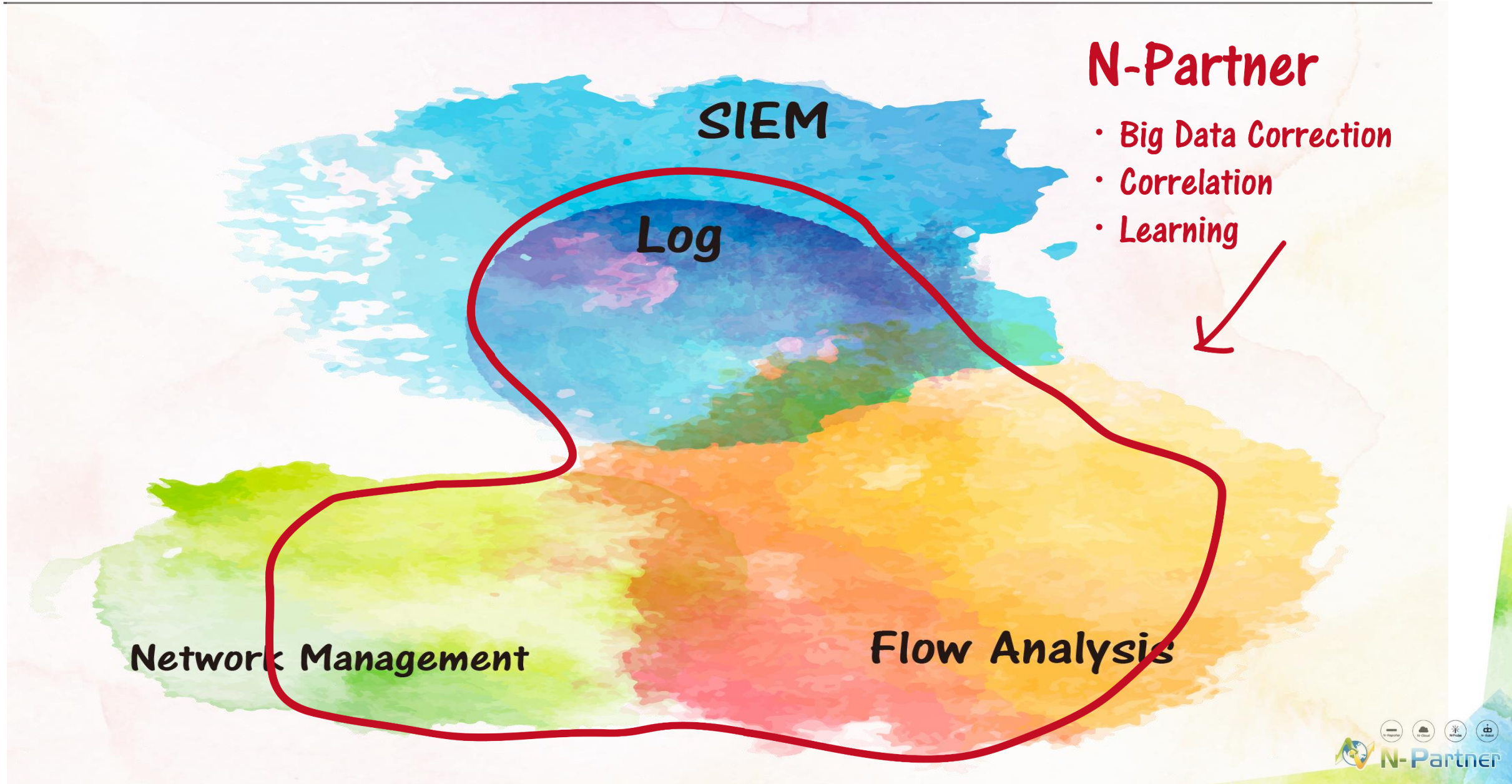
了解IT人的一天: 淺談網路管理/流量分析/日誌收集

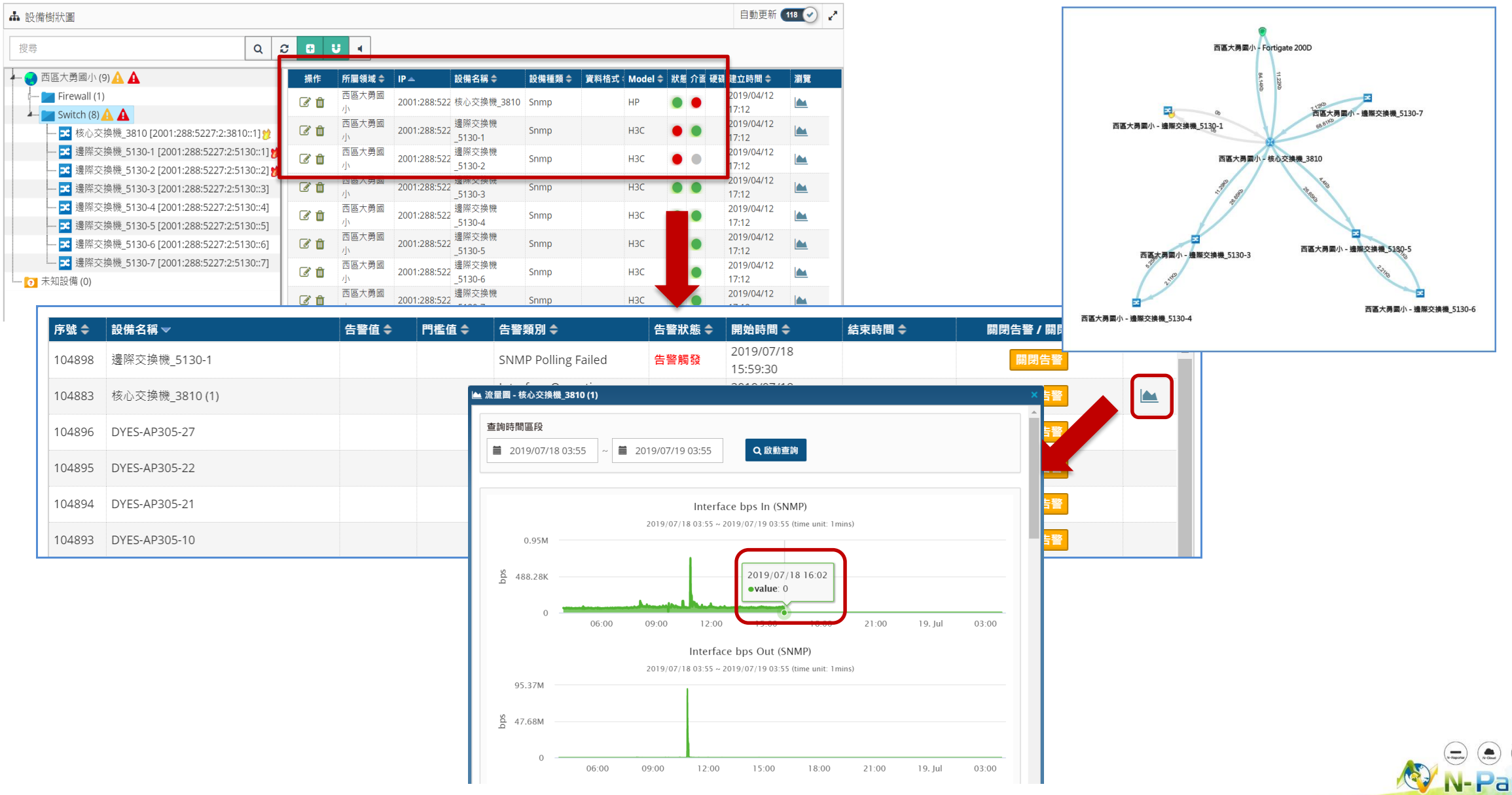
想想醫生診斷病因開立藥方的過程

收集資料 → 智慧分析 → 處置解決

多工多勞的IT人


SIEM
Log
Network Management
Flow Analysis
N-Partner
• Big Data Correction
• Correlation
• Learning

網管: 設備健康狀態的監控

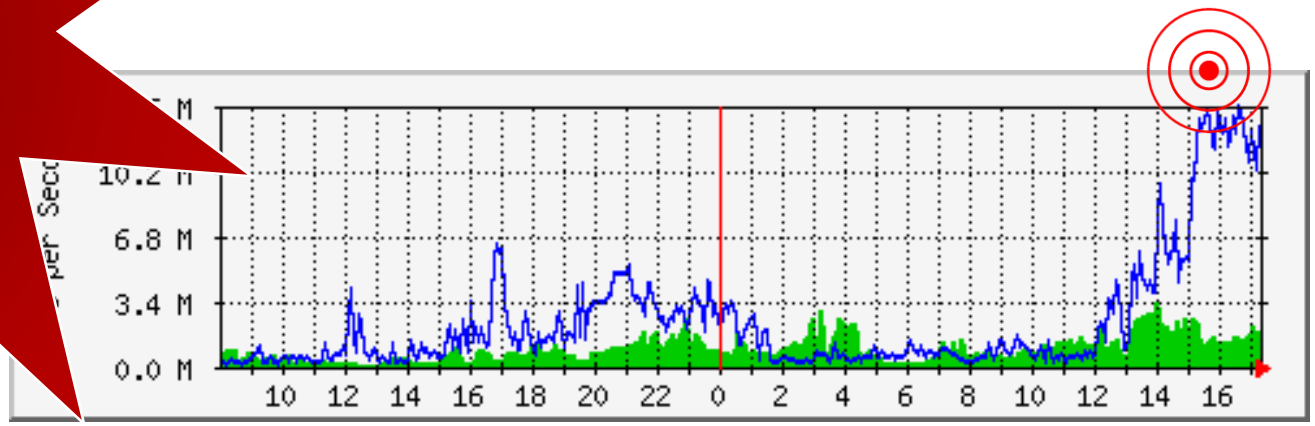


N-Partner

該是把舊的MRTG更換成Flow智慧系統的時候了!

以SNMP為技術基礎的MRTG無法告知異常原因,協助除錯!

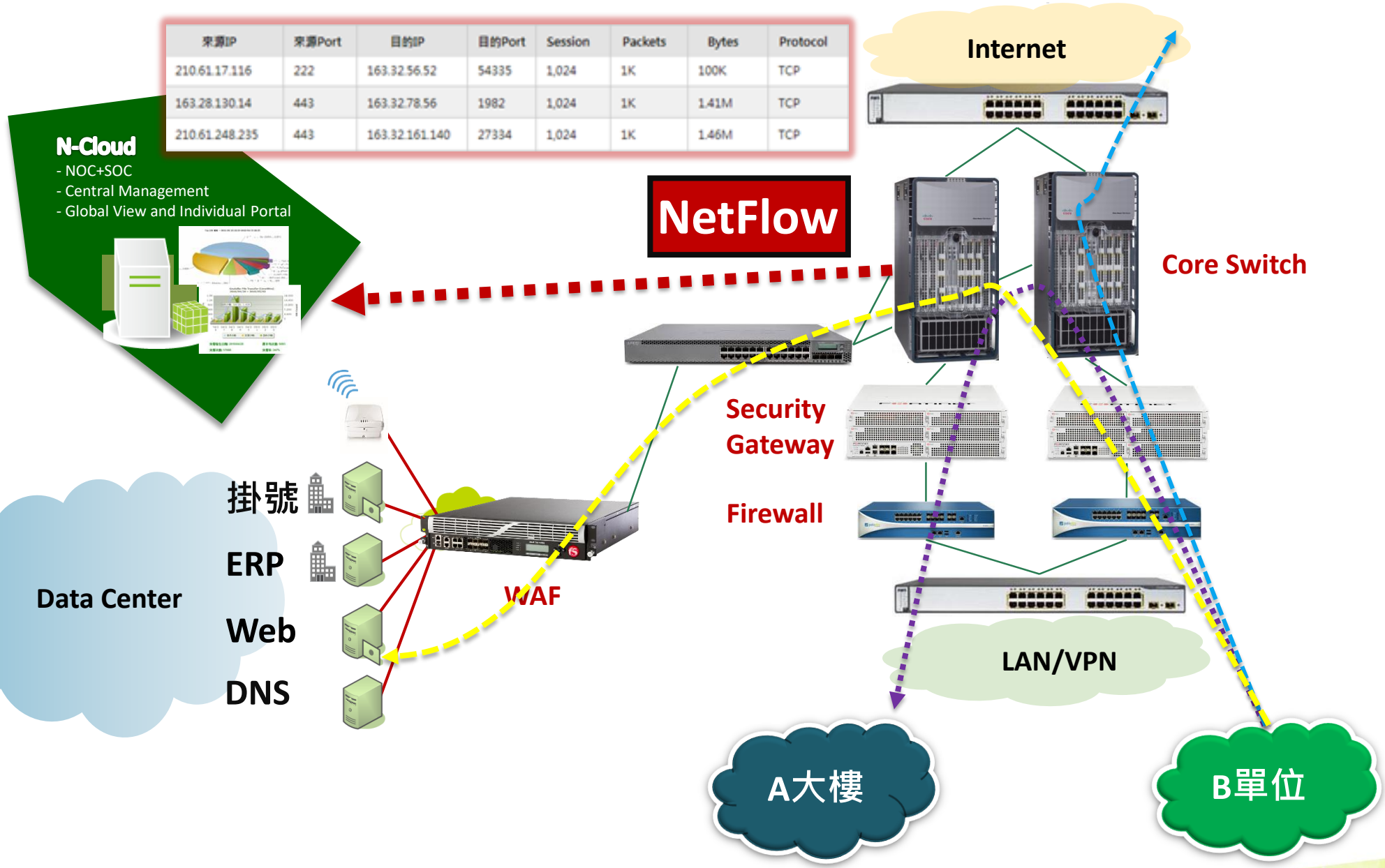
這異常爆量是誰造成的?
IP? 使用者? 所在位置?
甚麼樣的行為?



N-Partner

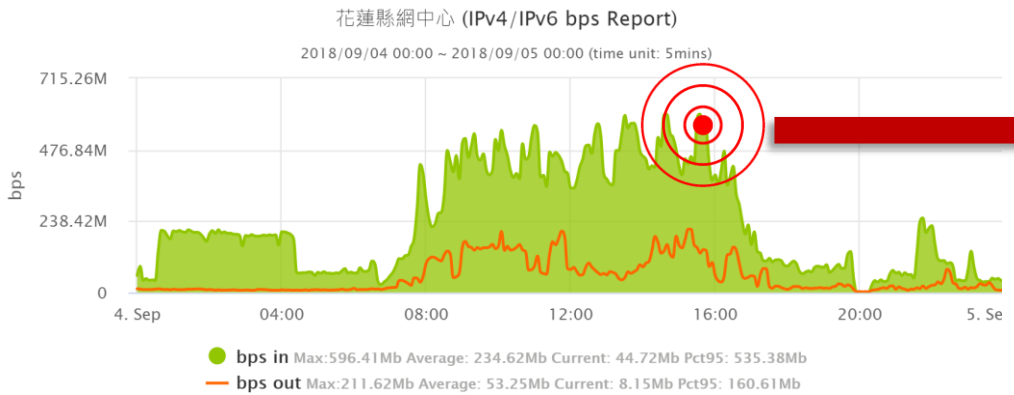
Flow(NetFlow/sFlow)採集

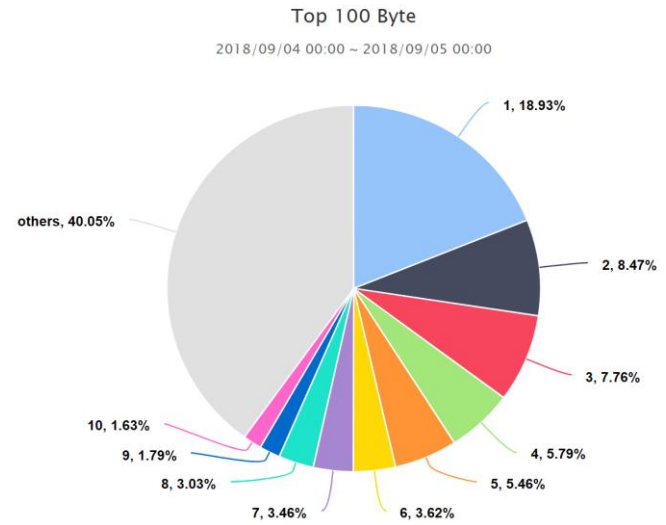
來源IP	來源Port	目的IP	目的Port	Session	Packets	Bytes	Protocol
210.61.17.116	222	163.32.56.52	54335	1,024	1K	100K	TCP
163.28.130.14	443	163.32.78.56	1982	1,024	1K	1.41M	TCP
210.61.248.235	443	163.32.161.140	27334	1,024	1K	1.46M	TCP



N-Partner

清楚掌握每個IP,單位,部門,使用者的網路用量

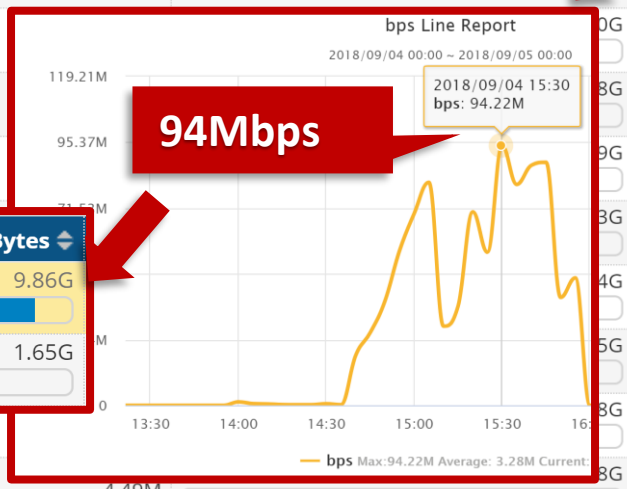




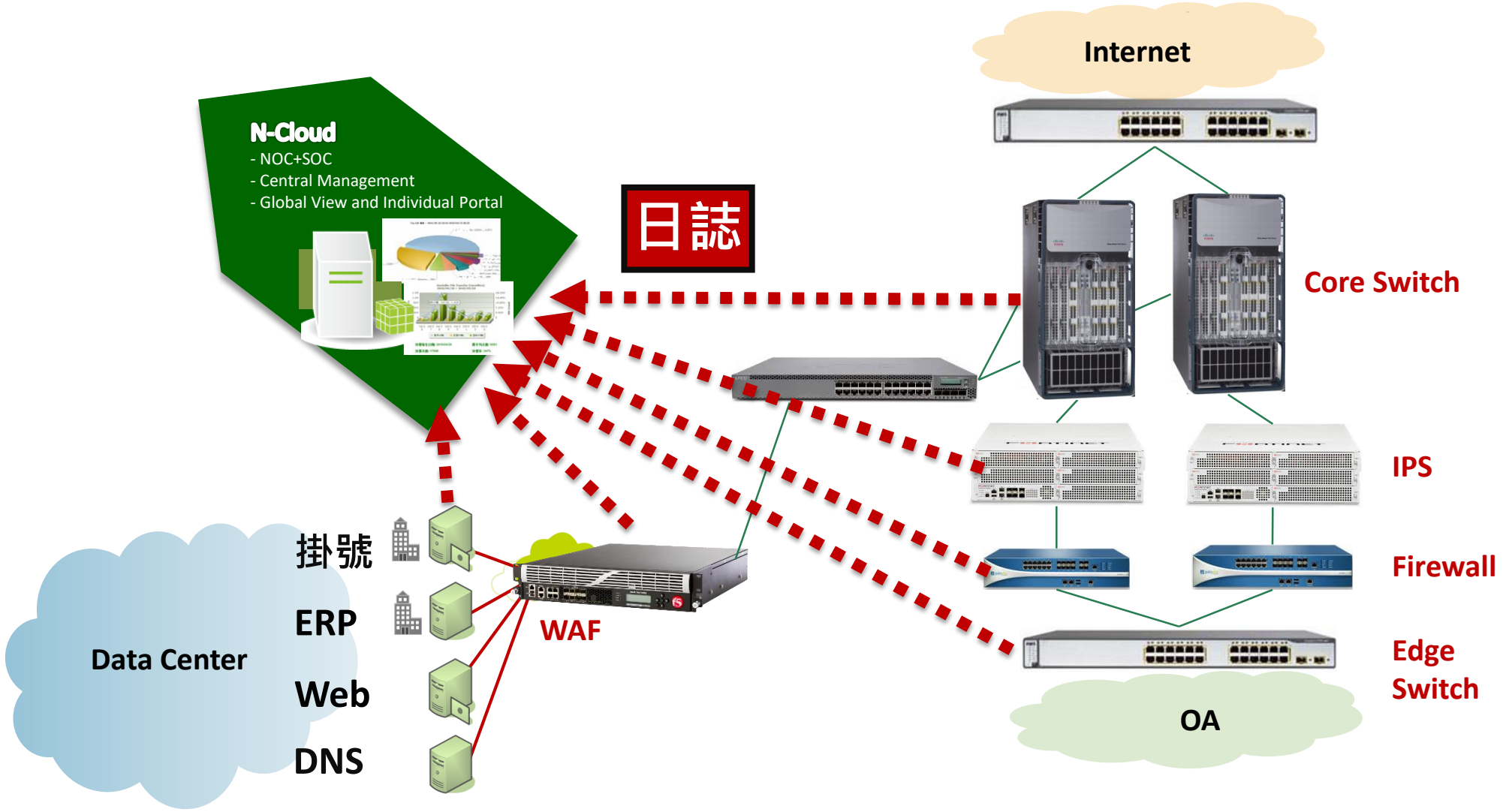
NO	來源 IP 名稱解析	Sessions	Packets	Bytes	流量圖
1	太昌國小	161.48K	28.89M	34.64G 18.93%	
2	新城國中	132.75K	14.15M	15 8.47%	
3	壽豐國小	96.13K		0G	
4	北昌國小	140.63K		8G	
5	春日國小	162.25K		9G	
9	港口國小	92.17K		8G	
10	志學國小	393.37K	4.49M	8G 1.63%	

掌握到重度使用者

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%



收集安全閘道設備/網路設備/伺服器等日誌(Syslog)



N-Partner

將各種日誌自動進行正規化切割,才能查詢與分析

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

N-Partner

N-Reporter/N-Cloud已內建多種日誌報表

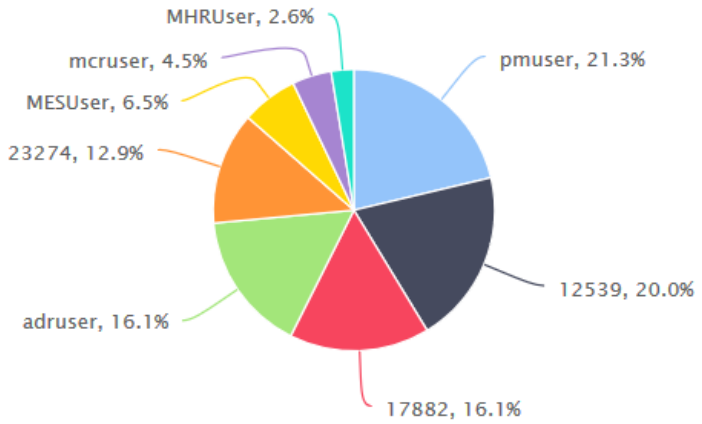
伺服器稽核 ▶ **MS SQL Server登入稽核**

時間區段 ▶ 起迄時間 **2016/11/16 ~ 2016/11/16**

資料時間範圍: 2016/11/16 09:33:01 ~ 2016/11/16

事件	來源IP	來源名
Logon Success	10.1.3.68	Serve
Login Failure	10.1.3.68	Serve
Logon Success	10.1.3.68	Serve
Login Failure	10.1.3.68	Serve
Logon Success	10.1.3.68	Serve
Login Failure	10.1.3.68	Serve
Logon Success	10.1.3.68	Serve
Login Failure	10.1.3.68	Serve

Top N Report – 2016/11/16 ~ 2016/11/16



總筆數: 8

NO	使用者帳號	次數
1	pm er	33
2	12	31
3	17	25
4	adr er	25
5	23	20
6	ME ser	10
7	mc er	7

總筆數: 1

設備名稱	登入成功	登入失敗
NewAP01	55 (95%)	8 (4.9%)

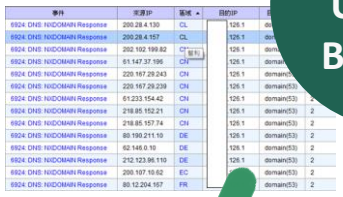
N-Partner

如果我的管理畫面可以變成這樣...

防火牆

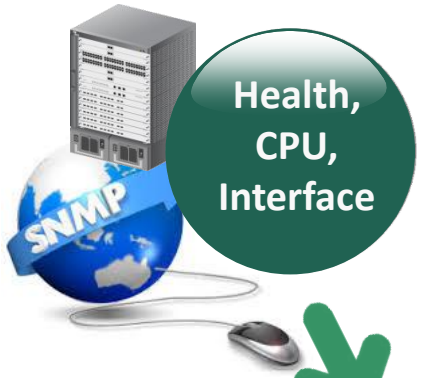
伺服器/AD

安全設備



Event, User ID, Behavior

Geo, Reputation, 單位



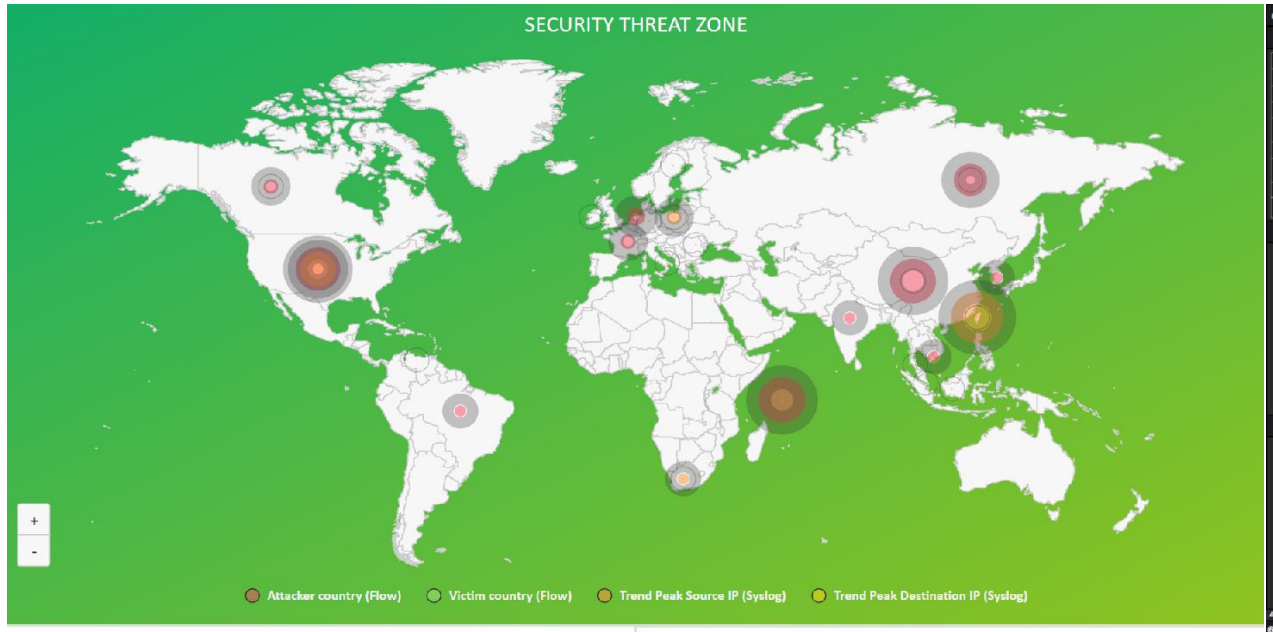
Health, CPU, Interface

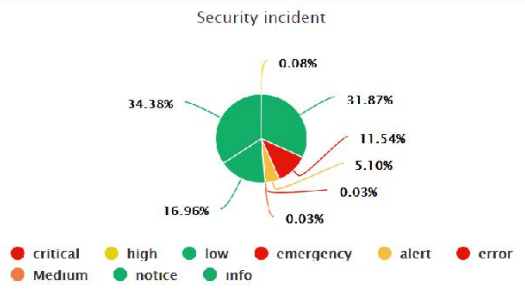
事件說明	來源 IP	目的 IP	單位	服務	Packet	Byte	使用者	位置
	192.168.1.222	168.95.1.1			60	4,260		
	192.168.1.33	8.8.8.8			251	203K		
	192.168.1.33	210.100.38.101			157	115K		
	192.168.2.88	210.71.213.25			19	3,822		
	192.168.2.88	121.2.15.177			4	617		

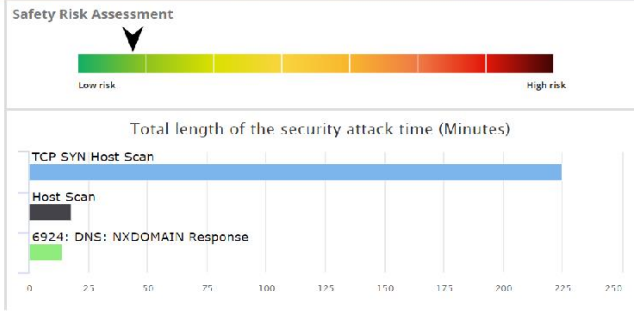
什麼人 → 什麼事情 → 什麼時間 → 什麼地方 → 什麼設備

N-Partner

每位使用者都可以自由設定專屬圖表與監控Dashboard





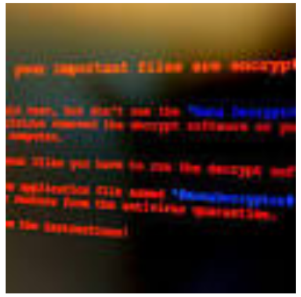


N-Partner產品賣點: 電信, 教育, 企業
流量報表, 智慧化分析與DDoS聯防

2017/5/12 WannaCry開始出現於新聞版面

網路 ▾ 所有新聞 ▾ **2017年3月1日 – 2017年5月12日** ▾ 依關聯性排序 ▾ 清除

WannaCry Ransomware Attack Hits Victims With Microsoft SMB Exploit
eWeek - 2017年5月12日
Ransomware is no longer just a nuisance. Now it's quite literally a matter of life and death. A massive ransomware attack being labeled as "WannaCry" has been ...



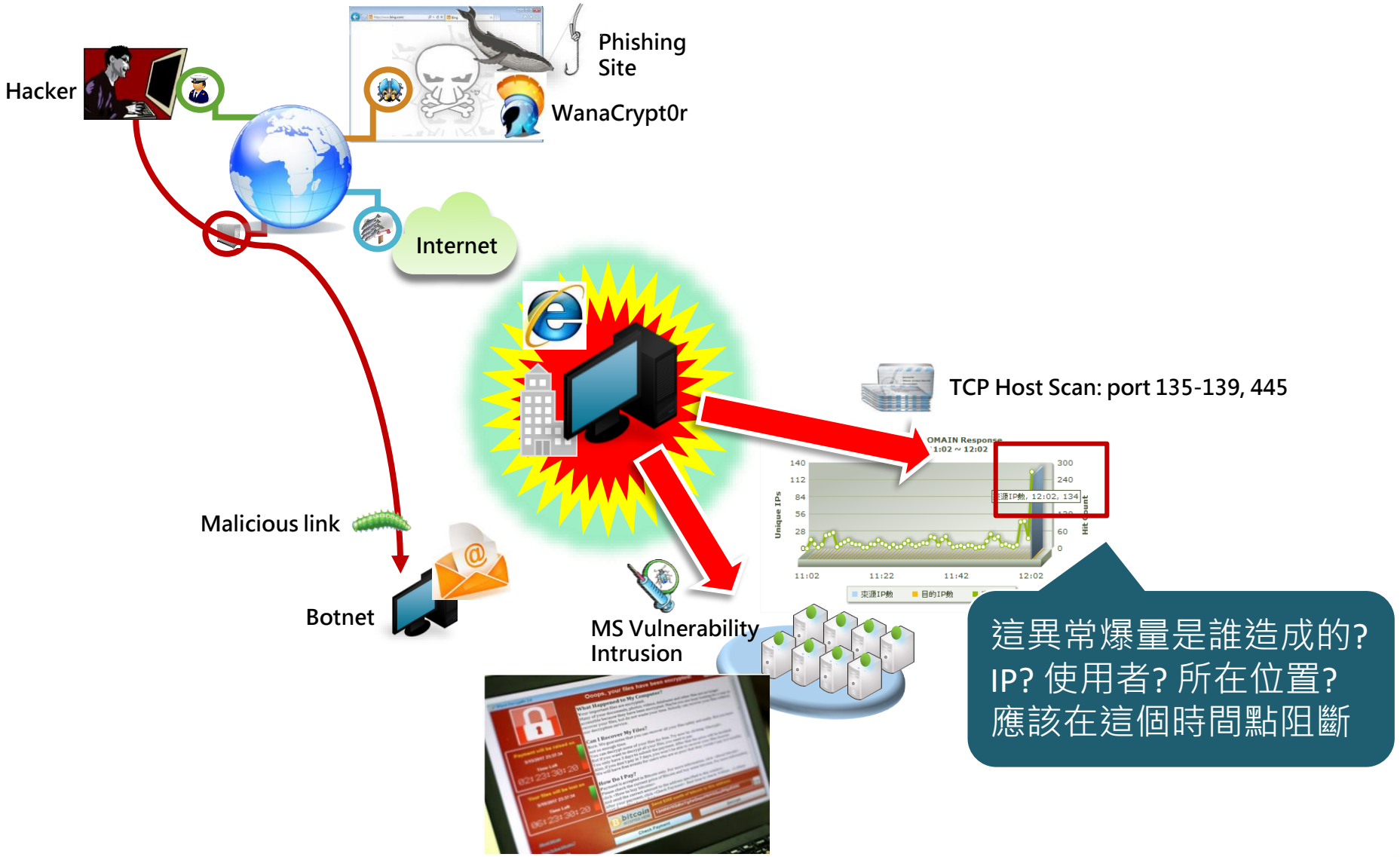
A 'kill switch' is slowing the spread of WannaCry ransomware
PCWorld - 2017年5月12日
The ransomware, called Wana Decryptor or WannaCry, has been found infecting machines across the globe. It works by exploiting a Windows vulnerability that ...

An NSA Cyber Weapon Might Be Behind A Massive Global ...
Forbes - 2017年5月12日
According to the MalwareHunterTeam, which said WannaCry was "spreading like hell," Russia has been the hardest hit, but Spain also seems to be under ...

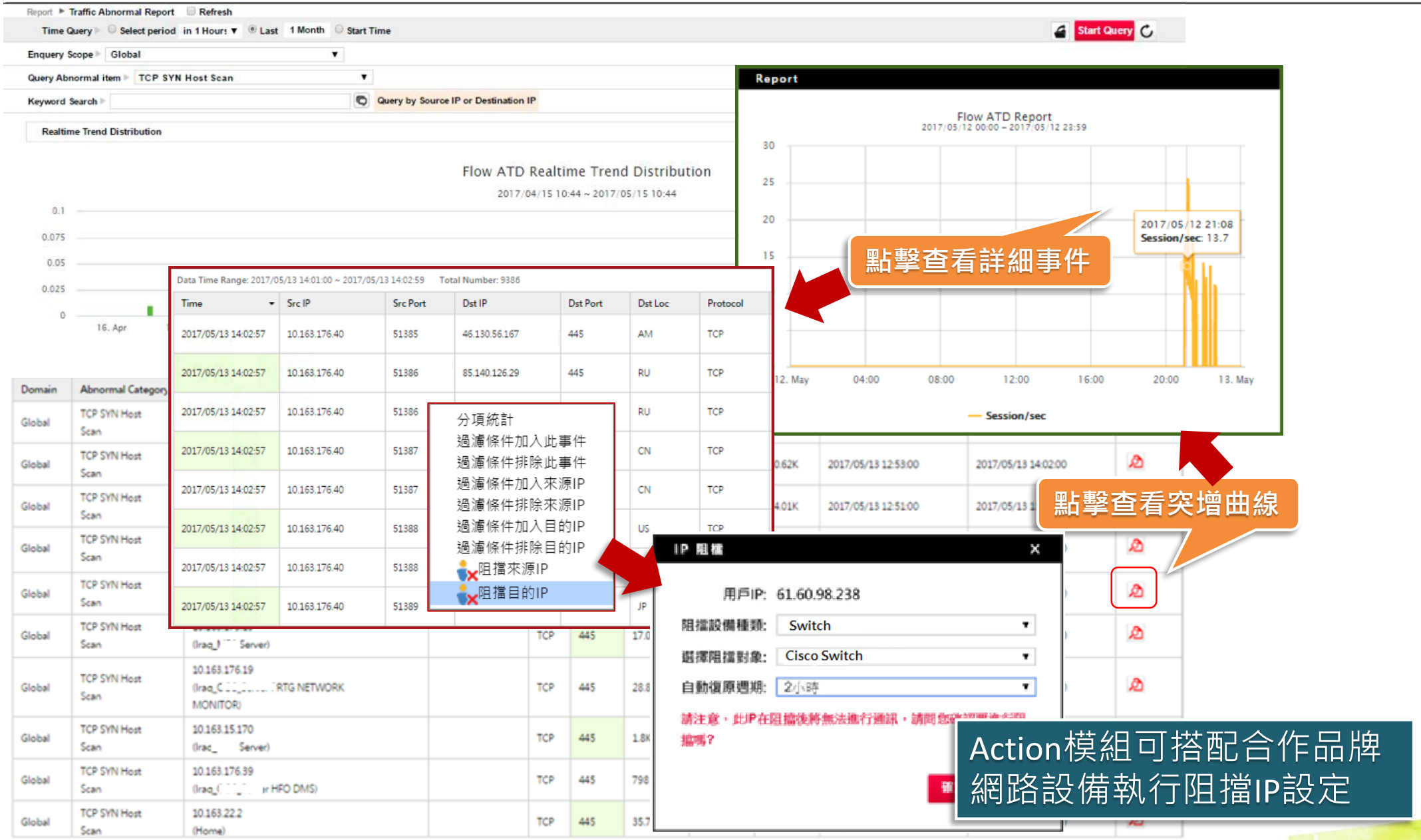
NSA-created cyber tool spawns global attacks — and victims include ...
引用次數最多 - Politico - 2017年5月12日

N-Partner

到底怎麼被癱瘓的?


Hacker
Phishing Site
WanaCrypt0r
Internet
Malicious link
Botnet
MS Vulnerability Intrusion
TCP Host Scan: port 135-139, 445
這異常爆量是誰造成的?
IP? 使用者? 所在位置?
應該在這個時間點阻斷

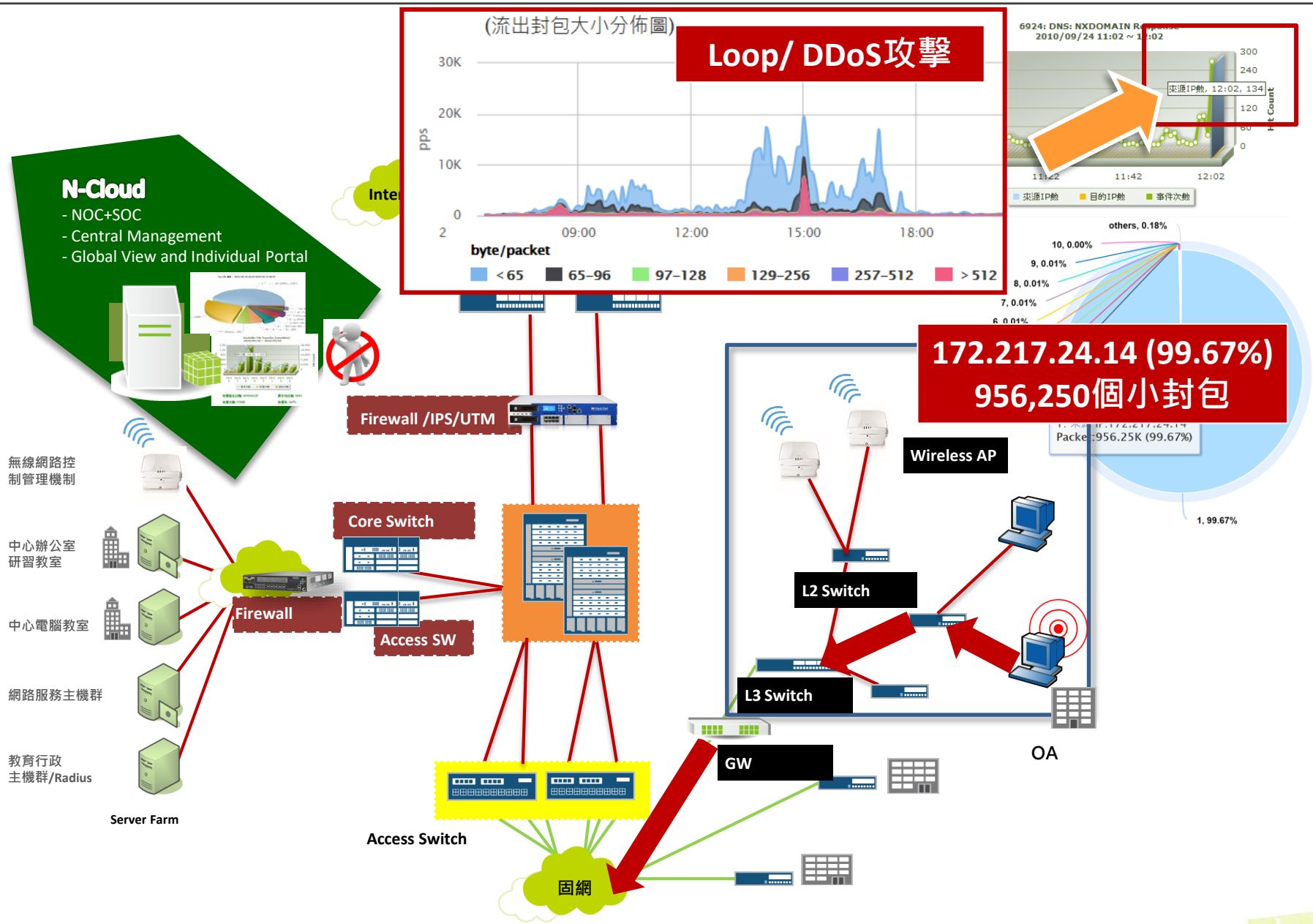
勒索軟體網內互打案例: 無須人工事先定義閥值的異常流量即時發覺



Action模組可搭配合作品牌網路設備執行阻擋IP設定

N-Partner

智慧化異常使用分析與即時聯防流程



N-Partner產品賣點: 政府, 金融, 醫療

安全事件暨系統日誌接收,分析與統計

資安合規應檢視項目與內涵

- **資訊架構檢視**
  - 評估網路架構之配置、資訊設備的管理方式和單點故障的風險承擔能力，以及組織對於營運持續採取的相關措施
- **網路活動檢視**
  - 包括網路相關設備的帳號權限管理和存取記錄、設備的監控與異常事件的處理，以及檢視網路封包是否存在網路異常連線和惡意行為
- **網路設備、伺服器及終端機等設備檢測**
  - 檢測設備的存取和連線機制、是否定期實施弱點掃描和修補作業，以及檢測是否存在惡意程式程後門程式
- **網路安全檢測**
  - 包括網站和客戶端軟體的弱點掃描、程式源碼的檢測、滲透測試，以及評估網站目錄權限設定的 問器適當性檢視系統是否存在可能易遭連線挾持程資源消耗等影響系統可用的情況
- **安全設定檢視**
  - 包括系統存取限制和特權管理、伺服器的設定原則、軟體更改、防火牆的連線設定以及金鑰的儲存保護和存取機制等
- **合規檢視**
  - 檢視整體的電腦系統是否符合標準或法令法規要求之要求

參考資料-「醫療資安論壇」 醫院資訊安全防護現況與精進之道

N-Partner

By量計價方式收集日誌，遇到異常爆量該怎麼辦?

上圖為真實案例:

某大證券公司實際案例:遭到DDoS攻擊時, 防火牆的日誌量從平時每秒600暴增到25,000(Event Per Second)的圖形, 攻擊發生兩小時內, 日誌量大漲到將近100 GB

目前所規畫之N-Cloud可以收容數萬EPS, 沒有效能問題, 費用低廉

N-Partner

N-Cloud成功協助第一金證券抵禦DDoS勒索

駭客向第一金勒索比特幣 調查局抓到了

第一金控集團前年9月驚傳遭駭客勒索「比特幣」，第一銀行、第一金證券所有電子交易因網路攻擊一度停擺。（資料照，彭博）

2018-03-07 16:59:05

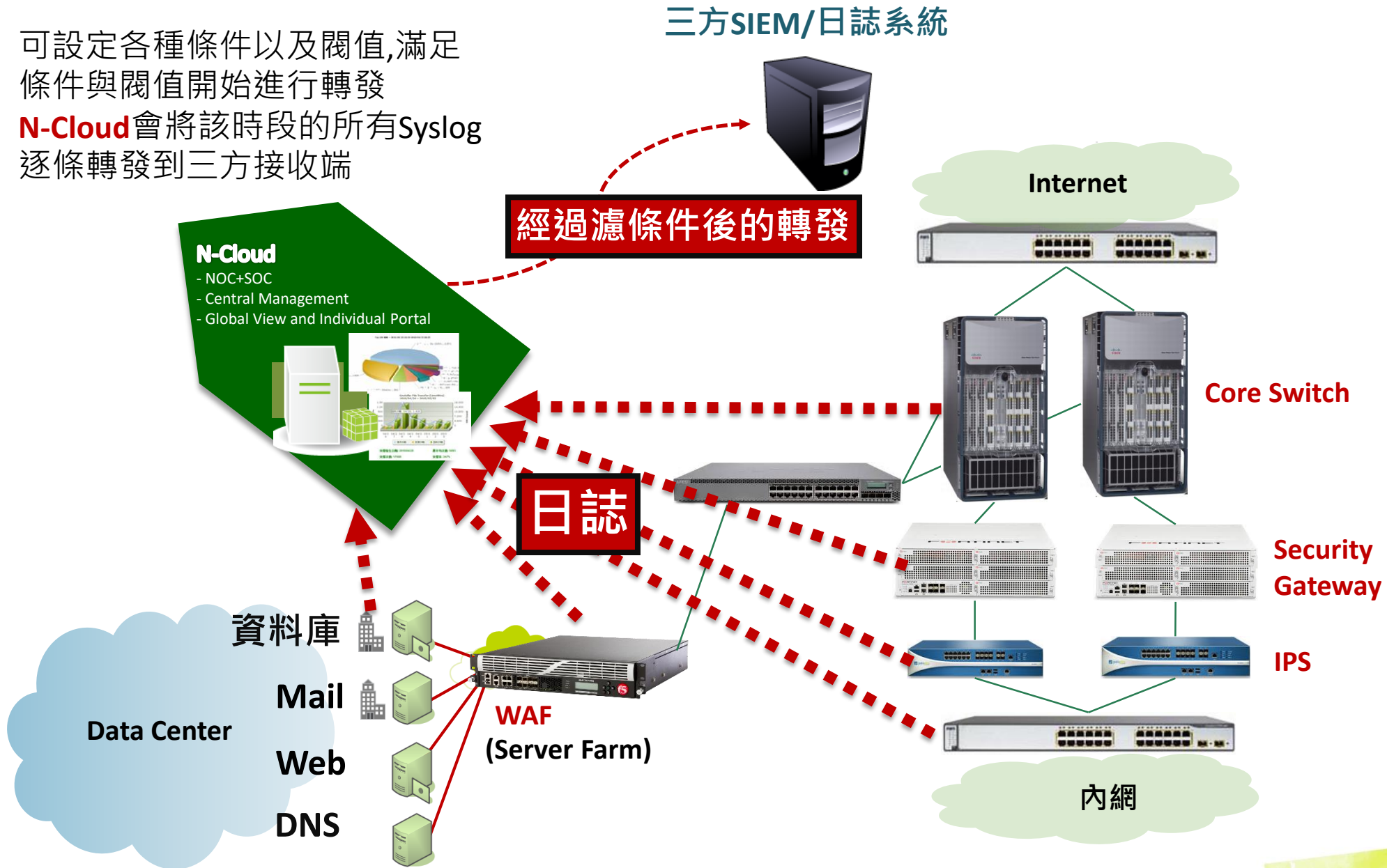
〔記者陳慰慈／新北報導〕第一金控集團前年9月傳出遭駭客寄信勒索50枚比特幣（當時市價約100多萬元），若不支付將癱瘓第一銀行與第一金證券的交易系統，經過一年半追查，調查局新北市調處鎖定家住彰化的23歲陳姓嫌犯，陳男到案認罪，檢方訊後請回。

調查局追查發現，高職資訊科畢業的陳男還以相同犯罪手法對國內、中國、新加坡等大型遊戲公司進

N-Partner

日誌過濾與減量

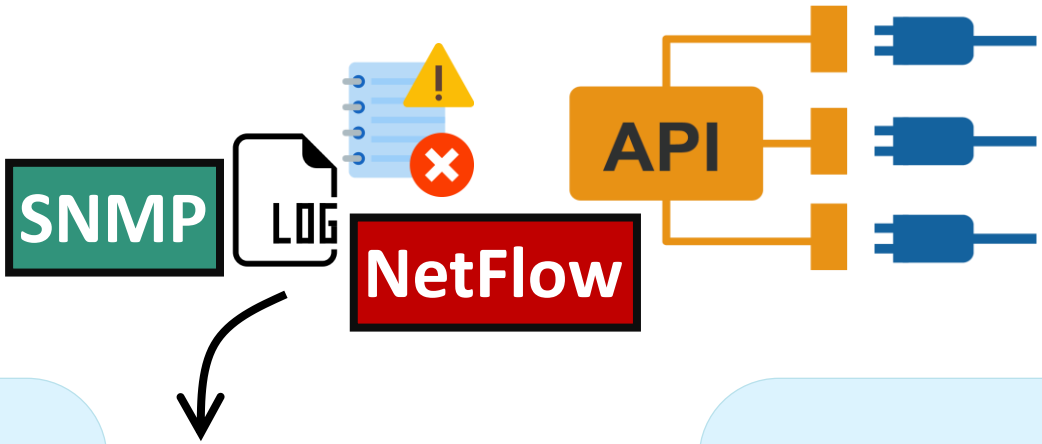
1. 可設定各種條件以及閥值,滿足條件與閥值開始進行轉發
2. **N-Cloud**會將該時段的所有Syslog逐條轉發到三方接收端



N-Cloud產品具備彈性擴容能力, 無懼日誌暴漲, 可處理百萬EPS

特點

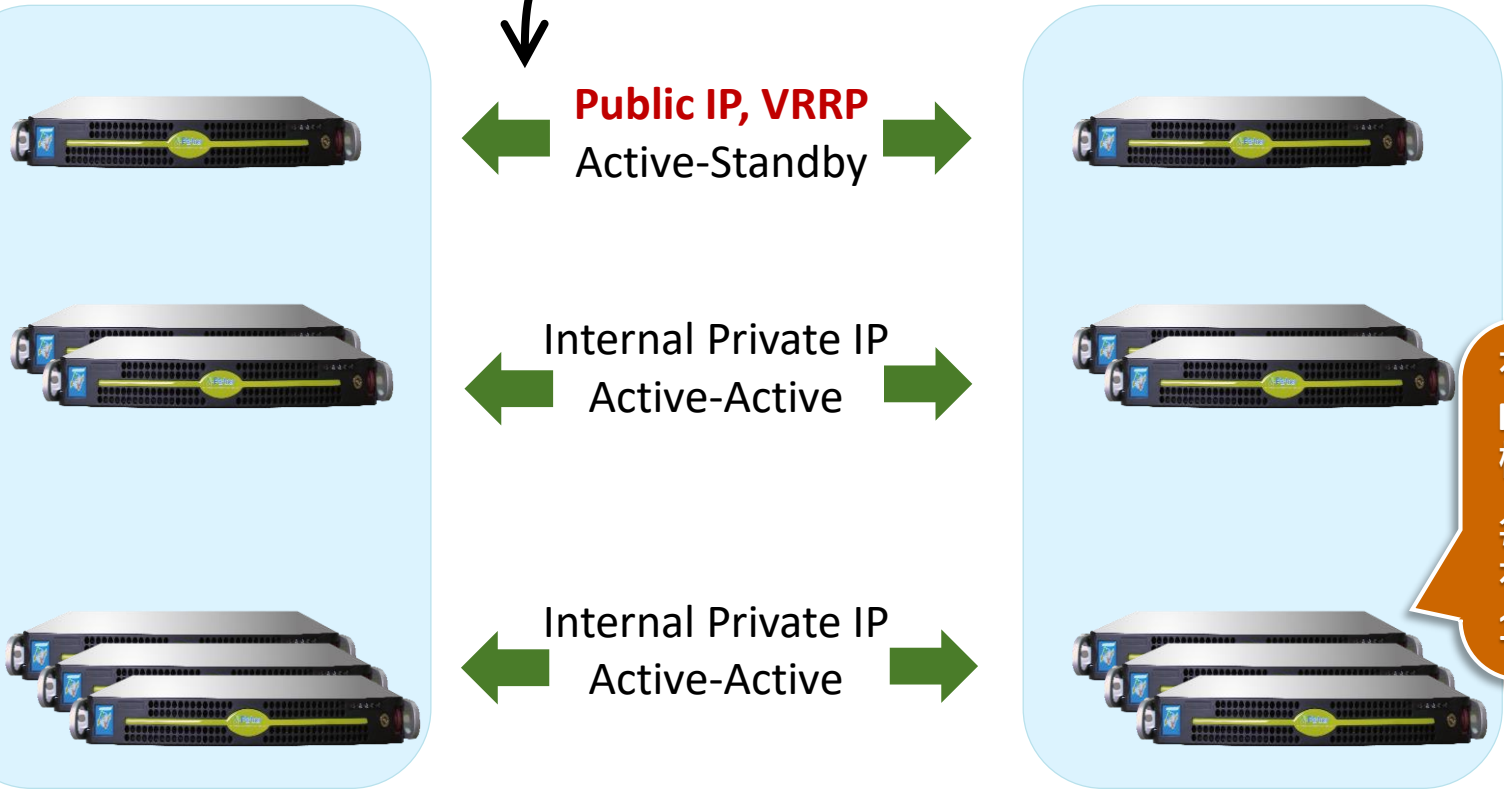
- 可隨網路成長擴容
- 軟體升級不停機
- 僅需在總部佈署



N-Balancer
系統負載均衡

N-Center
提供各客戶專屬Web UI

N-Receiver
資料儲存與分析運算



存取效能考慮, 採用N-Receiver原廠實體機Appliance

每台內建12TB可儲存空間, 可處理10,000 EPS

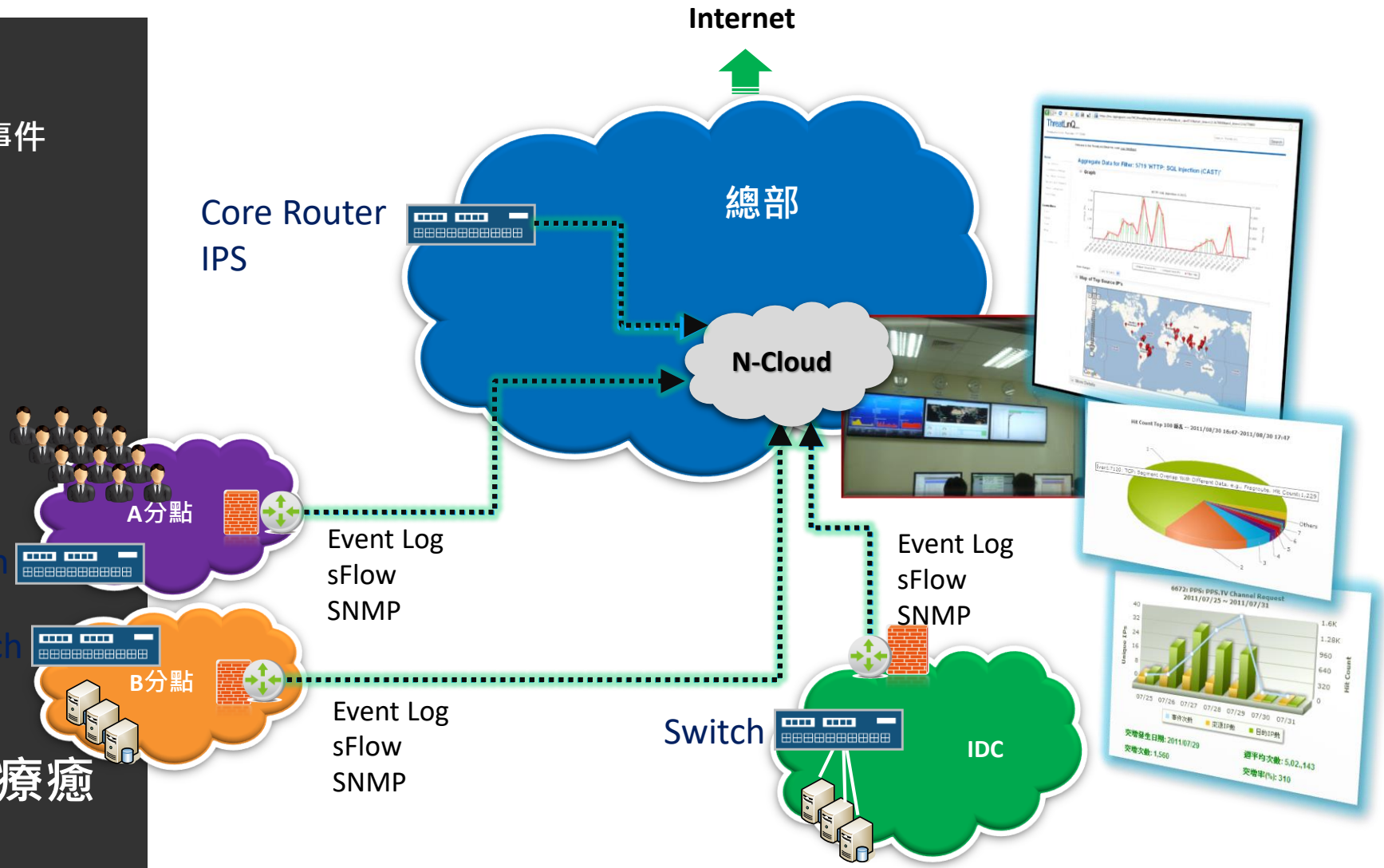
N-Partner

N-Cloud將規劃成收容設備日誌/流量/SNMP資料的平臺

收容
- 核心網路流量與資安設備的事件
- 各分點設備

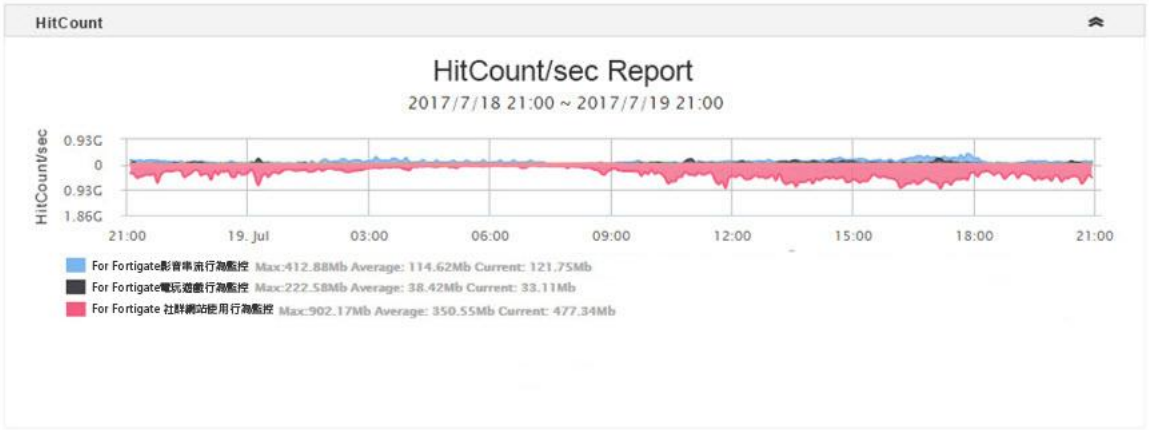
分析
- 設備與網路健康(SNMP)
- 1:1 流量(Flow)
- 資安事件(Syslog)

效果
- 維運單位掌握全域
- 客戶了解自己
- 障礙自動發覺,自我療癒



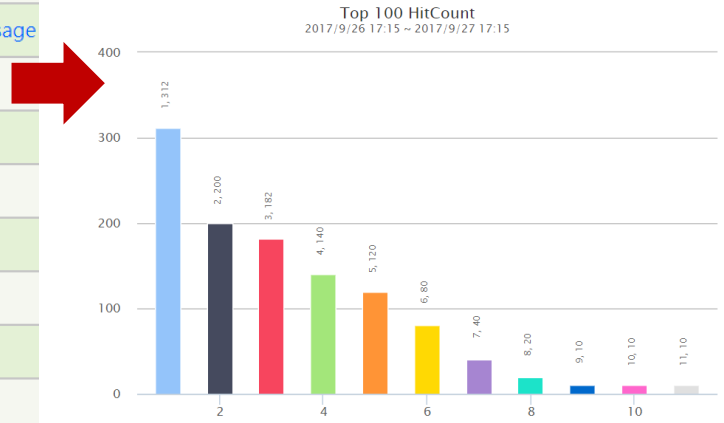
N-Partner產品賣點
專案中協助其他產品達成差異化

內建多種品牌專用圖形, 容易使用



操作	報表名稱
	For Fortigate 行為監控
	For Fortigate 高風險行為監控
	SMTP流量監控
	SSH流量監控
	http與https流量監控
	來自外部查詢DNS流量監控
	台灣與非台灣流量監控
	遠端桌面(RDP)流量監控

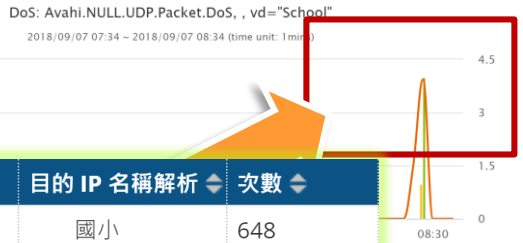
報表名稱
For Fortigate Key Applications Crossing The Network
For Fortigate Malwares Discovered
For Fortigate Top Allowed Applications by Bandwidth
For Fortigate Top Application Categories by Bandwidth Usage
For Fortigate Top Applications Running Over HTTP
For Fortigate Top Blocked Applications by Session
For Fortigate Top Categories and Applications (Hit Count)
For Fortigate Top User Sources By Sessions
For Fortigate Top Users By Bandwidth
For Fortigate Top Web Domains By Visits
For Fortigate Top Virus Victims
For Fortigate Top Viruses By Name
For Fortigate Top Web Categories By Hitcount Bandwidth



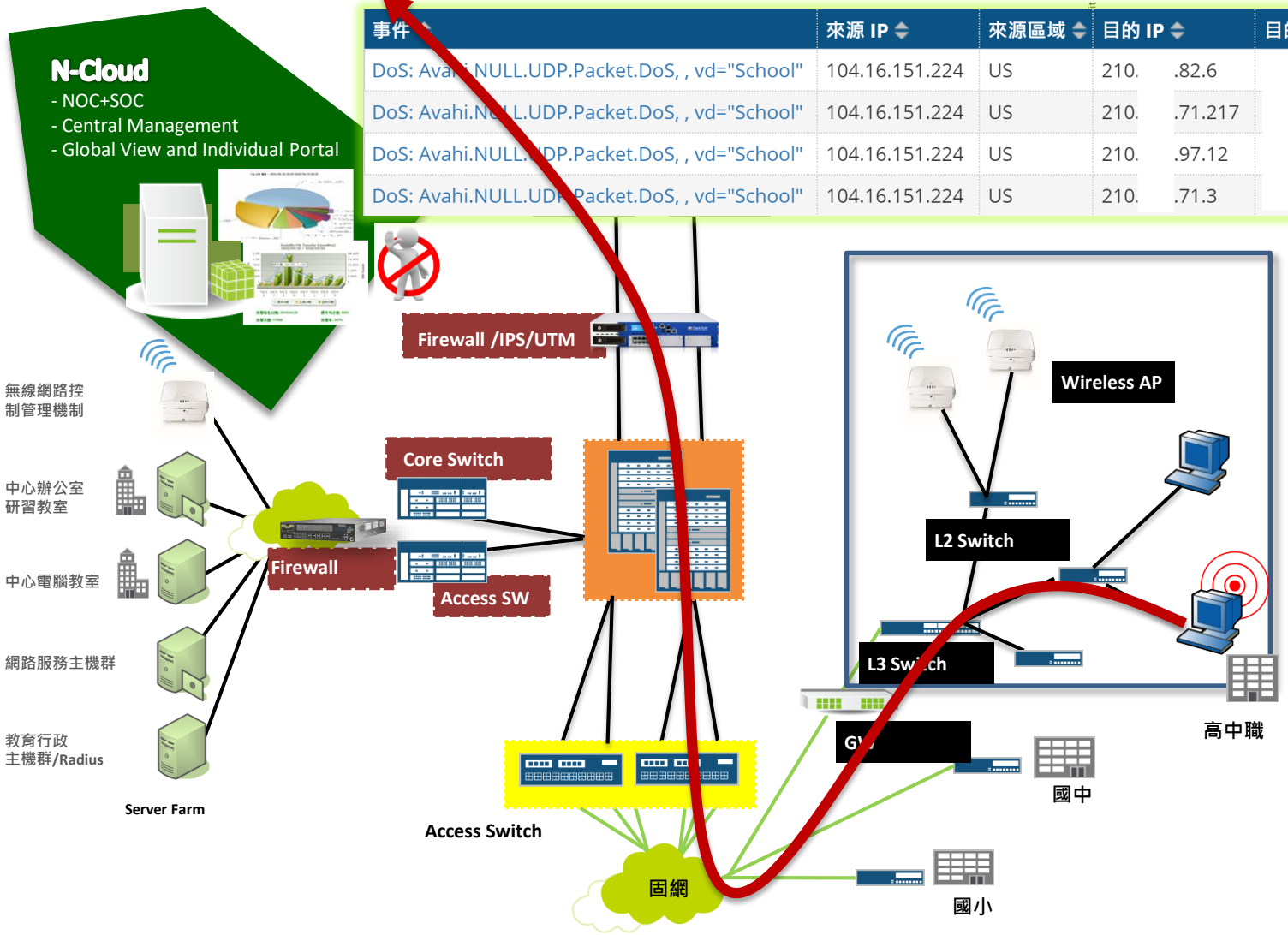
NO	應用服務	Hit Count	
1	SSL:HTTPS	27.76%	312
2	HTTP	17.79%	200
3	SSL_TLSv1.2:HTTPS	16.19%	182
4	Naver.Line:HTTP	12.46%	140
5	SSL_TLSv1.0:HTTPS	10.68%	120
6	Naver.Line:HTTPS	7.12%	80
7	HTTPS.BROWSER:HTTPS	3.56%	40
8	Yahoo.Slurpbot:HTTP	1.78%	20
9	Dropbox:HTTPS	0.89%	10
10	SSL_TLSv1.1:HTTPS	0.89%	10

N-Partner

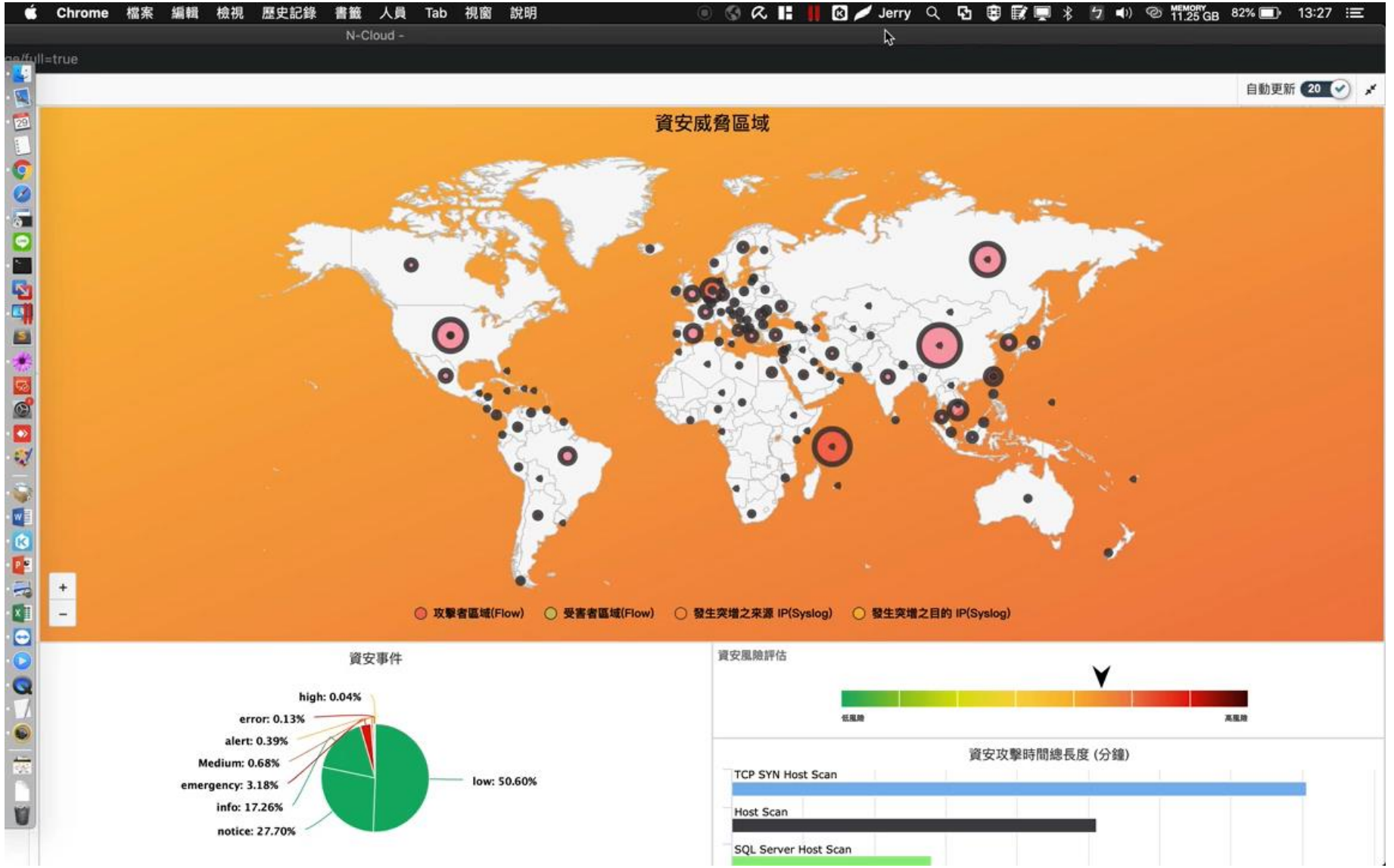
最便宜有效的資安防禦拓展



事件	來源 IP	來源區域	目的 IP	目的 IP 名稱解析	次數
DoS: Avahi.NULL.UDP.Packet.DoS, , vd="School"	104.16.151.224	US	210. .82.6	國小	648
DoS: Avahi.NULL.UDP.Packet.DoS, , vd="School"	104.16.151.224	US	210. .71.217	國中	667
DoS: Avahi.NULL.UDP.Packet.DoS, , vd="School"	104.16.151.224	US	210. .97.12	附小	646
DoS: Avahi.NULL.UDP.Packet.DoS, , vd="School"	104.16.151.224	US	210. .71.3	國中	661



資安威脅即時狀態呈現(跨品牌)



呈現無線網路使用即時狀態

聯防交換機封鎖IP/MAC

N-Partner

N-Partner為您構建

新一代智慧化IT維運系統

掌握
大小事

除錯
容易

資安
聯防