/09/20 00:00 ~ 2023/09/26 22:10	1G	0.15 %	0.01 %	1.53 %	0.41 %	0	0	0	0	0	0
上周 2023/09/13 00:00 ~ 2023/09/19 23:59	1G	0.19 %	0.01 %	3.42 %	0.13 %	0	0	0	0	0	0
上上周 2023/09/06 00:00 ~ 2023/09/12 23:59	1G	0.02 %	0 %	0.64 %	0.02 %	0	0	0	0	0	0

單一網段多期間比較

服務級別協定 (Service-Level Agreement, SLA)





平均值

流入量		流出量	
前天	686.16M	前天	370.4M
昨天	596.97M	昨天	377.97M
今天	491.23M	今天	273.7M

最大值

流入量		流出量	
前天	3.42G	前天	2.04G
昨天	3.04G	昨天	1.75G
今天	3.01G	今天	1.76G

關閉

SLA_DEV_G2

查詢時間區段

2024/05/13 14:35 ~ 2024/05/14 14:35 啟動查詢

設備群組可用率

設備名稱	監控設備名稱	可用率	尖峰可用率	平均回應時間	尖峰回應時間
R1	N-Cloud2 - 3.103 中文	99.48 %	99.75 %	1.08 ms	1.09 ms
R2	N-Cloud2 - 3.103 中文	99.48 %	99.75 %	1.08 ms	1.09 ms
LB1	N-Cloud2 - 3.103 中文	99.48 %	99.75 %	1.08 ms	1.09 ms
LB2	N-Cloud2 - 3.103 中文	99.48 %	99.75 %	1.08 ms	1.1 ms
Trista QANR v7.0 14.7	N-Cloud2 - 3.103 中文	99.48 %	99.75 %	1.39 ms	1.14 ms
Herb Tainan ESXi 192.168.14.3	NP_1424	99.20 %	99.08 %	1.08 ms	1.07 ms
192.168.5.232		0 %	0 %	0 ms	0 ms
Chiatest_192.168.5.233		0 %	0 %	0 ms	0 ms
Jenny_test_192.168.1.46	N-Probe-3.204	0 %	0 %	0 ms	0 ms
Jenny_test_192.168.1.46	N-Probe_2.6	0 %	0 %	0 ms	0 ms
C1	N-Cloud2 - 3.103 中文	0 %	0 %	0 ms	0 ms
Herb Tainan Debian 192.168.14.56		0 %	0 %	0 ms	0 ms

關閉

JuanTest-20240419

查詢時間區段

2024/05/13 14:35 ~ 2024/05/14 14:35 啟動查詢

介面群組可用率

介面名稱	Ifspeed	平均可使用率		平均頻寬使用率		尖峰頻寬使用率		流量異常告警次數		封包錯誤次數		封包丟棄次數	
		流入	流出	流入	流出	流入	流出	流入	流出	流入	流出	流入	流出
GigabitEthernet1/0/1	1G	97.22 %	97.22 %	0.02 %	0.13 %	0.31 %	1.58 %	0	0	0	0	0	0
Bridge-Aggregation14	2G	0 %	0 %	0 %	0 %	0 %	0 %	0	0	0	0	0	0

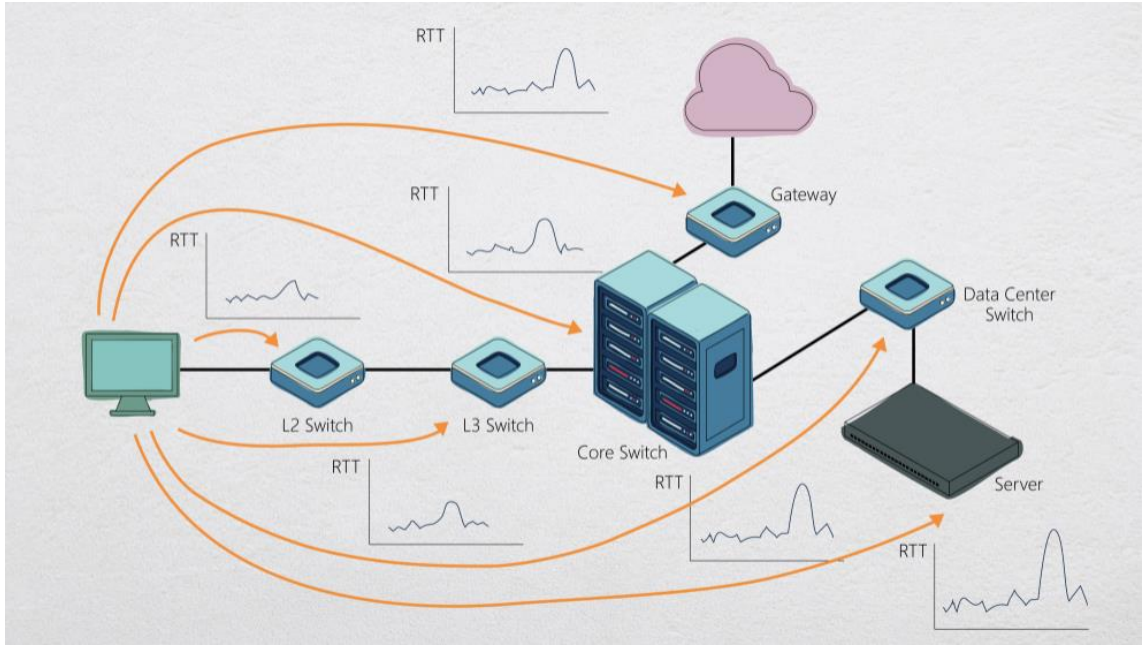
關閉

網路與網頁服務效能監測

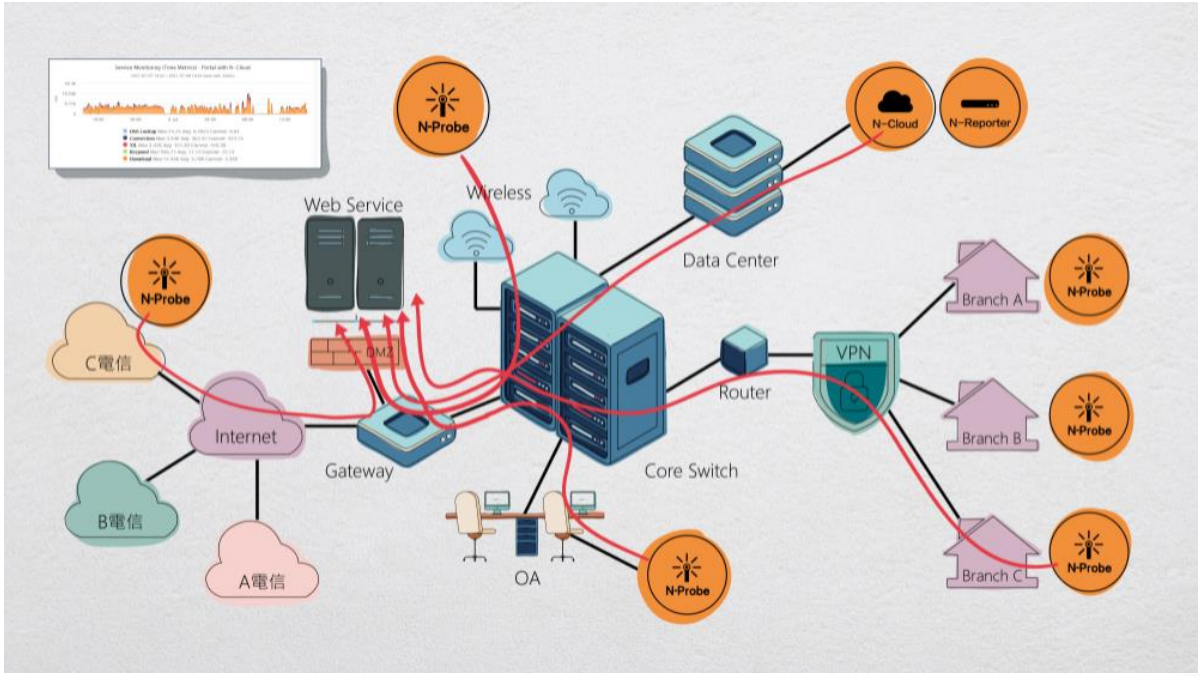
Performance Monitoring , PM

網路延遲與網頁服務瀏覽效能監測 (PM)

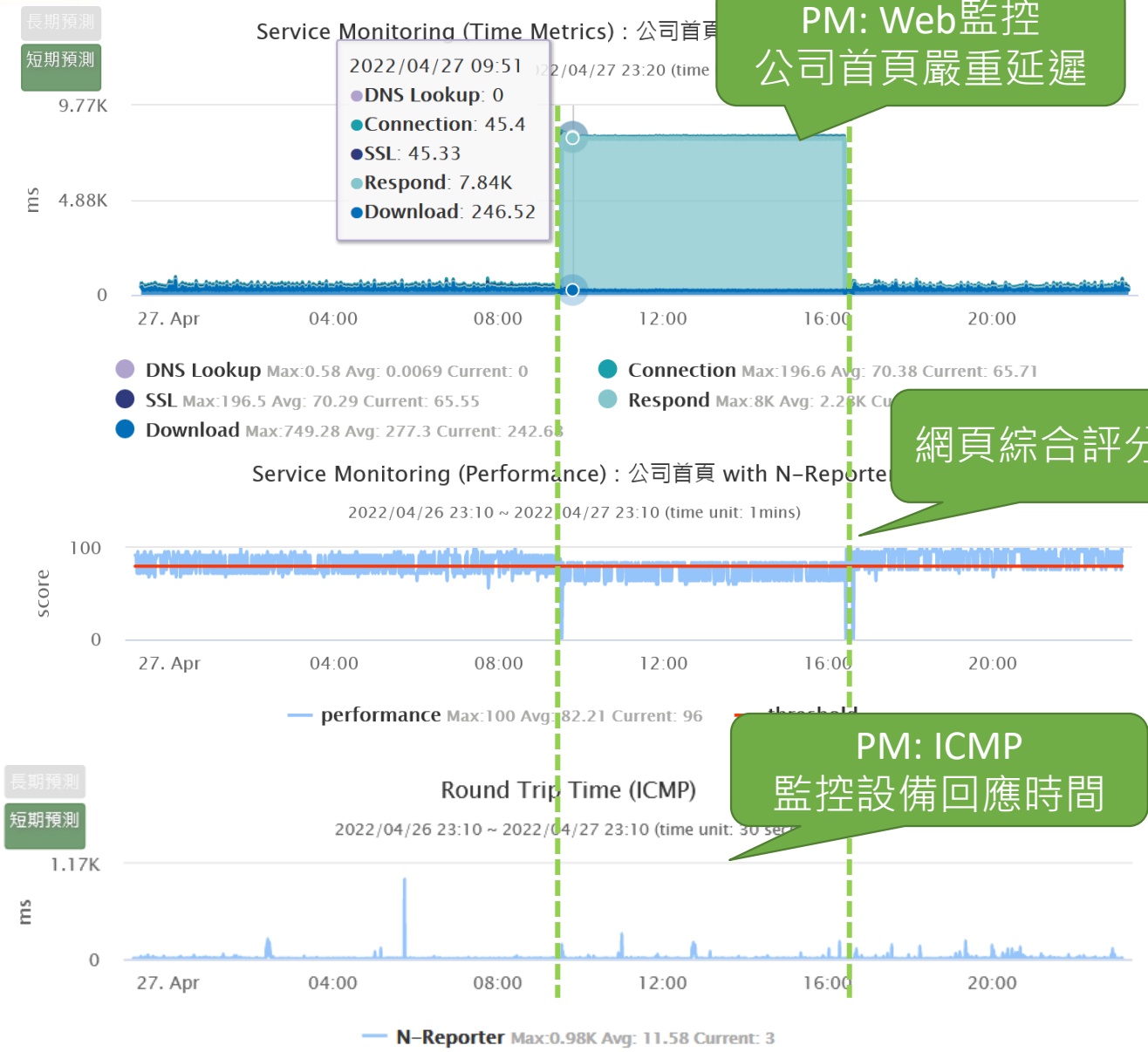
- 使用ICMP持續發出測試Ping封包用以收集各網路節點的延遲數據(Round Trip Time, RTT)



- 針對被監控的網頁服務(Web Service)同樣定時且持續地模擬人們瀏覽該網頁，將整個過程的反應時間記錄下來進行分析。



模擬真人進行網路與網頁服務效能監測



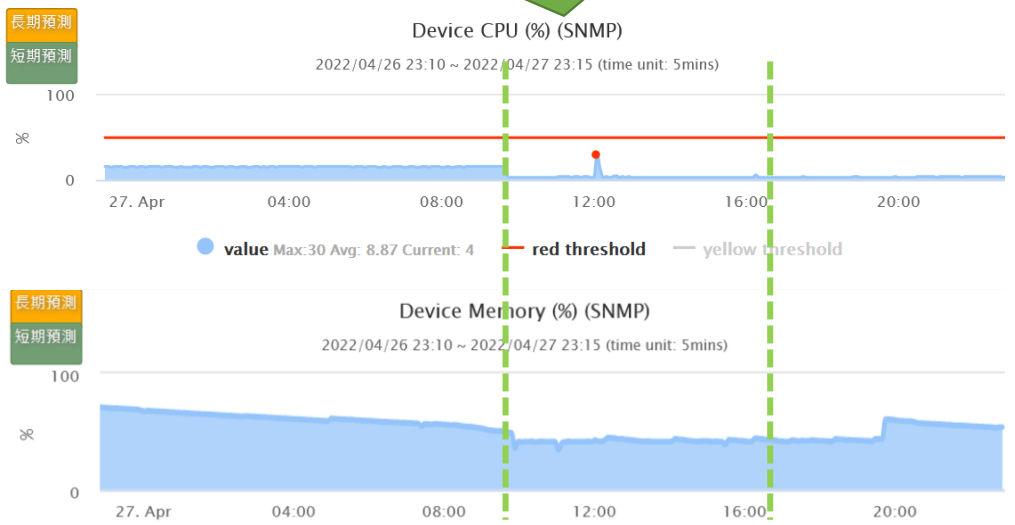
PM: Web監控
公司首頁嚴重延遲

關聯日誌內容
綜合判斷為應用系統改版造成網頁延遲

訊息	使用者 IP	記錄時間
Import System Image, [redacted].img	1.161.139.221	2022/04/27 09:45:50

網頁綜合評分

比對主機資源變化



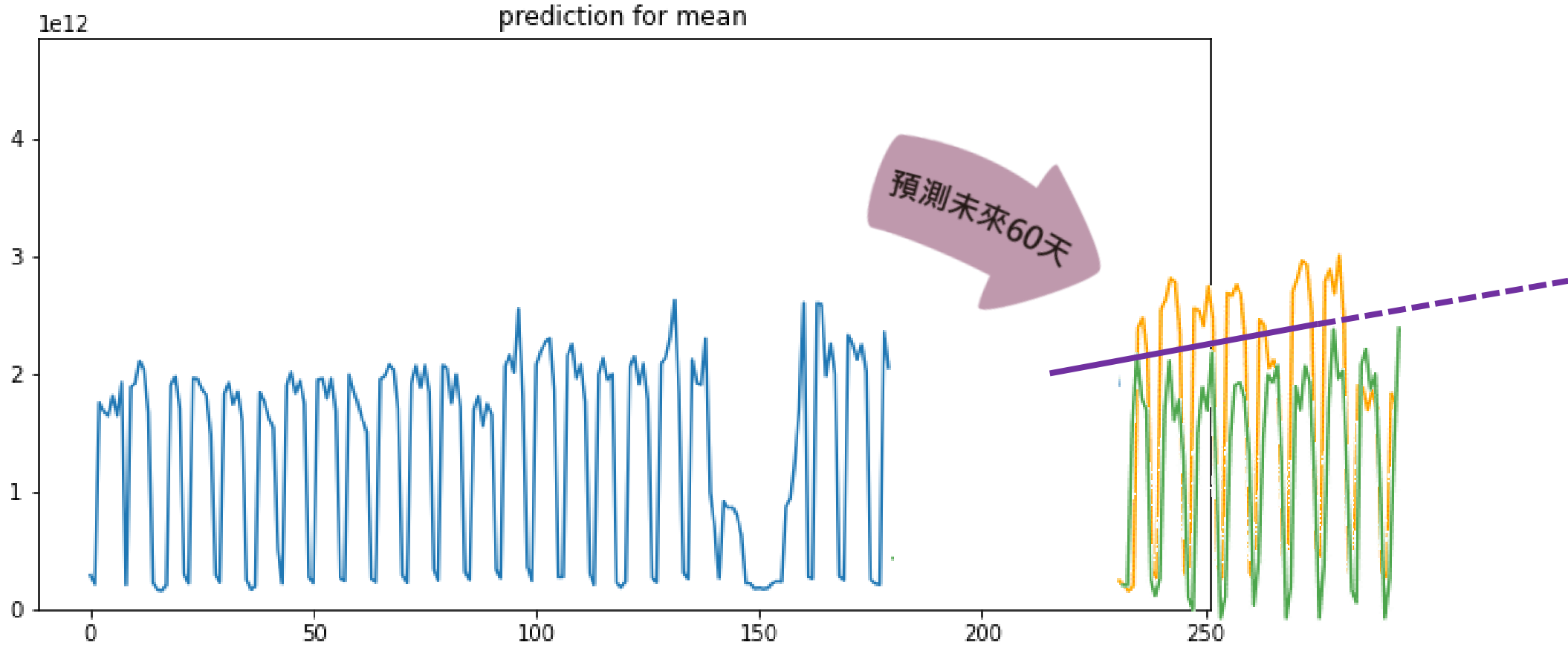
PM: ICMP
監控設備回應時間

未來2-3個月的走勢預測

CPU/Disk/Traffic/Round Trip Time

使用AI學習模型預測未來走勢

資料匯入 → 建立可輸入模型的資料格式 → 模型訓練 → 模型預測 → 結果與繪圖

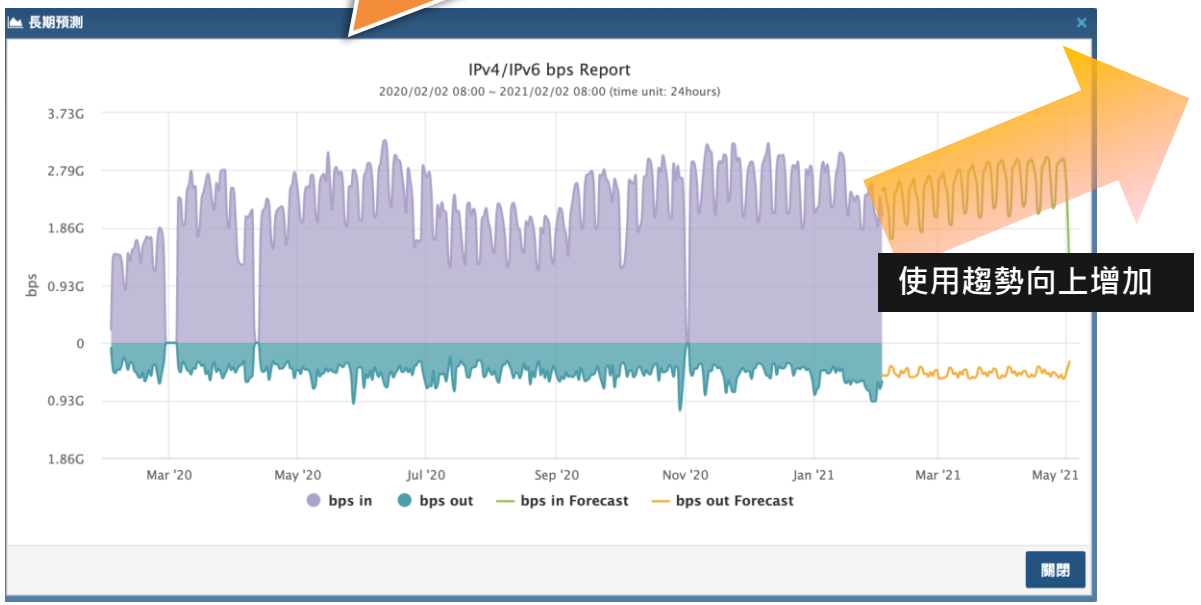


預測未來走勢與合理區間

長期預測
短期預測

短期預測，提供事件提前預警

長期預測，提供未來擴容依據



- 短期預測對流量使用率的預測

  (淡色區塊為合理使用區間)

- 對頻寬使用率的預測

  (未來數個月的走勢)

市場上最佳CP值日誌收集系統

內建法規報表與數百種知名日誌正規化功能

內建數百種日誌正規化格式,易於查詢與分析

正規化前

Hostname="f5demo.bestcom.coom.tw",SlotId="0",errdefs_msgno="22282249",Entity="ACL_FORCE",AggrInterval="300",EOCTimestamp="1500459900",HitCount="1",ApplicationName="<Unassigned>",RuleName="Allow_443",ContextType="Management Port",ContextInfo="/Common/self_1",Action="Accept",VLAN="/Common/int_1",Policy="Aggregated",SourceIp="210.71.213.29",SourceIpRouteDomain="0",SourcePort="35031",DestinationIp="192.168.10.145",DestinationIpRouteDomain="0",DestinationPort="443",SaTranslationPool="Aggregated",SaTranslationType="None",SelfIp="Aggregated",SelfRouteDomain="0",ServerIp="Aggregated",ServerRemoteRouteDomain="0",SrcCountry="TW",SrcRegion="N/A",DstCountry="N/A",DstRegion="N/A",SrcUserName="Aggregated",DstUserName="No-Lookup"

正規化後

事件	來源IP	來源Port	來源名稱解析	來源區域	目的IP	目的Port	目的名稱解析
Information Leakage,HTTP Parser Attack: HTTP protocol compliance failed,Illegal method,Illegal HTTP status in response	61.60.98.238	3700		TW	74.125.31.27	80	Google
Entity="ACL_FORCE", SaTranslationType="None"	210.71.213.29	35031		TW	192.168.10.145	443	Home

目的區域	來源Port解析	目的Port解析	Audit User	目的主機名稱	路徑	參數	狀態	分類	應用服務
US					gmail-smtp-in.l.google.com		405	Network Event	HTTP
				Aggregated	/Common/self_1				Unassigned

次數	Session	Packets	Bytes	Protocol	時間	設備	事件型態	等級	Policy ID	動作
1	0	0	0	N/A	2017/07/19 22:00:59	f5 asm10.10.10.73	traffic	Critical		Permit
1	0	0	0	N/A	2017/07/19 22:00:59	F5 LTM 10.10.10.56			Allow_443	Permit

來源使用者	目的使用者	來源MAC	目的MAC	Session ID	NAT 來源IP	NAT 來源Port	NAT 目的IP	NAT 目的Port	來源IP所屬交換機/介面	目的IP所屬交換機/介

內建多種好用的報表與稽核要求之法規報表

法規報表 法規類別

法規類別 ISO 27001 | 過濾條件 | 重新輸入 | 啟動查詢

- ISO 27001
- HIPPA
- SOX
- GDPR
- PCIDSS
- NIST
- GLBA
- ISLP

A.8.20 保全、管理及控制網路與網路裝置，以保護系統及應用程式中之資訊。
A.8.22 隔組織網路中各群組之資訊服務、使用者及資訊系統。

使用者活動

設備名稱	登入	登出	登入失敗
Herb Global Win2k3 file CHT 192.168.2.71	5757 (22.22%)	8635 (33.33%)	11514 (44.45%)
Herb Global Win2k3 AD ENG 192.168.2.72		2880 (100.00%)	
Herb Global Win2k3 AD CHT 192.168.1.70	5760 (22.22%)	2880 (11.11%)	17280 (66.67%)
Fortigate 60E 2.253中文測試	259 (50.00%)	259 (50.00%)	
Herb Win2k3 ENG 192.168.2.83	2879 (20.00%)	8635 (59.99%)	2879 (20.00%)

25 | 第 1 共1頁 | 顯示1到11,共11記錄

A.8.15 存錄：記錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。

物件存取報表

設備名稱	檔案讀取	檔案修改	檔案刪除	讀取錯誤	其它
Herb Global Win2k3 file CHT 192.168.2.71	2880 (25.00%)	5760 (50.00%)	2880 (25.00%)		
Herb Win2k3 ENG 192.168.2.83	2879 (25.00%)	2879 (25.00%)	2880 (25.00%)	2880 (25.00%)	
Herb Win2k8 ENG 192.168.2.84	2880 (16.67%)	8640 (50.00%)	2880 (16.67%)	2880 (16.67%)	
Hunter-Demo Server	1 (0.00%)	4 (0.00%)			162599 (100.00%)

25 | 第 1 共1頁 | 顯示1到4,共4記錄

A.8.15 存錄：記錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。

系統事件報表

設備名稱	開機	關機	程序起動	程序關閉	其它
No data!					

A.8.15 存錄：記錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。

追蹤帳戶管理的變更

設備名稱	建立使用者	刪除使用者	變更使用者密碼
Herb Global Win2k3 AD CHT 192.168.1.70	2880 (50.00%)		2880 (50.00%)
Wind2k8AD 8.90	2880 (100.00%)		
Herb Global Win2k8 CHT 192.168.1.90	2880 (16.67%)	2880 (16.67%)	11520 (66.67%)

A.8.5 安全鑑別：安全鑑別技術及程序應依資訊存取限制及關於存取控制之主題特定政策實做。

追蹤使用者群組的變更

設備名稱	建立群組	變更群組	刪除群組
Herb Global Win2k8 CHT 192.168.1.90	5760 (50.00%)		5760 (50.00%)

A.8.5 安全鑑別：安全鑑別技術及程序應依資訊存取限制及關於存取控制之主題特定政策實做。
A.8.15 存錄：記錄活動、異常、錯誤及其他相關事件之日誌，應產生、儲存、保護及分析之。

追蹤稽核規則的變更

設備名稱	使用者稽核	網域稽核
Herb Global Win2k8 CHT 192.168.1.90	20160 (87.50%)	2880 (12.50%)

N-Cloud 7

網路實名制

IP自動對應使用者名稱 定位所在Switch-Interface

網路實名制-以人的角度出發查找資訊

什麼時間　什麼事情　什麼人　什麼地方　什麼設備

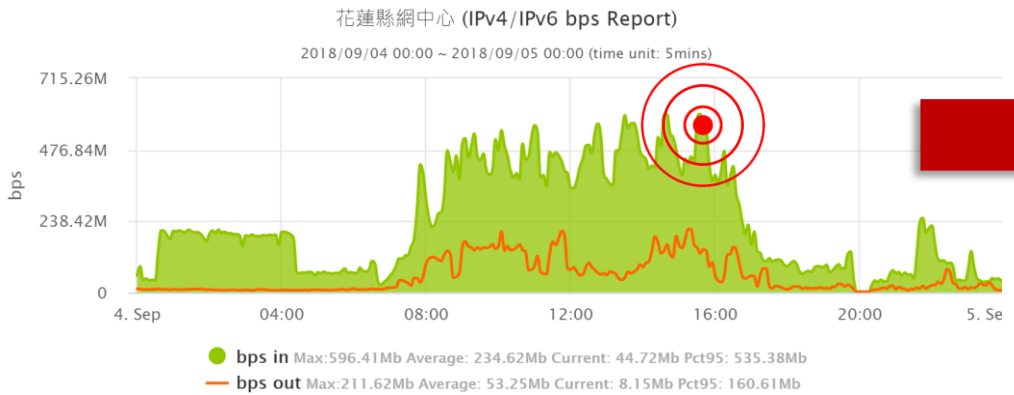
時間	事件	來源 IP	來源使用者名稱	來源 IP 名稱解析	來源 IP 所屬交換機/介面	目的 IP	目的 IP 名稱解析	目的區域	來源主機名稱	來源 Port	目的 Port
2023/09/18 15:44:50		10.10.0.58	nc70016	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	203.66.34.5	-	TW (臺灣)	Zipxcvrs-iPhone	57132	443
2023/09/18 11:19:09		10.10.0.58	nc70016	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	203.66.34.5	-	TW (臺灣)	Zipxcvrs-iPhone	55546	443
2023/09/18 11:16:06		10.10.0.58	nc70016	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	203.66.34.5	-	TW (臺灣)	Zipxcvrs-iPhone	55473	443
2023/09/18 11:16:01		10.10.0.58	nc70016	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	203.66.34.5	-	TW (臺灣)	Zipxcvrs-iPhone	55473	443
2023/09/18 10:46:35	50200 : TCP SYN Port Scan	192.168.5.55	husan	總公司辦公室 Office	NP Core Sw/GigabitEthernet1/0/6	181.191.243.254	-	BR (巴西)		-	-
2023/09/18 16:14:10		192.168.5.106	max	總公司辦公室 Office	NP Core Sw/GigabitEthernet1/0/16	210.65.144.163	-	TW (臺灣)		52594	80
2023/09/18 16:14:10		192.168.5.106	max	總公司辦公室 Office	NP Core Sw/GigabitEthernet1/0/16	13.35.166.109	Amazon	TW (臺灣)		52547	443
2023/09/18 16:14:09	Dns Response: a1961.g2.akamai.net	10.10.0.80	nc70053	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	8.8.8.8	Google	US (美國)	iPad-mini	53815	53
2023/09/18 16:14:09	Dns Response: uts-front.line-apps.com	10.10.0.80	nc70053	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	8.8.8.8	Google	US (美國)	iPad-mini	52201	53
2023/09/18 16:14:09	Dns Response: uts-front.line-apps.com	10.10.0.80	nc70053	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	8.8.8.8	Google	US (美國)	iPad-mini	63480	53
2023/09/18 16:14:09	Dns Response: ogs.google.com.tw	10.10.0.80	nc70053	13樓辦公室	Ruckus ICX/GigabitEthernet1/1/5	8.8.8.8	Google	US (美國)	iPad-mini	60234	53
2023/09/18 16:14:09	Dns Response: ogs.google.com.tw	192.168.5.141	claire	總公司辦公室 Office	NP Core Sw/GigabitEthernet1/0/16	74.125.23.188	Google	US (美國)		14683	5228
2023/09/18 16:14:08		192.168.5.14	kevin	總公司辦公室 Office	NP Core Sw/GigabitEthernet1/0/16	8.8.8.8	Google	US (美		53785	53

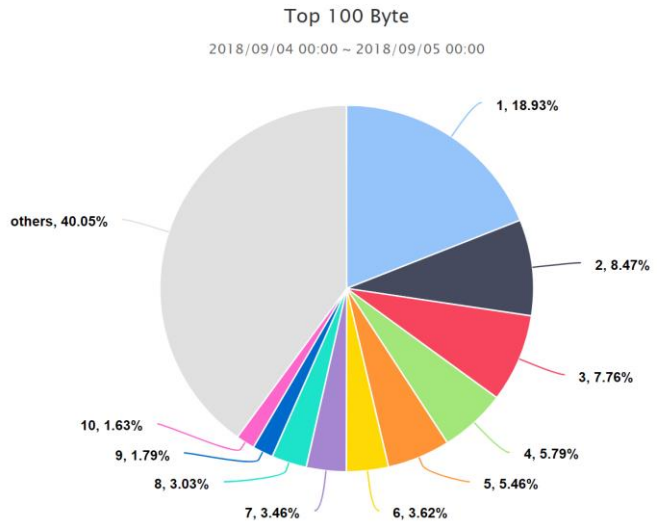
單一平台就可以總覽網路全貌，維運真有效率！

強大的網路流量數據分析能力

手握即時發覺爆發型病毒的利器

只要用滑鼠點擊, 就能簡單找到重度網路使用者

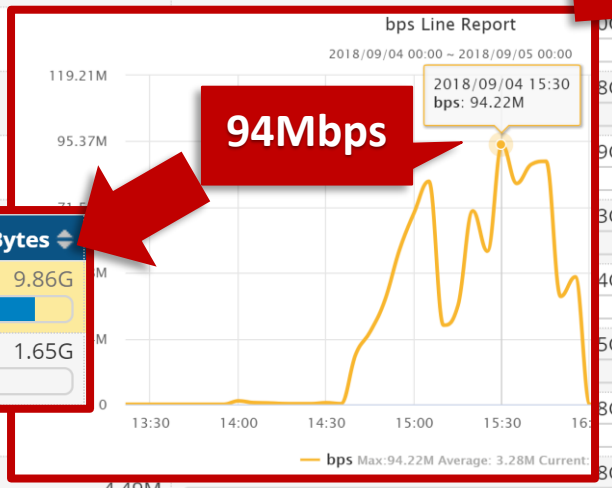




掌握到重度使用者

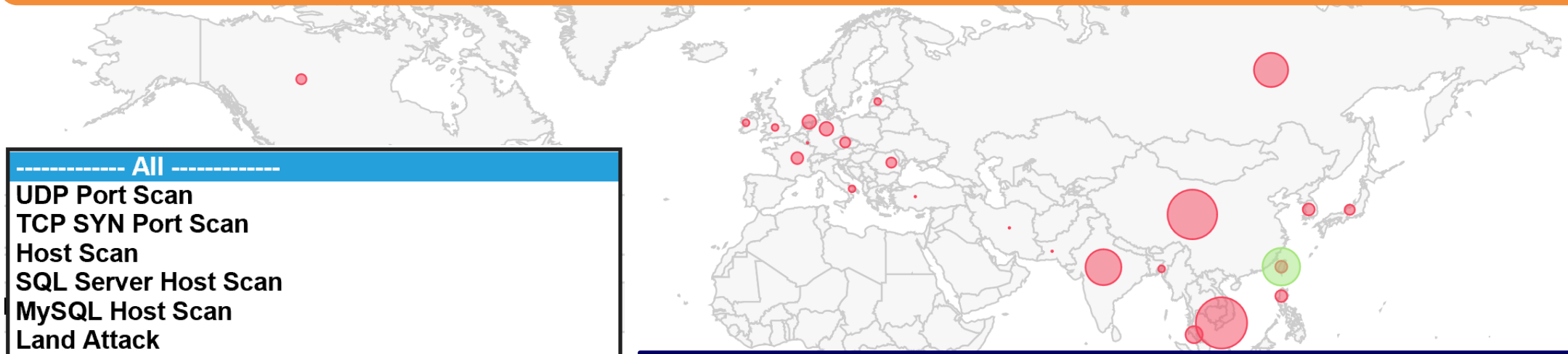
NO	來源 IP 名稱解析	Sessions	Packets	Bytes	流量圖
1	太昌國小	161.48K	28.89M	34.64G 18.93%	
2	新城國中	132.75K	14.15M	8.47%	
3	壽豐國小	96.13K			
4	北昌國小	140.63K			
5	春日國小	162.25K			
9	港口國小	92.17K			
10	志學國小	393.37K	4.49M	1.63%	

NO	來源 IP	目的 IP	目的 Port	目的 IP 名稱解析	目的區域	Sessions	Packets	Bytes
1	10.100.157.26	172.217.24.10	TCP:443	Google	US	41	6.79M	9.86G 85%
2	10.100.157.26	172.217.160.106	TCP:443	Google	US	11	1.12M	1.65G 14.19%



智慧學習Flow即時分析是發現網路攻擊行為的利器

內建多種分析演算法,根據NetFlow/sFlow資料即時且主動發掘網路攻擊行為

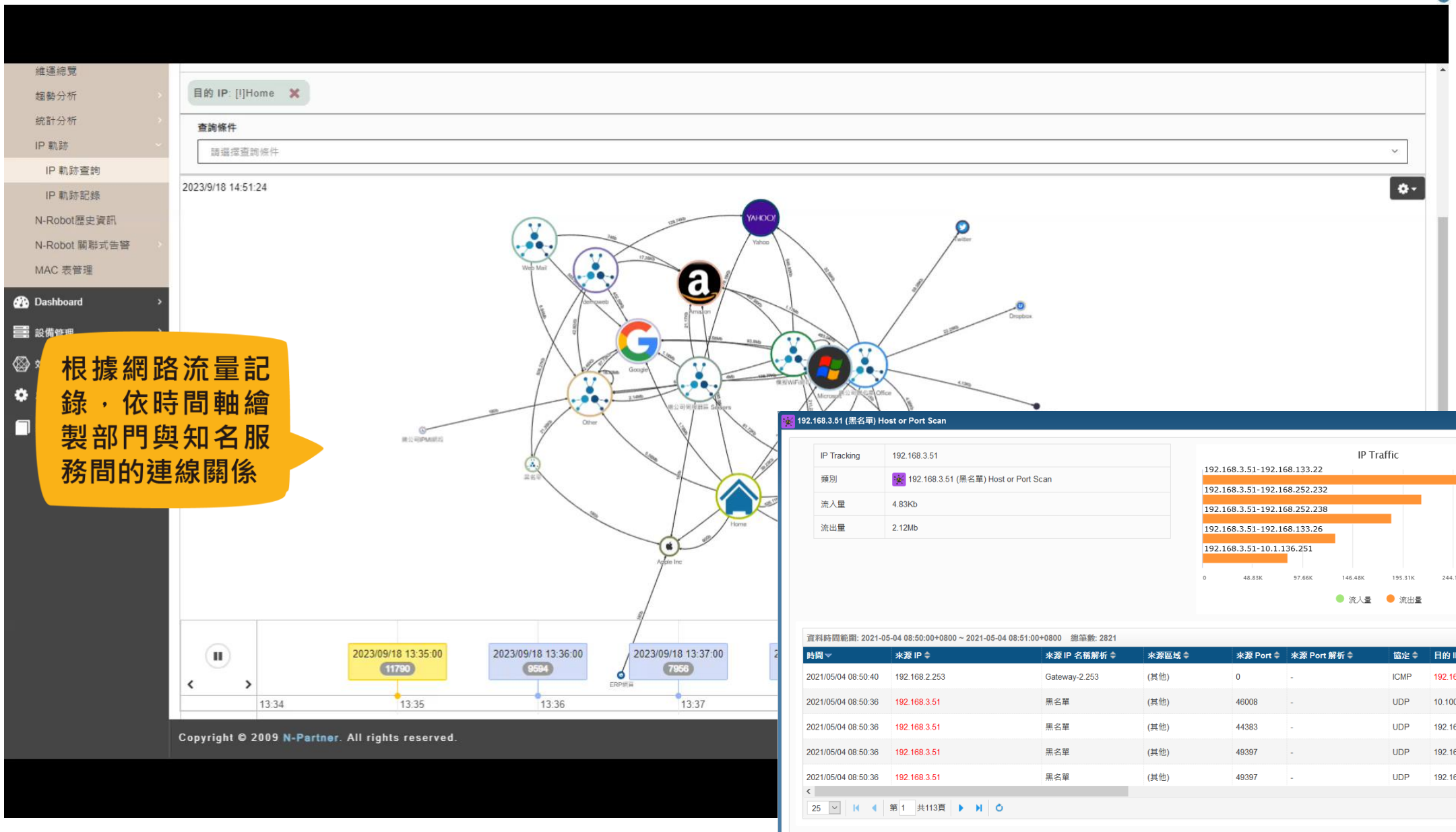


- ---------- All ----------
- UDP Port Scan
- TCP SYN Port Scan
- Host Scan
- SQL Server Host Scan
- MySQL Host Scan
- Land Attack
- Possible Spoofed TCP SYN DDoS Attack
- Possible Spoofed TCP SYN/ACK DDoS Attack
- Possible Spoofed TCP FIN/ACK DDoS Attack
- Possible Spoofed TCP Rst DDoS Attack
- Possible Spoofed TCP NULL Flag Attack
- Possible Spoofed ICMP DDoS Attack
- TCP SYN Host Scan
- Possible Spoofed UDP DDoS Attack
- Burst Session on Source
- Burst Session on Destination

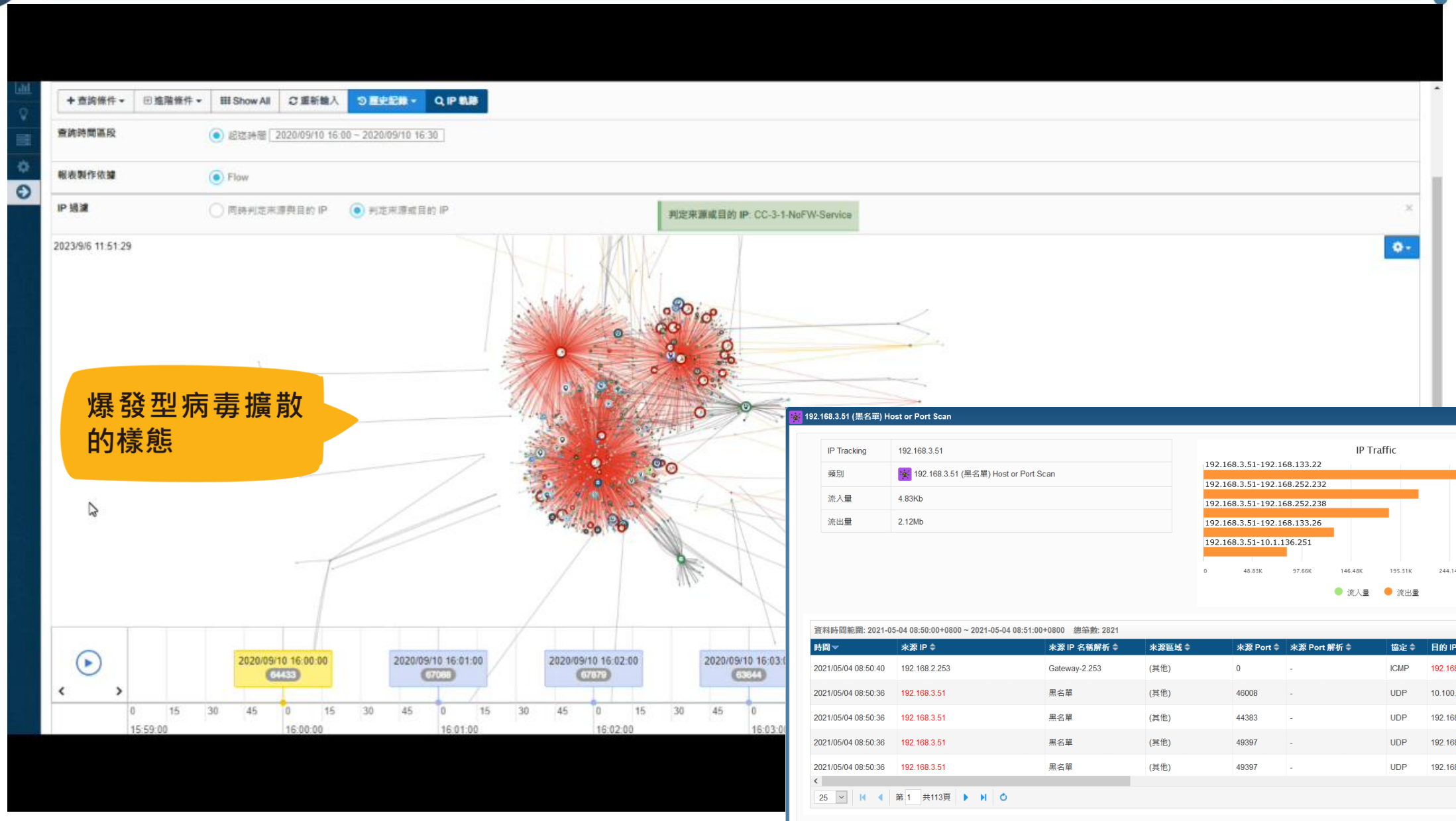
異常項目	攻擊者 IP	協定	目的 Por	Session	Packet	Byte	開始時間	結束時間	瀏覽
TCP SYN Host Scan	222.186.169.217 (CHINANET jiangsu province backbone)	TCP	28282	67.18K	78.19K	3.05M	2020/03/12 18:23	2020/03/12 18:26	
TCP SYN Host Scan	80.82.70.187	TCP	7777	28.36K	35.36K	1.38M	2020/03/12 17:34	2020/03/12 18:26	
TCP SYN Host Scan	222.112.107.46	TCP	8545	142.94K	165.94K	6.48M	2020/03/12 17:29	2020/03/12 18:26	
TCP SYN Host Scan	113.177.101.103	TCP	8291	53.14K	113.51K	5.69M	2020/03/12 18:25	2020/03/12 18:26	

攻擊者區域　受害者區域

網路數位足跡Flow分析(使用者行為掌握)



網路數位足跡Flow分析(爆發型病毒擴散圖樣)

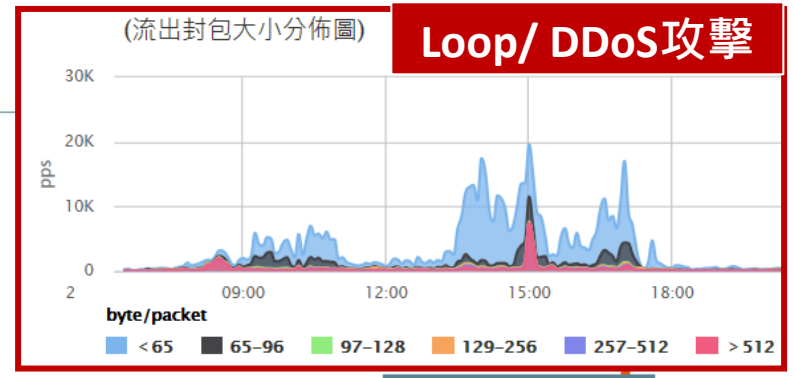


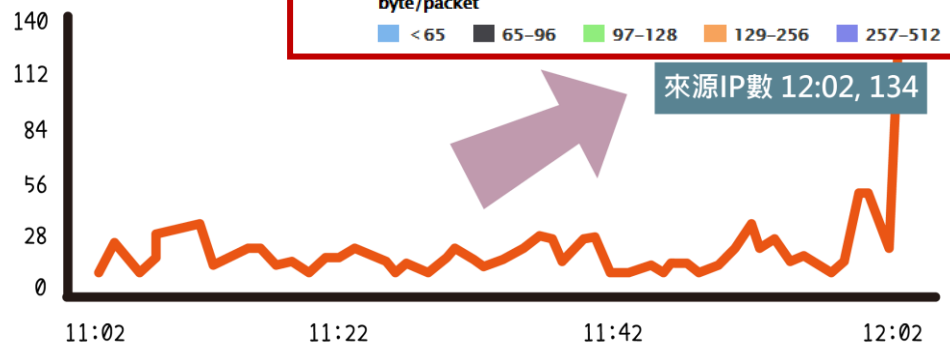
資安強化與聯合防禦

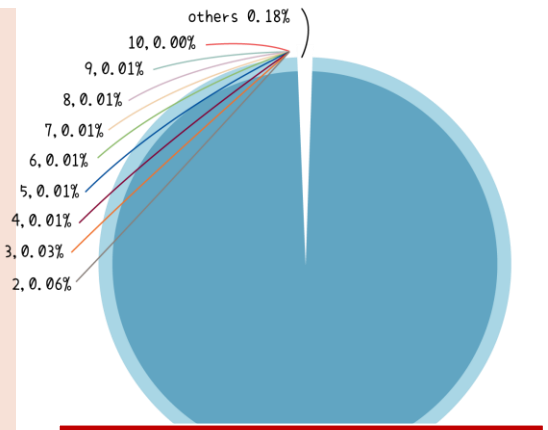
智慧化異常使用分析與即時聯防流程

- NOC+SOC
- Central Management
- Global View and Individual Portal

N-Cloud 7







172.217.24.14 (99.67%)
956,250個小封包

結合情資威脅資料庫

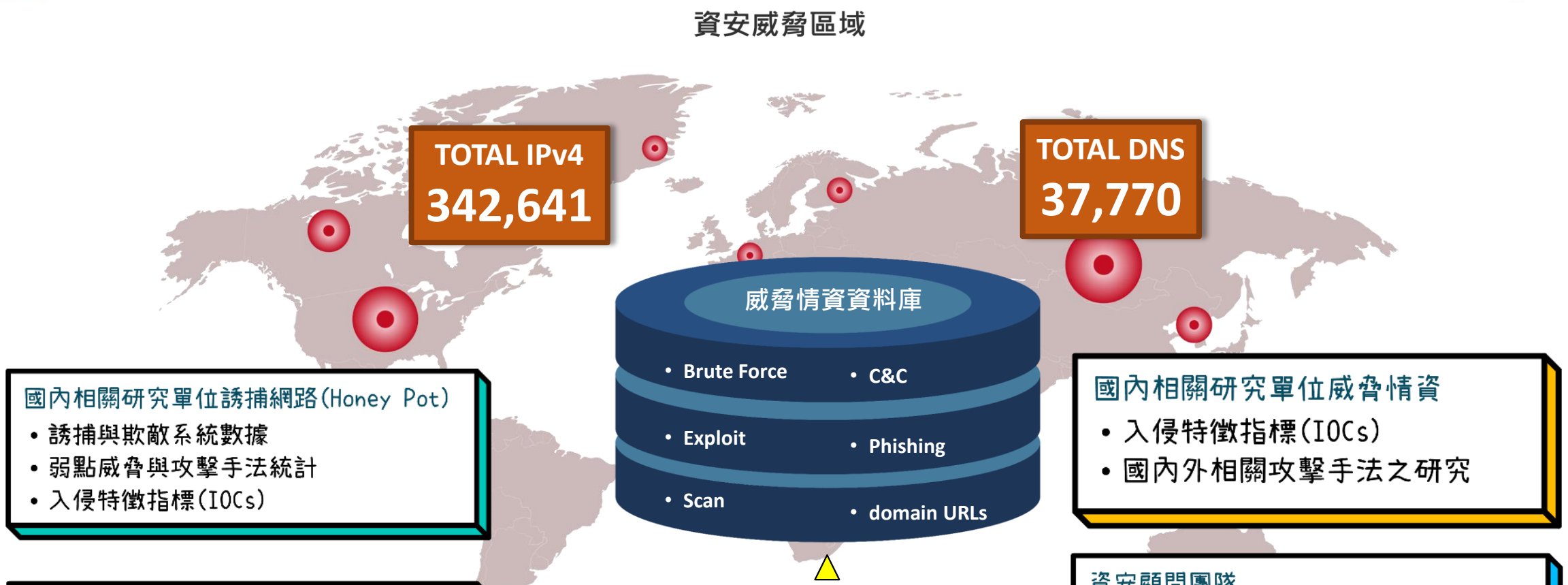
清除內網遭駭客潛伏設備

N-Partner自有威脅情資特點

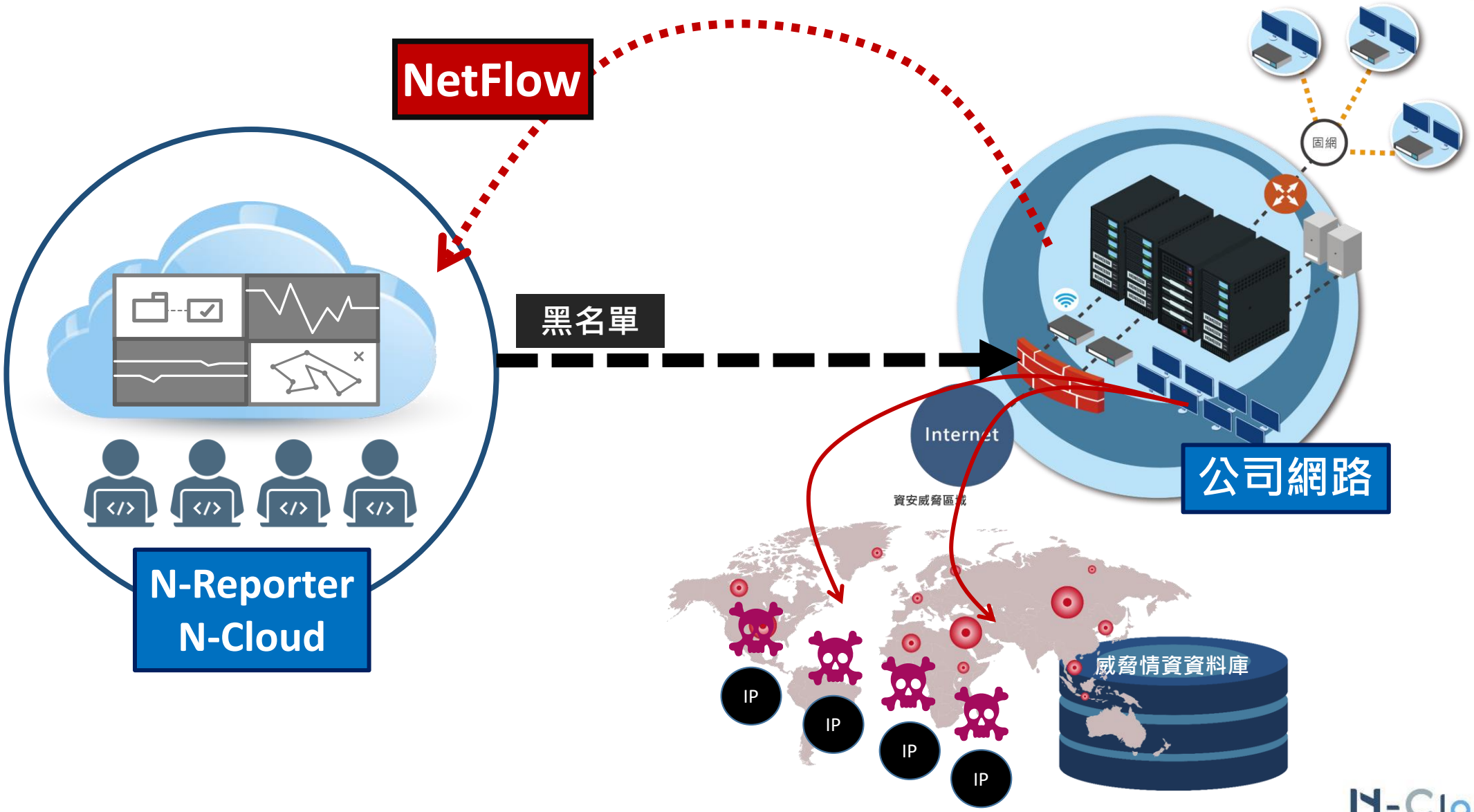
- 針對台灣環境搜集的威脅情資，最完整最符合台灣使用的需求
- 每天更新，確保情資準確性
- 威脅情資即時比對，免除雲端比對等待時間
- 不限特定資安設備聯防，即時攔阻可疑連線

- **客群廣度：超過800+用戶群**，涵蓋政府機關、中大型企業、教育網、金融機構、電信公司...等
- **服務深度：**得依據各個組織體系的需求，**提供對應程度的解決方案或客製服務**，創造競爭優勢。

內建威脅情資資料庫，大幅降低企業網路遭入侵風險



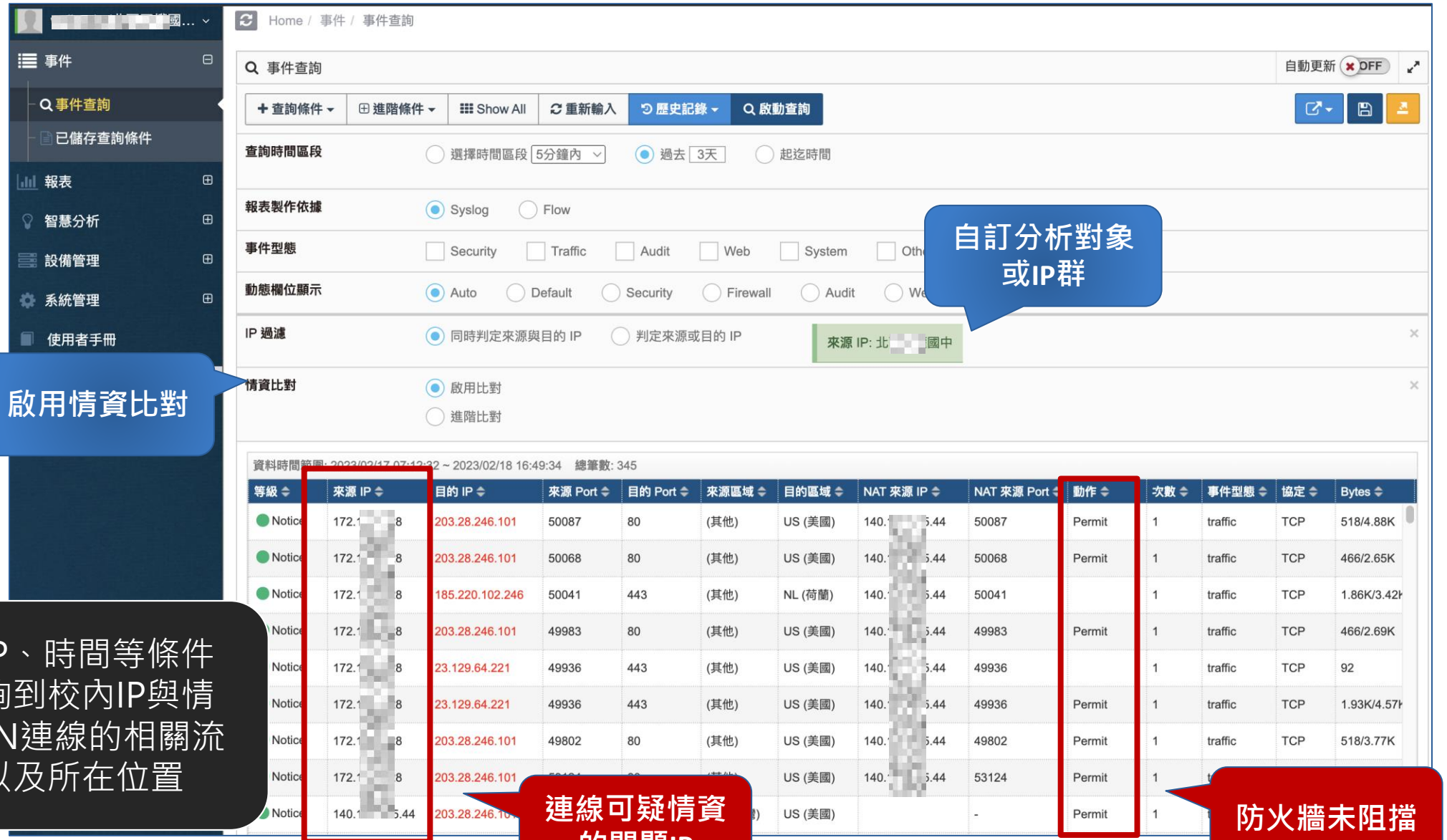
運用威脅情資的比對結果自動調整防禦策略



透過情資比對找出校內潛在風險IP

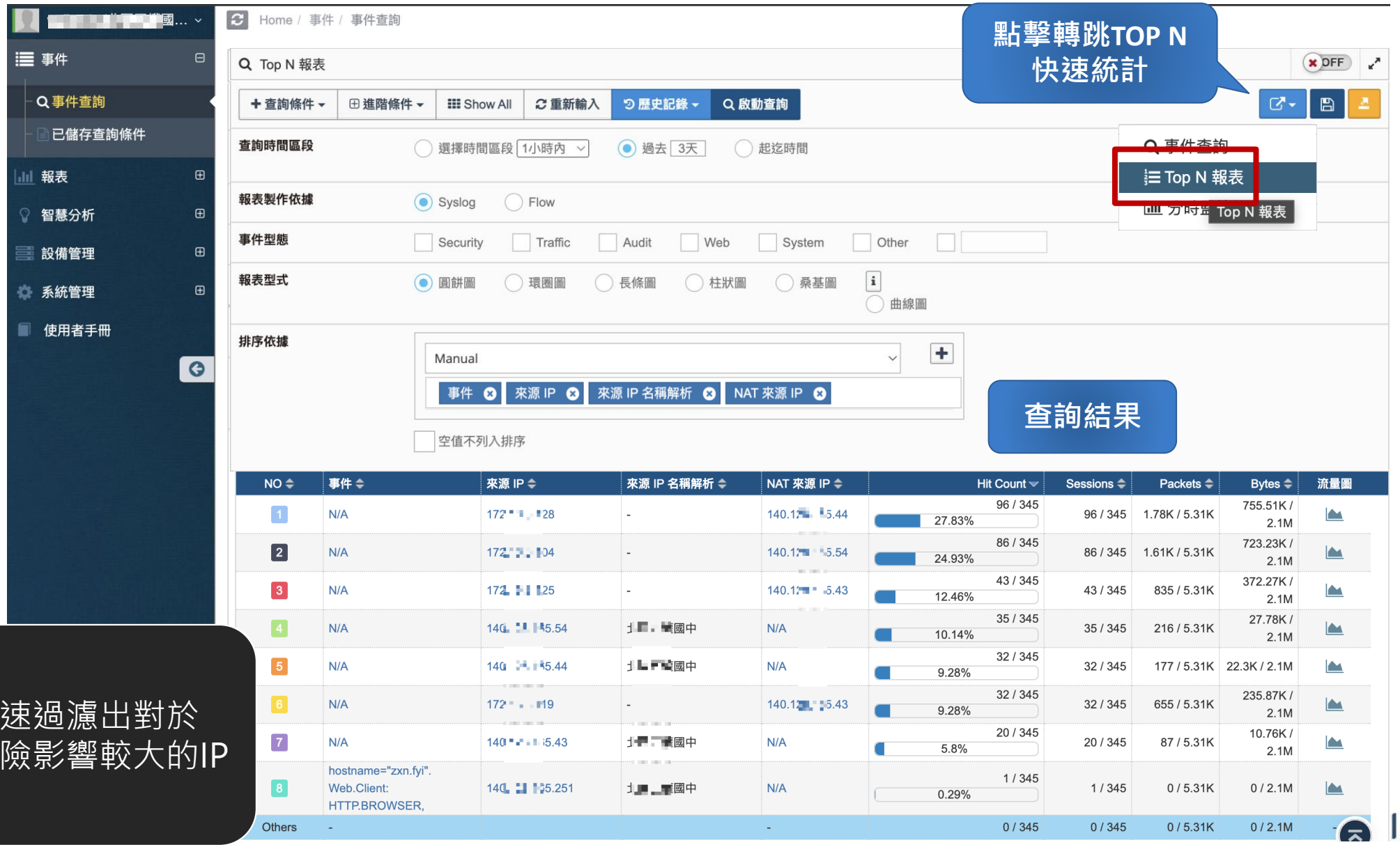
校內連線全球威脅情資黑名單監控

透過N-Reporter/N-Cloud查找校內潛在資安風險



簡單輸入IP、時間等條件可快速查詢到校內IP與情資IP/FQDN連線的相關流量紀錄，以及所在位置

校內連線全球威脅情資黑名單監控統計



透過統計快速過濾出對於
校內資安風險影響較大的IP

更美觀的Dashboard

創造專屬戰情中心

SNMP

設備健康狀態(Up/Down)

性能使用率(CPU/記憶體/頻寬)

資產清單

Flow

Syslog

Flow

封包大小與協議監控

NetFlow/sFlow

繪製流量圖

L3/L4 數據

流量使用分析

流量型DDoS分析依據

Syslog

L7 應用層資料

記錄使用者使用行為

用來分析資訊安全情況

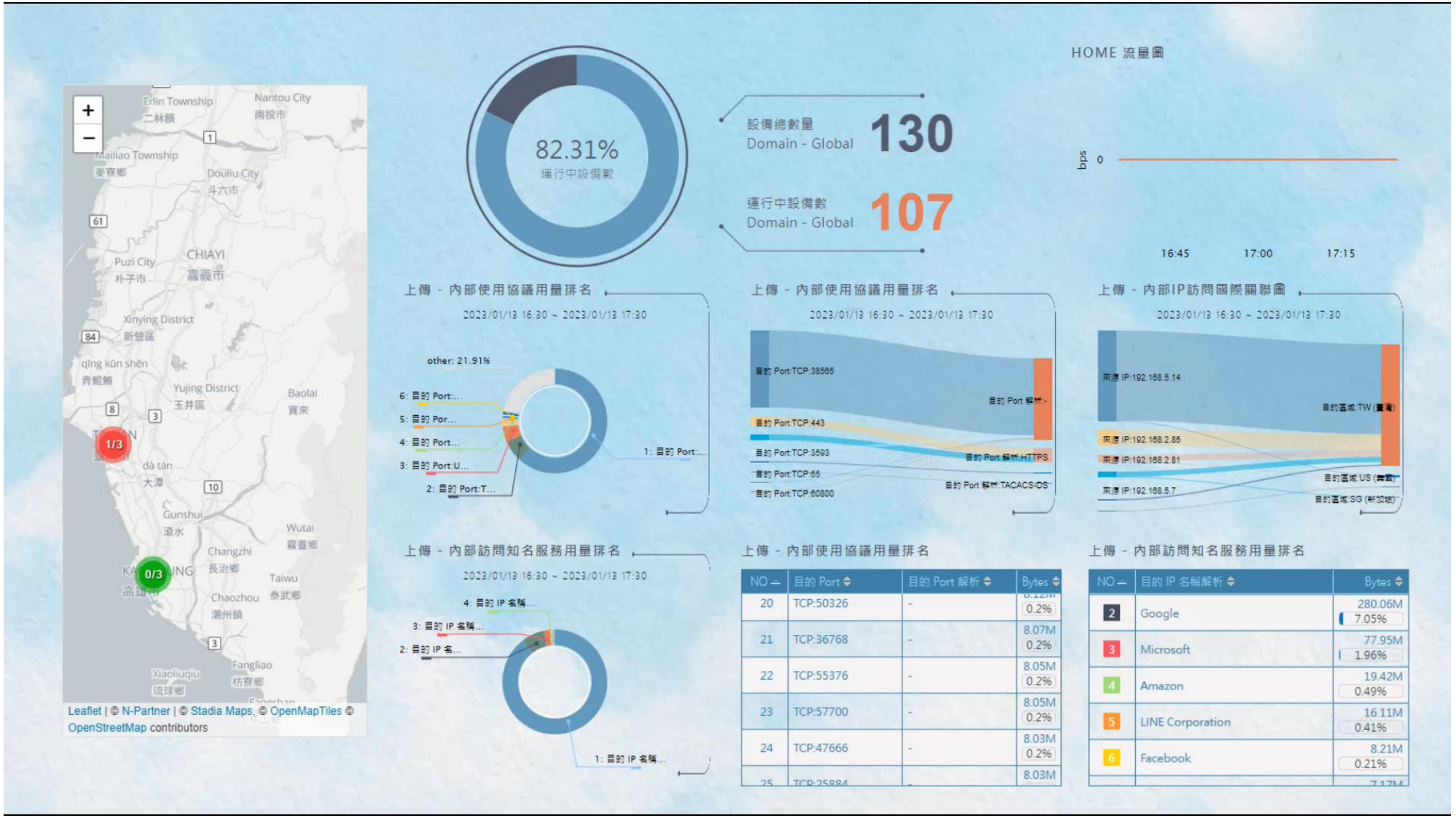
安全產品、網路設備、伺服器事件記錄

/稽核記錄/系統日誌

建構成全視角 NOC + SOC 的即時戰情中心

N-Cloud 7

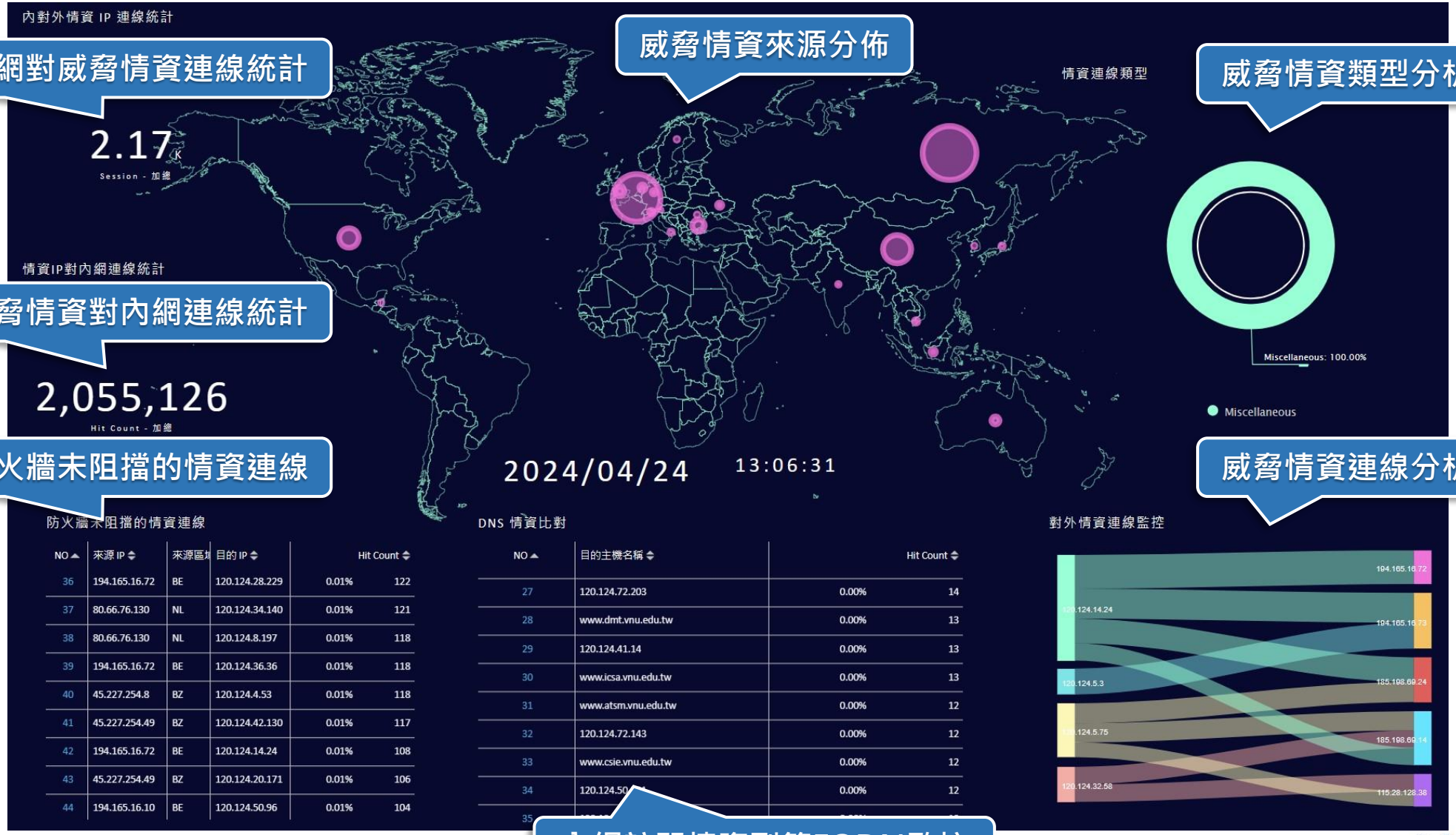
建構成全視角 NOC + SOC 的即時戰情中心



NO	目的 Port	目的 Port 解析	Bytes
20	TCP:50326	-	0.2%
21	TCP:36768	-	8.07M 0.2%
22	TCP:55376	-	8.05M 0.2%
23	TCP:57700	-	8.05M 0.2%
24	TCP:47666	-	8.03M 0.2%

NO	目的 IP 名稱解析	Bytes
2	Google	280.06M 7.05%
3	Microsoft	77.95M 1.96%
4	Amazon	19.42M 0.49%
5	LINE Corporation	16.11M 0.41%
6	Facebook	8.21M 0.21%

威脅情資可視化-系統內建威脅情資Dashboard



NO	來源 IP	來源區域	目的 IP	Hit Count	
36	194.165.16.72	BE	120.124.28.229	0.01%	122
37	80.66.76.130	NL	120.124.34.140	0.01%	121
38	80.66.76.130	NL	120.124.8.197	0.01%	118
39	194.165.16.72	BE	120.124.36.36	0.01%	118
40	45.227.254.8	BZ	120.124.4.53	0.01%	118
41	45.227.254.49	BZ	120.124.42.130	0.01%	117
42	194.165.16.72	BE	120.124.14.24	0.01%	108
43	45.227.254.49	BZ	120.124.20.171	0.01%	106
44	194.165.16.10	BE	120.124.50.96	0.01%	104

NO	目的主機名稱	Hit Count	
27	120.124.72.203	0.00%	14
28	www.dmt.vnu.edu.tw	0.00%	13
29	120.124.41.14	0.00%	13
30	www.icsa.vnu.edu.tw	0.00%	13
31	www.atsm.vnu.edu.tw	0.00%	12
32	120.124.72.143	0.00%	12
33	www.csie.vnu.edu.tw	0.00%	12
34	120.124.50.	0.00%	12
35			

提供多種類型的Dashboard選擇

資安　設備監控　流量分析　PM　SLA

資安通報單處理

快速反查校內異常IP

資安通報單範例-OO國民中小學

以下是資訊老師收到的資安通報單上範例，只有**IP**及事件**發現時間**資訊，缺乏詳細事件之條列

詳細資料			
發佈編號	ASOC-INT-202003-087[redacted]	發佈時間	2020-03-25 13:15:14
事件類型	對外攻擊	發現時間	2020-03-25 12:09:27
事件主旨	通報:[臺中市立[redacted]小學][redacted]86.89 General.Interest: Monero.Cryptocurrency.Miner,		
事件描述	ASOC發現貴單位(臺中市立[redacted]小學)所屬 [redacted]86.89 疑似對外進行 General.Interest: Monero.Cryptocurrency.Miner, 攻擊		
手法研判	手法研判		
處理建議	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠。 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.確實安裝修補程式並且更新系統。 5.攻擊名稱相關參考資料網站： https://fortiguard.com/appcontrol/44016 https://github.com/fireice-uk/xmr-stak-cpu https://en.wikipedia.org/wiki/Monero_(cryptocurrency)		
參考資料	無		

IP

時間

過往的做法: 請ASOC調閱詳細事件

透過信件方式來往不僅費時費力，取得的詳細資安事件內容又常與資安通報單上所標註的時間不符，造成資訊老師在查找與回覆障礙根源時的困難

向ASOC調閱來的事件內容
只有校內對外NAT IP

開始時間	結束時間	名稱	訊息	設備事件彙總的事件計數	攻擊者位	攻擊者連接埠	攻擊者主	攻擊者 F	攻						位置	要求 URI
2020/3/25 10:59	2020/3/25 10:59	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57179									NL
2020/3/25 10:59	2020/3/25 10:59	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57179									NL
						86.89	57179									NL
						86.89	57179									NL
						86.89	57165			TW		255.96.192	3333		荷蘭	NL
						86.89	57165			TW	台灣	5.255.96.192	3333		荷蘭	NL
						86.89	57165			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:59	2020/3/25 10:59	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57165			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:57	2020/3/25 10:57	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57147			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:57	2020/3/25 10:57	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57147			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:57	2020/3/25 10:57	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57147			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:57	2020/3/25 10:57	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57147			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:57	2020/3/25 10:57	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57147			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:57	2020/3/25 10:57	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57147			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:56	2020/3/25 10:56	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57122			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:56	2020/3/25 10:56	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57122			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:56	2020/3/25 10:56	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57122			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:56	2020/3/25 10:56	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57121			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:56	2020/3/25 10:56	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57121			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:55	2020/3/25 10:55	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57120			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:55	2020/3/25 10:55	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57120			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:55	2020/3/25 10:55	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57119			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:55	2020/3/25 10:55	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57119			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:55	2020/3/25 10:55	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57119			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:53	2020/3/25 10:53	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57112			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:52	2020/3/25 10:52	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57109			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:52	2020/3/25 10:52	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57109			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:52	2020/3/25 10:52	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57109			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:52	2020/3/25 10:52	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	57109			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:00	2020/3/25 10:00	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	56283			TW	台灣	5.255.96.192	3333		荷蘭	NL
2020/3/25 10:00	2020/3/25 10:00	utm: app-ctrl	General.Interest: Monero.Cryptocurrency.Miner	utm:app-ctrl		86.89	56283			TW	台灣	5.255.96.192	3333		荷蘭	NL

詳細資料

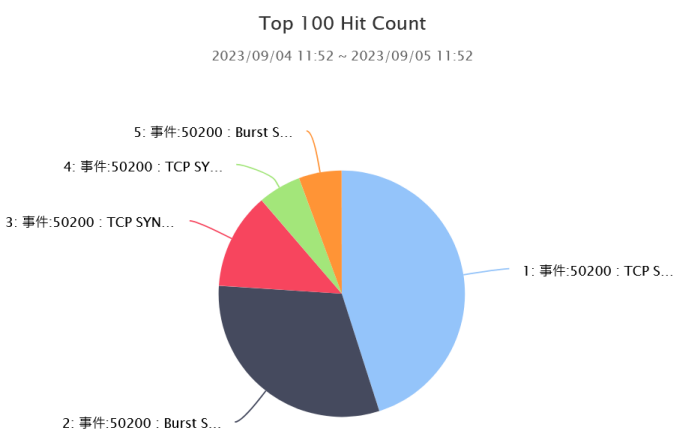
發佈編號	ASOC-INT-202003-0871	發佈時間	2020-03-25 13:15:14
事件類型	對外攻擊	發現時間	2020-03-25 12:09:27

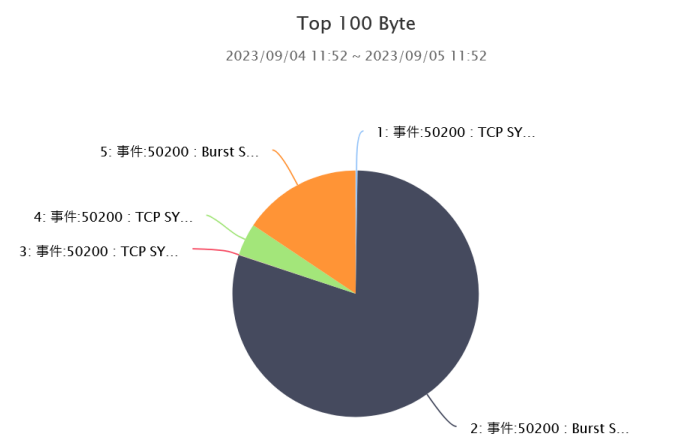
透過N-Reporter/N-Cloud查找資安通報單相關事件

1. 簡單輸入IP、時間等條件可快速查詢到與資安通報單所述IP與行為的相關流量紀錄，以及所在位置
2. 確認後可直接在畫面上按右鍵封鎖有問題的電腦設備IP或是MAC

從一個好用工具變成維運助手

自然語言的互動設計，不會下條件也能輕鬆查障礙



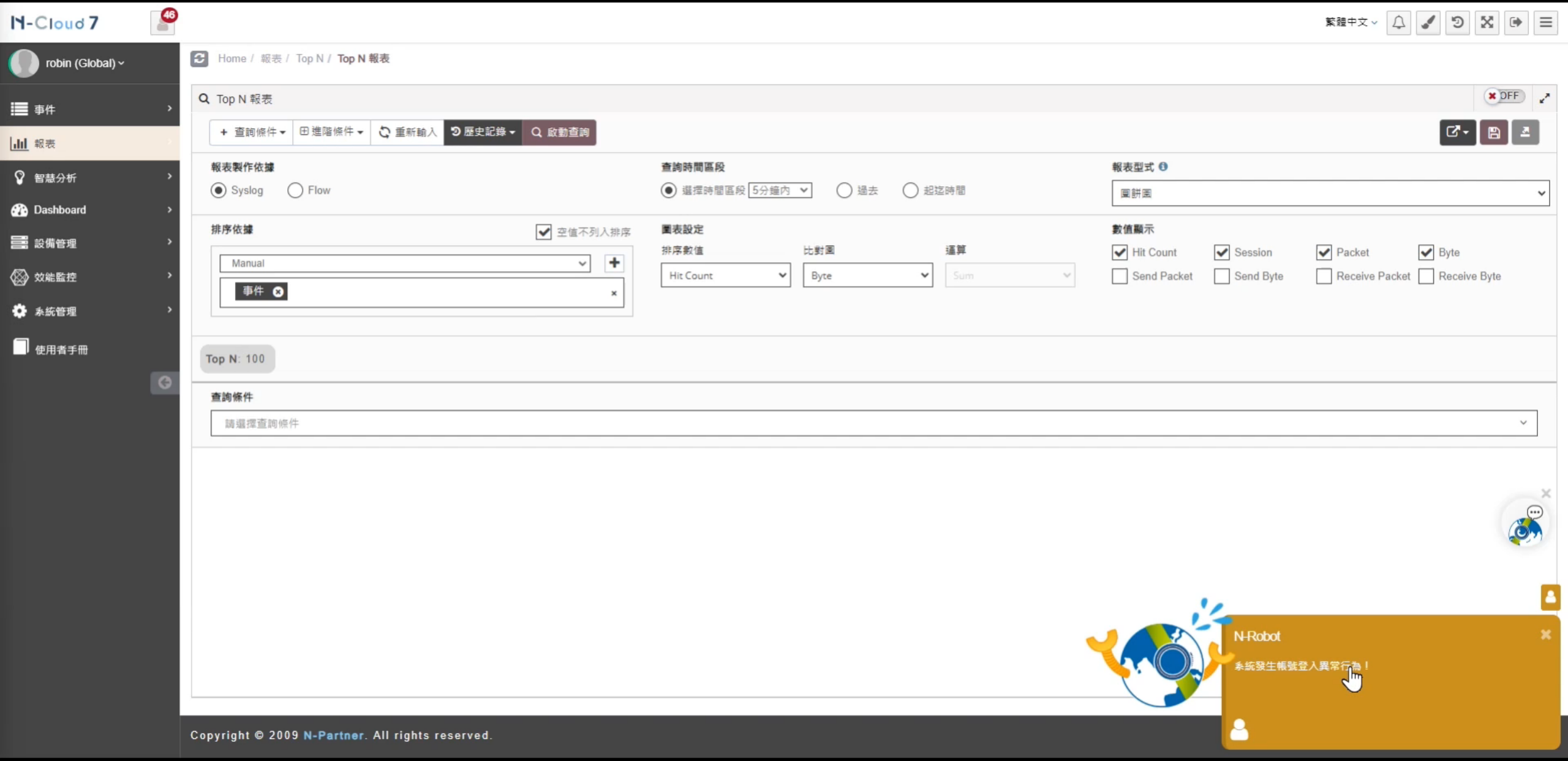


NO	事件	Hit Count	Sessions	Packets	Bytes	流量圖
1	50200 : TCP SYN DDoS Flooding	96 / 213 45.07	149.02K / 31.77M	447.13K / 82.93M	20.67M / 8.27G	
2	50200 : Burst Session on Destination	66 / 213 30.99	25.83M / 31.77M	65.68M / 82.93M	6.61G / 8.27G	
3	50200 : TCP SYN Host Scan	27 / 213 12.68	121.05K / 31.77M	121.11K / 82.93M	4.97M / 8.27G	
4	50200 : TCP SYN Port Scan	12 / 213 5.63	596.2K / 31.77M	3.25M / 82.93M	359.38M / 8.27G	
5	50200 : Burst Session on Source	12 / 213 5.63	5.09M / 31.77M	13.44M / 82.93M	1.29G / 8.27G	
Others	-	0 / 213	0 / 31.77M	0 / 82.93M	0 / 8.27G	-

N-Cloud 7

AI自動學習與預警，主動發覺異行為並與管理者互動處理

除了提供告警資訊，亦可與聯防設備進行阻檔


N-Cloud 7
46
繁體中文
robin (Global)
事件
報表
智慧分析
Dashboard
設備管理
效能監控
系統管理
使用者手冊
Home / 報表 / Top N / Top N 報表
Top N 報表
OFF
+ 查詢條件
進階條件
重新輸入
歷史記錄
啟動查詢
報表製作依據
Syslog
Flow
查詢時間區段
選擇時間區段
5分鐘內
過去
超迄時間
報表型式
圓餅圖
排序依據
空值不列入排序
Manual
事件
圖表設定
排序數值
Hit Count
比對圖
Byte
運算
Sum
數值顯示
Hit Count
Session
Packet
Byte
Send Packet
Send Byte
Receive Packet
Receive Byte
Top N: 100
查詢條件
請選擇查詢條件
N-Robot
系統發生帳號登入異常行為！
Copyright © 2009 N-Partner. All rights reserved.

歡迎加入我們的自營社群

Line官方帳號

FB粉絲團

N-Partner官網

Youtube頻道

N-Partner 為您建構

新一代智慧化IT維運系統

掌握
大小事

除錯
容易

資安
聯防