106年度臺中區域網路中心資安防護研討會

物聯網盛行下的資安防護思維

時 間	主 題	講 師
09:00 – 09:30	報到	
09:30 – 09:40	致歡迎詞	中興大學
09:40 – 10:30	無所不在的資安挑戰- 新世代的資安防護思維	華電聯網 副總經理 鄭炤仁 博士 華電聯網 資深協理 楊仁吉
10:30 – 10:50	Break	
10:50 – 11:40	物聯網下的資安挑戰- 協同式巨量資料分析的資安平台	工研院-資通所 卓傳育 博士 華電聯網 經理 杜偉欽
11:40 – 12:00	Q & A	

Hwacom 華電聯網

無所不在的資安挑戰

鄭炤仁, Joe Cheng, Ph.D.
0955-326-094
Joe.cheng@hwacom.com

People-to-People + People-to-Machine + Machine-to-Machine

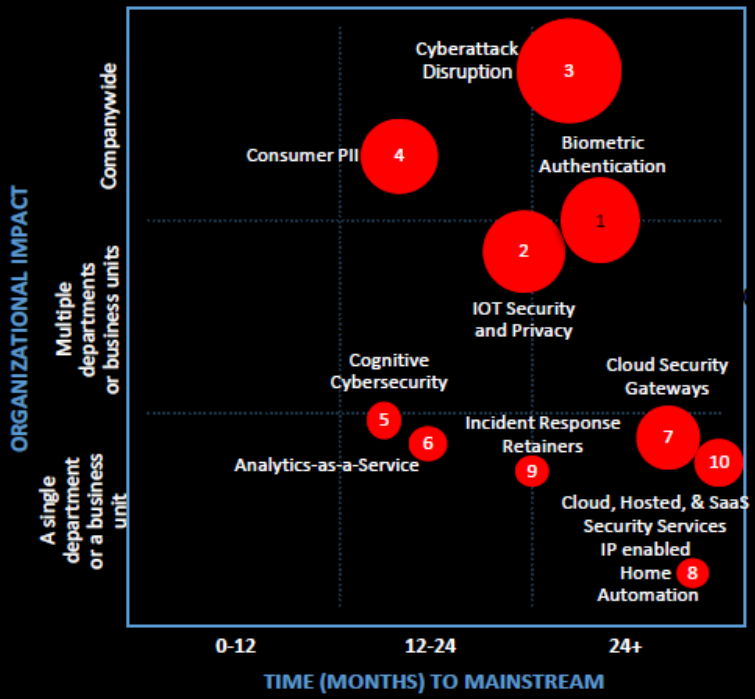
Agenda

- Emerging cyber security landscape
- IoT的資安議題
- Wrap up

2017 CEO Concerns

- 全球性的不景氣
- 培養擁有改造能力的下一代領導人(數位化轉型)
- 網路安全

IDC FutureScape:
IT Security Products and Services - APeJ Implications



1. By 2019, 50% of all online transactions will incorporate biometric authentication driven by a ubiquitous technology infrastructure that enables low implementation costs and broad user acceptance.
2. By 2019, more than 75% of IOT device manufacturers will use security and privacy as competitive positioning to capture the attention of security and privacy advocates and earn consumer trust.
3. By 2019, nearly every major multinational corporation with ties to the U.S. or Europe will face significant cybersecurity attacks aimed at disruption of commodities.
4. Over the next two years, 80% of consumers in developed nations will defect from a business because their personally identifiable information is impacted in a security breach.
5. By 2018, 30% of enterprise cybersecurity environments will incorporate cognitive/AI technologies to assist humans in dealing with the vastly increasing scale and complexity of cyber threats.
6. By 2018, 30% of enterprise customers will leverage analytics-as-a-service to help solve the challenge of combing through security related data and events
7. By 2020, cloud security gateway functionality begins to be integrated as part of web service offerings to entice IT leaders to move offerings to the cloud.
8. By 2020 30% of U.S. broadband homes will have at least one IP enabled home automation or security monitoring sensor/device
9. Reactive security services such as Incident Response and Forensics services will marginally increase by 2020 but still overshadowing proactive services
10. By 2025, on premises security management will be a thing of the past subsumed by SaaS security and Network-based security.

IDC Analyze the Future

IDC FutureScape: Worldwide IT Security Products and Services 2017 Predictions – Asia/Pacific Excluding Japan Implications. Doc #AP42209917

Getting Past The Eye Test (on Previous Slide)

- Mobile biometrics
- IoT
- Cyber-terrorism/warfare
- Consumer reaction
- Machine learning/ AI
- Analytics
- Cloud security
- Incident response and Forensics
- Security as a service

IDC
Analyze the Future

智慧化的趨勢

網路的連結

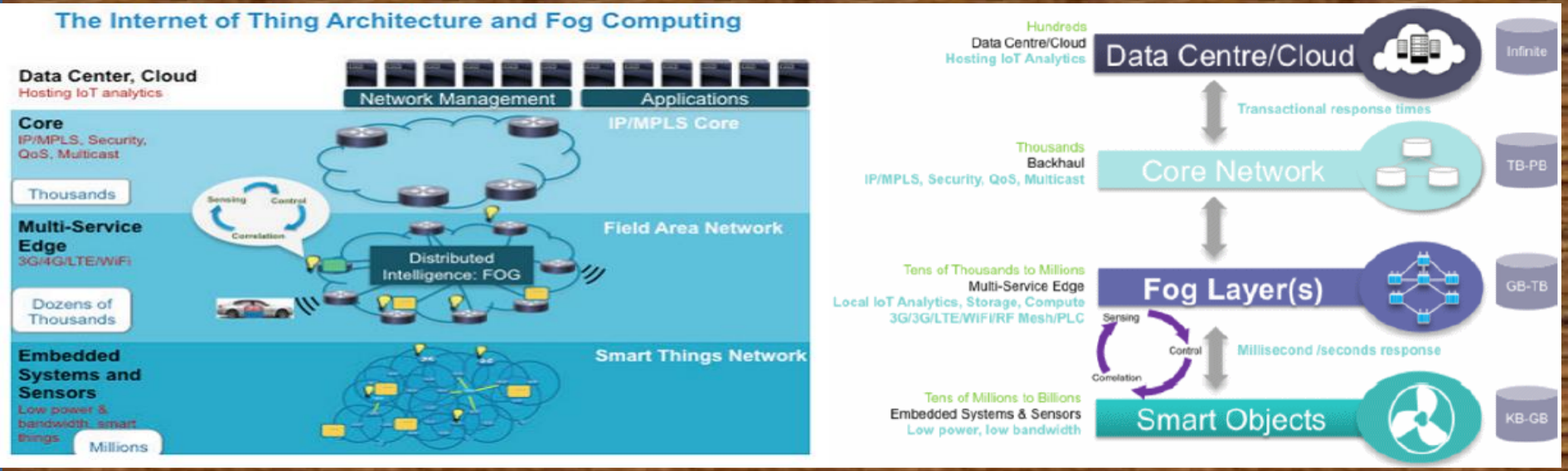
有線網路

無線網路

LAN

WAN

IoT Multi-Layers Architecture



How Many Devices Will Connect to Your Network by 2030?

500 B devices will be connected worldwide

70% of professionals will conduct their work on personal smart devices by 2018

DDoS 攻擊上升 6%：IoT 物聯網是主要攻擊原因！

無所不在的資安挑戰

Attacks are Everywhere!

IDC
Analyze the Future

資安不再只是IT的議題

資安已是商務風險的議題

Thank You

Hwacom

華|人|寬|頻|世|界|的|首|席|建|構|家

Hwacom 華電聯網

新世代的資安防護思維

楊仁吉, *Jerry Yang*
資安服務處
Jerry.Yang@HwaCom.com

Agenda

- 智聯網時代資安面臨的風險與挑戰
- 如何建構安全的資安環境與有效的管理

資安已是「商務風險」的議題
資安不在只是 IT (MIS) 的問題

資安造成的商務風險

營業秘密遭竊取

全球會計師事務所德勤(Deloitte)，09/25日傳出**遭到駭客竊取機密文件**的消息，公司雲端更有多達5百萬封電子郵件的個資恐遭外洩。(路透)

資安造成的商務風險

勒索軟體

導致 產線停止、金錢、數位資產的損失

本田(Honda)表示，雖然針對WannaCry提高防護，但仍發現日本、北美、歐洲、中國等地網路遭到攻擊，因此決定暫時關閉琦玉縣一座工廠。

資安造成的商務風險

殭屍電腦

攻擊其他企業

- 2.5萬監視器成DDoS殭屍網路大軍，多數來自台灣！
- 傀儡網路氾濫，臺灣成為全球DDoS攻擊幫兇！

資安造成的商務風險

營收X競爭力X商譽損失

智聯網時代資安面臨的挑戰

入侵點的增加
防禦邊界擴大

智聯網時代資安面臨的挑戰

智聯網時代資安面臨的挑戰

智聯網時代資安面臨的挑戰

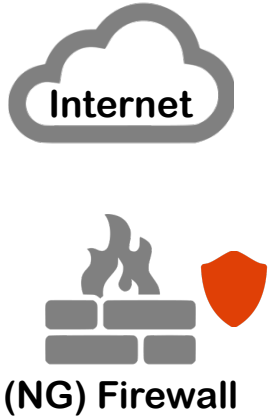
看不到防護狀況

無法安排優先順序

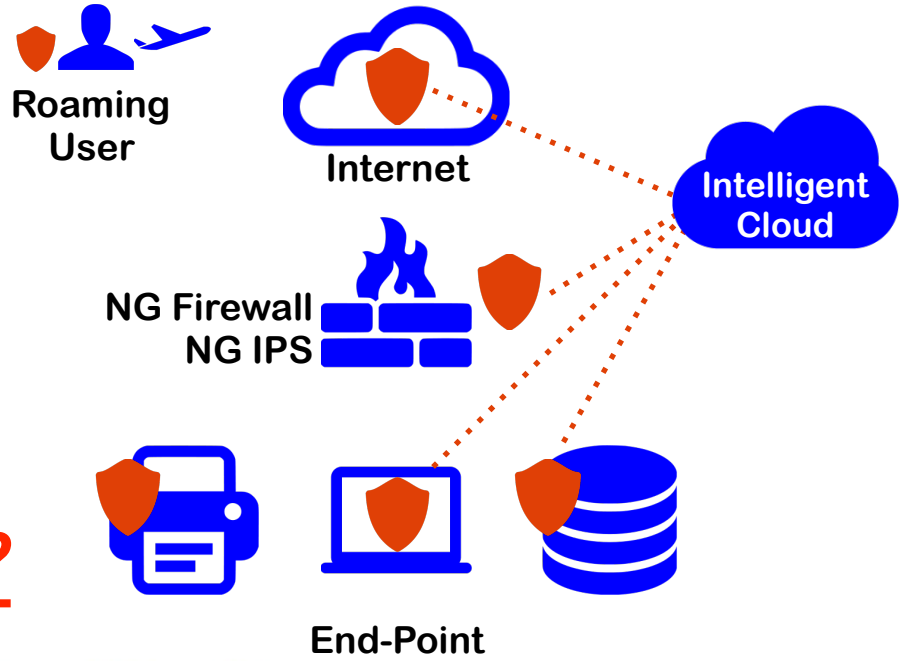
如何建構
安全的資安環境
有效的管理

強化縱深防禦 – 空間換取時間

傳統資安防禦架構



新世代資安防禦架構



But Is This Enough ?

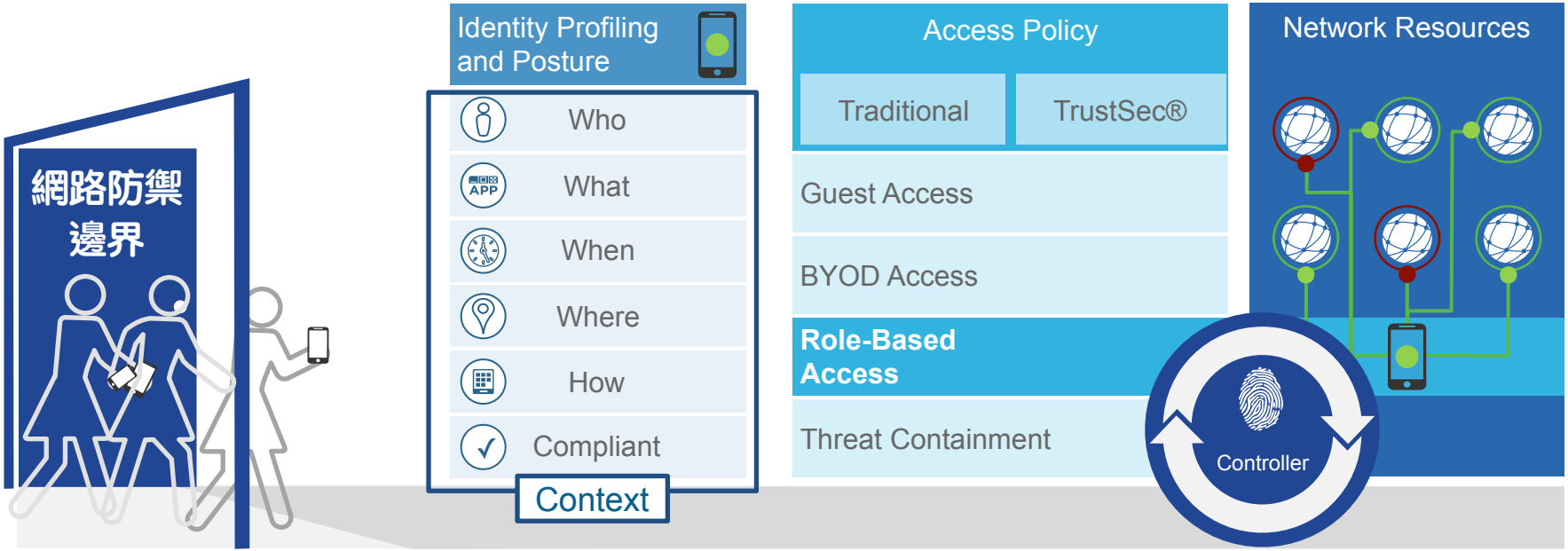
可控的資安管理環境

- 為什麼已經 **重兵部署** 但仍然會遭木馬、勒索軟體感染？
- 已經是 **封閉式環境**，但還是有木馬、勒索軟體感染？
- 內部雖有相關的資安作業規範，但執行上仍有落差！

可控的資安管理環境

But Is This Enough ?

集中安全管理方式，自動依據 資安合規狀態 執行 網路資源訪問授權 並 共享 數據。

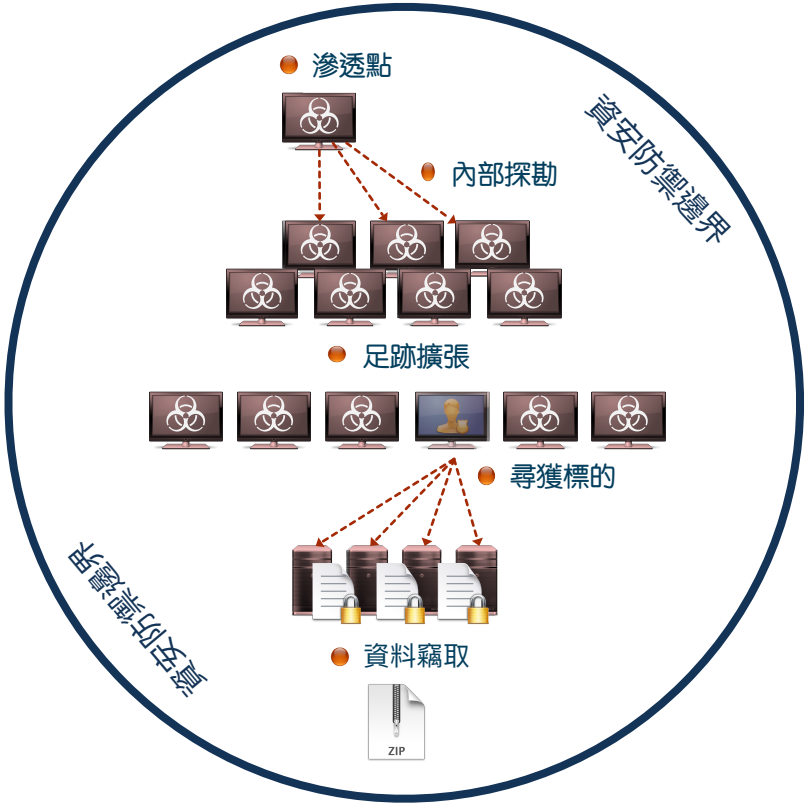


駭客如何進到我們的環境？

- 木馬程式

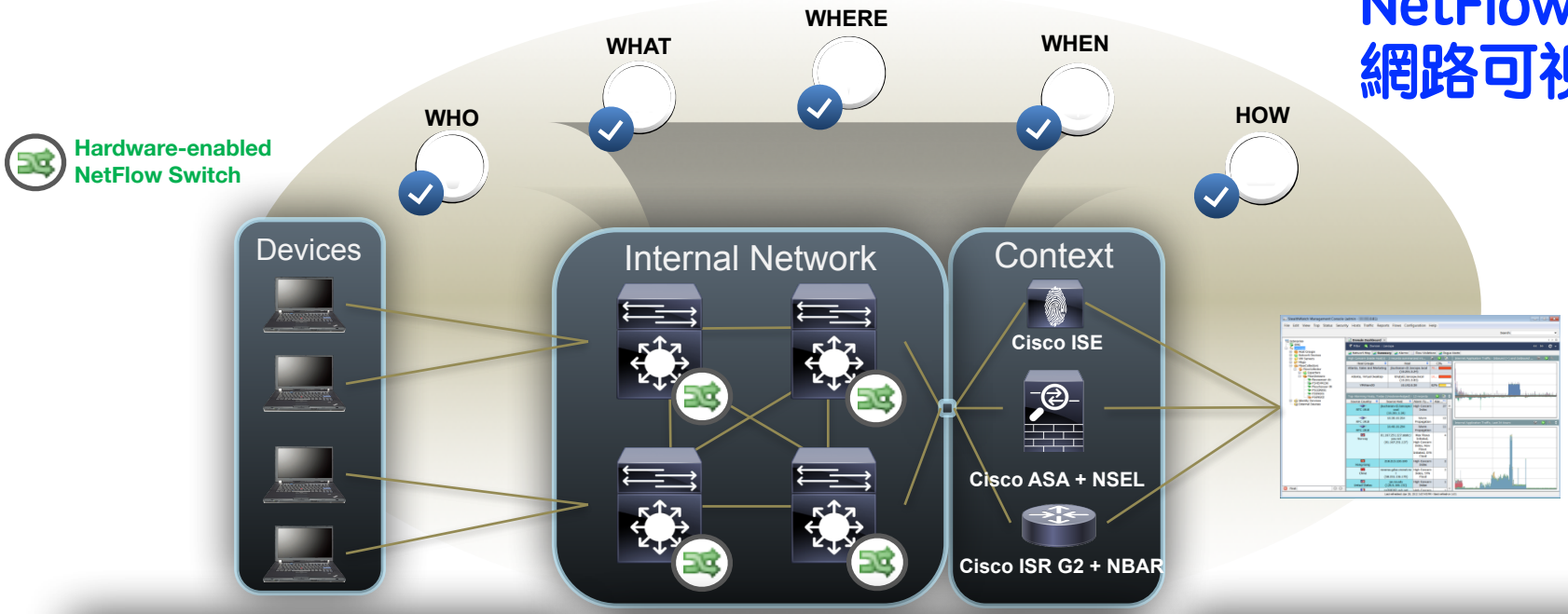
渗透勘查管道

- 銷售資料獲利



資安可視化架構

NetFlow 提供網路可視性



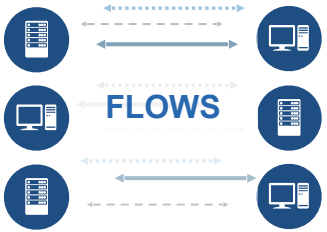
Use NetFlow Data to Extend Visibility to the Access Layer

Enrich Flow Data With Identity, Events and Application to Create Context

Unify Into a Single Pane of Glass for Detection, Investigation and Reporting

行為和異常檢測模型

COLLECT AND ANALYZE FLOWS



SECURITY EVENTS (94 +)

Addr_Scan/tcp
Addr_Scan/udp
Bad_Flag_ACK**
Beaconing Host
Bot Command Control Server
Bot Infected Host - Attempted
Bot Infected Host - Successful
Flow_Denied
.
.
ICMP Flood
.
.
Max Flows Initiated
Max Flows Served
.
Suspect Long Flow
Suspect UDP Activity
SYN Flood

ALARM CATEGORY

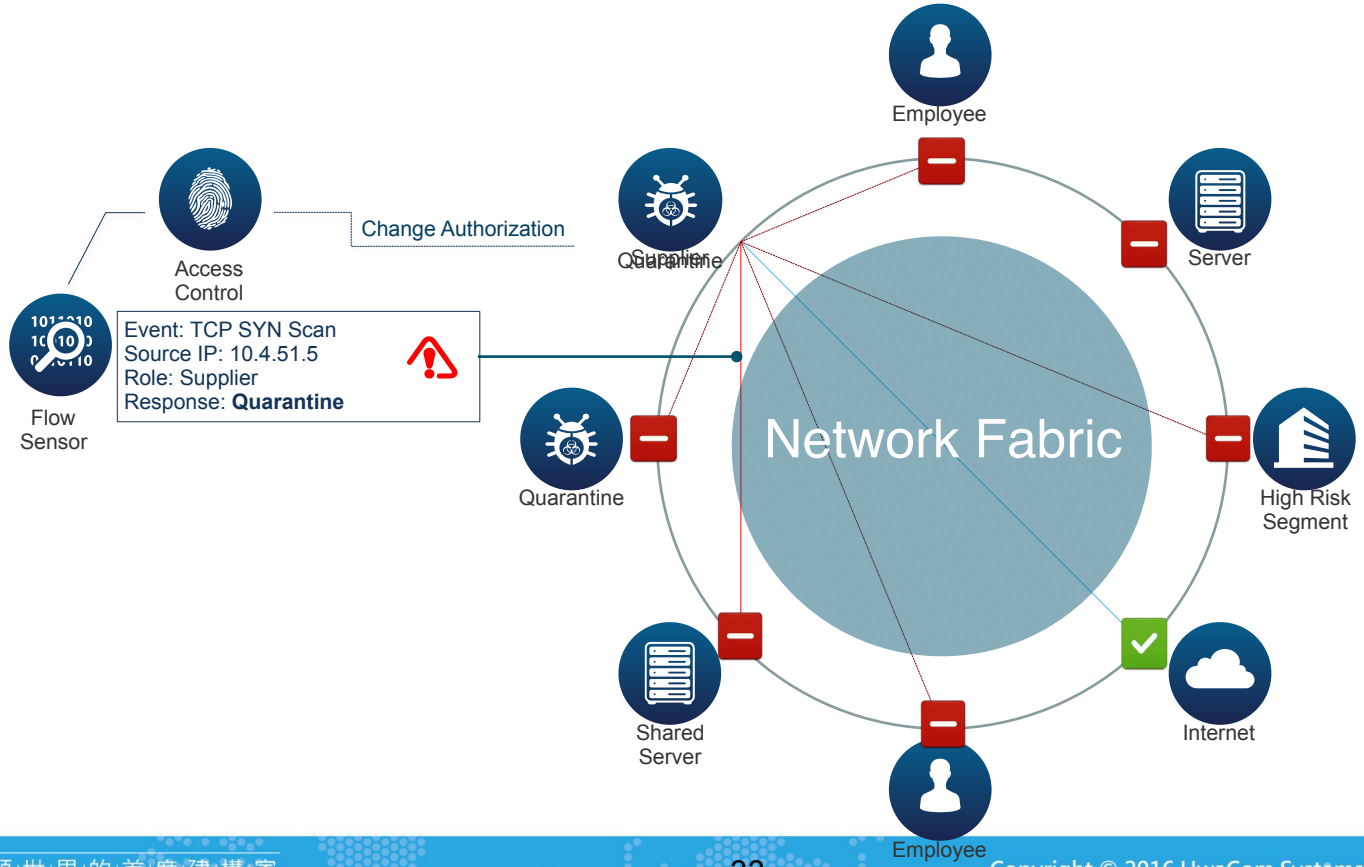
- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

RESPONSE

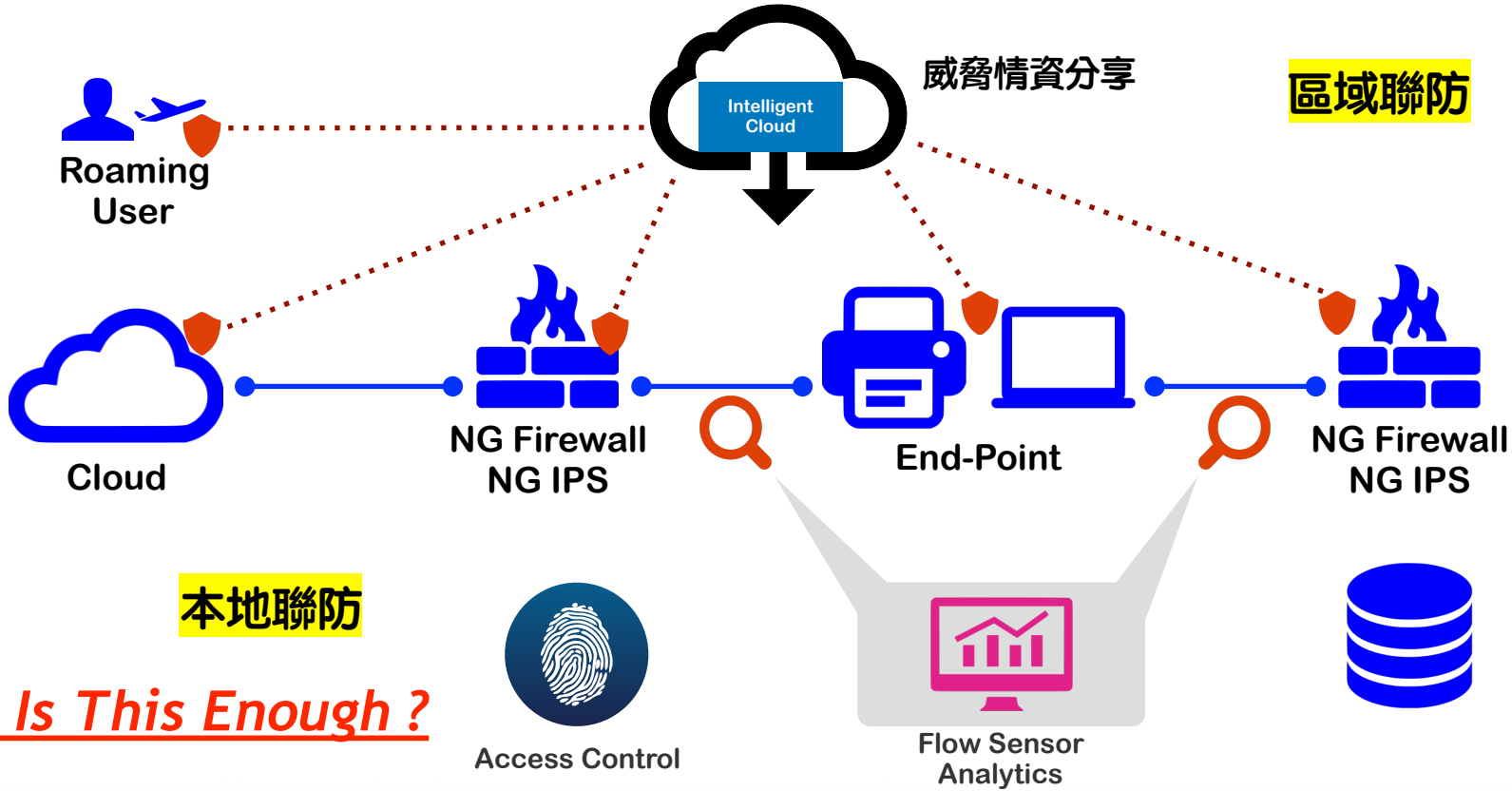
- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation

But Is This Enough ?

自動化本地聯防



自動化聯防機制



But Is This Enough ?

Something We Can Do Better 

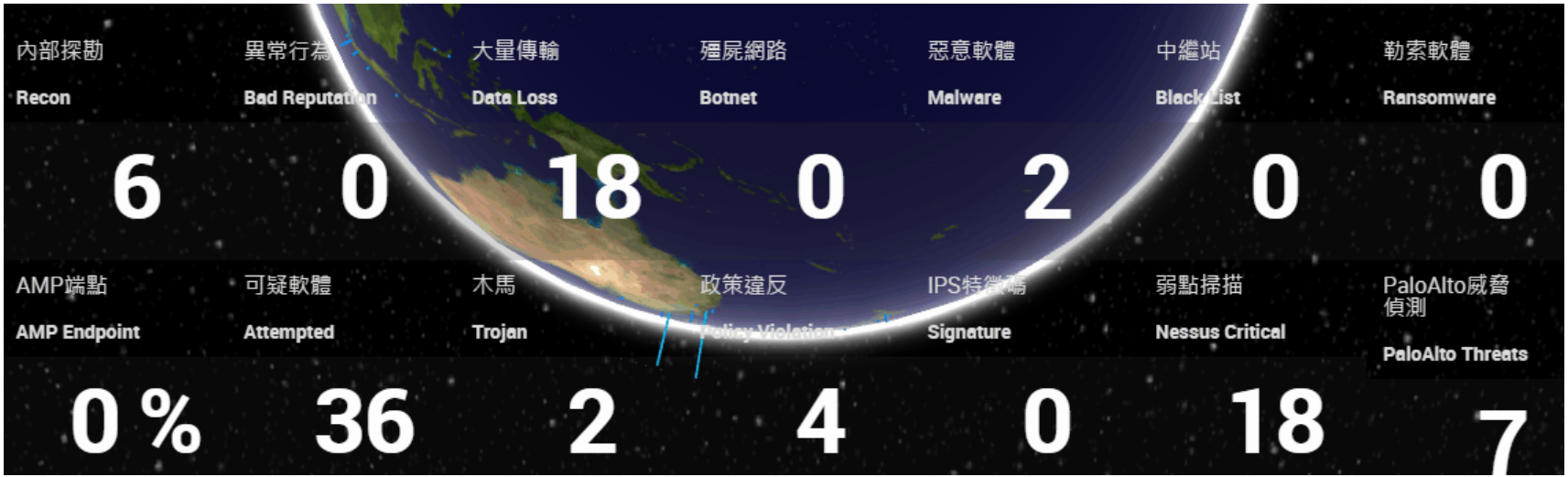
Something We Can Do Better ^^

應用程式白名單技術

我們不應該允許未知的程式在系統中執行！

資安視覺化儀表板

- 看到資安防護狀況，安排處理優先順序。
- 進行交叉關聯式分析，找出害群之馬。
- 自動化通知相關負責人，立即處理問題。



One more thing …

定期執行滲透測試了解防護能力

- 利用軟體定期檢測網路、系統是否有弱點(漏洞)存在?
- 僅是利用軟體檢測還是會有失誤的時候！
- 滲透測試可以：
  - 有效地確認現有資訊作業環境的**弱點**與**風險**
  - 直接**改善**測試所得知的弱點。
  - 可規劃**更為安全**的資訊系統架構，以抵禦更多可能的入侵。

Summary

- 強化縱深防禦。
- 可控的資安管理環境。
- 資安可視化架構。
- 行為和異常檢測模型。
- 自動化聯防機制。
- 限定執行的應用程式。
- 資安視覺化儀表板。
- 定期執行滲透測試。

華|人|寬|頻|世|界|的|首|席|建|構|家

物聯網下的資安挑戰
–安全執行平台與行動應用管理

卓傳育 博士

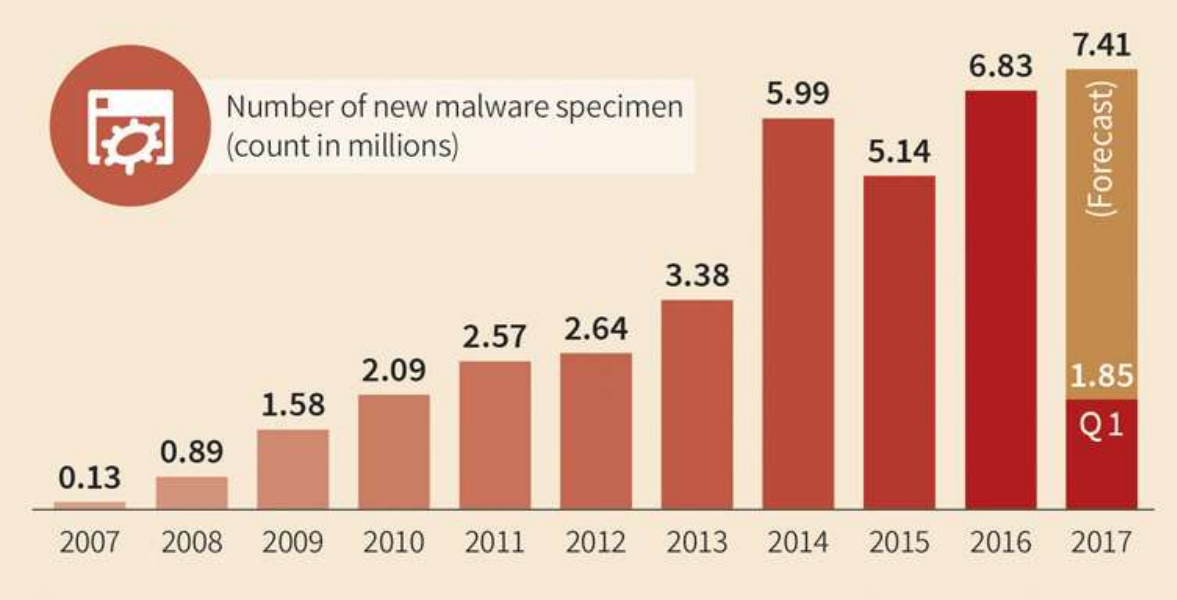
資訊與通訊研究所

Information and Communication Research Lab (ICL)

ITRI
Industrial Technology Research Institute

傳統資安面對的問題

- 越來越多的惡意程式，防毒軟體難以對抗



資料來源: Malware Trend 2017, G-Data Security blog, https://blog.gdatasoftware.com/2017/04/29666-malware-trends-2017

- 因此，端點防護需要有些改變
  - 防止惡意程式: Cloud antivirus
  - 防止非信任程式: Application whitelisting

白名單為何難以普及？

- 難以管理的白名單系統
  - 不好處理軟體更新
  - User 隨便安裝軟體，而被白名單系統阻擋，因此沒辦法正常使用
  - 需要專家設定應用程式白名單資料庫或規則
  - 造成效能損耗

- 因此，適合高安全需求的系統
  - 系統較少更動
  - 若是遭植入惡意程式便損失慘重

需要更堅強的安全系統

- 自駕車、工業 4.0
  - 任何的資安事件發生都可能造成極大損失
  - 目標針對 Industrial Control System 與 CAN Bus

年份	工業與汽車資安大事紀
2010	Stuxnet
2011	Duqu
2012	Flamer
2014	North Korea hacks nuclear plants in South Korea
2015	Duqu 2.0
2015	Car hack on Jeep
2015	Ukraine power grid cyberattack
2016	Ukraine again
2016	Take control of PLCs in Kemuri Water Company

高風險高資安需求系統

- 【詳細圖解】駭客入侵一銀ATM流程追追追
  - 資安專家建議使用白名單來保護高安全需求之系統
- 物聯網裝置
  - 工業 4.0、Security Gateway
- 關鍵伺服器
  - GSN DNS
- 自動駕駛、車聯網
  - In-vehicle computer

資料來源: iThome http://www.ithome.com.tw/news/107294

- **限制可執行的應用程式和 Driver**
  - 應用程式白名單
    - 僅允許可信的程式執行

應用程式白名單技術

Released by CC0, http://maxpixel.freegreatpicture.com/It-Security-Cyber-Security-Computer-Security-1784985

我們不應該允許未知的程式在系統中執行！

安全執行平台

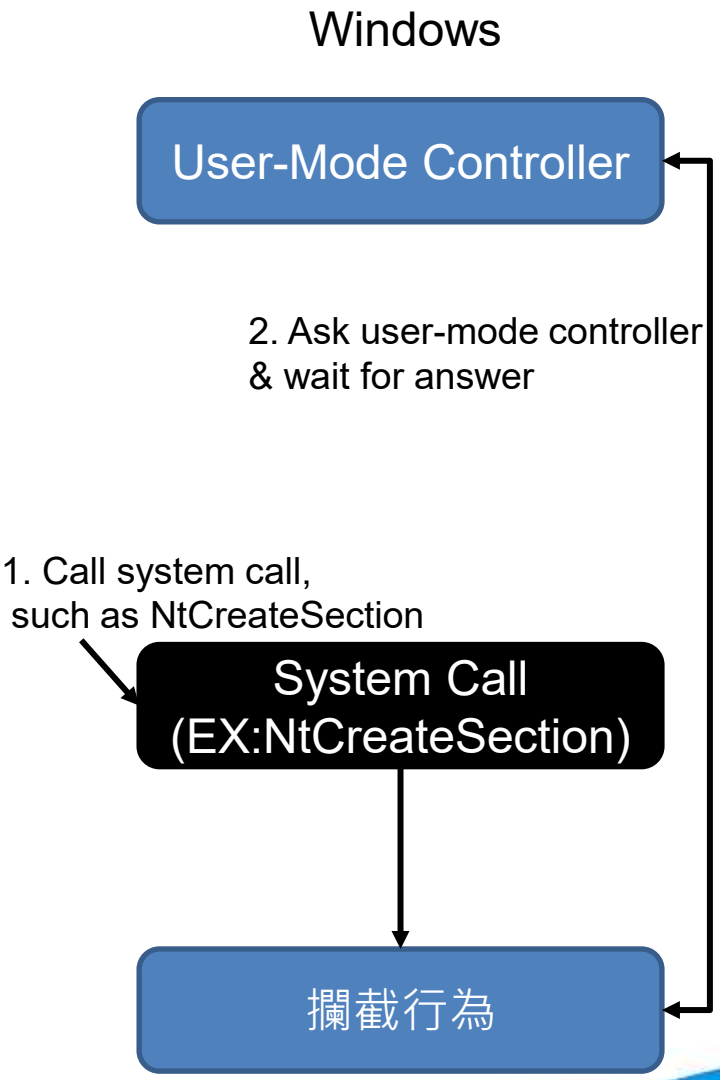
- 針對 Windows / Linux 提供白名單保護
  - 自動建立白名單資料庫

- 檢查類型
  - Executable
  - DLL / shared object
  - Script
  - Kernel driver

- 二階段驗證更新、安裝
  - 應用程式安裝、更新與白名單資料庫更新去耦合化
  - 自動更新時，紀錄寫入的 Executables

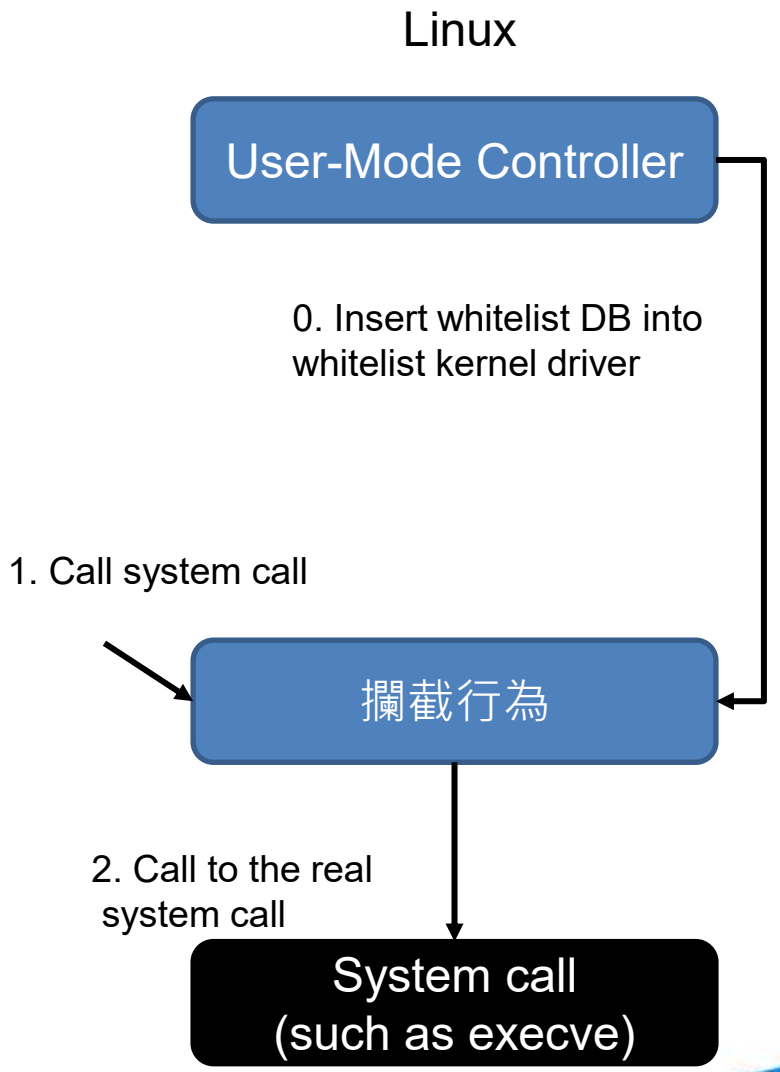
Windows Application Whitelisting

- 攔截以下
  - 載入執行映像檔 (Executable / DLL)
  - 載入驅動程式 (SYS)
  - 嘗試執行 script
- 在 Executable image 被載入的時候檢查 SHA512 checksum 是否符合原先紀錄的可信程式



Linux Application Whitelisting

- 攔截關鍵 system call
  - 載入 shared objects
  - 執行程式
  - 載入 kernel modules
  - 執行 script
- 呼叫 system call 時會先檢查 SHA512 checksum 是否符合原先紀錄的可信程式

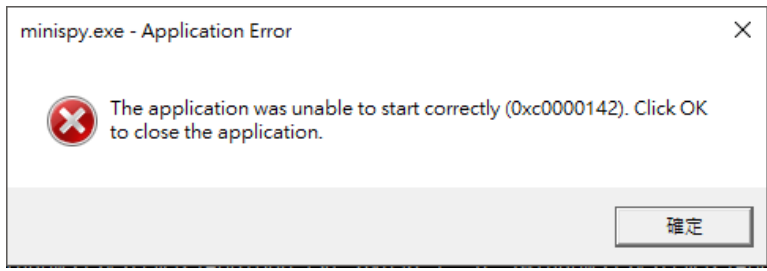


阻擋執行!

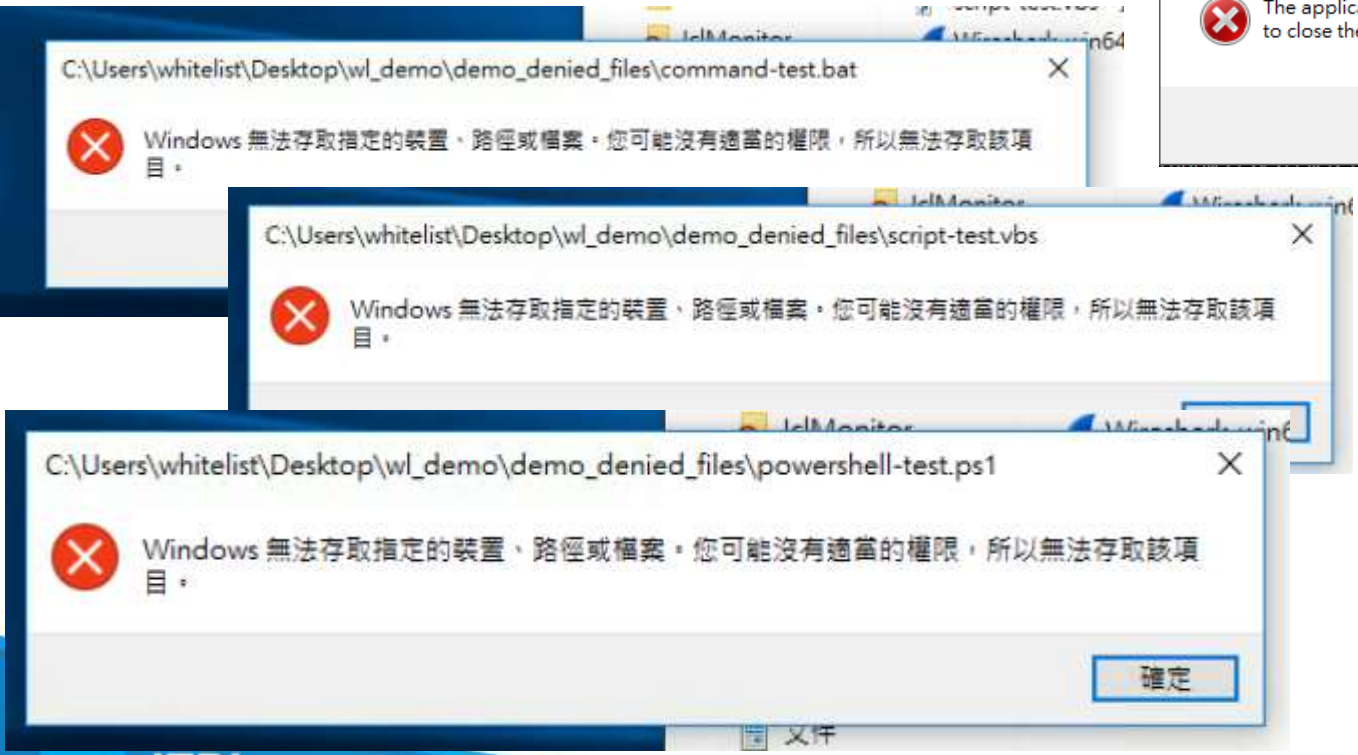
Execute Driver

```
C:\Windows\system32>net start minispy
Reject reason: not IsWhiteListedBinary  C:\windows\system32\drivers\minispy.sys
```

Execute EXE



Execute script

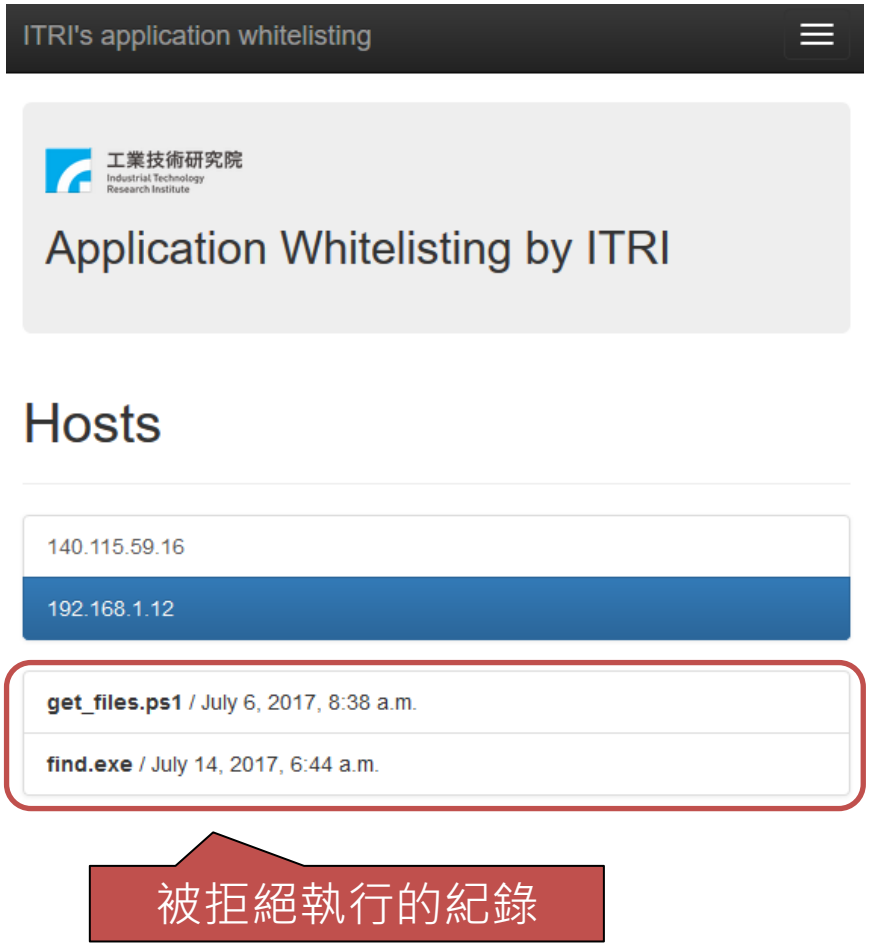


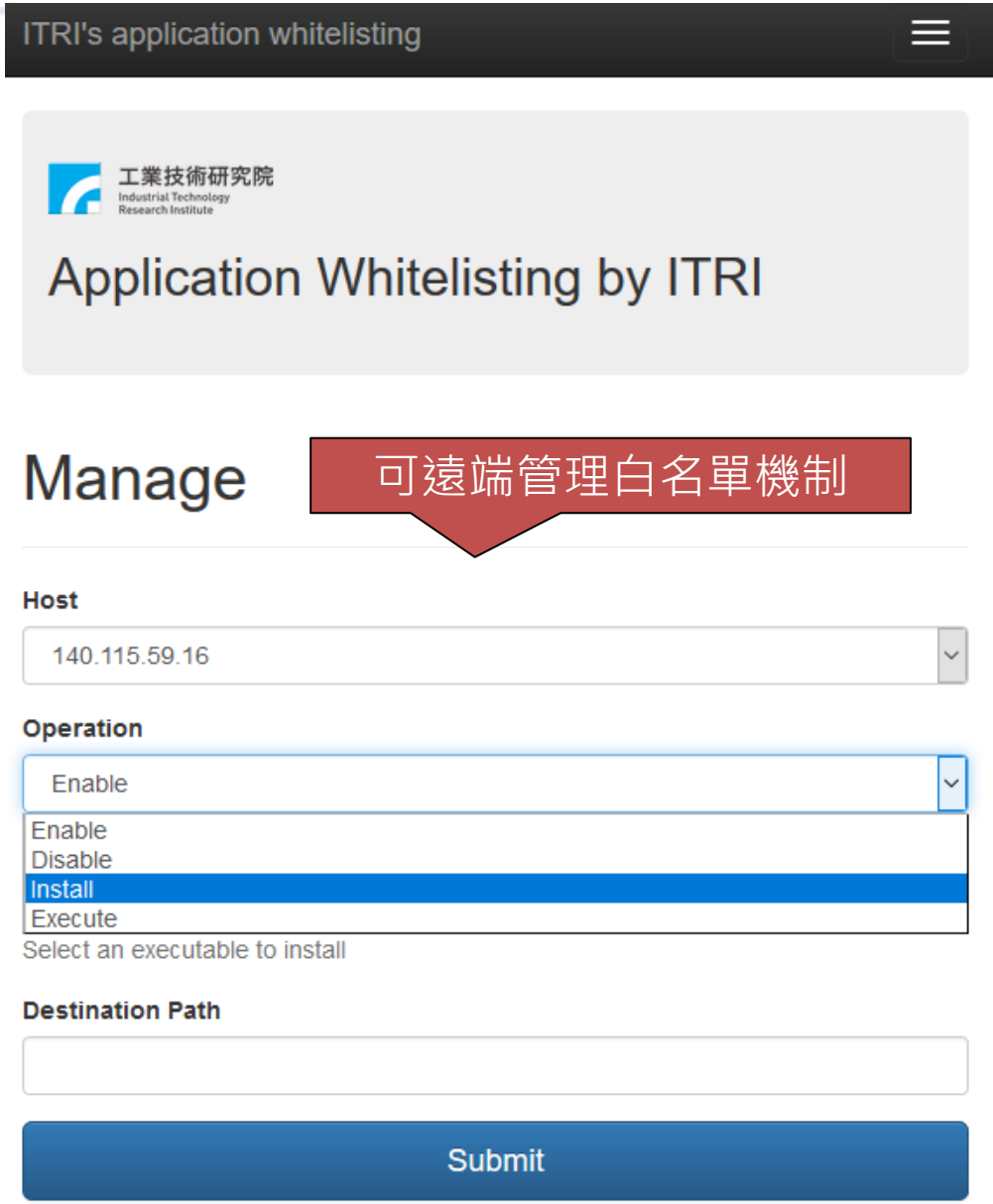
自我保護與管理介面

- 自我保護
  - 防止 DLL injection / ptrace
  - 防止被移除
  - 防止 Registry / Configuration files 被修改

- Web 管理介面
  - 蒐集不在白名單的程式嘗試執行紀錄
  - 可開 / 關遠端主機的白名單機制
  - 管理白名單資料庫
  - 可用於上傳 Zip 或安裝檔
  - 二階段安裝 / 更新確認
    a. 通知管理者正要進行的安裝，並要求管理者的確認

Web-based 管理介面



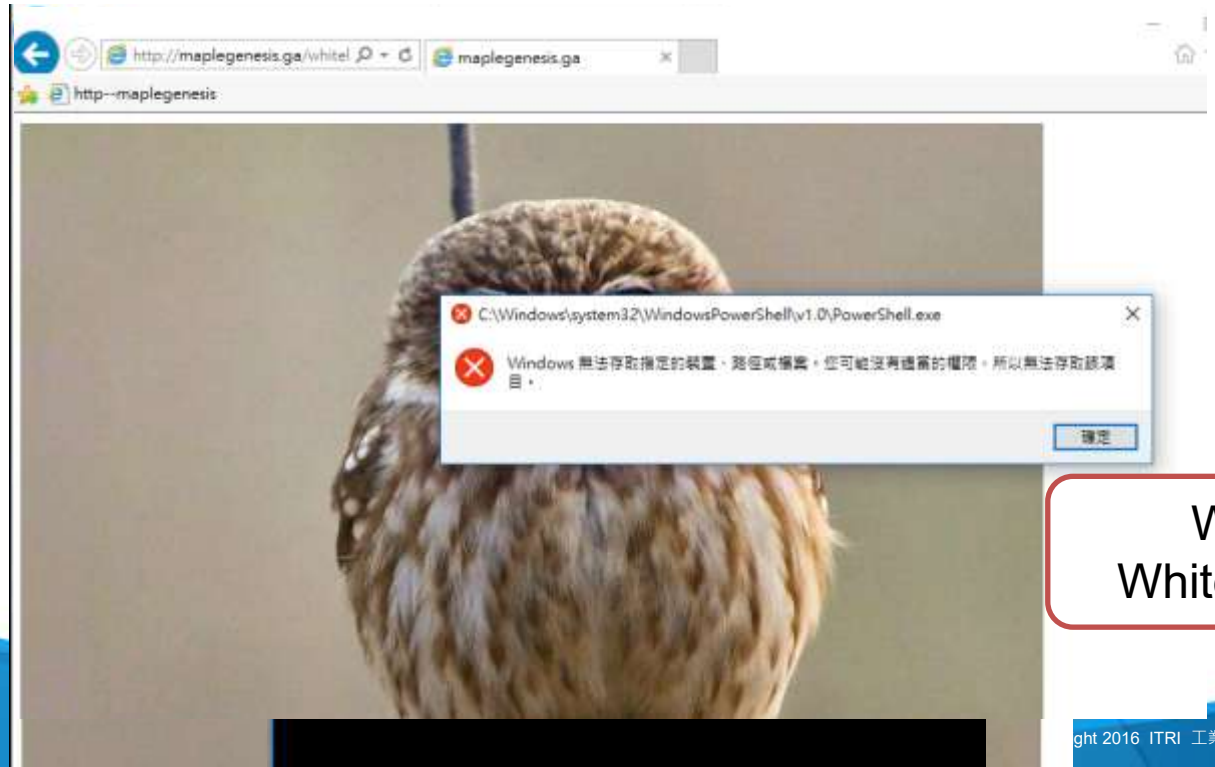


二階段驗證安裝

網頁攻擊範例

- CVE-2016-0189: Scripting Engine Memory Corruption Vulnerability on IE 11

- 用 Internet Explorer 開啟惡意網頁，並從網路上下載 hack.exe
- 沒有白名單機制的 VM 會執行惡意程式 hack.exe
- 再利用管理介面開啟白名單功能



With Whitelisting

Trust level

- Kernel-level solution: 相信 OS Kernel 為安全的
  - 當然攻擊者可以透過 Kernel 漏洞可以關閉整個系統，但 …
- Memory attacks 與 Fileless malware 無法檢查
  - 攻擊者有機會由有漏洞的軟體 → 核心攻擊皆不產生檔案，但可能性微乎其微

應用情境

連網伺服器

- 自建伺服器
  - 政府 GSN DNS / Mail server
  - 關鍵伺服器
- 面對風險
  - Advanced Persistent Threat
  - Data loss

工業 4.0 應用

- 工業系統的 Lifecycle 高達 15~20 年
  - 軟體與系統都難以更新，Patch 需要嚴格測試，成本過高
  - 內部系統充滿漏洞，風險極高
  - 資料交換區很可能是關鍵問題

- 面對風險
  - 資料交換
  - 外包管理

PLC

Control center

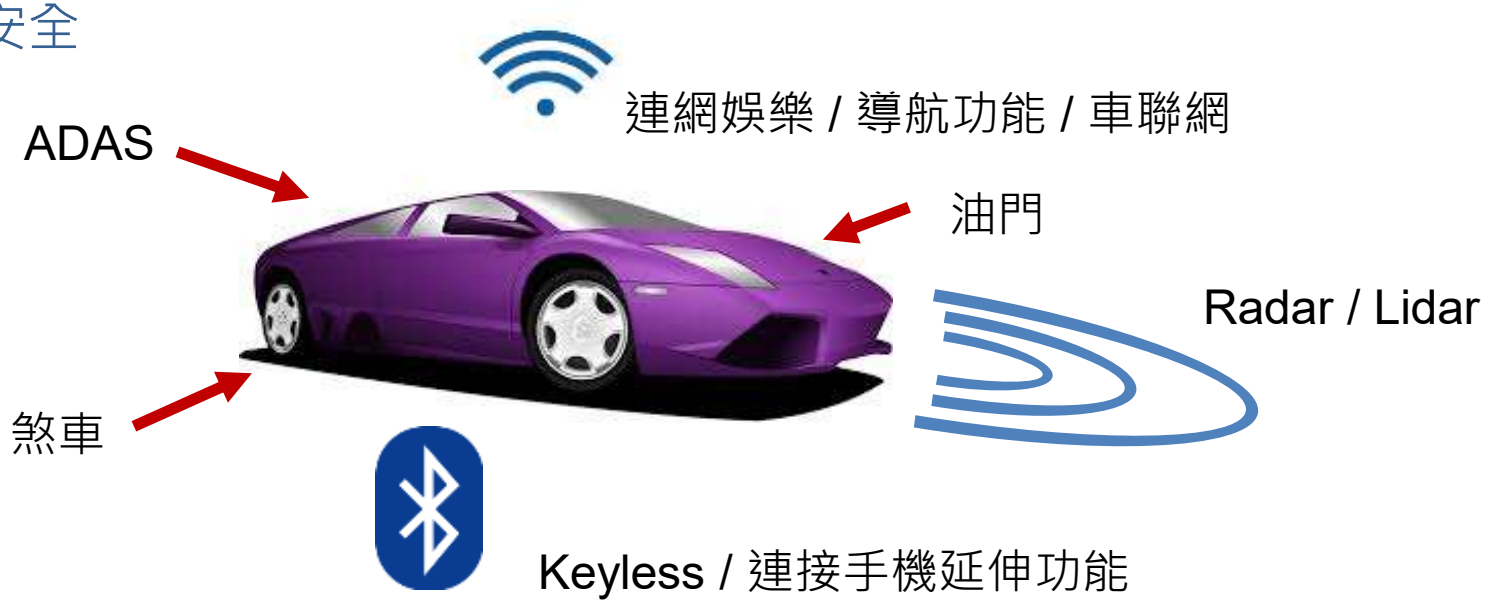
IoT device

ICS

車聯網與自駕車

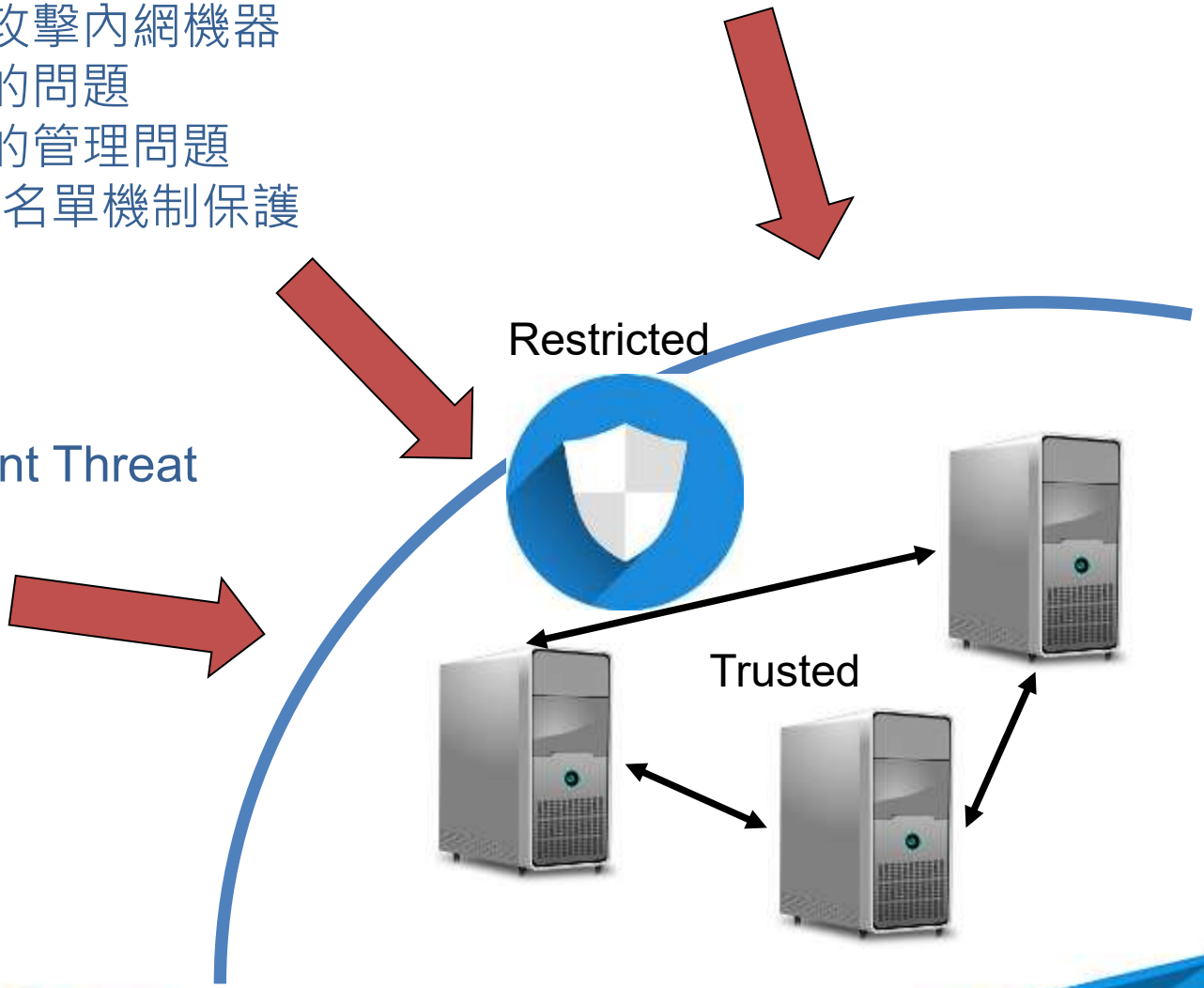
- 透過藍芽、網路
  - 攻擊 ECU (Engine control unit)
  - 攻擊 Infotainment system
  - 攻擊 Gateway

- 面對風險
  - 行車安全



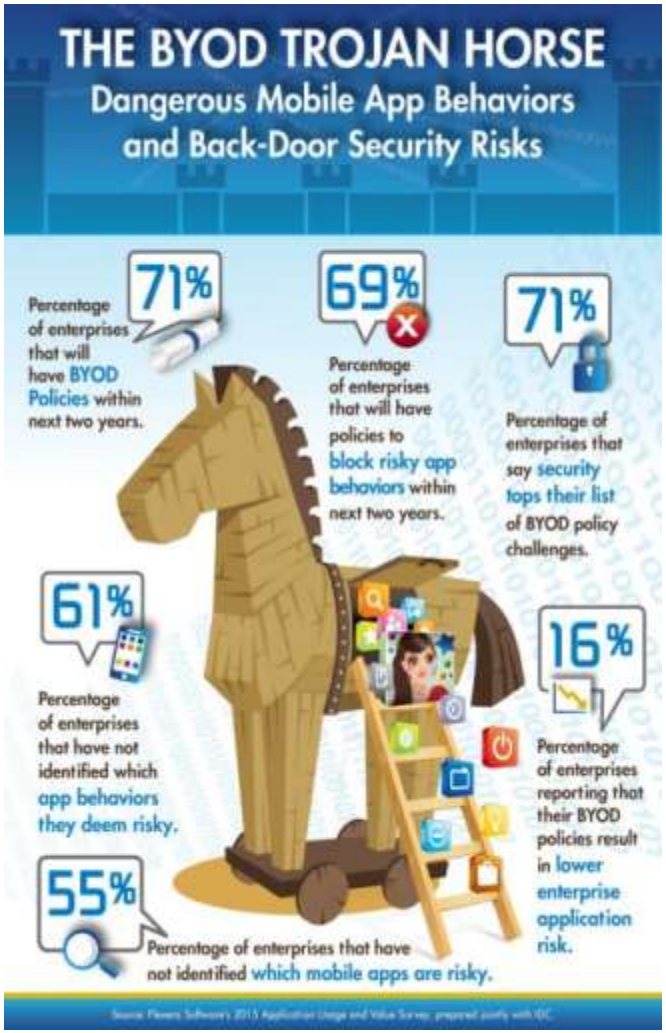
ATM 與銀行

- ATM 盜領事件
  - 透過外網的伺服器攻擊內網機器
  - 也可能面對著內鬼的問題
  - 內網與更新伺服器的管理問題
  - ATM 本身應使用白名單機制保護
- 面對風險
  - 信譽與金錢損失
  - Advanced Persistent Threat



資料不落地的行動安全管理

Risk of BYOD (Bring Your Own Device)



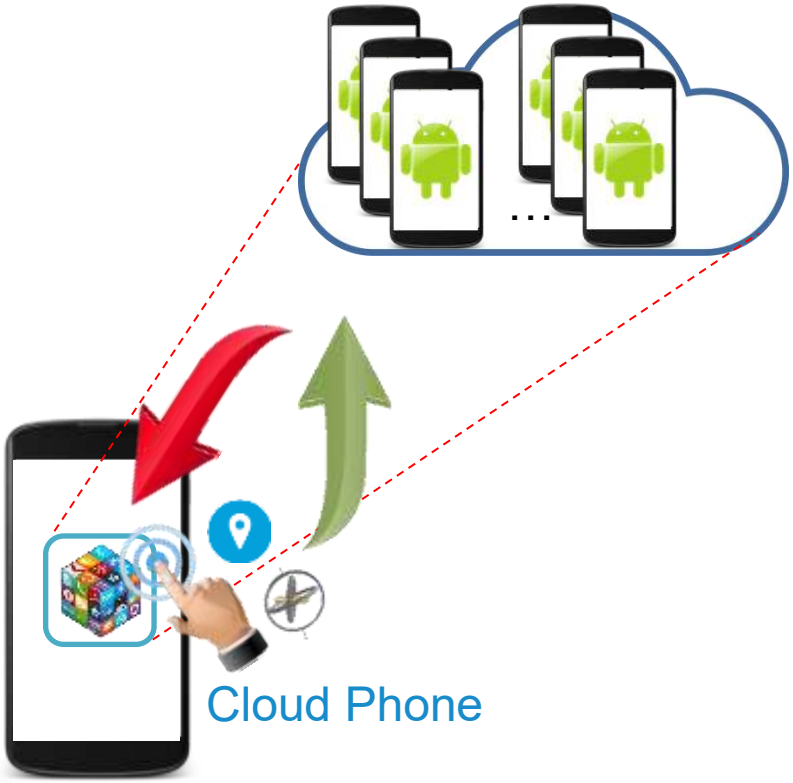
Productivity versus Security

Management control versus Privacy

Business (with MDM)

Privacy (Gaming, Shopping, Social)

Virtual Mobility Infrastructure (VMI)



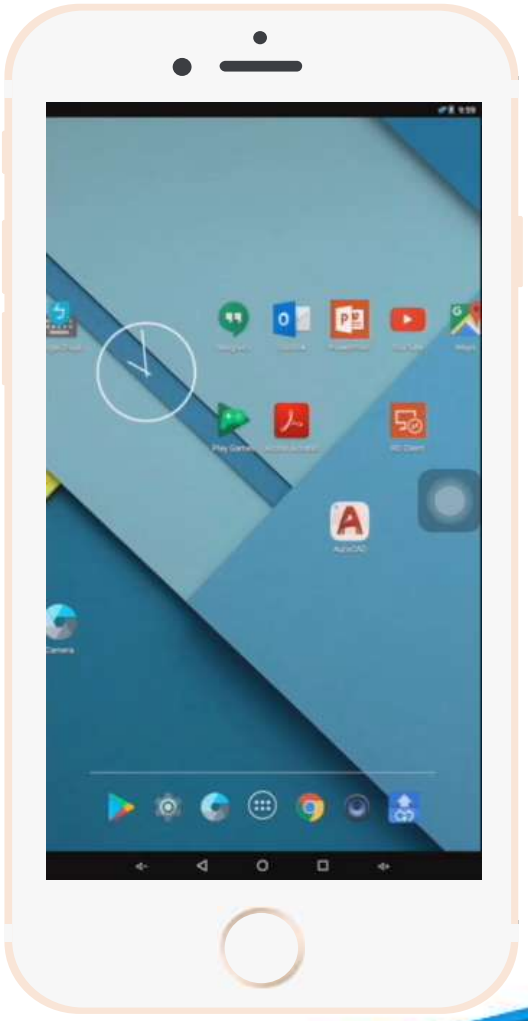
Secure APP Execution Platform

To Enterprise

Data & binary secured mobility
資料不落地行動辦公室

To Service/Solution providers

Secure APP Deployment & Access
安全APP佈署與執行

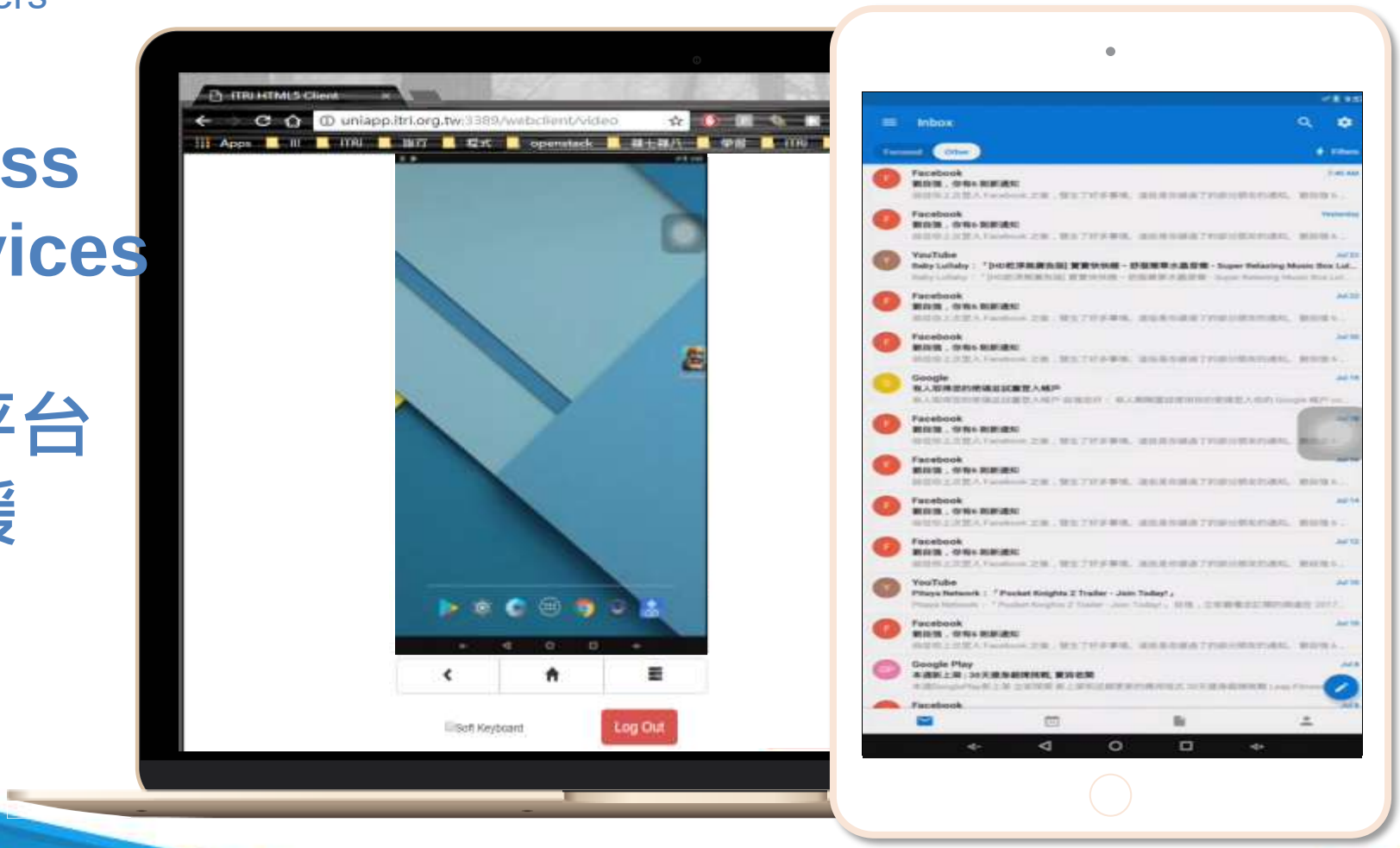


One platform for Development & Maintenance

To Users

Cross Devices

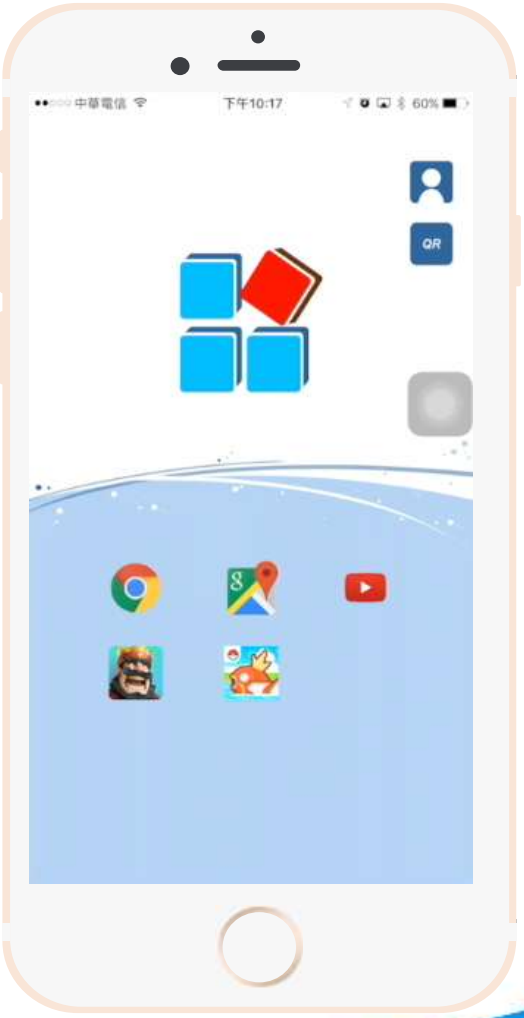
跨平台支援



To Users

Secure Browsing
Instant Play

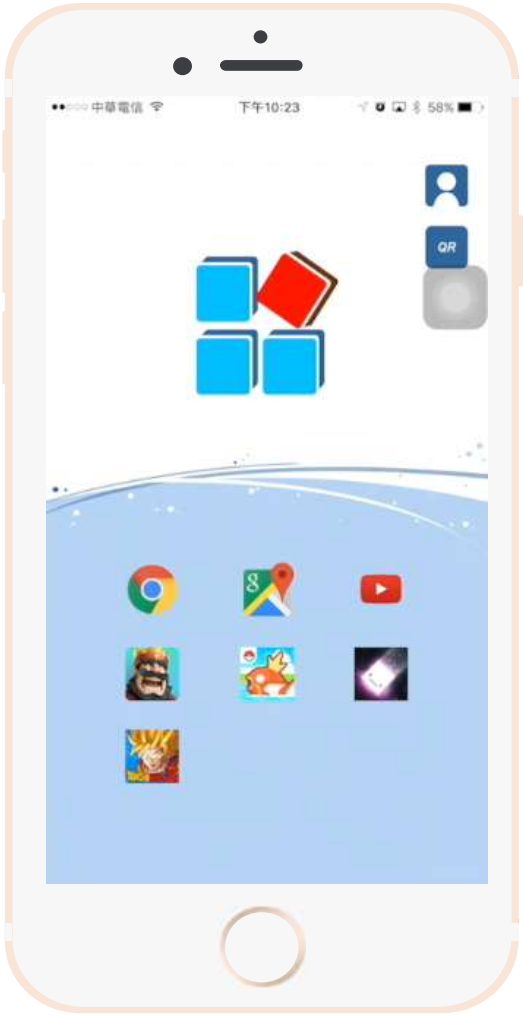
安全瀏覽
免下載立即玩



To Users

QR Code
Scan and Play

隨掃即用



Secure APP Execution Platform for BYOD

Enterprise & National Security

Data & binary secured mobility

Service/Solution providers

Secure APP Deployment & Access

One platform for Development & Maintenance

Users/Consumers

Cross Devices

Secure Browsing

Instant Play

QR Code

Scan and Play

結語

面對更多資安威脅，我們需要更安全的系統

- 應用程式白名單嚴守安全執行的最後一哩
- 資料不落地的行動企業管理

Thank you!

Questions and Comments?

ares@itri.org.tw

What are we facing today?

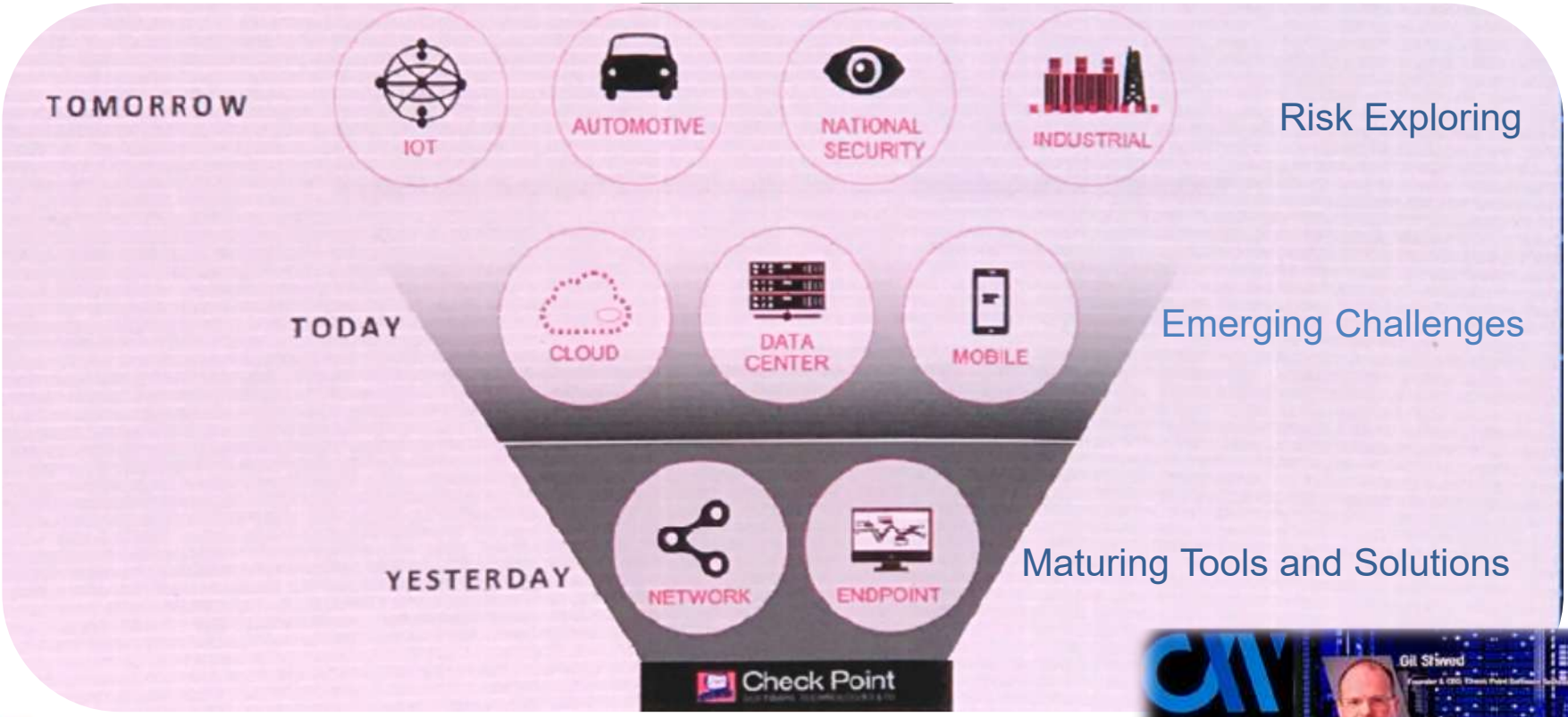
- Everything is connected

- Attacks everywhere

- Mobile Attacks

- The most dangerous tools

Secure Every Environment



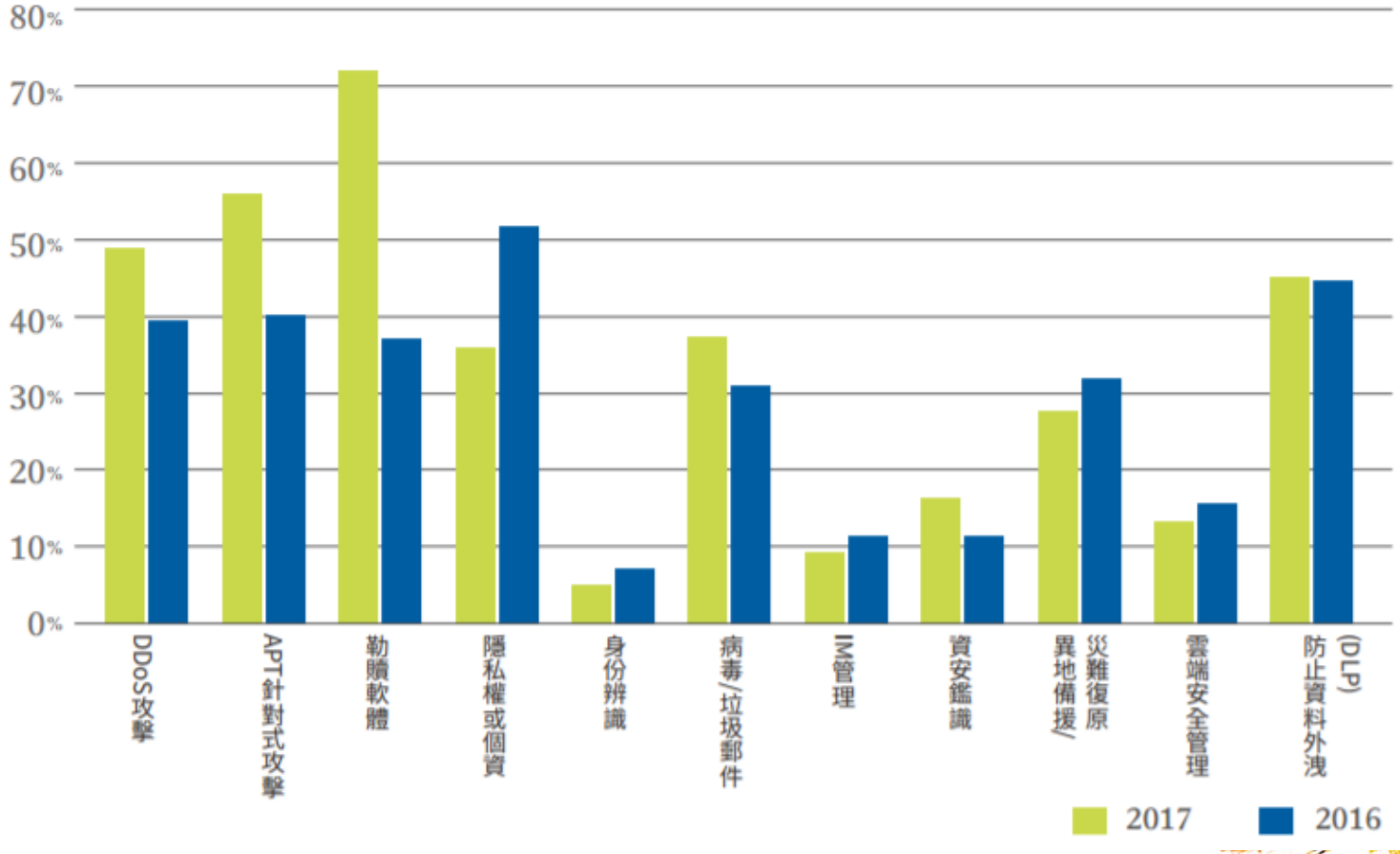
Hwacom 華電聯網

協同式巨量資料分析的資安平台

資安產品應用部
杜偉欽 Kelvin Tu
0952-492-435
Kelvin.tu@hwacom.com

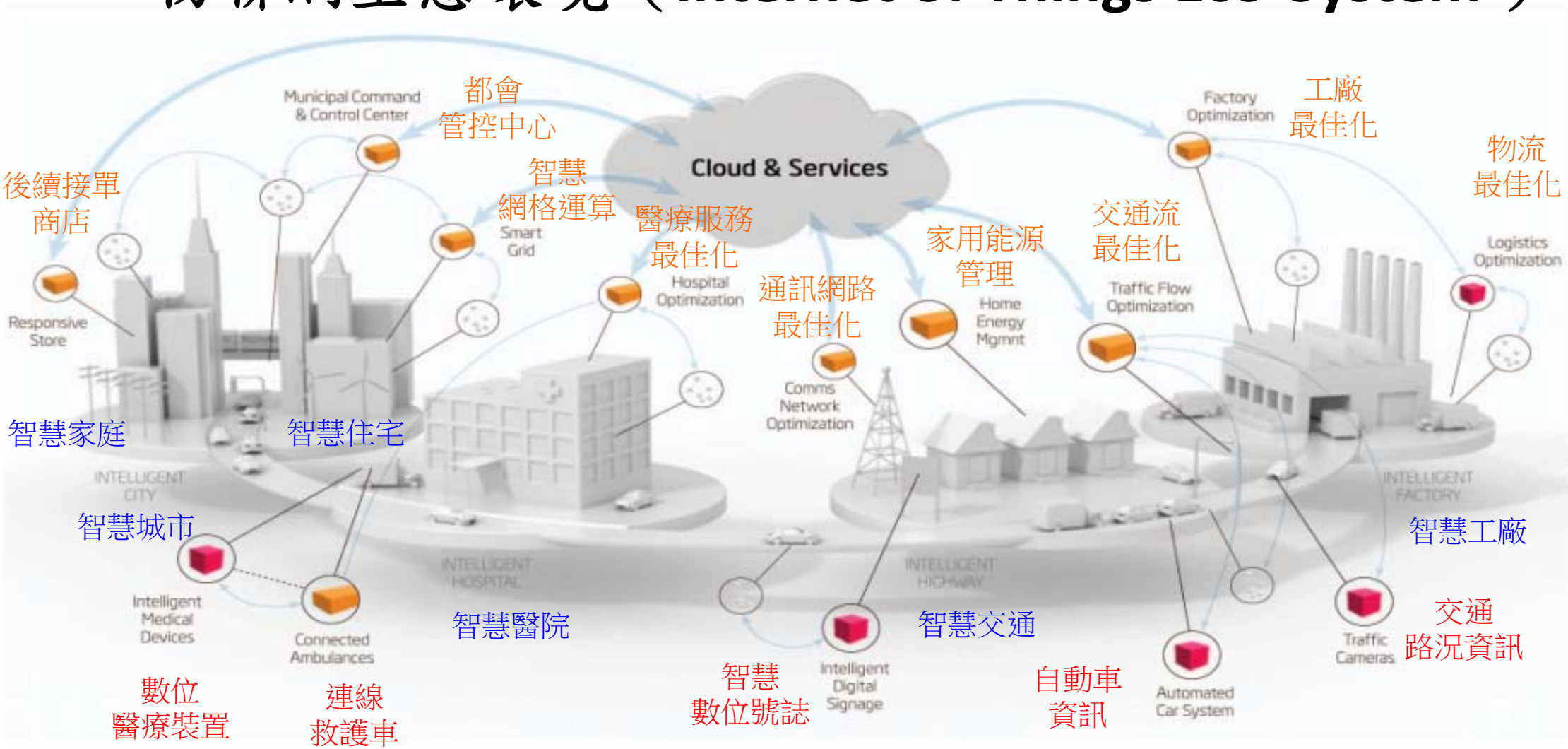
華|人|寬|頻|世|界|的|首|席|建|構|家

2017 資安事件議題



圖表參考資料：IThome

物聯網生態環境（Internet of Things Eco-System）



圖片來源：http://www.satiztpm.it/internet-things/

比以前更難看得出，誰在網路上做什麼？

90% 在調查中有百分之90的組織無法完全察覺有其他裝置連入企業組織的內部網路裡。

75% 75%的公司都會受到廣告軟體感染的影響。惡意人士會使用這些感染發動其他惡意軟體攻擊。

新的應用帶來新的威脅

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation

行動裝置

Organizations *lack visibility* into the behavior of devices on their network

企業購併

Acquisitions, joint ventures, and partnerships are *increasing in frequency*

雲端應用

Cloud usage is becoming more prevalent, but so is the *lack of visibility into the cloud*

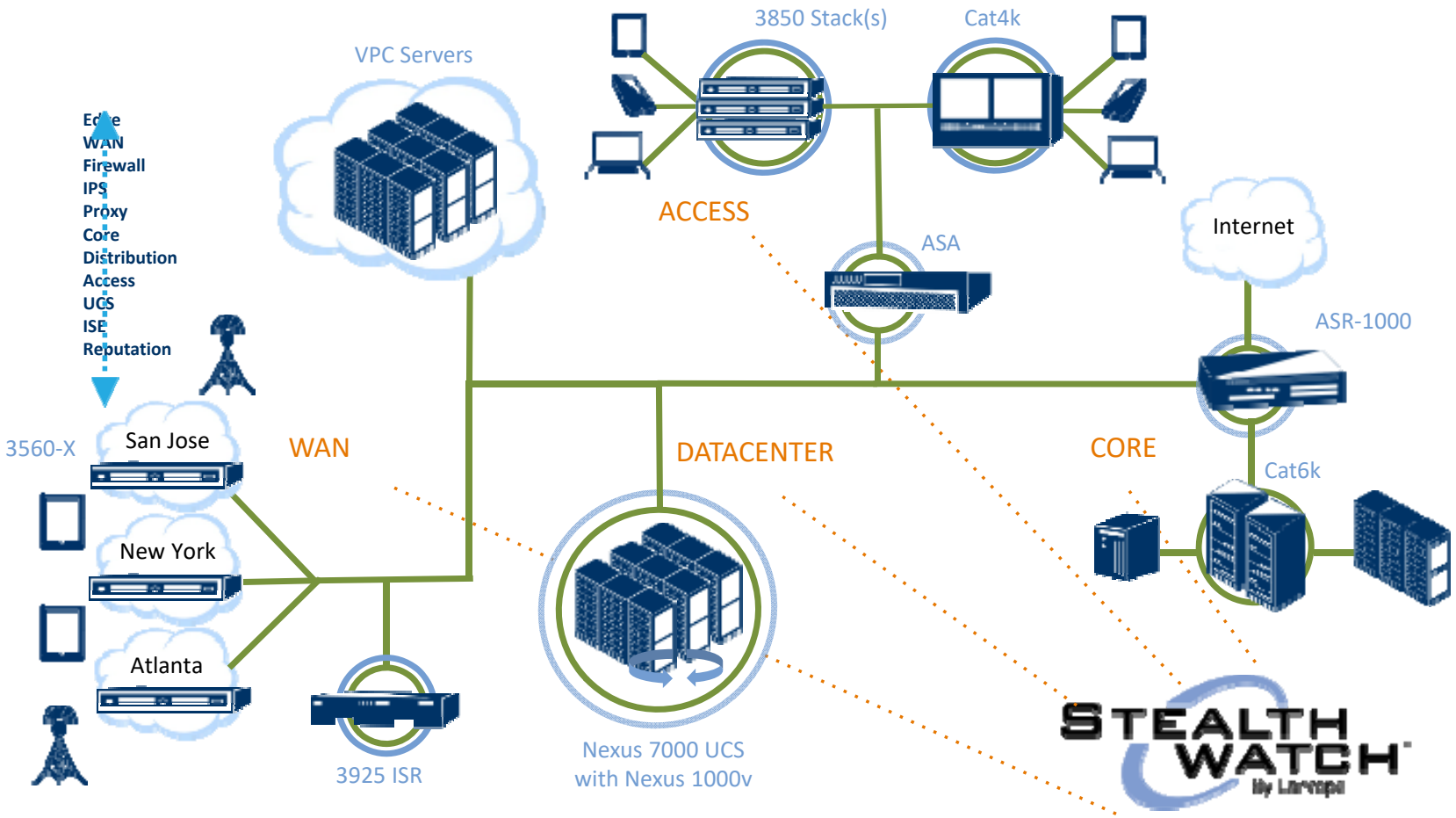
物聯網

Over *50 billion* connected "smart objects" are projected by 2020

打擊面不斷變大….

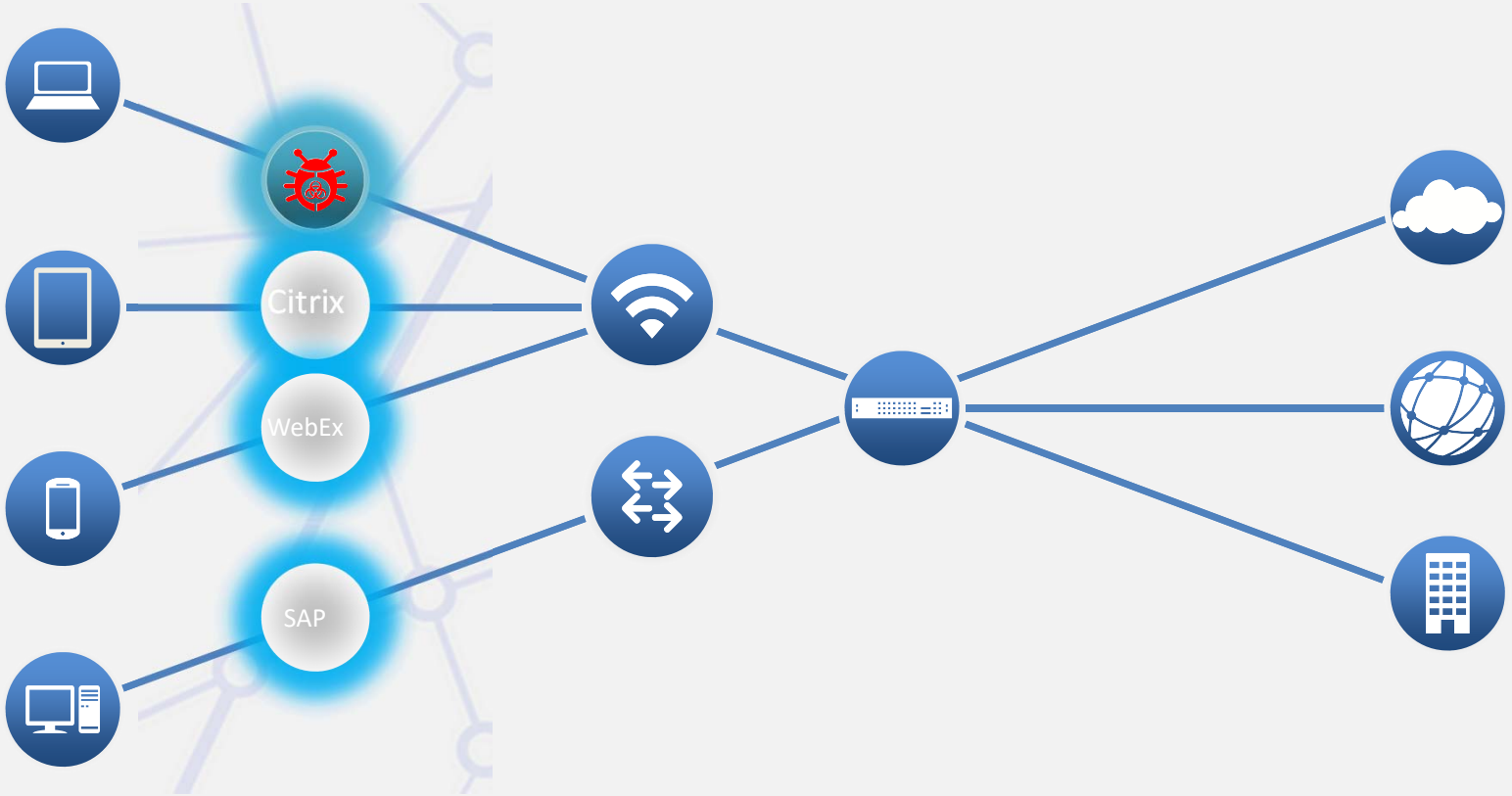
問題不在是否被入侵，而是何時

面對新型態的資安威脅，更需要重新界定新的網路資安防護邊界



網路行為可視化分析

立即找出潛藏在網路內的駭客行為




ISE
眾多不同種類的設備
電腦、移動行動裝置、物聯網裝置的可視性及區域控管


控管每台裝置必須遵循的資安政策


可搭配威脅偵測軟體找出裝置的漏洞及威脅

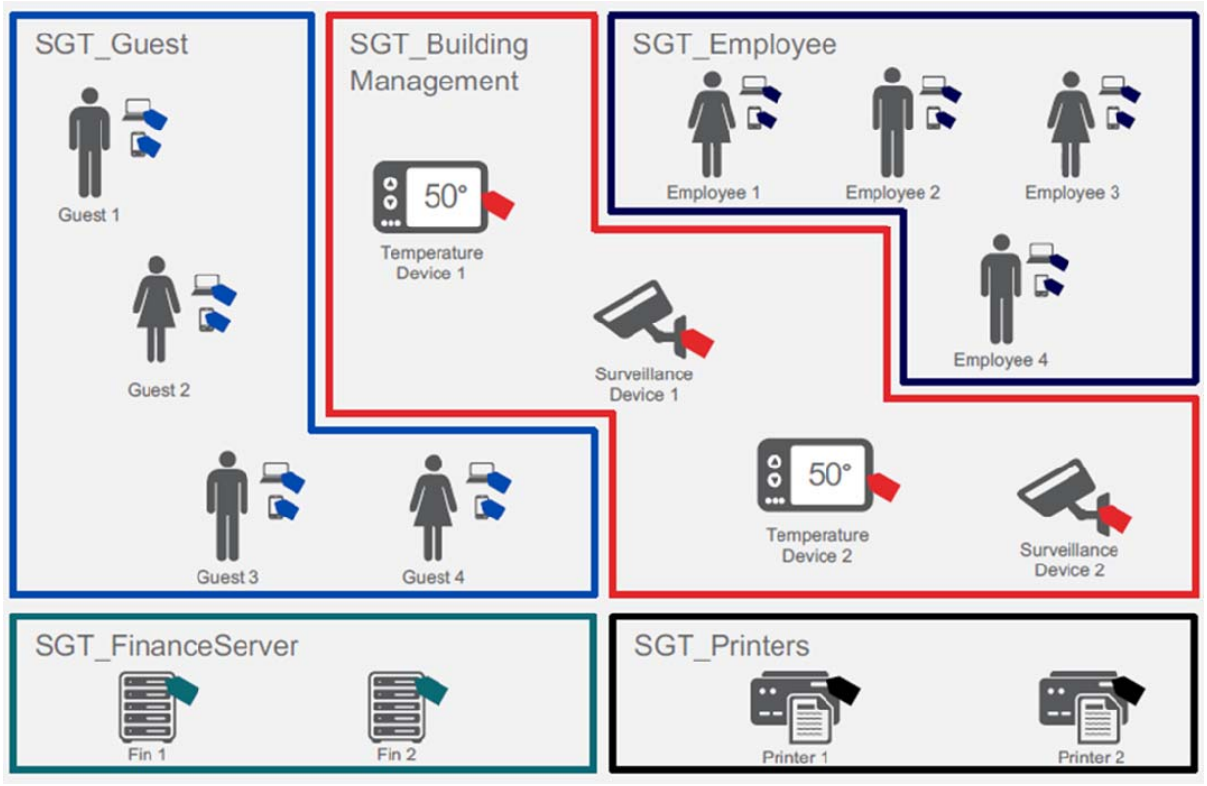
Who	Kevin
Device	Tablet, iOS, v9.1x
Location	Building 200, first floor
When	11:00 am EST on April 10
How	Wireless
Contact	555.111.3333

裝置**身份的可視性**、**可控性**和**防護**功能

以身份認證為基礎進行防禦

進一步擴展了以軟體為定義的業務政策，支援精細地劃分終端、使用者和地域的存取

藉由內部網路區域的隔離，防止惡意軟體的橫向攻擊及感染



Cisco ISE and AnyConnect

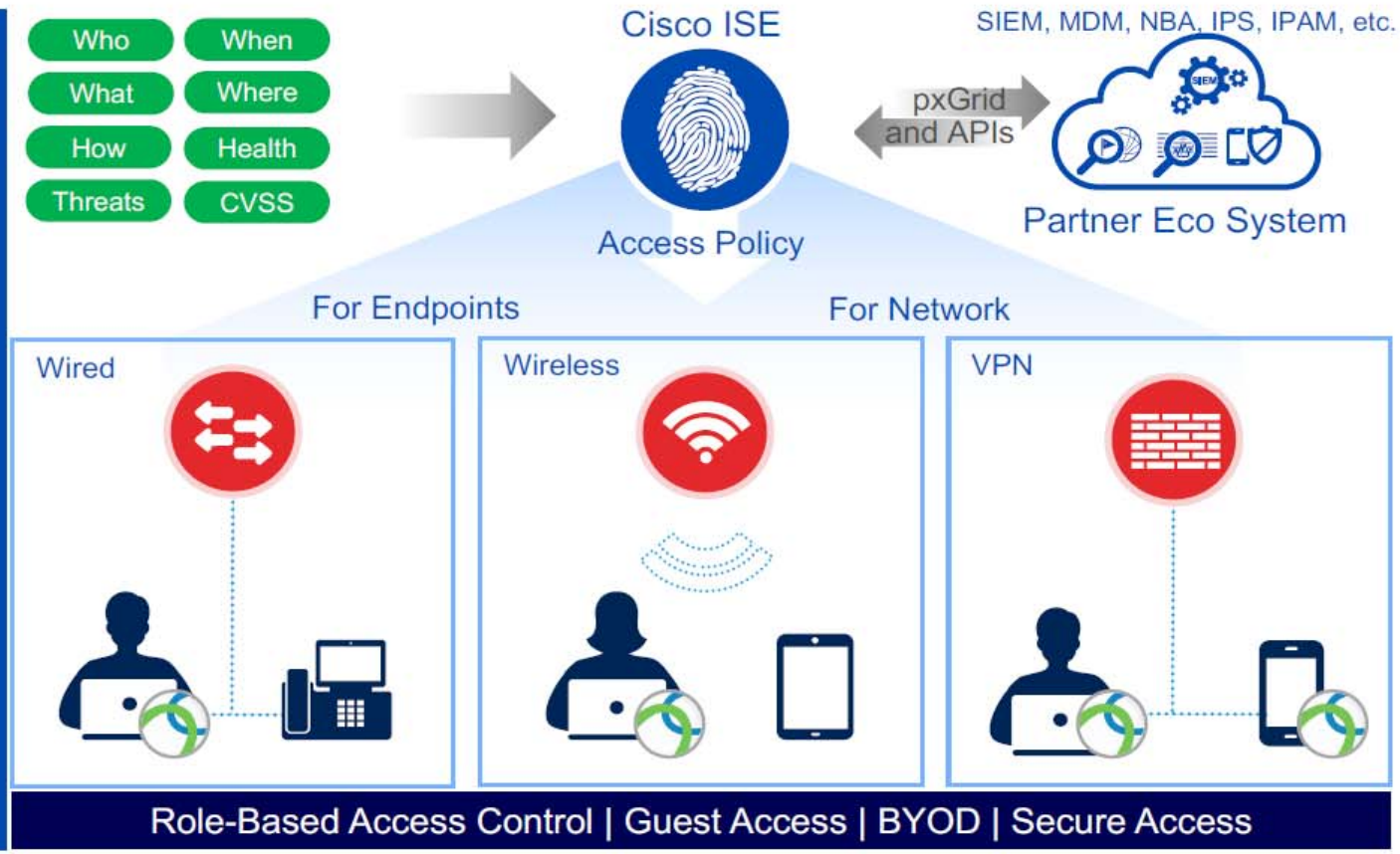
與第三方軟體分享資訊阻絕威脅

Cisco ISE

Context aware policy service, to control access and threat across wired, wireless and VPN networks.

Cisco Anyconnect

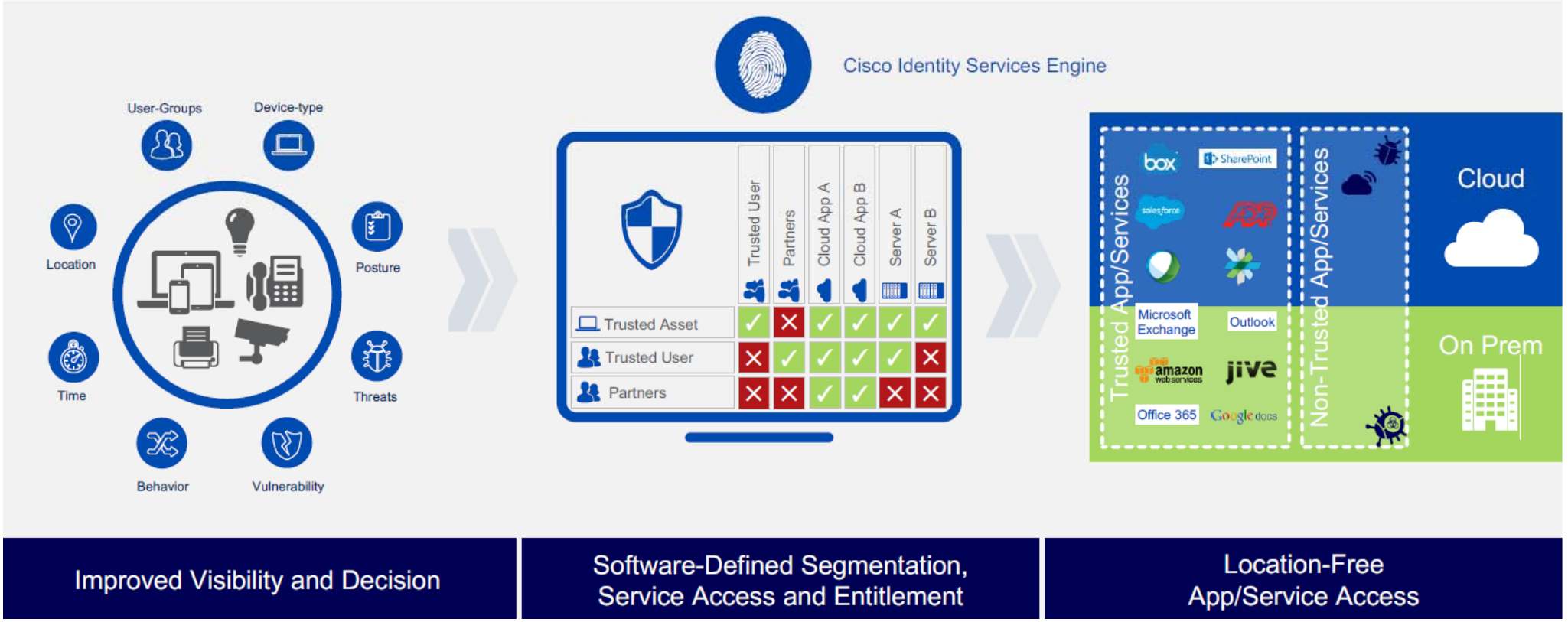
Supplicant for wired, wireless and VPN access. Services include: Posture assessment, Malware protection, Web security, MAC Security, Network visibility and more.



有線網路　無線網路　VPN加密網路

Managing Policy Based on 'Trust'

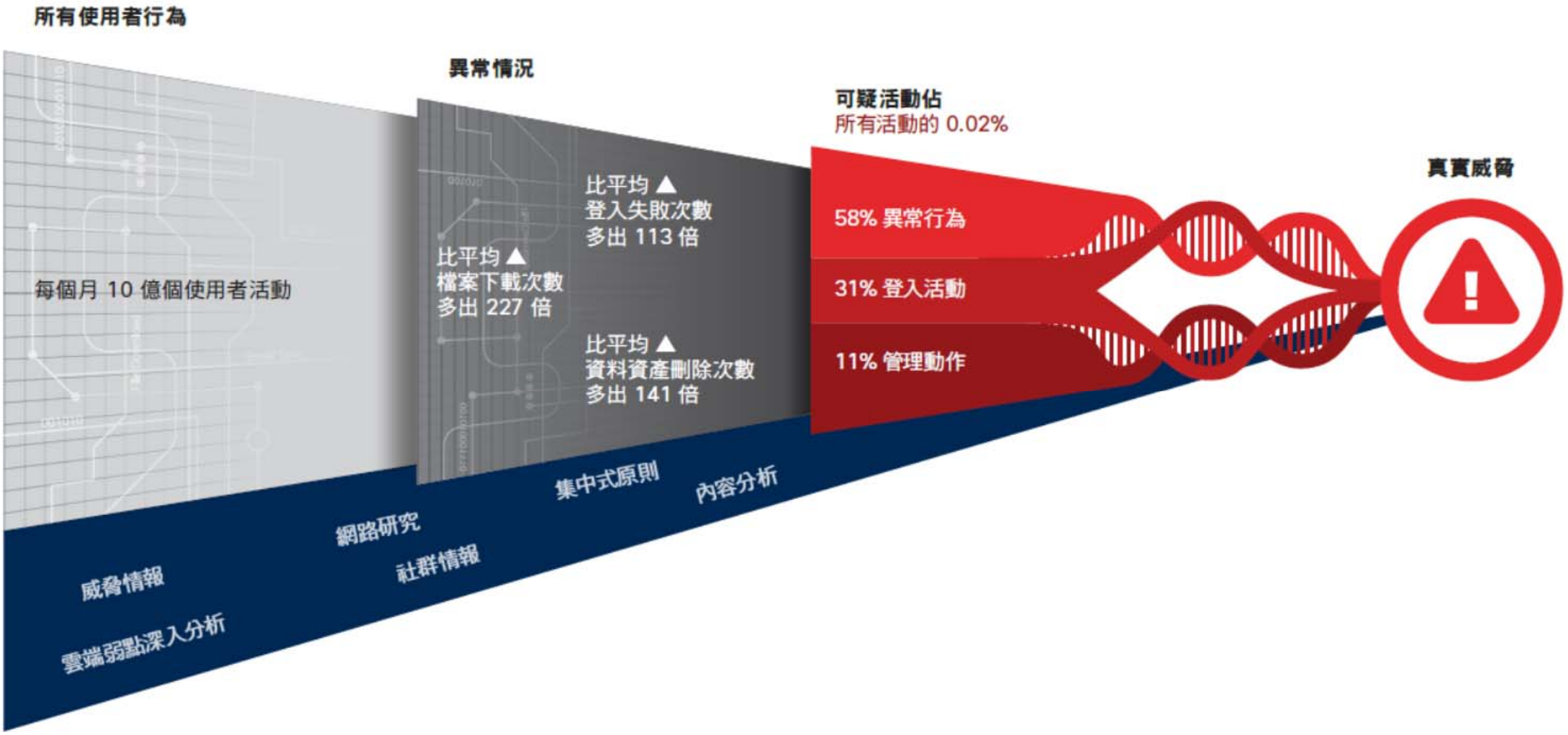
Connecting Trusted Users and Devices to Trusted Services



Improved Visibility and Decision	Software-Defined Segmentation, Service Access and Entitlement	Location-Free App/Service Access

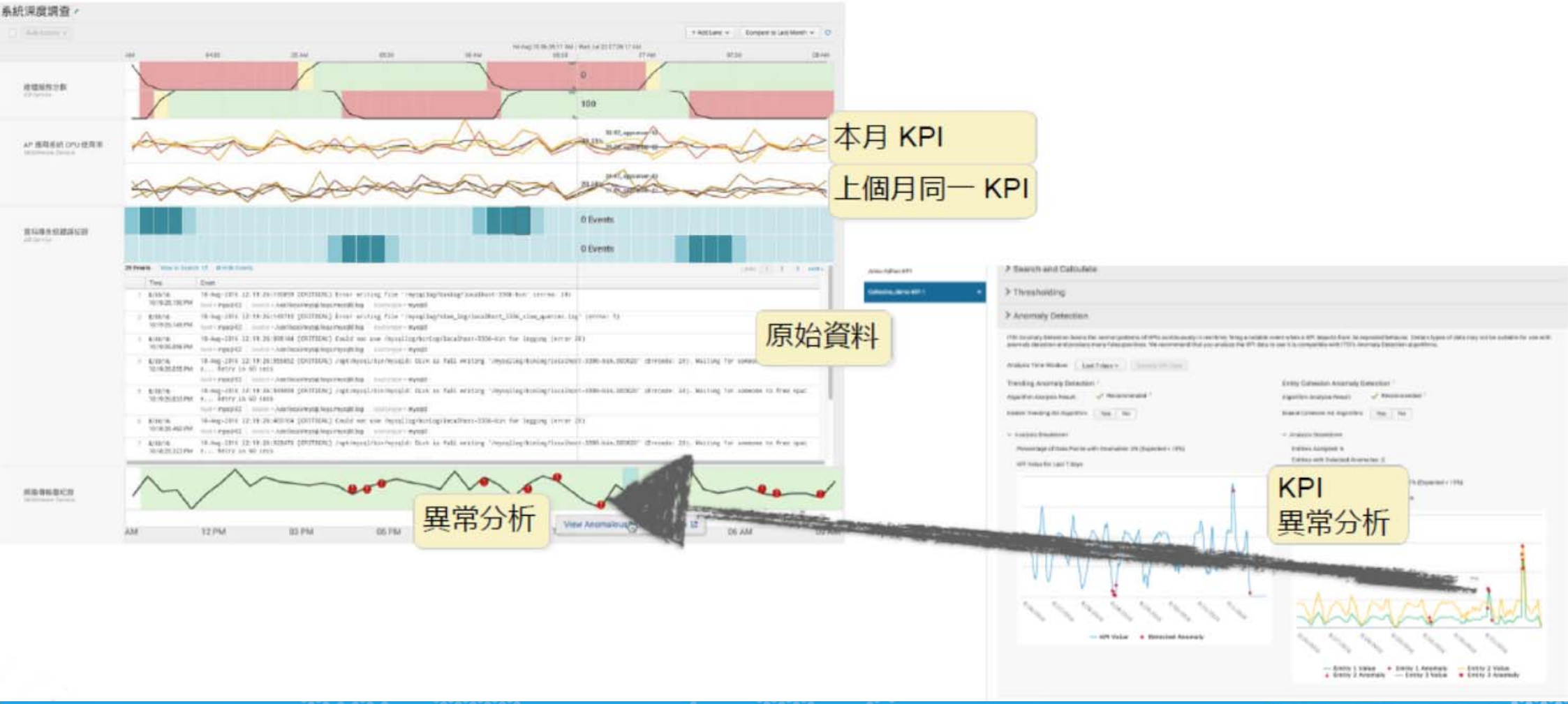
何種身分角色的裝置 >> 根據制定政策 >> 決定可去的區域


METRICS
Total Endpoints
55534
Active Endpoints
34258
Authenticated Guests
4234
BYOD Endpoints
1341
Compliance
22%
COMPLIANT
5109
AUTHENTICATIONS
Identity Store | Identity Group | Network Device | Failure Reason
other: [5%]
samsu...evice: [2.97%]
apple-idevice: [4.05%]
android: [4.33%]
apple-iphone: [5.73%]
unknown: [12.7%]
profiled: [14.15%]
workstation: [27.2%]
apple-device: [24.28%]
NETWORK DEVICES
Device Name | Type | Location
other: [5%]
ntn01-11a-sw4: [3.1%]
rcdn5...tana1: [3.73%]
eng-b...a-sw1: [5.79%]
sjc14...alwar: [6.33%]
eng-b...a-sw1: [11.22%]
sbg-b...-wlc1: [11.94%]
sampg...-wlc1: [26.77%]
sjc19...u-wlc: [26.62%]
ENDPOINTS
Type | Profile
other: [7%]
cisco-device: [4.61%]
intel-device: [5.06%]
apple-idevice: [5.46%]
apple-iphone: [7.45%]
windo...ation: [9.43%]
micro...ation: [15.53%]
apple-device: [29.87%]
unknown: [15.88%]
中央控管介面方便查找各種接入裝置資訊
BYOD ENDPOINTS
Type | Profile
printers: [0.3%]
misc: [1.64%]
workstations: [46.91%]
mobil...vices: [51.16%]
ALARMS
Sever... Name Occurre... Last Occurred
Misconfigured Supplicant Detected 2205 10 mins ago
RADIUS Request Dropped 6363 12 mins ago
Supplicant stopped responding 3796 17 mins ago
Misconfigured Network Device Dete... 715 44 mins ago
Unknown SGT was provisioned 54 3 hrs 56 mins ago
Configuration Changed 703 6 hrs 3 mins ago
SYSTEM SUMMARY
9 node(s)
All
24HR
npf-sjca-mnt01
CPU
Memory
Authentication Latency
npf-sjca-mnt02
CPU
Memory
Authentication Latency
npf-sjca-pap01



資料來源：思科 CloudLock

機器學習自動化比對分析



機器學習自動化比對分析

實例關聯性 – 資料外洩

來源

20130806041221.000000Caption=ACME-2975EE\Administrator Description=Built-in account for administering the computer/domainDomain=ACME-2975EB InstallDate=NULL LocalAccount = IP: 10.11.36.20
TrueName=Administrator SID =S-1-5-21-1 45543 50
Status=Degradedwmi_ type=UserAccounts

預設管理員帳號

來源IP

Aug 08 06:09:13 acmesep01.acmetech.com Aug 09 06:17:24 SymantecServer acmesep01: Virus found,Computer name: ACME-002,Source: Real Time Scan,Risk name: Hackertool.rootkit,Occurrences: 1,C:/Documents and Settings/smithe/Local Settings/Temp/evil.tmp," ed,Requested ed, time: 2009-01-23 03:19:12,Inserted: 2009-01-23 03:20 :19:12,Domain : My Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 10.11.36.20

發現惡意程式

來源IP

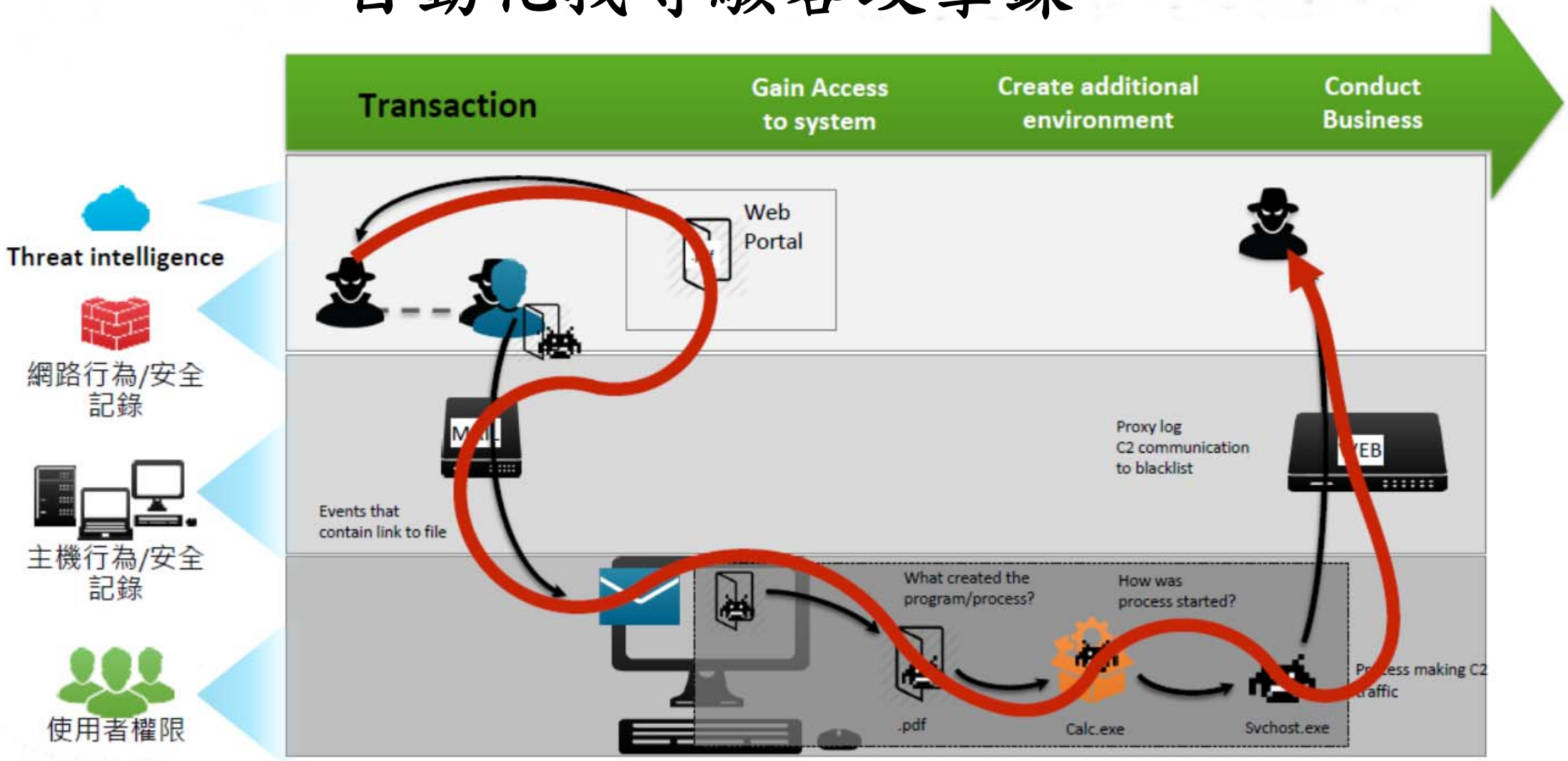
Aug 08 08:26:54 snort.acmetech.com {TCP} 10.11.36.20 :5072 -> 10.11.36.26:443 itsec snort[18774]: [1:100000:3] [Classification: Potential Corp bliation] Credit Card Number Detected in Clear Text [Priority: 2]:

來源IP

資料外洩

三個狀況都發生在24小時內

自動化找尋駭客攻擊鍊



傳統的資安防禦思維

1 社交工程

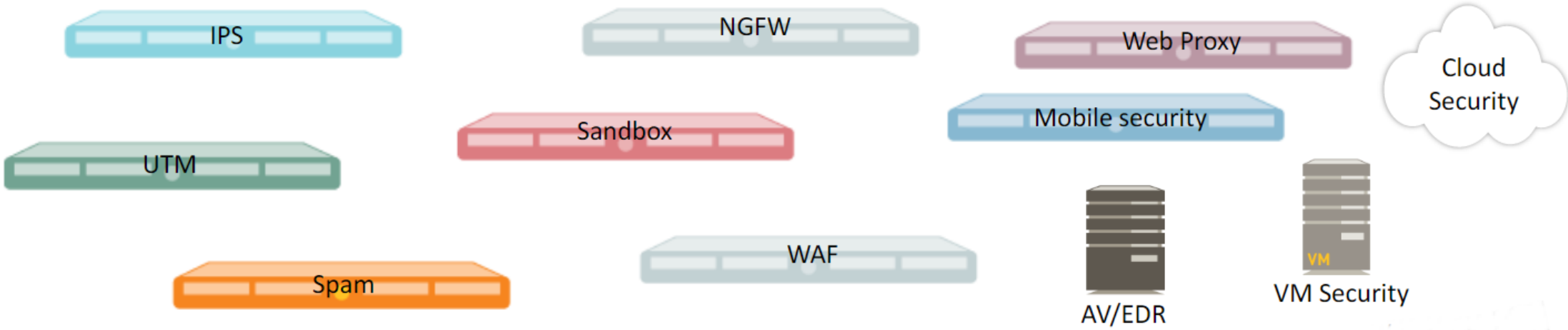
2 偷渡並植入惡意檔案

3 內部感染惡意活動

4 機密竊取 系統、資料破壞 等目的

嘗試未授權的存取

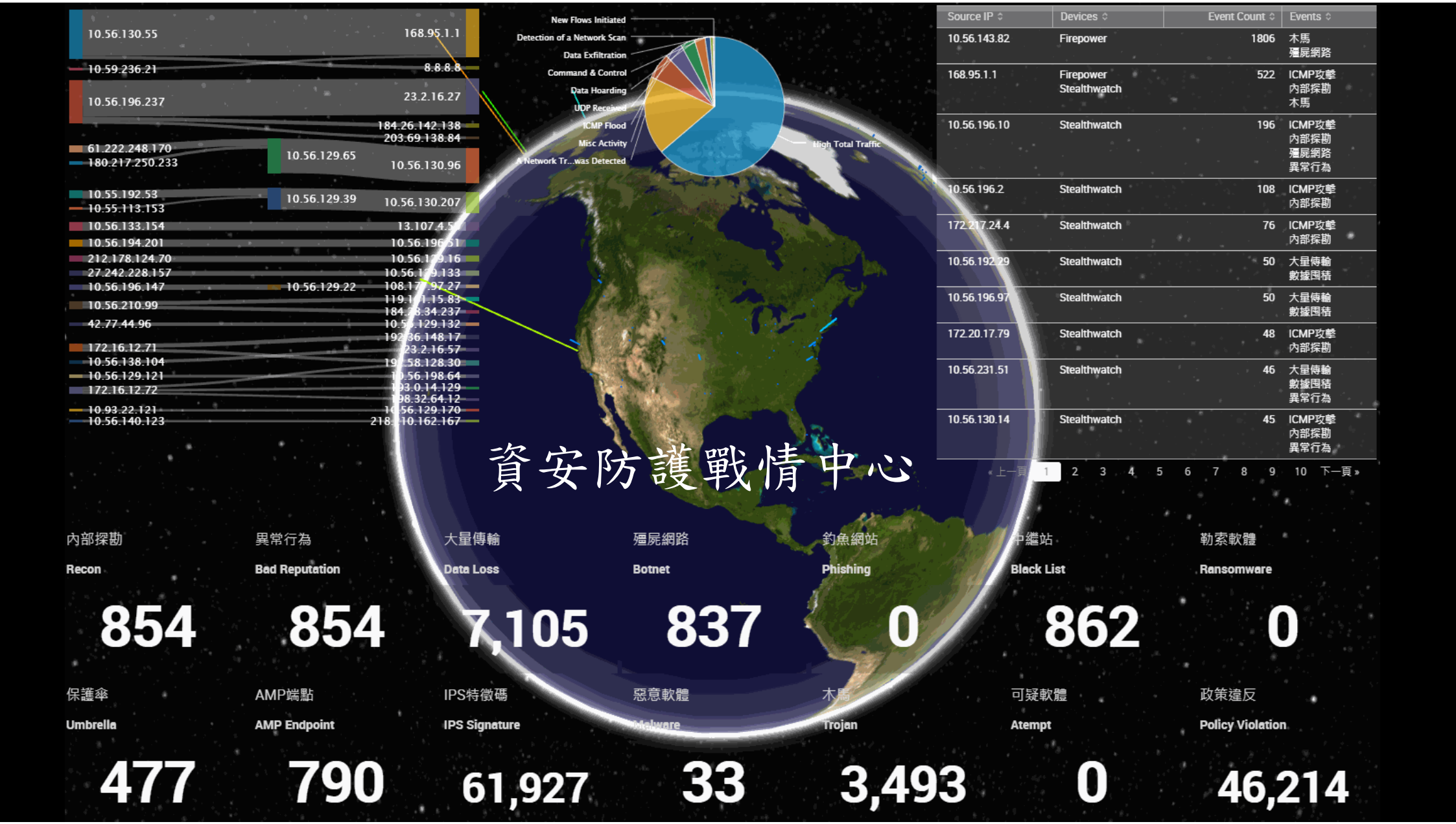
執行未授權的行為



新世代資安防護平台

新世代資安防護平台

	傳統 SIEM 平台	新世代資安防護平台
資料來源	有限	適用任何技術、裝置
量身訂做的裝置支援	困難	簡單
增加情報	困難	簡單－不分時間、即時或歷史資料均可
量身訂做的回報機制	需要第三方應用程式	內建 （來自搜尋結果）
搜尋/回報的速度	緩慢且不堪使用	快速反應
找出關聯性	困難 （以角色為基礎）	簡單 （以搜尋為基礎）
擴充能力	有限	可延伸



Source IP	Devices	Event Count	Events
10.56.143.82	Firepower	1806	木馬 殭屍網路
168.95.1.1	Firepower Stealthwatch	522	ICMP攻擊 內部探勘 木馬
10.56.196.10	Stealthwatch	196	ICMP攻擊 內部探勘 殭屍網路 異常行為
10.56.196.2	Stealthwatch	108	ICMP攻擊 內部探勘
172.217.24.4	Stealthwatch	76	ICMP攻擊 內部探勘
10.56.192.29	Stealthwatch	50	大量傳輸 數據囤積
10.56.196.97	Stealthwatch	50	大量傳輸 數據囤積
172.20.17.79	Stealthwatch	48	ICMP攻擊 內部探勘
10.56.231.51	Stealthwatch	46	大量傳輸 數據囤積 異常行為
10.56.130.14	Stealthwatch	45	ICMP攻擊 內部探勘 異常行為

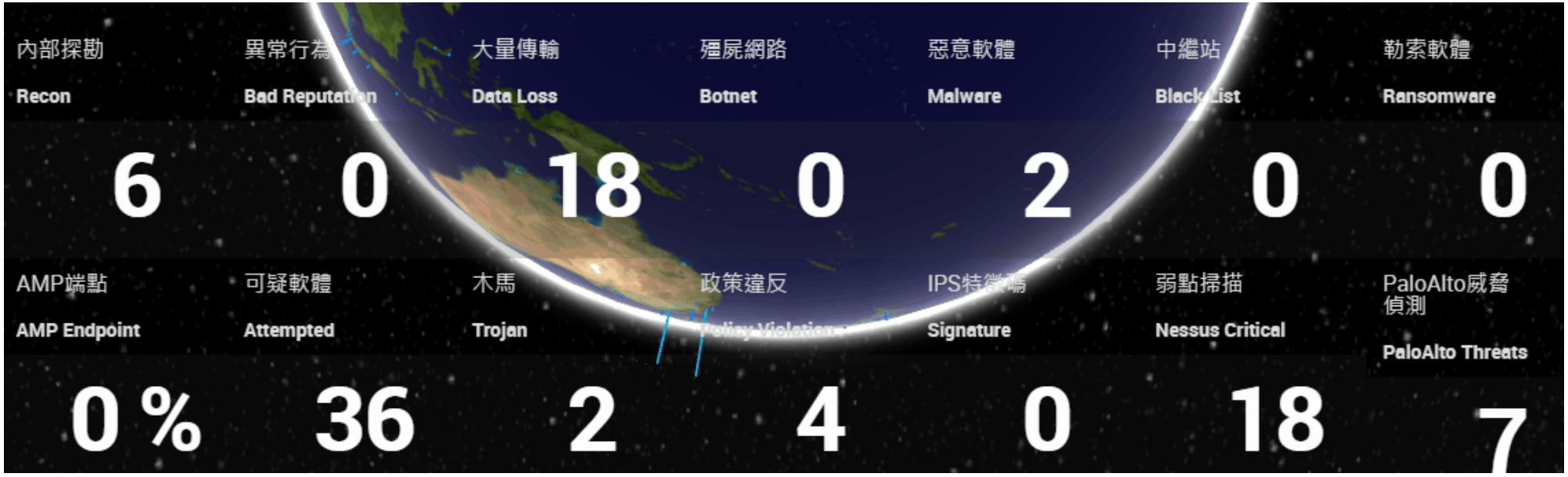
« 上一頁 1 2 3 4 5 6 7 8 9 10 下一頁 »

內部探勘	異常行為	大量傳輸	殭屍網路	釣魚網站	中繼站	勒索軟體
Recon	Bad Reputation	Data Loss	Botnet	Phishing	Black List	Ransomware
854	854	7,105	837	0	862	0

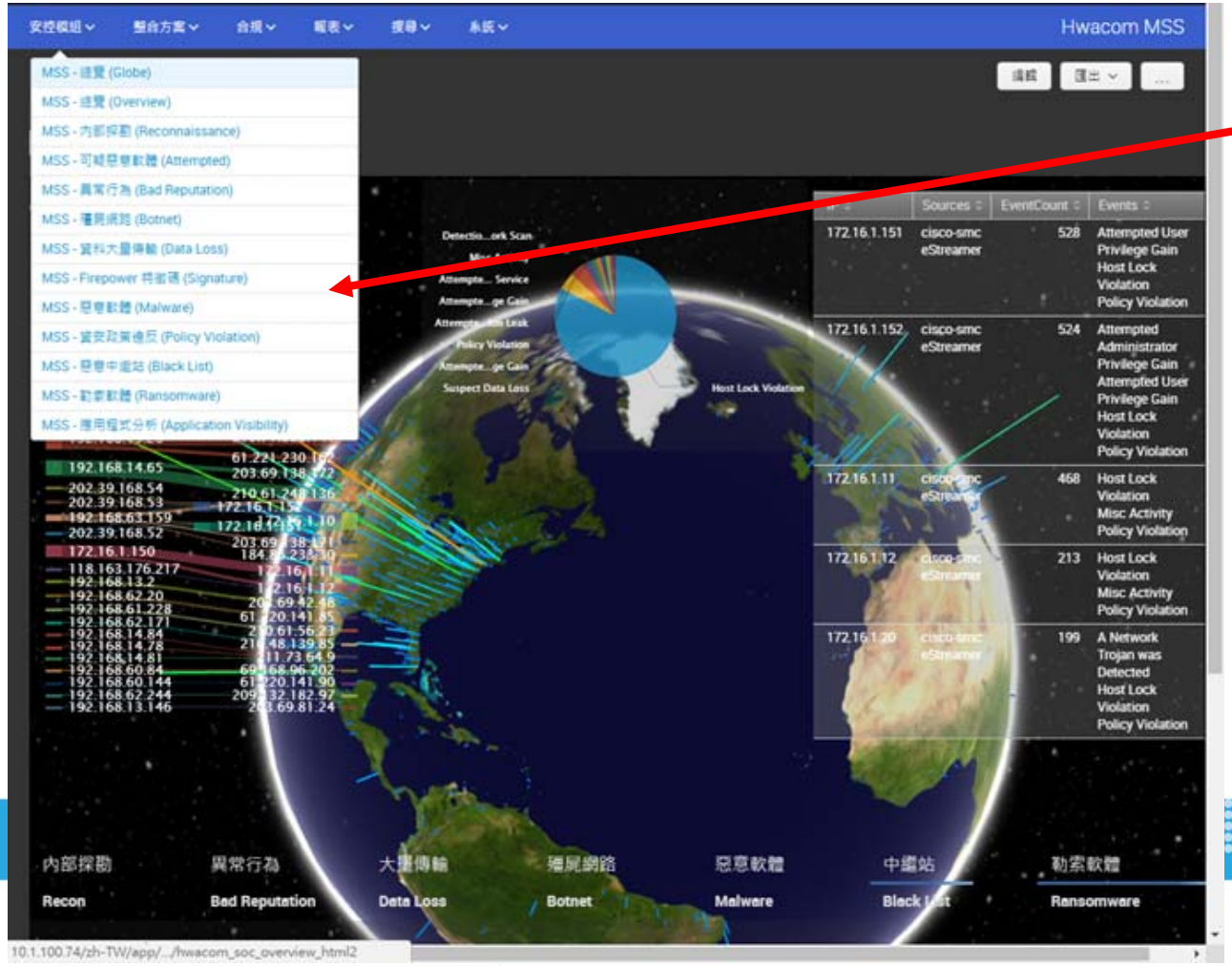
保護傘	AMP端點	IPS特徵碼	惡意軟體	木馬	可疑軟體	政策違反
Umbrella	AMP Endpoint	IPS Signature	Malware	Trojan	Atempt	Policy Violation
477	790	61,927	33	3,493	0	46,214

使用者行為分析模組

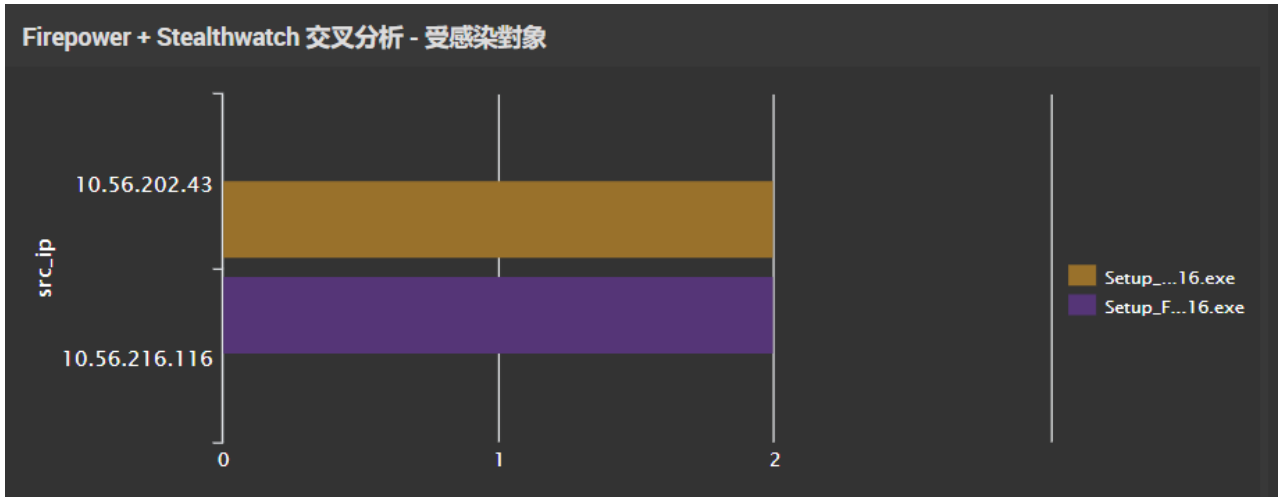
- 可視性行為分析模組，快速查詢安全威脅。
- 進行交叉關聯式分析，找出害群之馬。
- 自動化通知相關負責人，立即處理問題。

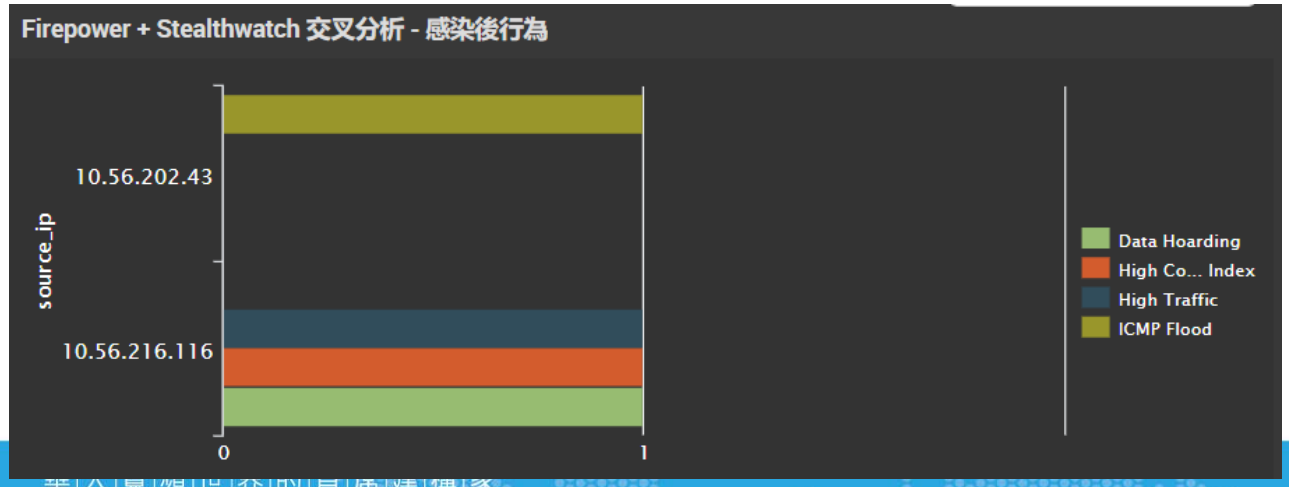


多樣性安控模組



Firepower+StealthWatch 交叉分析感染來源





快速察知

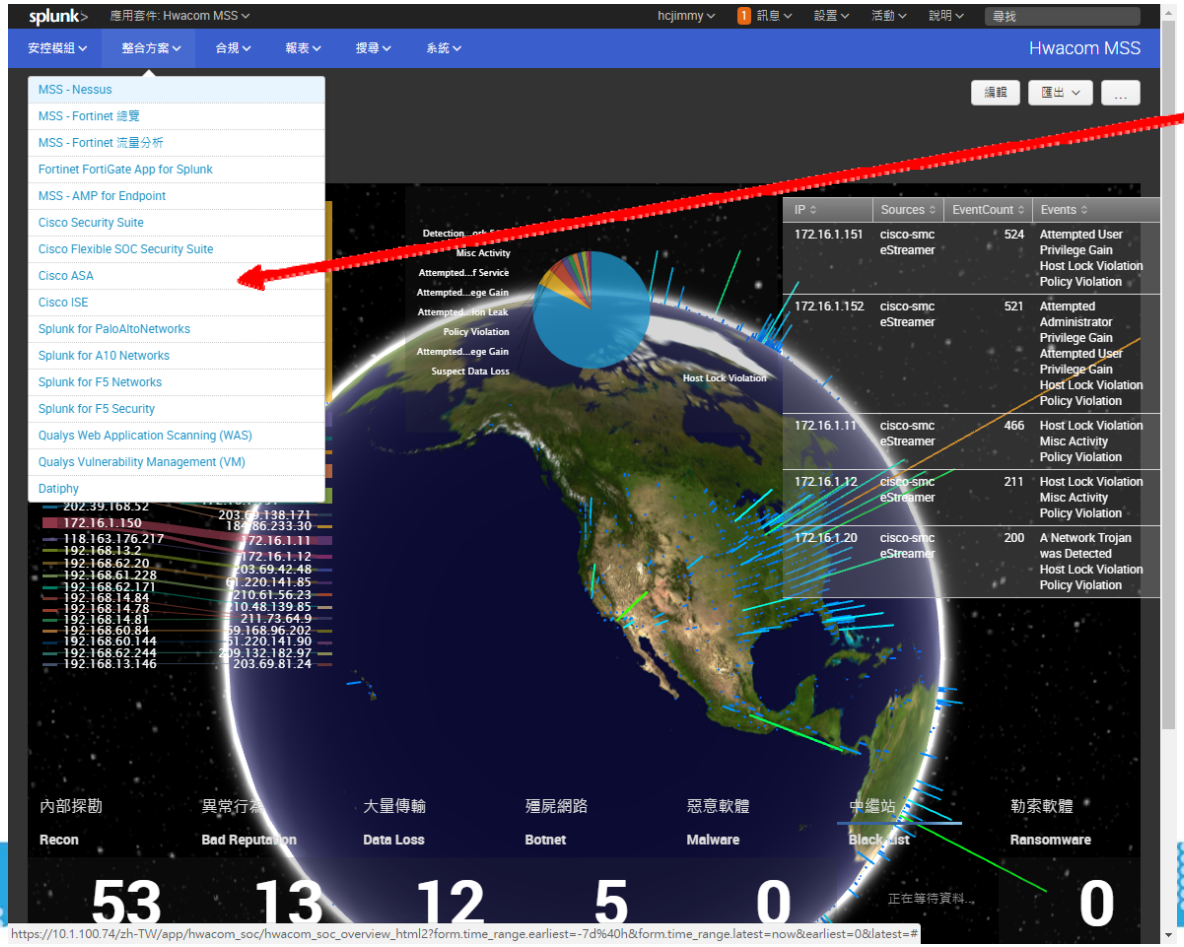
惡意檔案來源:
/file-downloads/builds/static_delivery/installers/fileviewpro/spf/101816_build/Setup_FileViewPro_2016.exe

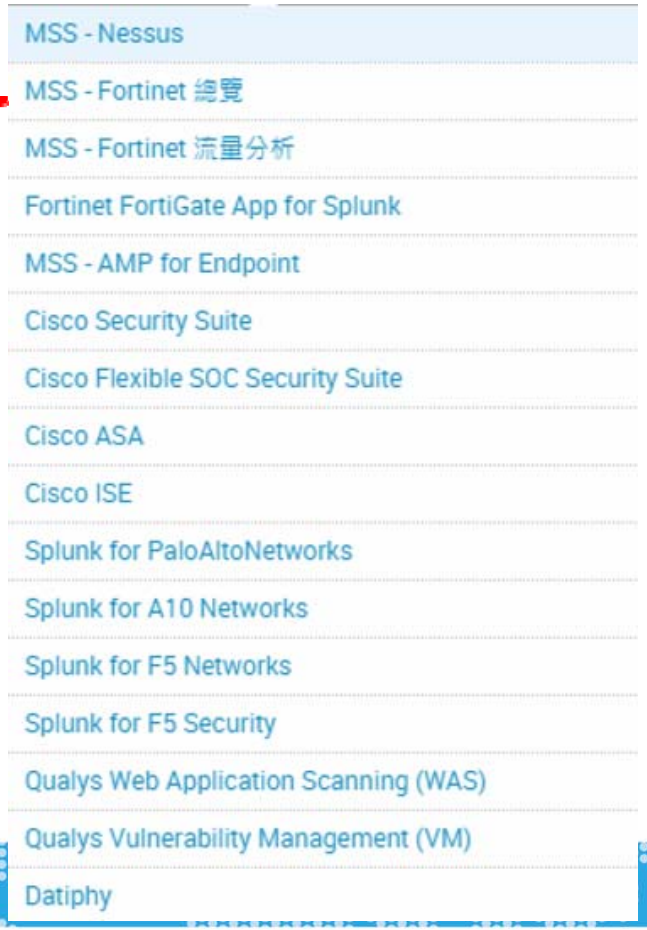
惡意檔案來源:
http://www.solvusoft.com/file-downloads/builds/static_delivery/installers/driverdoc/spf/build_100716/Setup_DriverDoc_2016.exe

程式服務派送異常監控


MSS - 內部探勘 (Reconnaissance)
MSS - 異常行為 (Bad Reputation)
MSS - Nessus
內部探勘
Recon
6
異常行為
Bad Reputation
0
Data Loss
18
AMP端點
AMP Endpoint
0 %
可疑軟體
Attempted
36
木馬
Trojan
2
政策違反
4
IPS特徵碼
Signature
0
弱點掃描
Nessus Critical
18
PaloAlto威脅偵測
PaloAlto Threats
7

全方位異質平台設備整合方案





Cisco Umbrella

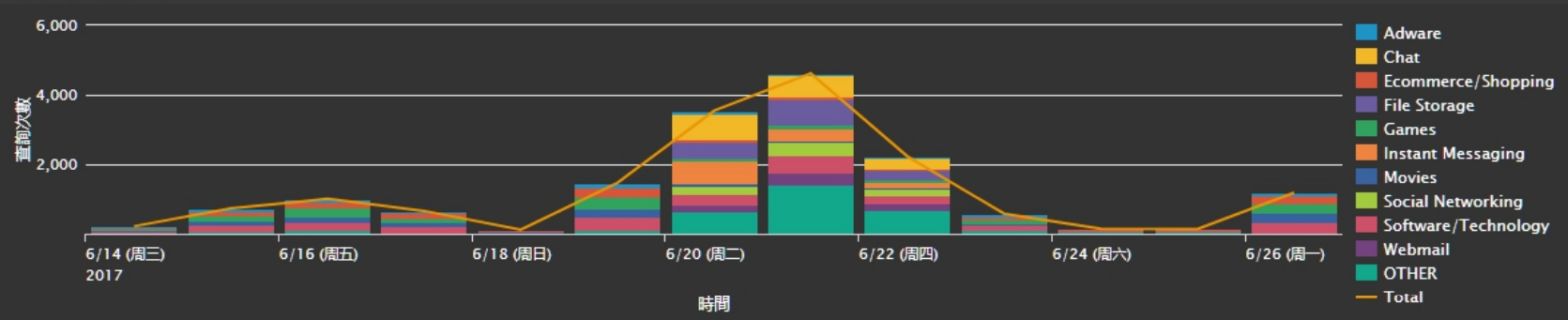
一小時內已阻擋 7 筆 -1

惡意網站 3 筆 3

可疑網站 1 筆 1

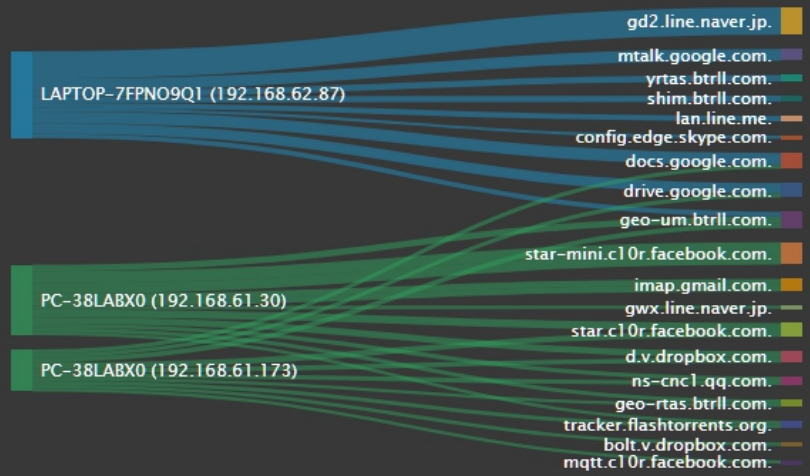
色情網站 2 筆 2

已阻擋網址類型



已阻檔的分類

已阻擋網址清單



30

華電安控中心 - FireAMP

編輯 | 更多資訊

前 30 天

受威脅比例 (Threat Ratio)

58 %

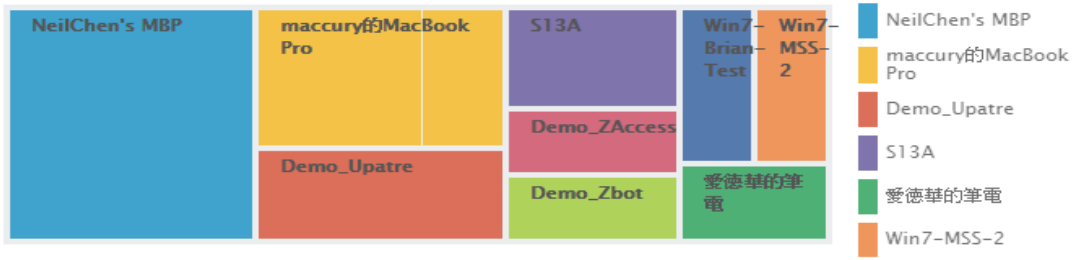
已安裝數量

9 Client(s)

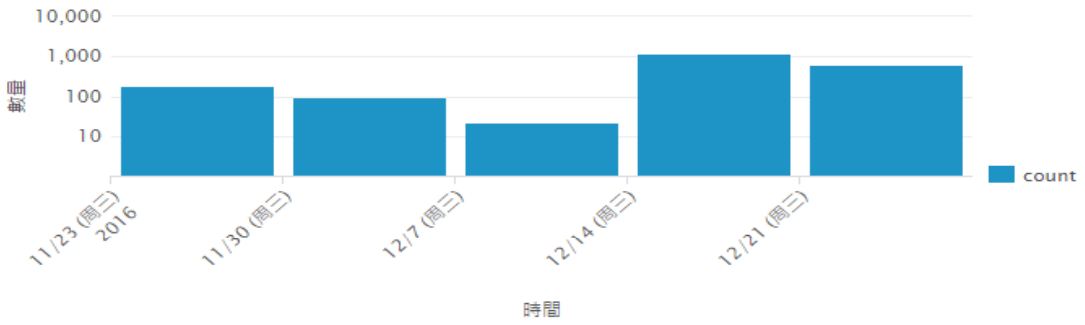
線上數量

2 Client(s)

受威脅電腦 (Top Computers)



受威脅趨勢 (Threat Trend)

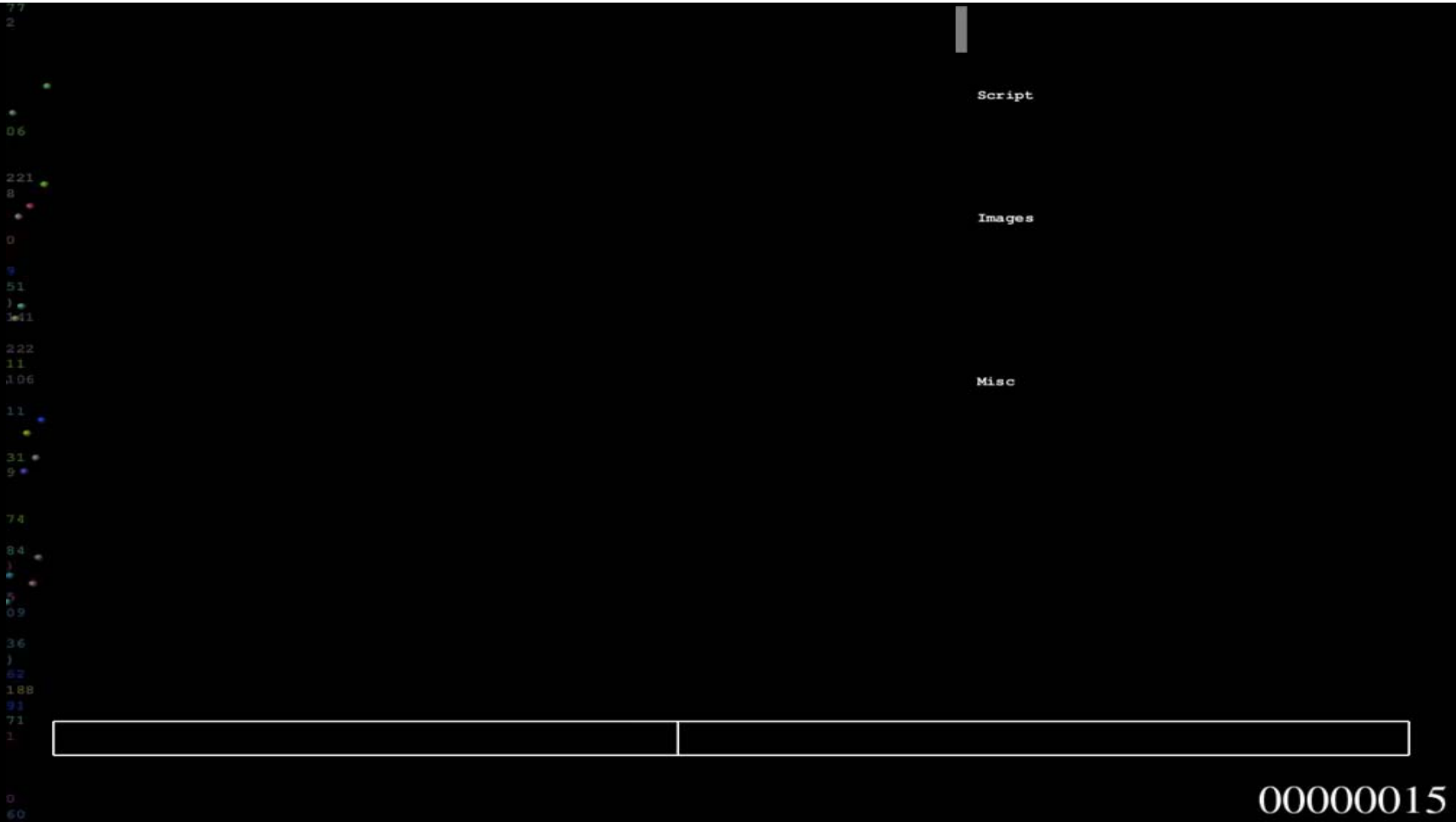


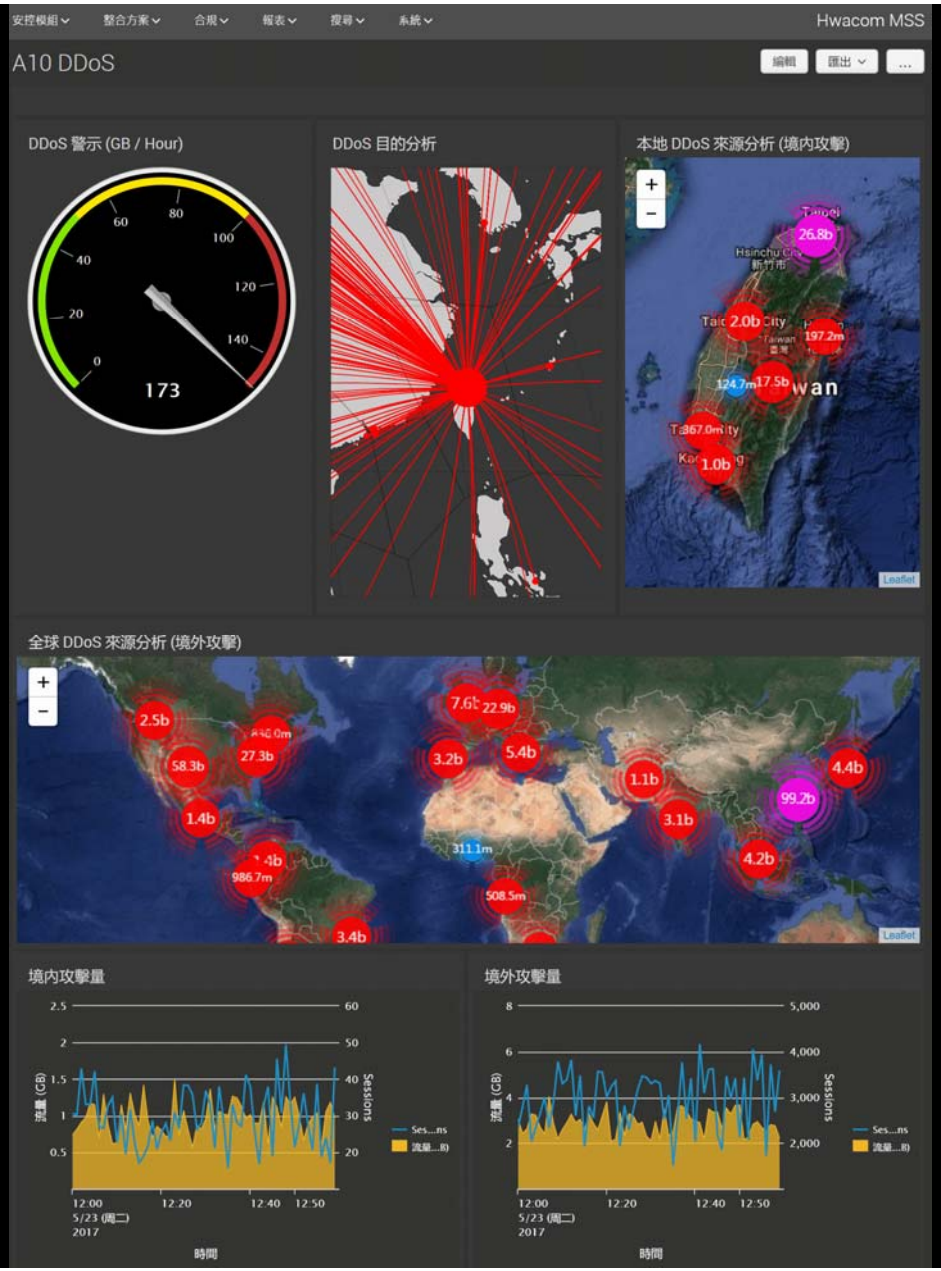
威脅事件排名 (Top Threats)

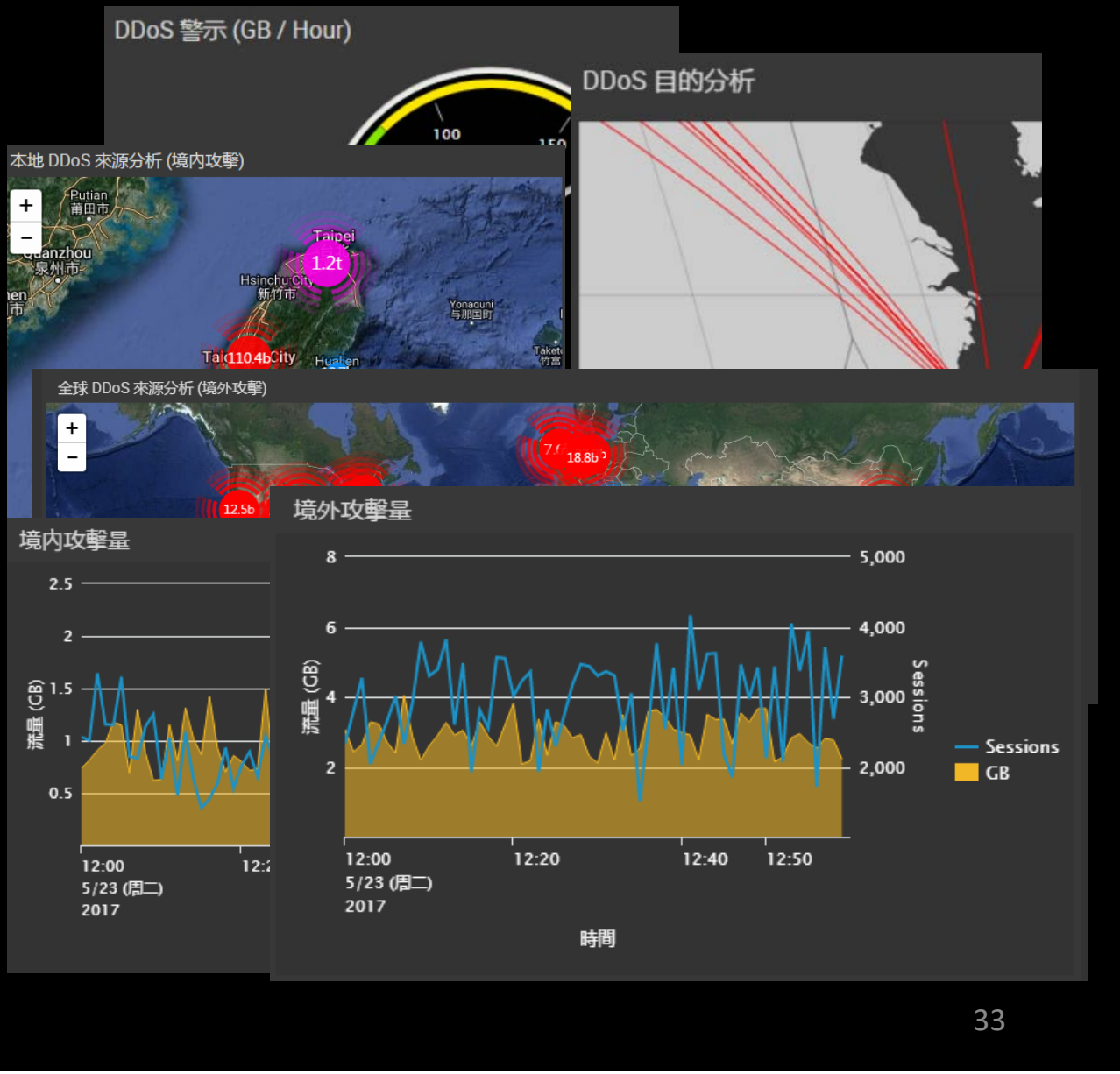
當前威脅 (Recent Threats)

時間	電腦名稱	Detection	檔案名稱
12/09 21:00	Win7-MSS-2	W32.GenericKD:WpakillA.19nf.1201	442.7z
12/09 21:00	Win7-MSS-2	W32.Variant:Gen.19ni.1201	Windows Loader 3.1.exe
12/09 21:00	Win7-MSS-2	W32.GenericKD:WpakillA.19nf.1201	Re-LoaderByR@1n.exe
12/09 21:00	Win7-MSS-2	W32.Auto:d17340.in03.Talos	Windows Loader 3.1 Final.zip
12/09 20:00	maccury的MacBook Pro	W32.Auto:d17340.in03.Talos	Windows Loader 3.1 Final.zip
12/09 20:00	maccury的MacBook Pro	W32.Auto:d17340.in03.Talos	1sjAm2Pl.zip.part
12/01 21:02	maccury的MacBook Pro	W32.Auto.8f2eac.182044.in01	o+xyBle0.zip.part
12/01 21:02	maccury的MacBook Pro	W32.Auto.8f2eac.182044.in01	dQQVjTkt.zip.part
11/30 15:03	NeilChen's MBP	W32.3B810F316C-90.LP.RET.SBX.TG	launcher.exe
11/30 15:03	NeilChen's MBP	W32.3B810F316C-90.LP.RET.SBX.TG	f_00bf56

« 上一頁 1 2 3 4 5 下一頁 »


Script
Images
Misc
00000015

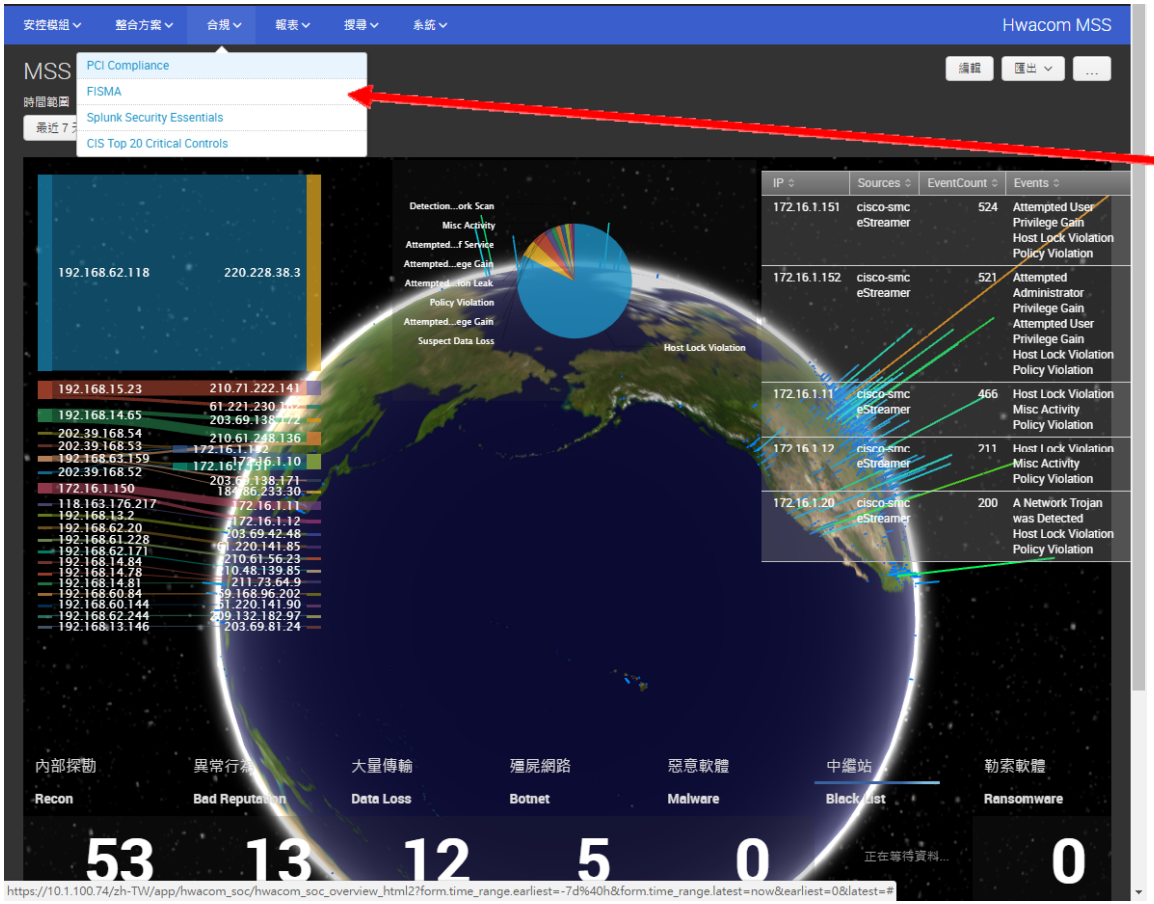

安控模組
整合方案
合規
報表
搜尋
系統
Hwacom MSS
A10 DDoS
編輯
匯出
DDoS 警示 (GB / Hour)
DDoS 目的分析
本地 DDoS 來源分析 (境內攻擊)
全球 DDoS 來源分析 (境外攻擊)
境內攻擊量
境外攻擊量
流量 (GB)
Sessions
時間

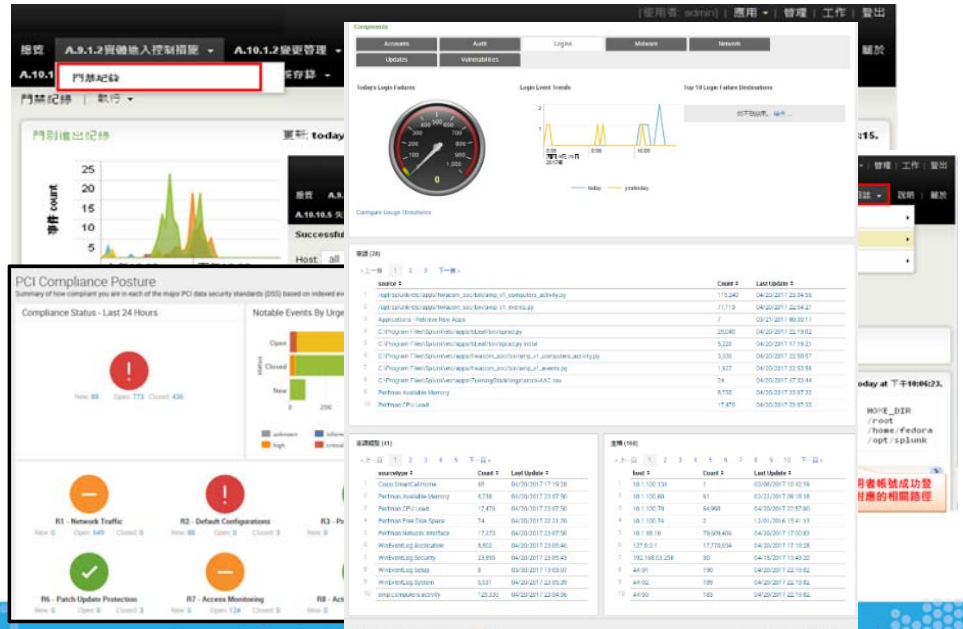

DDoS 警示 (GB / Hour)
DDoS 目的分析
本地 DDoS 來源分析 (境內攻擊)
全球 DDoS 來源分析 (境外攻擊)
境內攻擊量
境外攻擊量
流量 (GB)
Sessions
GB
時間
5/23 (周二)
2017

感染惡意軟體(Malware)內部IP

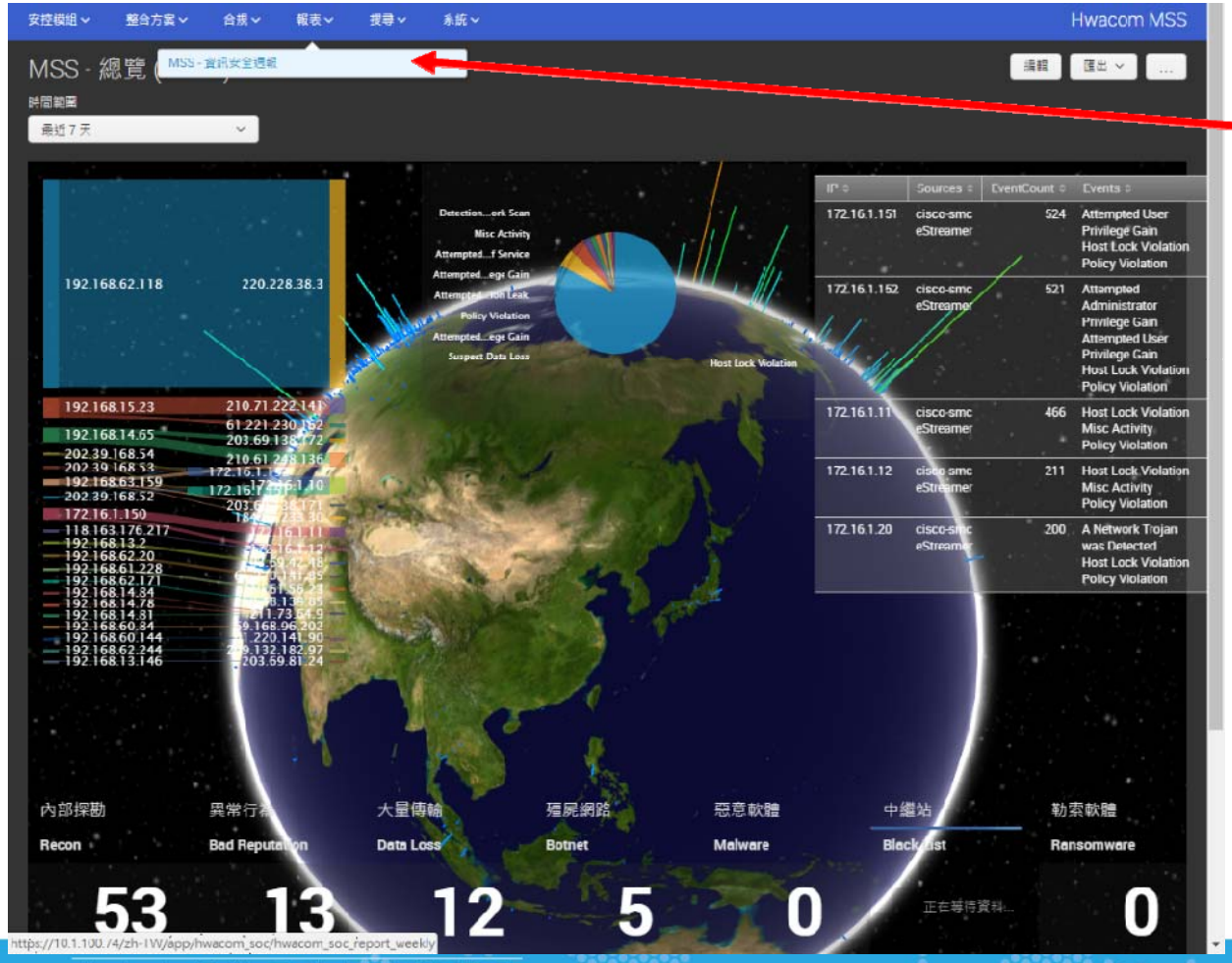
快速察知內部IP 主機已感染惡意軟體。

各式合規規範整合



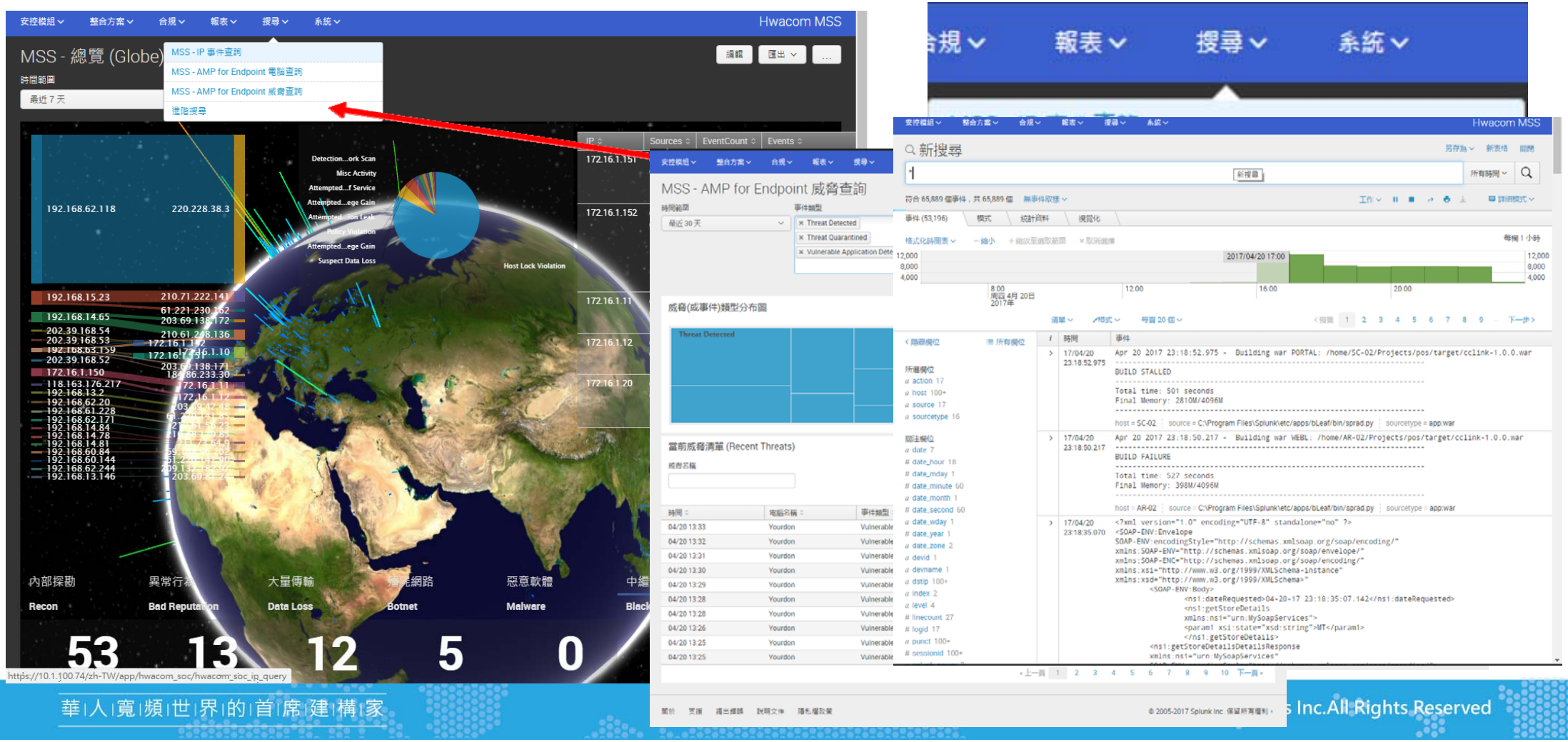


每週自動化資訊安全報表

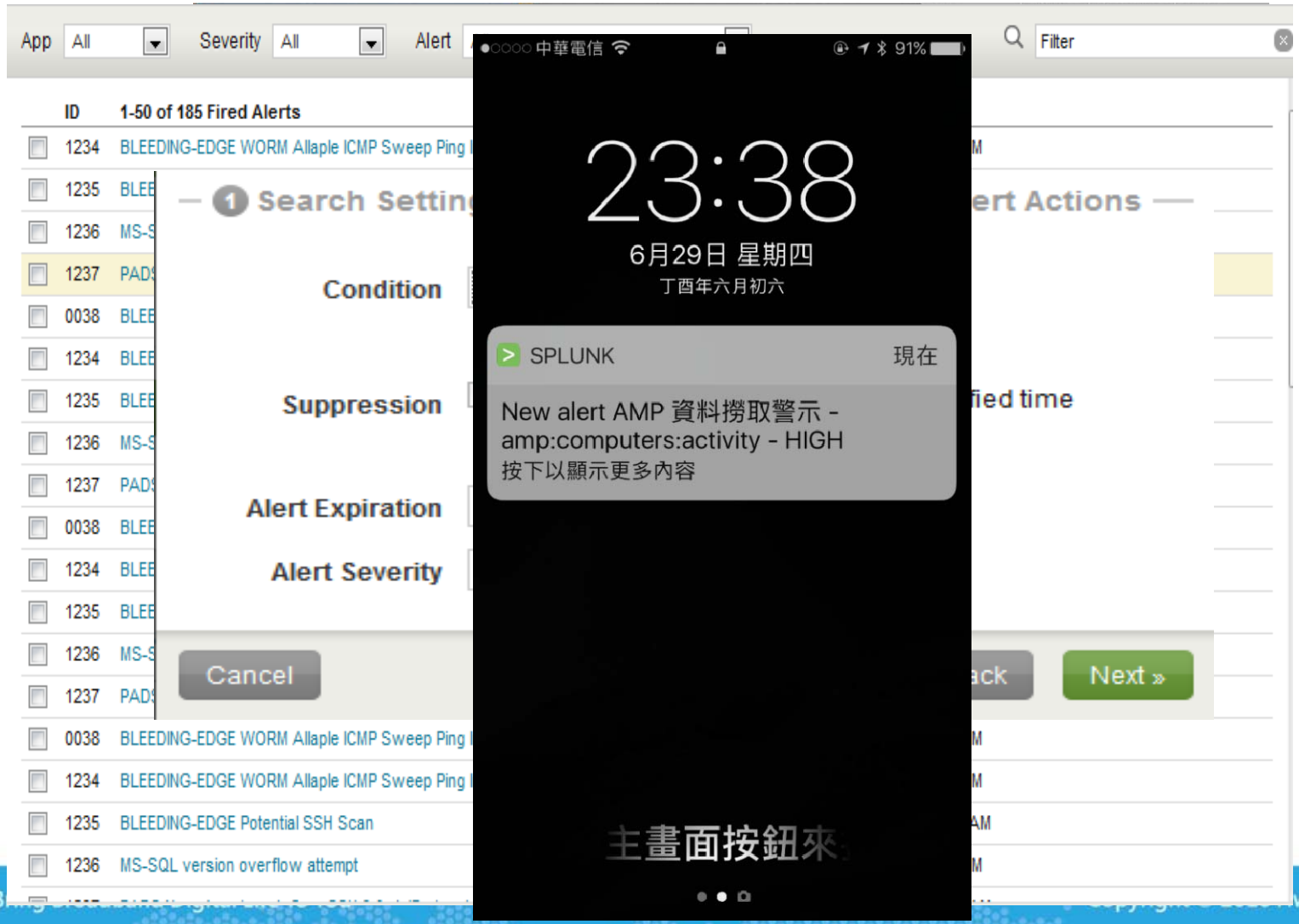


可自訂或定時自動化資訊安全報表寄送。

智慧化搜尋


安控模組
整合方案
合規
報表
搜尋
系統
Hwacom MSS
MSS - 總覽 (Globe)
MSS - IP 事件查詢
MSS - AMP for Endpoint 電腦查詢
MSS - AMP for Endpoint 威脅查詢
進階搜尋
編輯
匯出
時間範圍
最近 7 天
IP
Sources
EventCount
Events
172.16.1.151
172.16.1.152
172.16.1.11
172.16.1.12
172.16.1.20
192.168.62.118
220.228.38.3
Host Lock Violation
Suspect Data Loss
內部探勘
Recon
異常行為
Bad Reputation
大量傳輸
Data Loss
殭屍網路
Botnet
惡意軟體
Malware
53
13
12
5
0
MSS - AMP for Endpoint 威脅查詢
Threat Detected
Threat Quarantined
威脅(或事件)類型分布圖
當前威脅清單 (Recent Threats)
新搜尋
Apr 20 2017 23:18:52.975 - Building war PORTAL: /home/SC-02/Projects/pos/target/cclink-1.0.0.war
BUILD STALLED
Total time: 501 seconds
Final Memory: 281M/4096M
Apr 20 2017 23:18:50.217 - Building war WEBL: /home/AR-02/Projects/pos/target/cclink-1.0.0.war
BUILD FAILURE
Total time: 527 seconds
Final Memory: 398M/4096M
華|人|寬|頻|世|界|的|首|席|建|構|家
Inc.All Rights Reserved

警訊即時通報



手機即時監控畫面