NEITHNET
Accelerate Your Insight

疫情過後，駭客攻擊演化趨勢解析

NEITHNET 騰曜網路科技
技術經理 Peter Peng

關鍵在地情資，化解遇駭危機

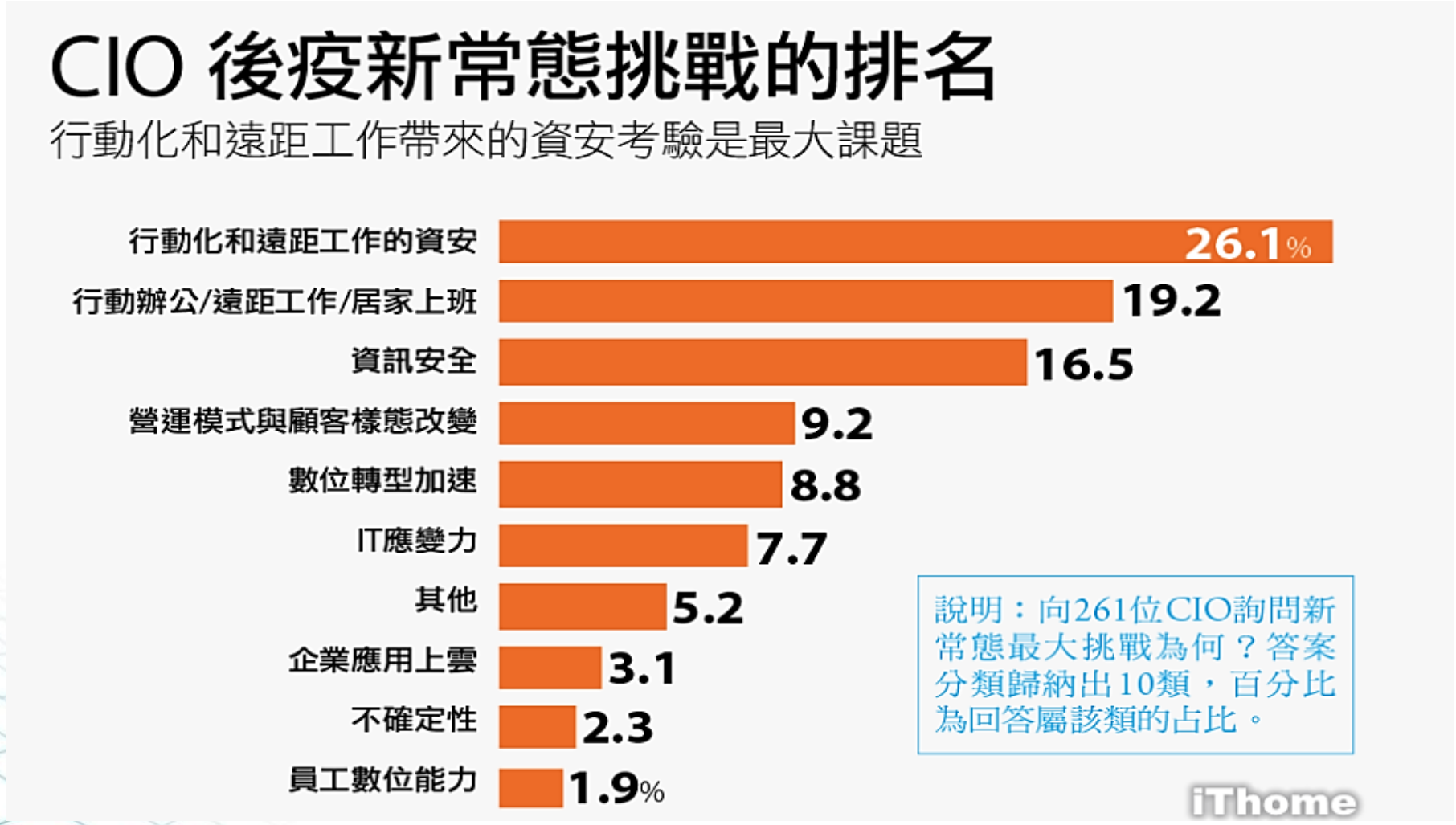
疫情減緩，居家上班熱度未減

據史丹佛大學經濟學教授Nicholas Bloom等三名學者，調查受訪者平均認為WFH等同加薪8%。

1111人力銀行資料庫顯示截至6月30日，一共有19,878個WFH工作機會數，相較於2021年同期成長33%。

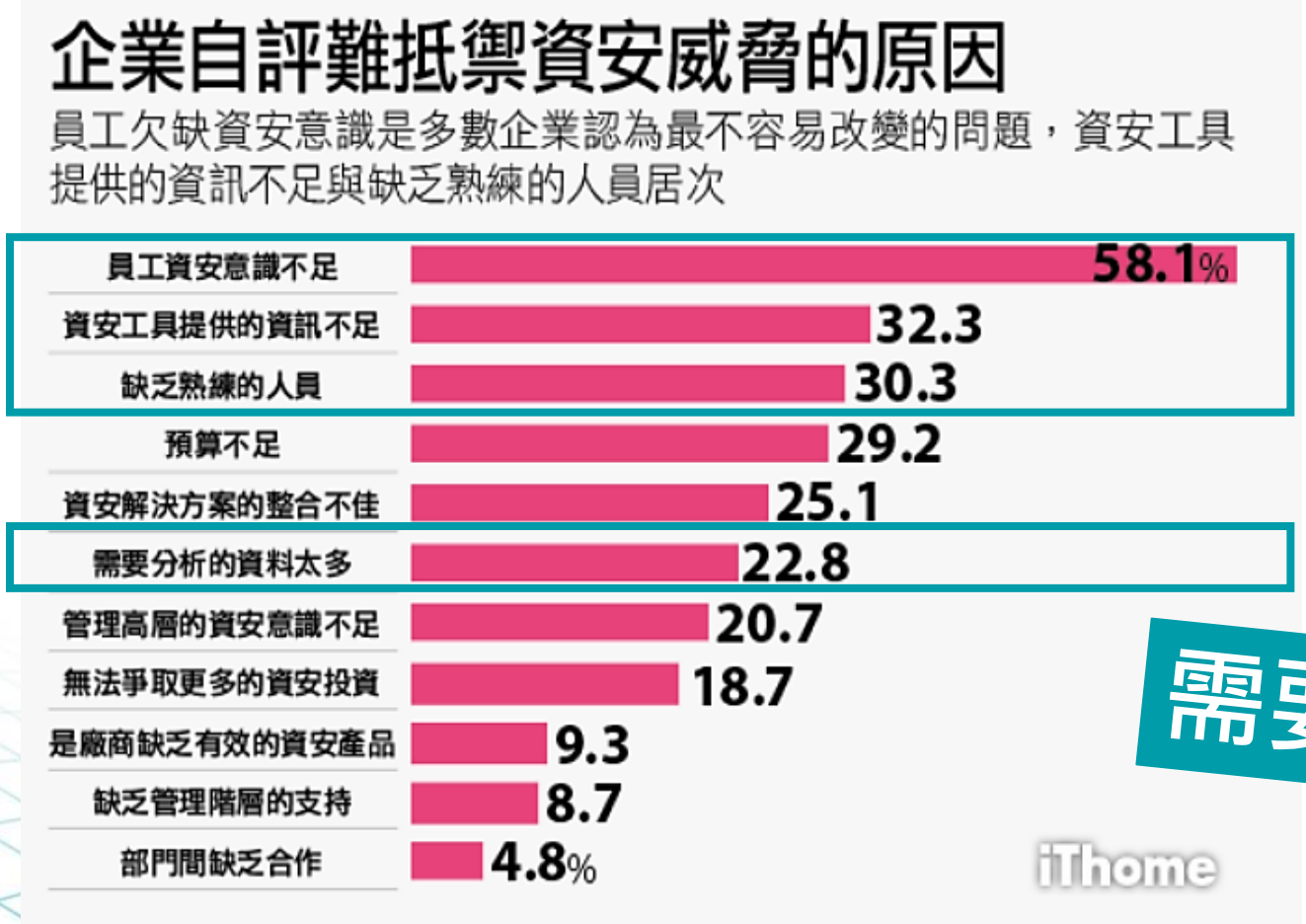
工作內容多數可線上完成，加上Google和蘋果近日接連宣布未來採用「混合工作模式」，科技業彈性上班風氣已然成形，即便是疫情過後仍看好持續釋出WFH或混合工作模式職缺。

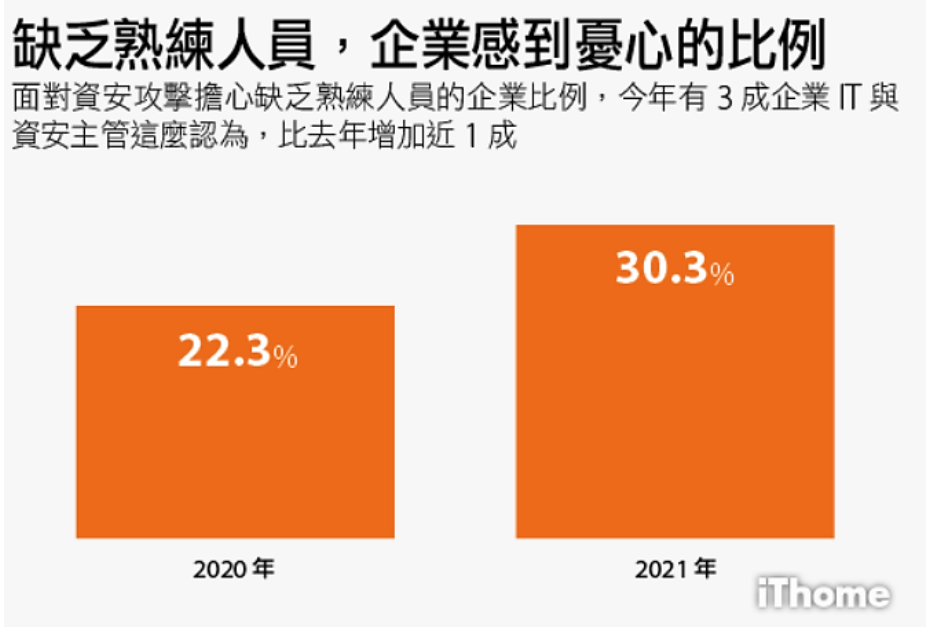
疫情減緩後的考驗



資料來源：iThome

ITHOME 2021企業資安大調查





需要更專業的人來幫忙?

資料來源：iThome

資安人員壓力大增而萌生辭意

資安廠商 Deep Instinct 日前針對多家 1,000 名員工以上公司資安人員的調查，指出有高達 46% 的高階與資深資安人員，因近年駭侵攻擊次數與強度不斷提升，導致工作壓力大增，因而考慮辭去相關工作。

47% 的人指出單位期待他們能阻擋一切資安威脅，但這是不可能的，因此而感到壓力沉重

43% 資安人員指出他們必須隨時待命

40% 資安人員表示組織的資安編制人員不足，資源短缺，也造成其工作壓力大增。

發布日期：2022-06-17 本文摘自TWCERT https://www.twcert.org.tw/tw/cp-104-6223-bc820-1.html?fbclid=IwAR3YRmT5PKByMGC8gWje_XDIsbqE4xxKkJQkghSA2FgspSObFsNTtcZ77j0

駭客已經準備好，入侵居家辦公設施

駭客看準企業員工在家工作，資安人員在遠距工作的資安問題，可能會有以下的挑戰：

- **不信任的基礎設施**
- **不信任的網路連線**
- **不安全的使用行為**
- **不安全的上網行為**

當員工回到公司，駭客更能入侵企業資訊系統，因為遠距辦公已降低入侵企業的難度！

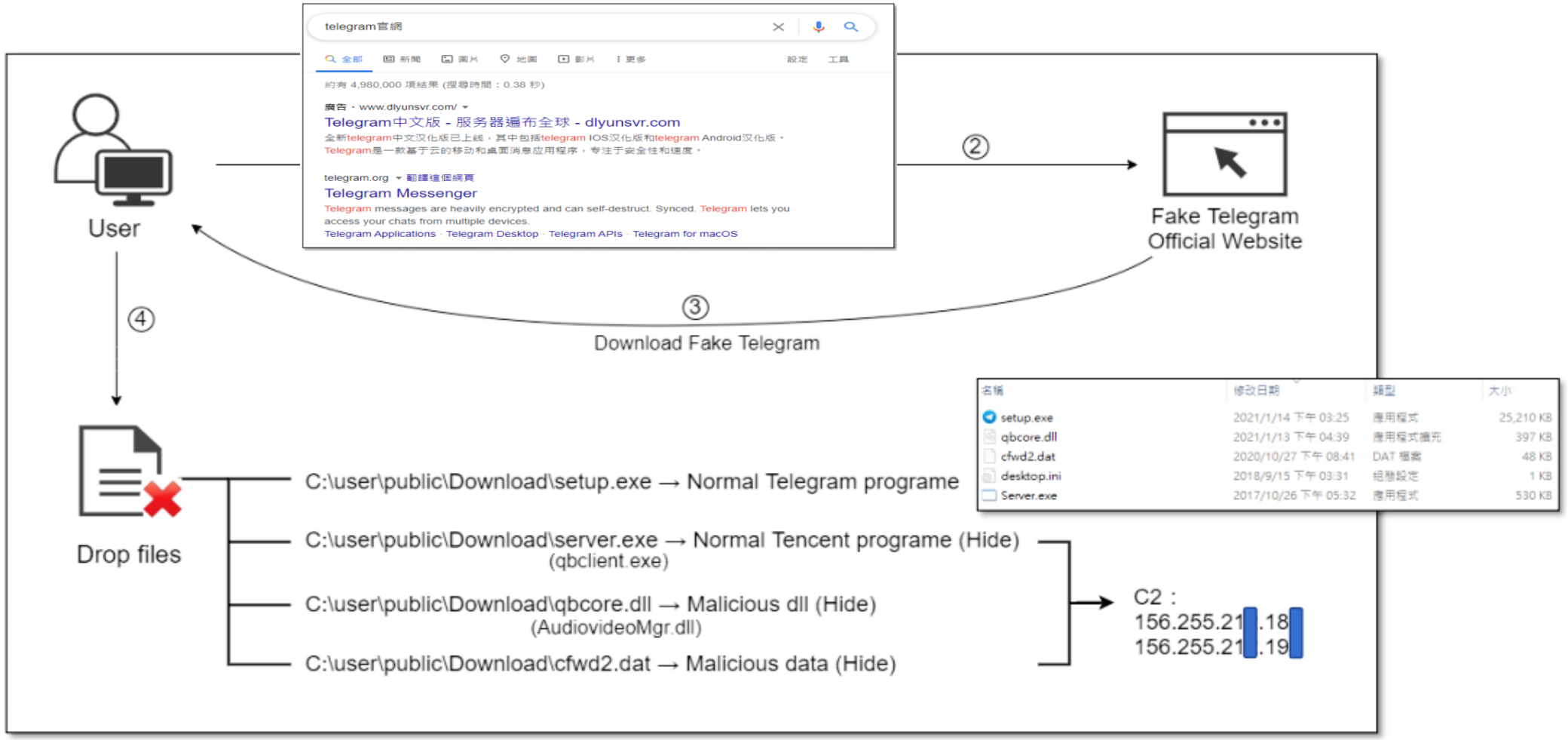
資安人員不可疏忽的基礎設施漏洞

Citrix VPN	Pulse Secure VPN	Cisco AnyConnect	Fortinet	SonicWall	F5
CVE-2021-22941	CVE-2021-22893	CVE-2021-1568	CVE-2021-32588	CVE-2021-20016	CVE-2021-23008
CVE-2020-8195	CVE-2020-8260	CVE-2021-1366	CVE-2021-22123	CVE-2020-5135	CVE-2021-22986
CVE-2020-8196	CVE-2020-8243	CVE-2020-3153	CVE-2020-12812	CVE-2019-7481	CVE-2021-22992
CVE-2019-11634	CVE-2019-11539	CVE-2020-3433	CVE-2019-5591	CVE-2020-5144	CVE-2021-22991
CVE-2019-19781	CVE-2019-11510	CVE-2019-1853	CVE-2018-13379	CVE-2019-7483	CVE-2020-5902
Palo Alto	**QNAP**	**MS Exchange**	**MS SharePoint**	**MS Windows**	**MS Office**
CVE-2021-3045	CVE-2021-28797	CVE-2021-34523	CVE-2021-28474	CVE-2021-31166	CVE-2021-40444
CVE-2021-2037	CVE-2021-28799	CVE-2021-34473	CVE-2021-31950	CVE-2021-36942	CVE-2017-0199
CVE-2020-2034	CVE-2020-36197	CVE-2021-31207	CVE-2021-26420	CVE-2020-1472	CVE-2021-11882
CVE-2020-2021	CVE-2020-36198	CVE-2021-26855	CVE-2020-1181	CVE-2019-0708	CVE-2021-31178
CVE-2019-1579	CVE-2020-2509	CVE-2021-33766	CVE-2019-0604	CVE-2021-26431	CVE-2020-17123
vCenter	**FileZen**	**Accellion**	**MS Azure**	**Atlassian**	**Zoho Corp.**
CVE-2021-21985	CVE-2021-3156	CVE-2021-27101	CVE-2021-38647	CVE-2021-26084	CVE-2021-40539
CVE-2021-22005	CVE-2021-20655	CVE-2021-27102	CVE-2021-36949	CVE-2020-36289	CVE-2021-31159
CVE-2021-21985	CVE-2020-5639	CVE-2021-27103	CVE-2021-28476	CVE-2020-14181	CVE-2021-37927
CVE-2021-21972	CVE-2019-0708	CVE-2021-27104	CVE-2021-27047	CVE-2020-15944	CVE-2021-37761
CVE-2021-3952	CVE-2018-0694	CVE-2019-5622	CVE-2021-27080	CVE-2019-3396	CVE-2020-11518
Cisco ASA	**Honeywell**	**Trend Micro**	**Juniper**	**Check Point**	**Sophos**
CVE-2020-3187	CVE-2021-3156	CVE-2021-32457	CVE-2021-0223	CVE-2020-6015	CVE-2020-12271
CVE-2020-3452	CVE-2020-1472	CVE-2021-32458	CVE-2021-0256	CVE-2021-30356	CVE-2020-25223
CVE-2020-3580	CVE-2020-2569	CVE-2021-32459	CVE-2020-1611	CVE-2020-6020	CVE-2020-15504
CVE-2020-3125	CVE-2019-0708	CVE-2020-8469	CVE-2020-1615	CVE-2019-8463	CVE-2018-3970
CVE-2018-0296	CVE-2019-18226	CVE-2020-8604	CVE-2020-1664	CVE-2019-8453	CVE-2018-3971

實際案例 -居家辦公入侵

許多企業實施員工分流或在家上班等措施，現階段可能是駭客攻擊最猖獗的時刻

實際案例 (A)-居家辦公入侵



Telegram 中文化

Record date	Create date	
2021/9/24	2021/9/22	telegerns[.]com
2021/9/24	2021/9/23	zh[.]tele2021[.]com
2021/9/25	2021/9/24	teleglm[.]com
2021/9/29	2021/9/27	telenewcc[.]com
2021/10/8	2021/10/6	www[.]telegramlll[.]com
2021/10/8	2021/10/8	telergems[.]com
2021/10/9	2021/10/8	teeldown[.]com
2021/10/13	2021/10/12	teledai[.]com
2021/10/13	2021/10/13	telegramlia[.]com
2021/10/20	2021/10/16	telezhcn[.]com

真正屬於台灣的情資

博杯

（自由時報特派記者林岳甫攝）

遠端網路攻擊型態

- 程式掃描找尋目標
- 針對弱點->應用程式 作業系統 網路設備 虛擬主機
- 暴力破解 RDP VPN VNC
- 癱瘓網路

方便的遠端桌面 駭客入侵的好機會

方便遠距工作的同仁作業，開啟RDP讓同仁進行遠端連線作業

NAD: TOP-10 Events (table)

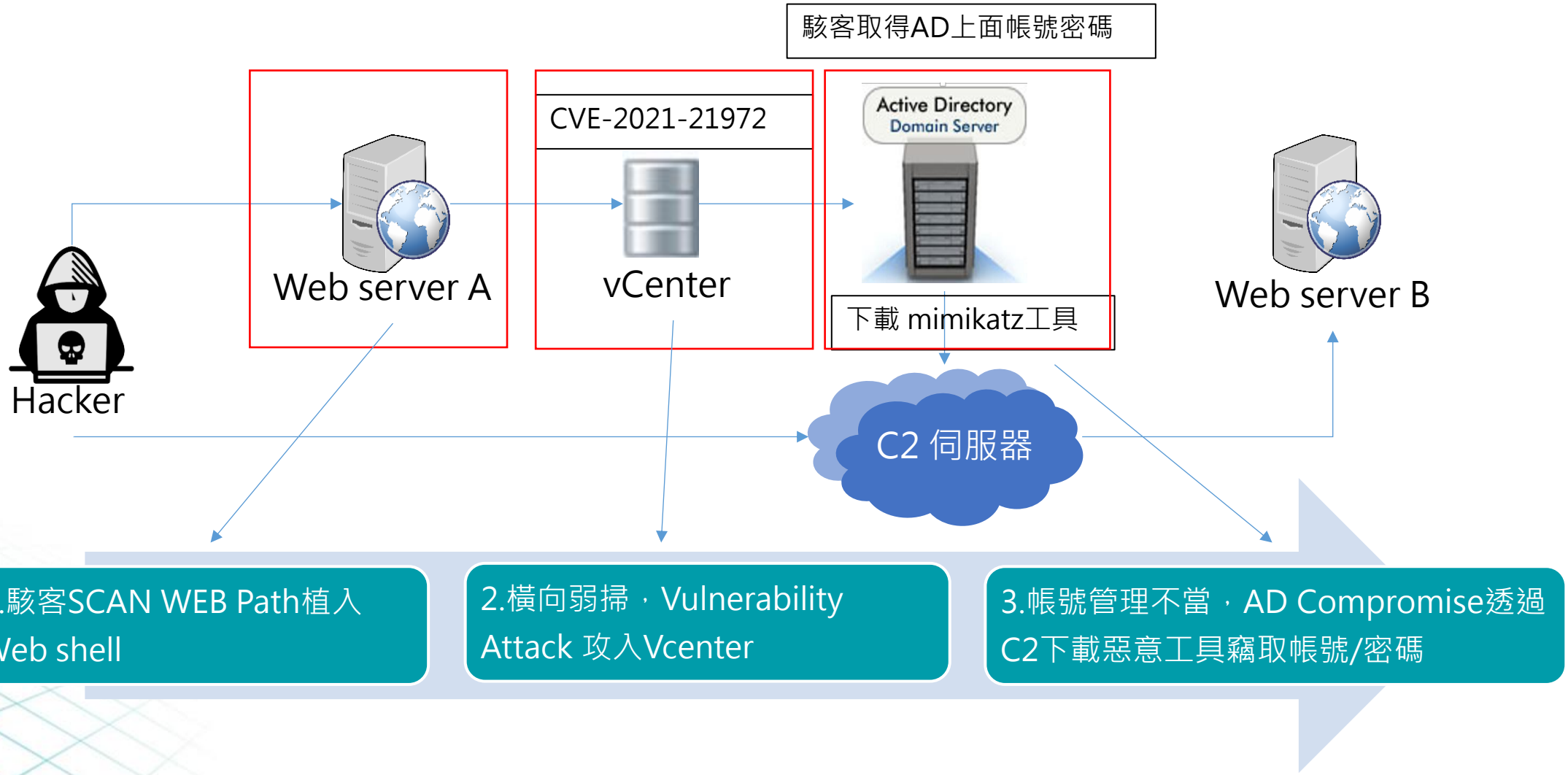
Event Name	Count
ET POLICY MS Remote Desktop Administrator Login Request	5,128

NAD: TOP-10 Source IP / Destination IP by Event Count (table)

Source IP	Destination IP	Event Count
92.255.85.155	192.168.3.4	2,818
62.233.50.179	192.168.3.4	722
31.43.185.3	192.168.3.4	618
194.[illegible]	192.168.3.4	[illegible]
192.168.100.253	192.168.3.4	[illegible]
92.255.85.173	192.168.3.4	111
185.156.72.25	192.168.3.4	44
141.98.9.199	192.168.3.4	36
185.156.72.29	192.168.3.4	31
87.251.75.145	192.168.3.4	31

監控三天網路行為
每天超過一千次嘗試用Administrator進行登入嘗試

實際案例 - AD伺服器入侵



實際案例 - AD伺服器入侵

3/15 22:01:35 使用Administrator登入AD

3/15 22:06:10
Command line
使用Powershell連線
至中繼站

3/15 22:08:22
下載security.zip放置桌面
mz.exe、p.exe
(minikatz.exe)、(psexec.exe)

執行mz.exe
產出密碼hash

3/15 22:11:13
密碼hash儲存csv並
使用notepad.exe檢視

3/15 22:12:41
使用test帳號權限
使用P.exe將檔案
傳回C2伺服器

C2 伺服器

實際案例 - NEITHNET解決方案

針對長期潛伏的惡意行為與重要主機竊取機敏資料的防護措施

1. **NEITHDNS**
   上網第一道檢查點，主動阻隔惡意網站、釣魚網站與社交工程活動

2. **NEITHSeeker**
   端點惡意威脅自動化分析、主動隔離威脅檔案與主機，專家協助找出問題

3. **NEITHViewer**
   專為內部橫向移動設計，有效偵測網路攻擊，監控橫向擴散與監控流量，整合資訊可視化報表

企業面臨各種不同的入侵威脅，防守永遠困難於攻擊，提升駭客入侵的難度，才是唯一之道，在此案例中可能面對以下的問題:

- 使用者上網的問題
- 對外伺服器的問題
- 內對內攻擊的問題
- 主機入侵的問題

NEITHNET在地化情資全面防護

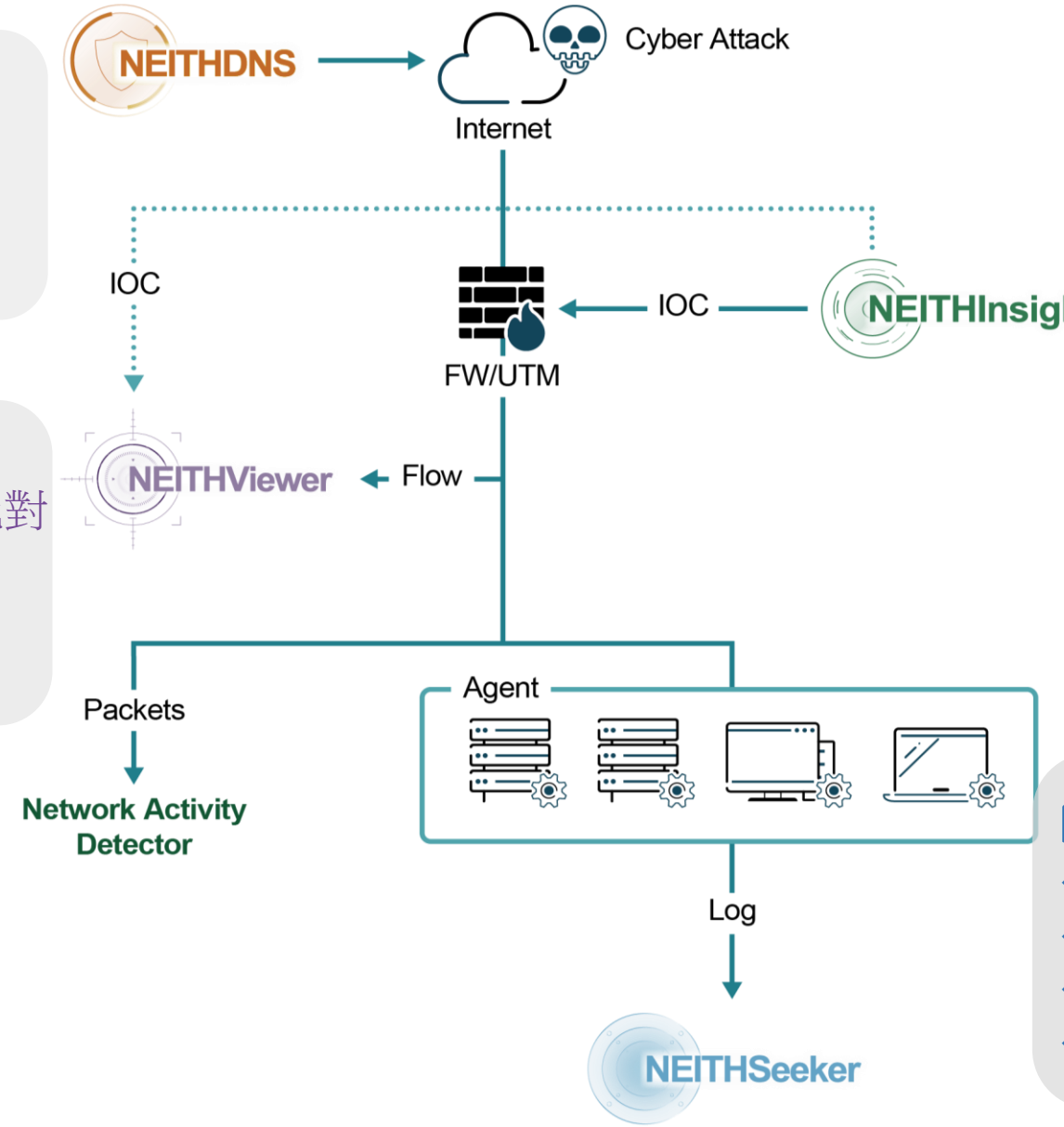
NEITHNET
Accelerate Your Insight

NEITHDNS

- 檢查DNS queries內容，即時阻擋Callback連線/惡意網址

NEITHViewer

- 外對內、內對外情資比對
- 內網可疑行為分析
- 橫向連線分析
- 網路攻擊行為分析



NEITHInsight

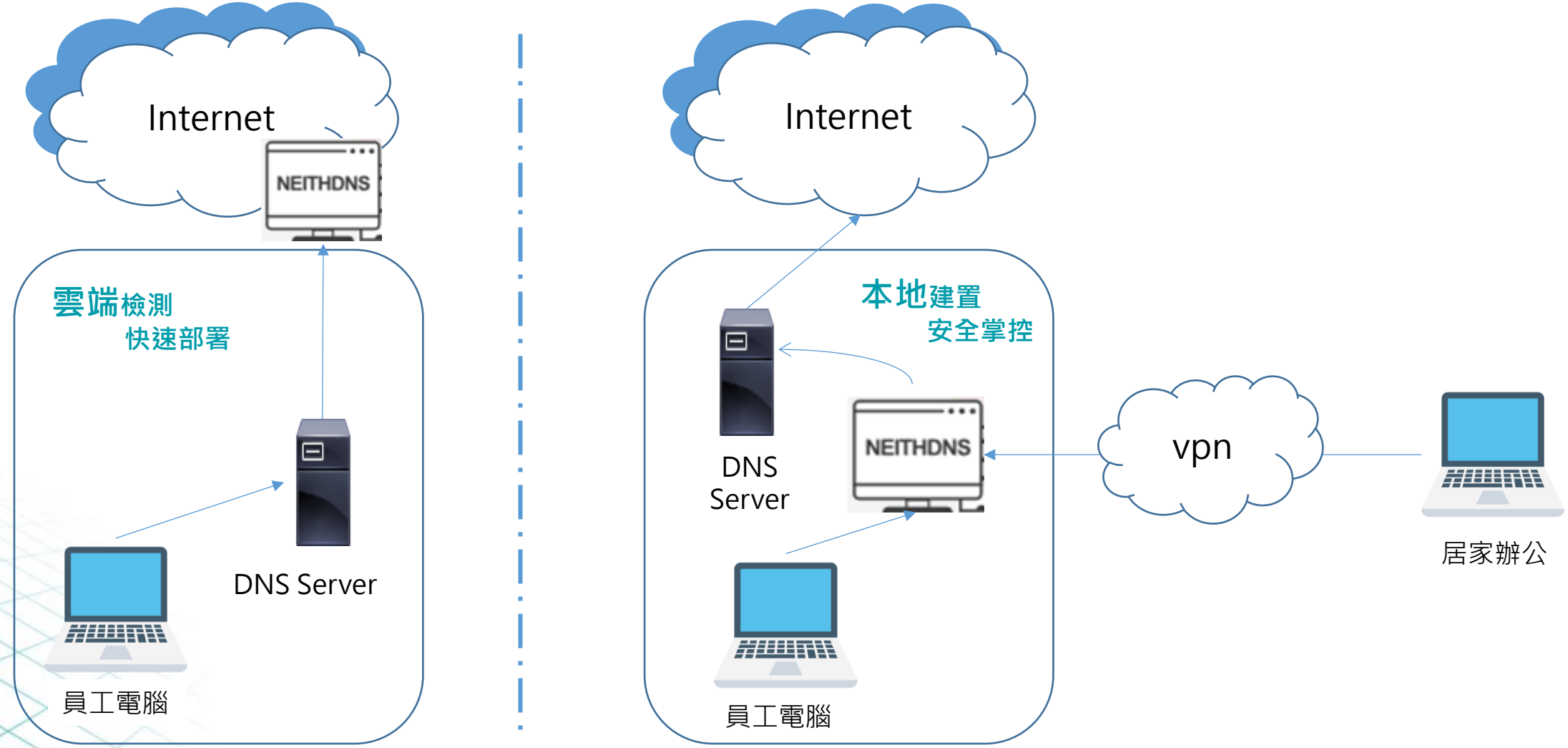
- 威脅情資分類
- 關鍵在地情資
- 整合SIEM / SOC
- 結合防火牆政策

NEITHSeeker

- 異樣端點分析，查找惡意程式
- 中斷勒索攻擊
- 中斷惡意行為
- 專家提供事件分析與解決方案

NEITHDNS惡意連線快速定位

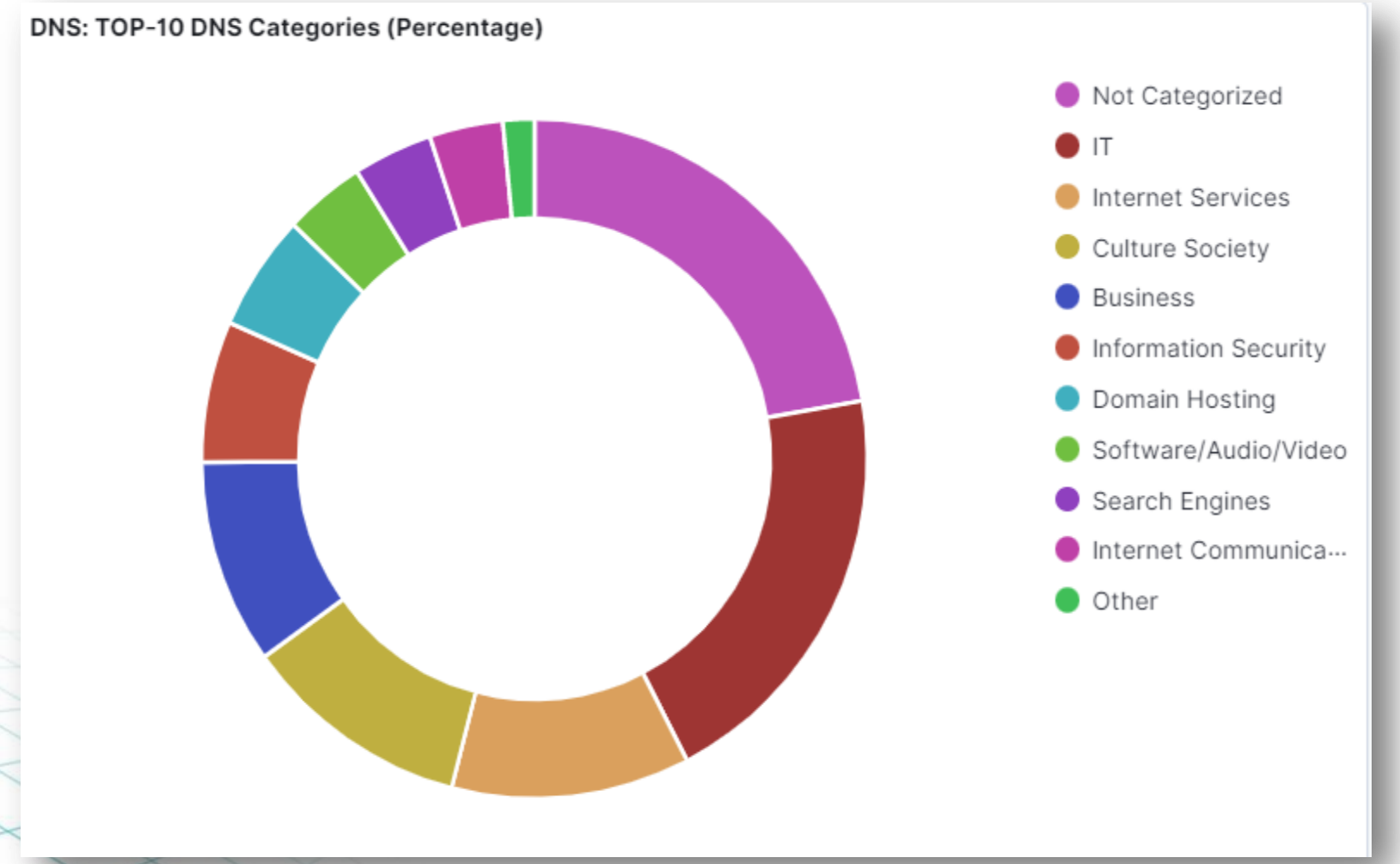
對企業來說，只需調整 DNS 設定，就可從基礎上提供第一道防護，在使用情境上，也能提供企業內網或遠端操作時的彈性，透過NEITHDNS防護，更可以降低連結到詐騙網站或惡意連結後所帶來的危害。



精準威脅情資

當NEITHDNS在接收 DNS 要求時，使用即時的NEITHInsight精準情資判斷該請求是否安全，並根據此檢查結果，決定允許或封鎖該連線

員工上網行為分析



色情

酒精、菸草、藥物

暴力

武器、炸藥、煙火

徵人

匿名網站

軟體、音訊、視訊

賭博、彩券、賭馬

社群網路

聊天論壇

網誌

交友網站

線上商店、銀行、支付系統

加密貨幣和挖礦

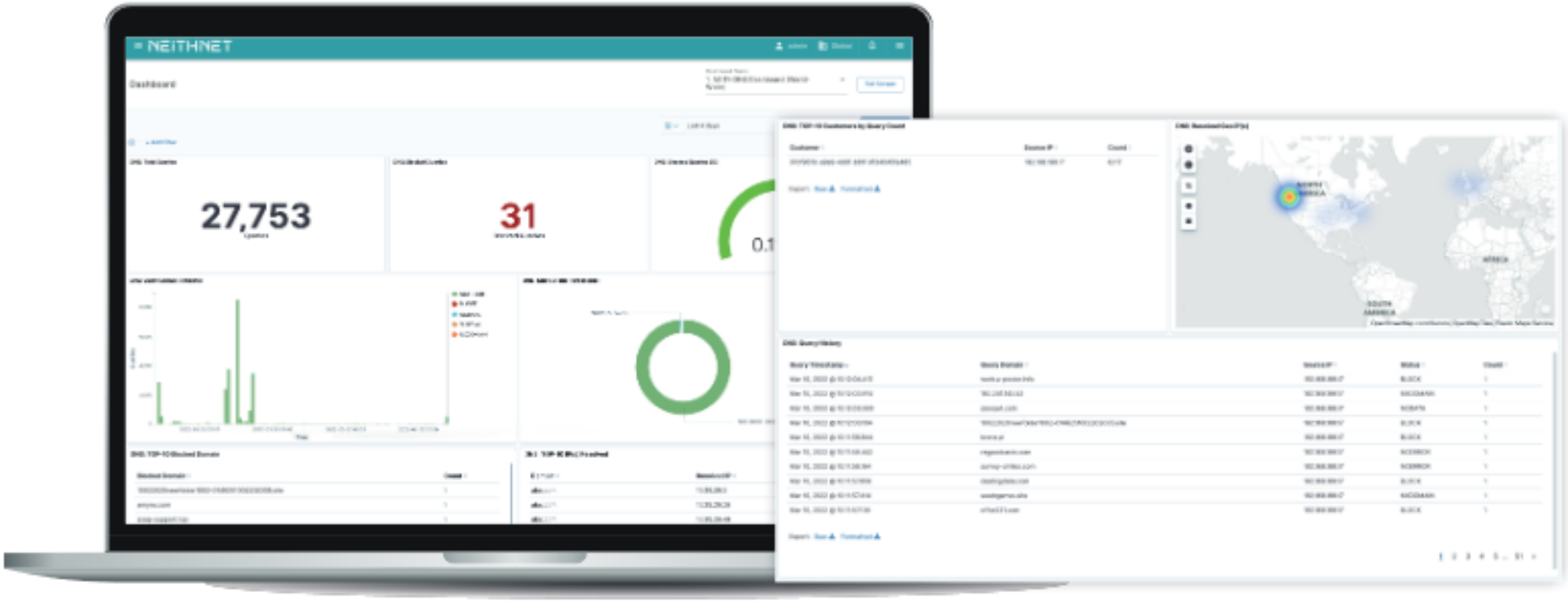
休閒遊戲

宗教、宗教協會

新聞媒體

上網行為可視化分析

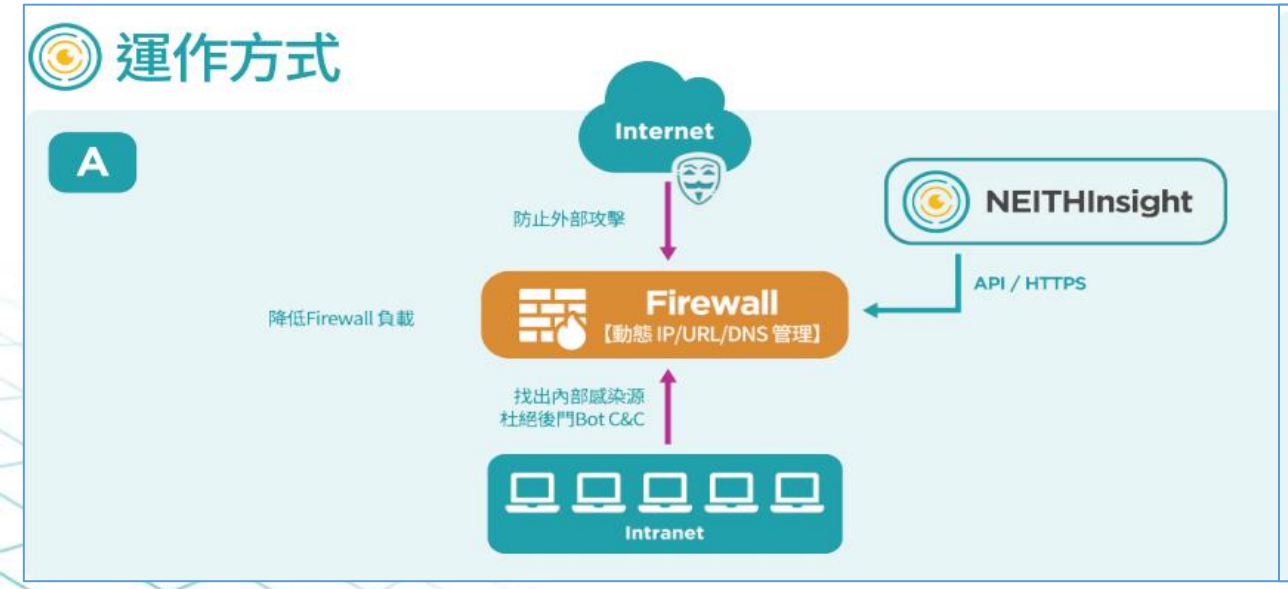
透過深入分析和即時日誌所設計出豐富的報表數據，讓IT管理者快速評估企業 DNS 使用情形。

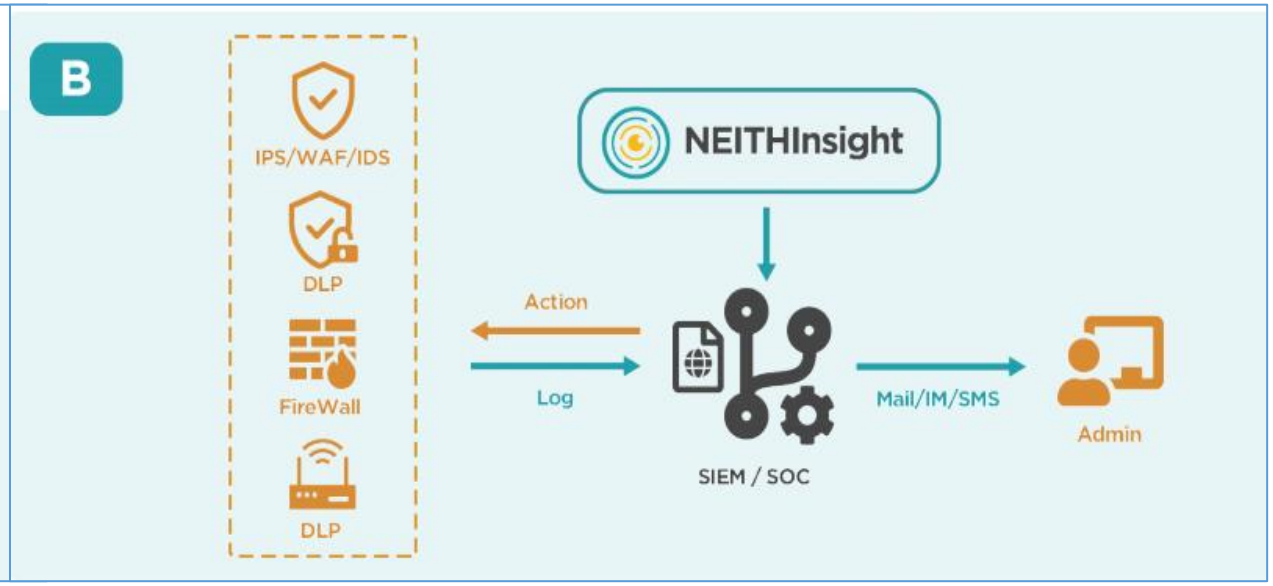


豐富的報表數據，可讓IT管理者等人員快速地評估企業的DNS使用情形

NEITHInsight 在地化情資防禦

可支援的內容	資安防護
選用Botnet、嘗試惡意登入、惡意弱點掃描、DoS、惡意暴力多連線IP等情資，匯入第三層、第四層網路資安設備 URL與Domain資訊可部署至第七層資安設備，更細膩的加強資安防護與偵測	UTM、Firewall、SOC、IPS、WAF
檔案型 HASH可配置於端點設施	Anti-virus、EDR等



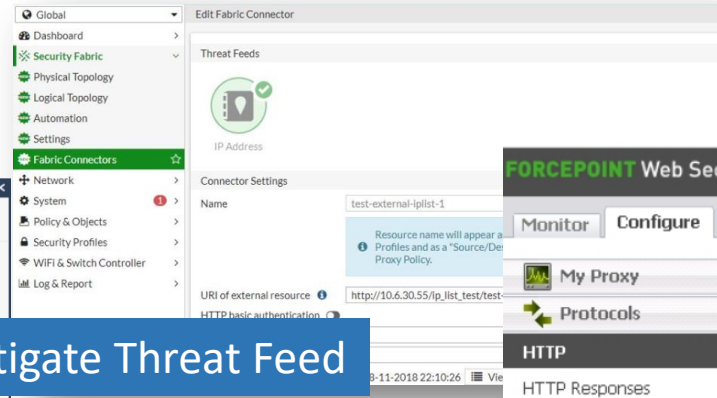


NEITHInsight 應用：整合現有防火牆

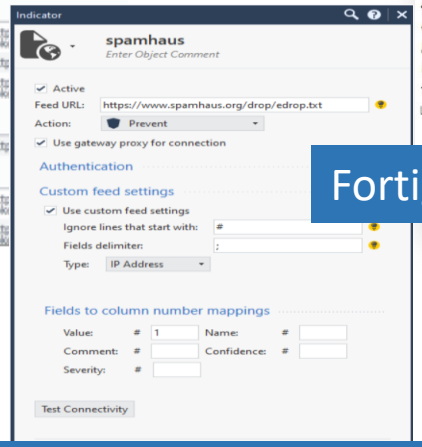
IT管理者可依防火牆的部署，全域應用NEITHInsight情資，即使過保的防火牆也適用

- 結合目前UTM，直接實現多層次的資安防護，加入在地化的情資，完整保護企業資產

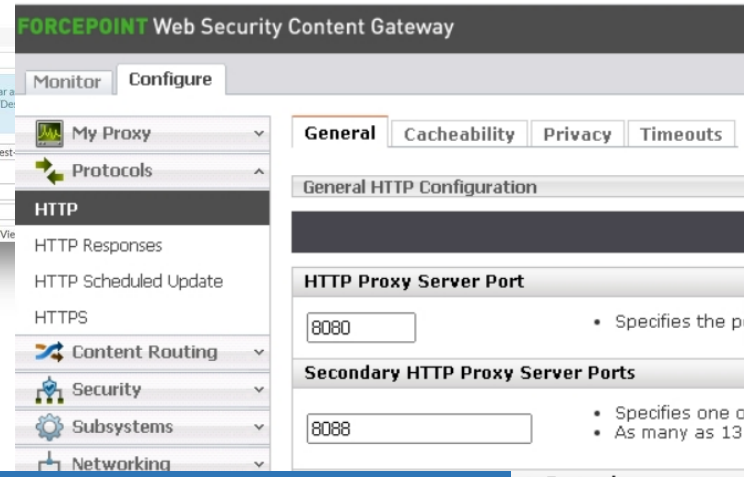
Paloalto External Dynamic List



Fortigate Threat Feed



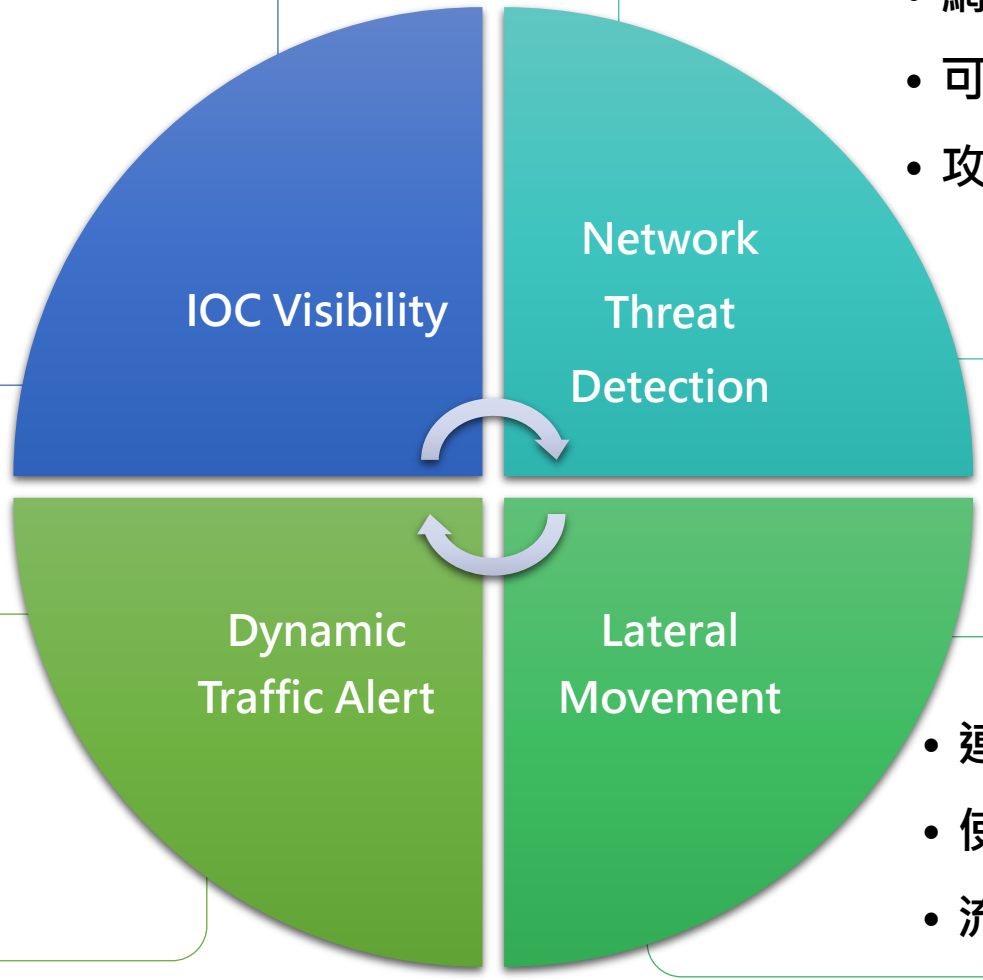
Checkpoint External Indicator



Forcepoint API Connector

NEITHViewer如何找到內部威脅

- 惡意位址來源/目的
- 惡意類別分析
- 惡意風險分析
- 惡意活動時間

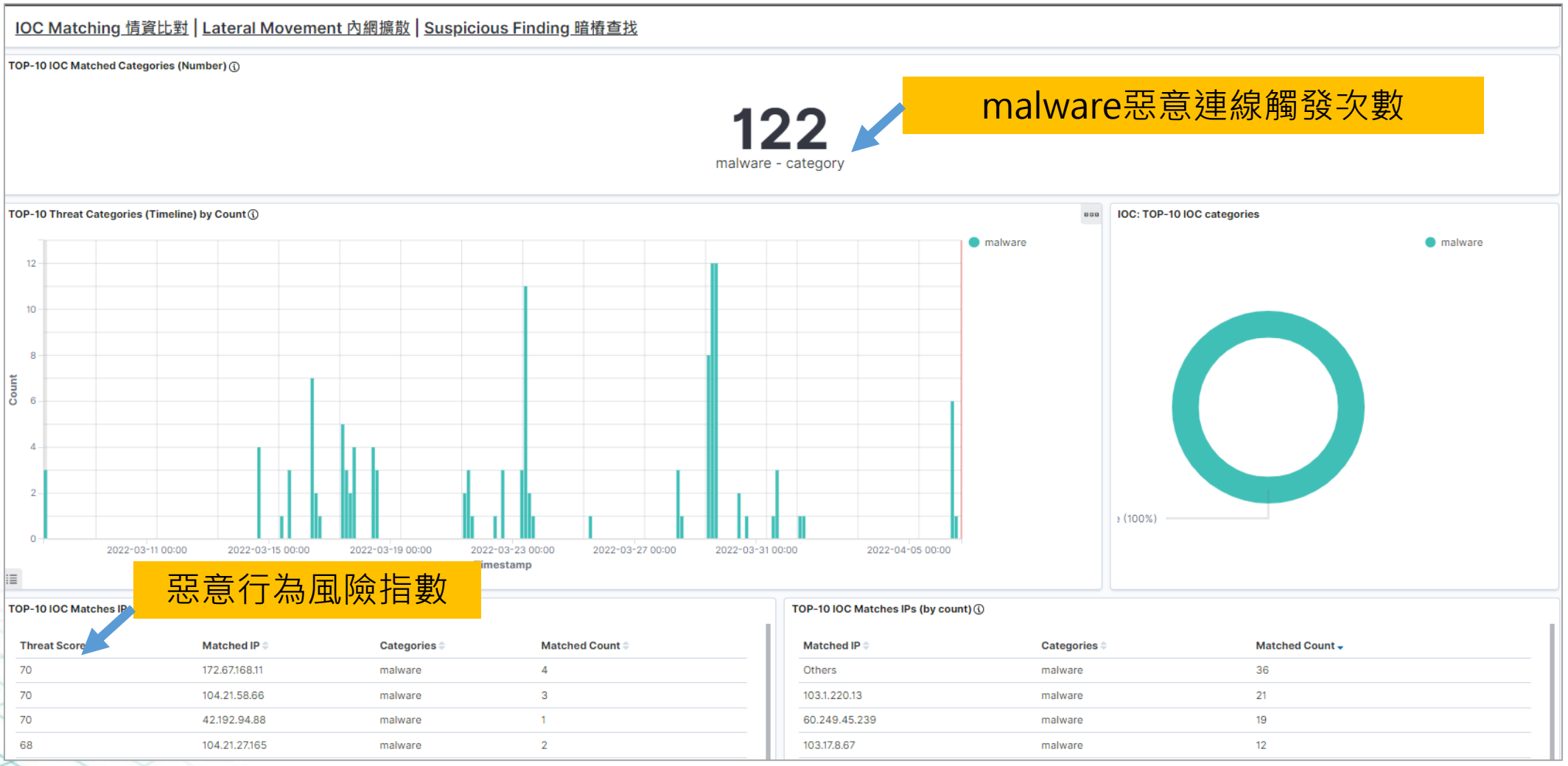


- 網路攻擊行為
- 可疑應用程式行為
- 攻擊網路拓樸圖

- Machine Learning
  學習動態流量
- 異常流量告警

- 連線位址
- 使用服務
- 流量分析

實例說明：利用情資類別找出內部主機(1)



實例說明：利用情資類別找出內部主機(2)

NEITHNET
Accelerate Your Insight

利用風險指數找出危險主機

TOP-10 IOC Matches IPs (by score)

Threat Score	Matched IP	Categories	Matched Count
70	172.67.168.11	malware	4

Export: Raw Formatted

風險指數

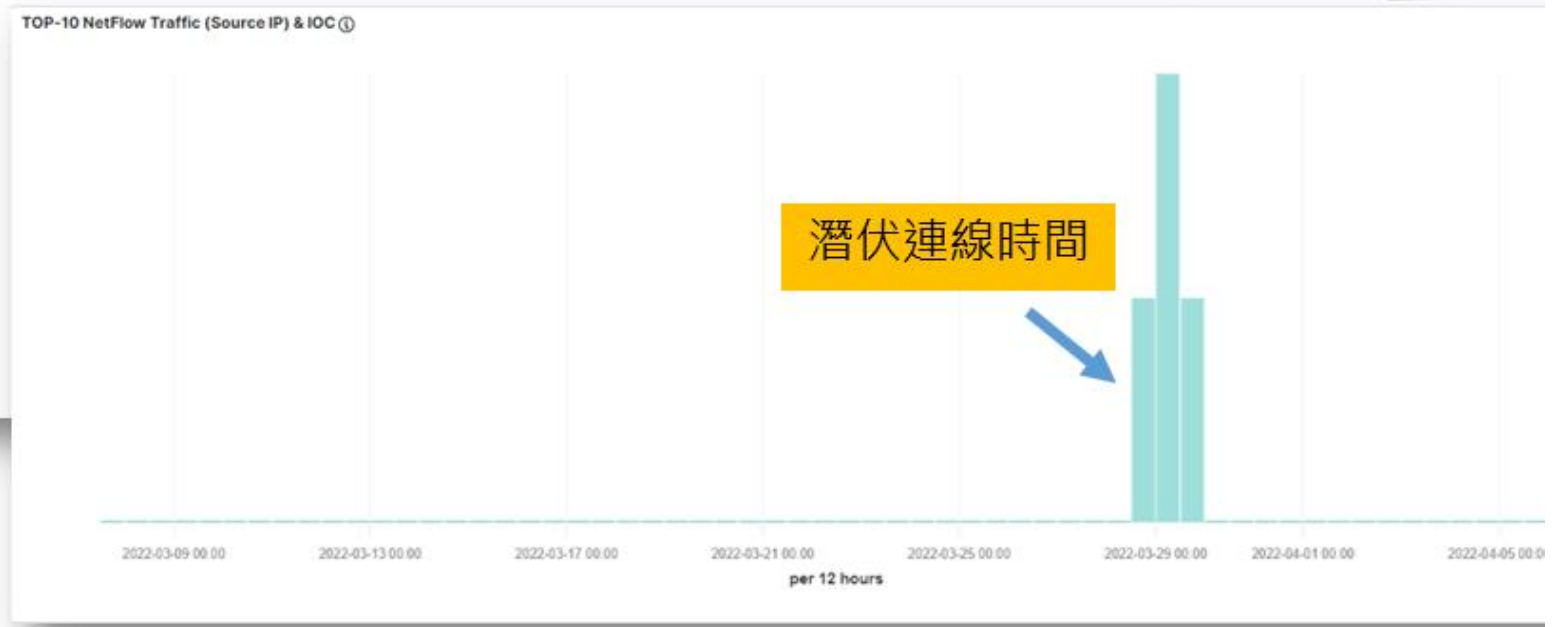
TOP-10 Src/Dest IPs by IOC Matches

Source	Destination	Category	Threat Score	Matched Count
172.67.168.11	192.168.189.244	malware	70	3
192.168.189.244	172.67.168.11	malware	70	1

Export: Raw Formatted

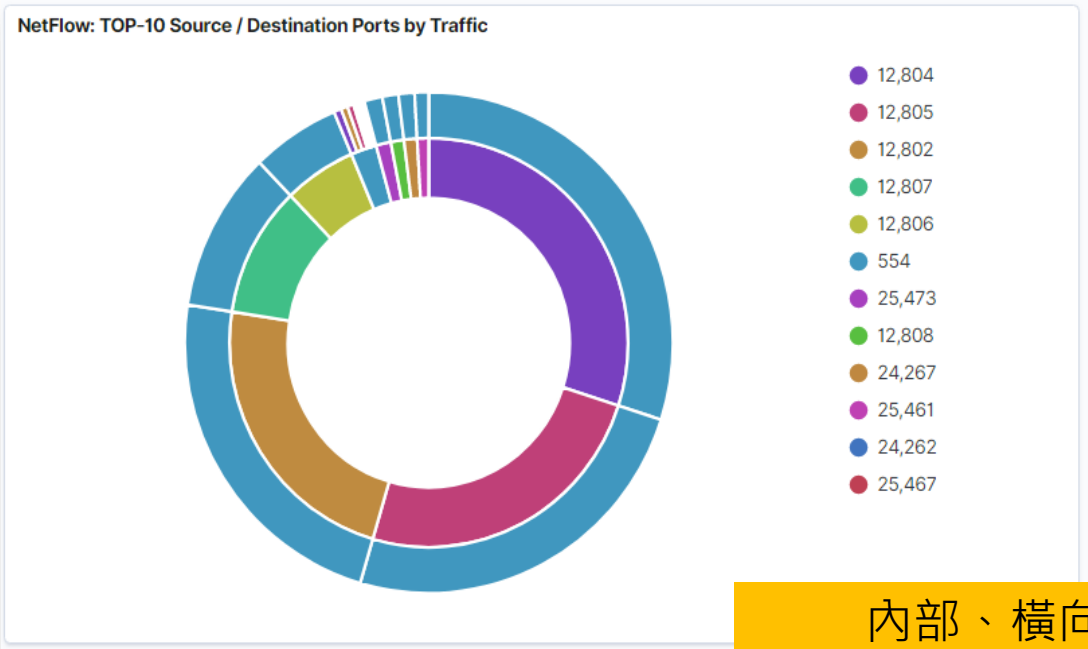
內部主機連線

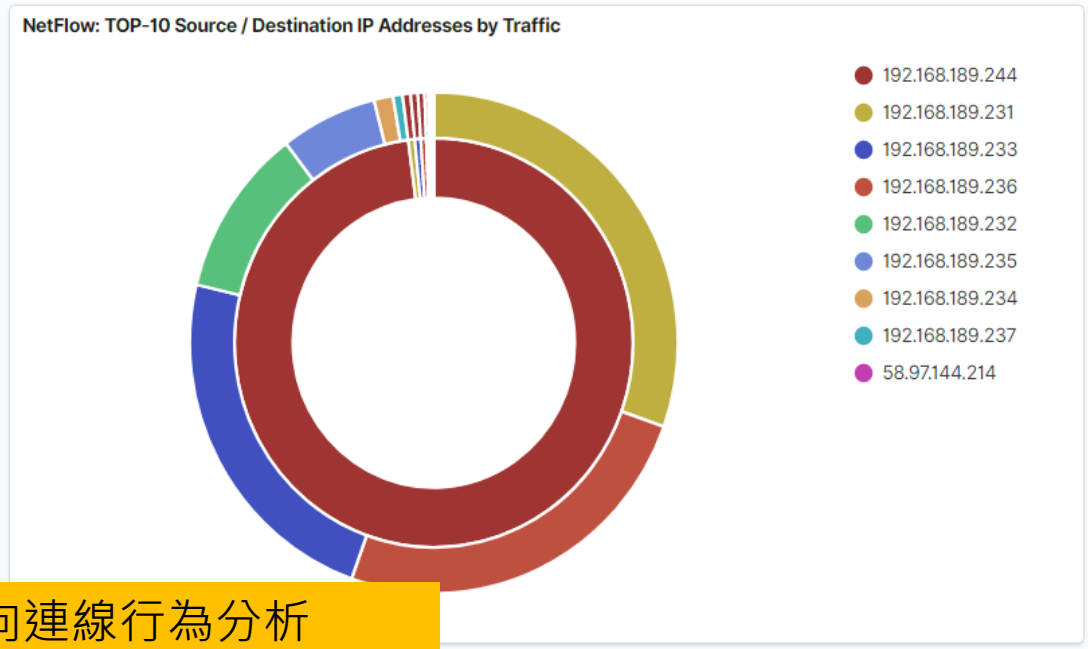
TOP-10 NetFlow Traffic (Source IP) & IOC



實例說明：利用情資類別找出內部主機(3)

NEITHNET
Accelerate Your Insight





內部、橫向連線行為分析

NetFlow: Conversation Partners

Source	Destination	Bytes	Packets	Flow Records
192.168.189.244	58.97.144.214	56B	1	1
192.168.189.244	192.168.189.237	4.5KB	96	83
192.168.189.244	192.168.189.234	5.2KB	111	89
192.168.189.244	192.168.189.235	10.8KB	234	128
192.168.189.244	192.168.189.232	13.6KB	290	132
192.168.189.244	192.168.189.236	24.6KB	532	110
192.168.189.244	192.168.189.233	27.3KB	596	105
192.168.189.244	192.168.189.231	30KB	665	90
192.168.189.237	192.168.189.244	35.2KB	174	113

實例說明 ：利用情資類別找出內部主機(4)

NEITHNET
Accelerate Your Insight

NAD: TOP-10 Classification (table)

Classification Name	Count
insite network access	5,754
A Network Trojan was detected	156
Attempted Information Leak	38
Potentially Bad Traffic	23

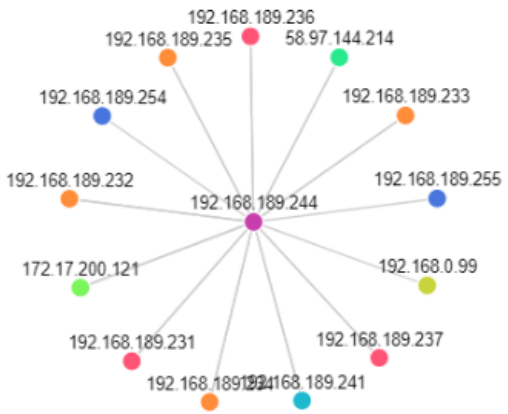
Export: Raw Formatted

NAD: TOP-10 Events (table)

Event Name	Count
inside	5,754
ET INFO Java Serialized Data via vulnerable client	78
ET INFO Java Serialized Data	78
GPL SCAN webtrends scanner	38
ET POLICY Vulnerable Java Version 1.8.x Detected	23

內部、橫向惡意行為分析

NAD : Topology for Network Activities(IPv4)



可疑或惡意行為辨識

該主機被利用進行JAVA弱點掃描其他主機，可能尋找Log4j弱點伺機攻擊

NEITHNET
Accelerate Your Insight

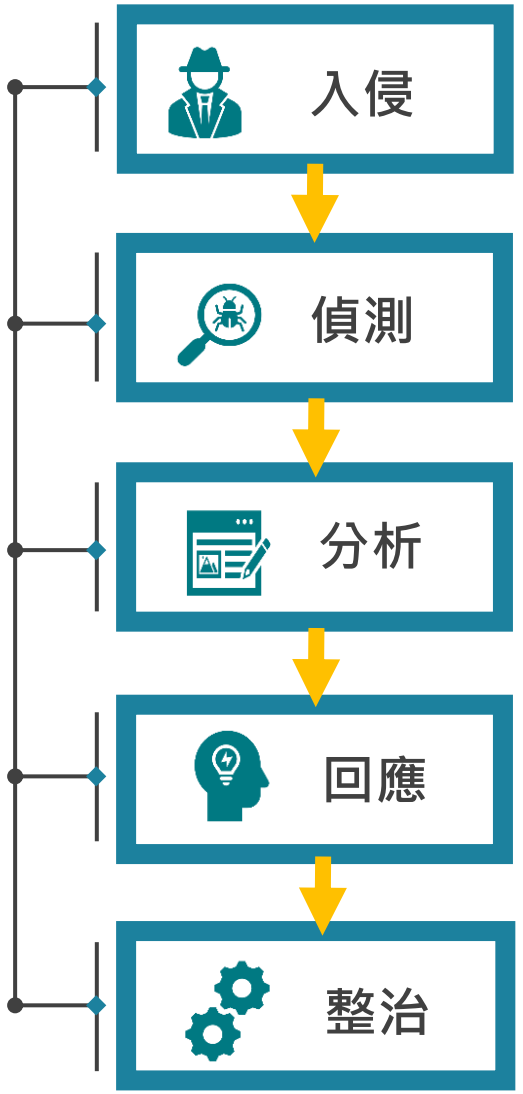
NEITHSeeker MDR

監控端點資料，釐清惡意跡象

建置環境確認
Server/PC都一樣
Win/Linux/Mac都支援

運作架構確認
直接安裝->雲端/代理/地端
無痕安裝->離線

Agent安裝容易
一鍵安裝、相容性高，可透過AD大量部署



NEITHSeeker 事件處理流程

安裝Agent

- 收集Raw log
- 即時分析

偵測威脅

- 分析師進行分析
- 發布告警

惡意程序處理

- 停止程序
- 隔離程式
- 清查感染主機
- 隔離主機

回收樣本分析

- 沙箱分析
- 逆向工程分析
- 惡意行為分析

事件分析

- 入侵時間
- 入侵方式
- 入侵階段
- 漏洞修補建議

完整清除威脅

NEITHSeeker-MDR威脅鑑識的主要核心

威脅入侵

已知威脅	未知威脅	事件調查
透過情資收集、樣本分析,取出攻擊的Pattern或hash	透過[情資+攻擊手法規則]辨認各種行為，是否有偽裝程式或異常行為的狀態	調查事件脈絡，標明事件發生之人事時地物 建議資安措施，針對環境漏洞或規範進行調整

透過MDR服務避免進入IR資安事件處理

Thank you!

NEITHNET

www.neithnet.com

NEITHNET
Accelerate Your Insight

《議程問卷》

憑填寫完成畫面，於出口處領取精美小禮

關鍵在地情資，化解遇駭危機