CLOUDSEC2018

Freedom to Connect

CLOUDSEC2018
Freedom to Connect

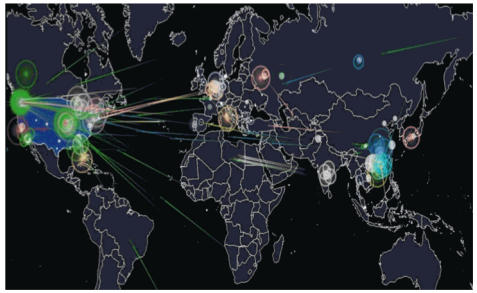
企業如何與ISP合作建構資安縱深防禦網

王信富 資深資安架構規劃師
中華資安國際

2018需重視的資安威脅

CLOUDSEC2018
Freedom to Connect

勒索軟體轉型威脅



DDoS攻擊量屢創新高

IoT物聯網裝置受駭頻傳

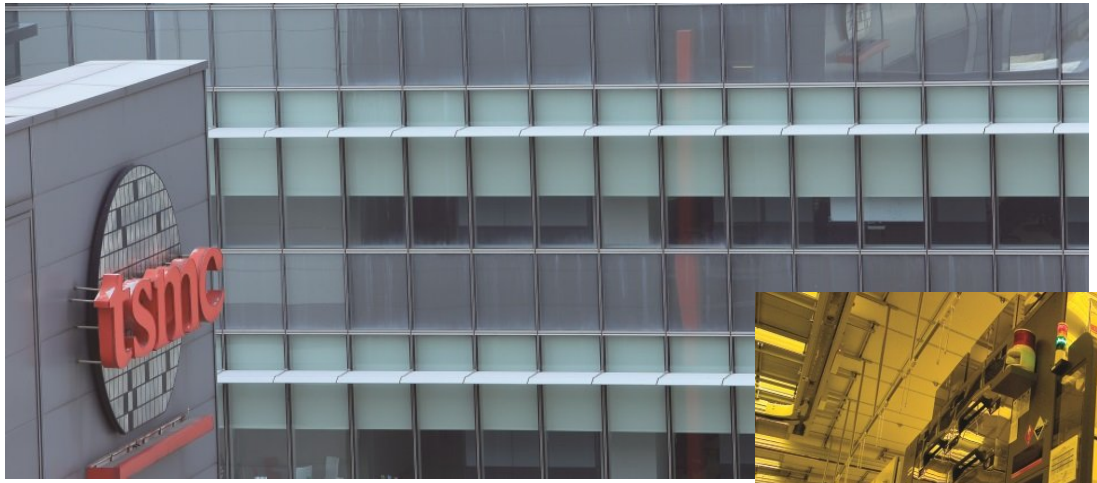
軟體供應鏈攻擊事件增多

挖礦攻擊大幅增長

#cloudsec

台積電產線機臺中毒事件

CLOUDSEC2018
Freedom to Connect



事件摘要：

- WannaCry勒索軟體變種
- 人為操作疏忽沒有按照SOP
- 作業系統沒有安裝安全修補更新
- 臺灣廠區的生產網路全部連結在一起

來源: iThome 2018/08

重點心得

- 勒索攻擊盛行
- 已知漏洞修補不完
- 人的問題始終存在
- 企業內網未必安全

勒索軟體全球肆虐

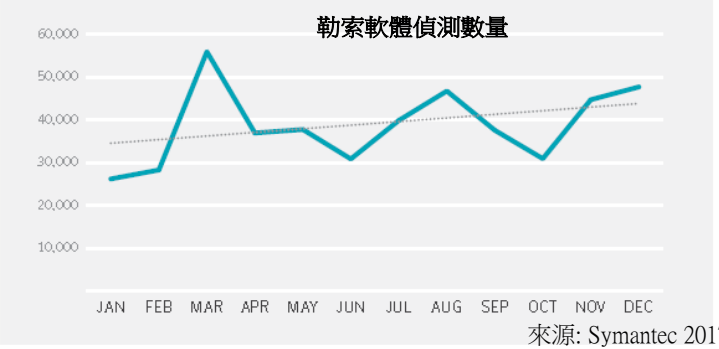
CLOUDSEC2018 Freedom to Connect

全球勒索軟體數量持續成長：

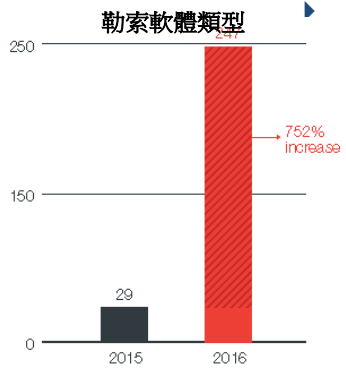
- 趨勢科技指出，2016年新增的勒索軟體類型達247種，是2015年的7.5倍
- 賽門鐵客觀察，偵測到的勒索軟體由2016年初每月約35,000筆增長至年末40,000筆

WannaCry橫空出世襲捲全球：

- 2017/5利用MS系統漏洞，對SMB(TCP 445)攻擊
- 未安裝Patch終端受感染，檔案遭RSA 2048高強度加密，勒索$300美金，且會橫向擴散
- 全球至少數十萬台電腦受感染影響



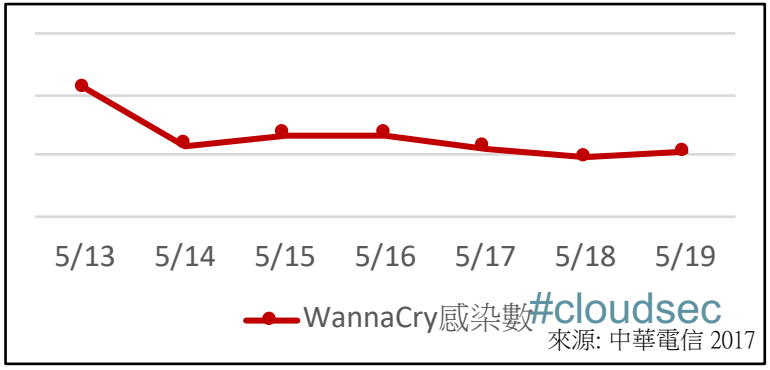
來源: Symantec 2017



來源: 趨勢科技 2017

HiNet SOC觀察：

- **台灣受勒索軟體危害嚴重，2016年每日約750個企業或使用者遭到感染**
- **106年5/13~19約有OO台電腦感染WannaCry**
  - 未裝Patch又曝露在網路就有可能感染
  - 今年可能會有模仿犯複製此模式攻擊
  - 駭客無法確認被害人是否付款→**可能無法贖回!**
  - **持續修補**非常重要



來源: 中華電信 2017

WannaCry感染流程剖析&中華採取行動

駭客

惡意網站/郵件

1.以MS017-010 SMB漏洞進行感染

<感染後註冊為服務>

被害者

2.進行連線探測下列網址是否存在
www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

<檢查Kill Switch>

Internet

3a.若連線失敗則開始進行勒索作業

3b.若連線成功則停止動作

區域網路

4.1.掃描周圍電腦以步驟1攻擊

<橫向擴散>

4.2.執行加密程序
(約數分鐘至數十分)

5.加密完成，顯示勒索訊息及贖款交付方式

惡意中繼站

6.向Tor C&C檢查是否有付贖款

http://gx7ekbenv2riucmf.onion
http://57g7spgrzlojinas.onion
http://xxlvbrloxvriy2c5.onion
http://76jdd2ir2embyv47.onion
http://cwwnhwhlz52maqm7.onion

<按下Check Payment>

- 5/13出現大規模爆發，影響未安裝微軟3月份更新(KB4012215)設備
  - **98%**感染設備為Windows 7 (卡巴斯基)
- HiNet SOC極快採取以下措施，防止威脅進一步擴大：
  - 5/13早：分析惡意程式，並盤點HiNet受影響客戶
  - 5/13午：更新防駭守門員服務阻擋政策，並發布通告提醒客戶更新作業系統
  - 5/14：總公司發佈內部資安通告提醒同仁檢查終端
  - 5/14：HiNet骨幹與防駭守門員針對國外高頻攻擊IP進行阻擋，降低感染機率
  - 5/15：HiNet SOC對國內高頻攻擊IP進行勸說離線
  - 5/16：全面佈署MS017-010攻擊防護特徵至入侵防護服務，徹底攔阻相關攻擊
- 現正密切注意變種或類似攻擊手法出現

比特幣(匿名特性)金流助長駭客勒索行為

CLOUDSEC2018 Freedom to Connect

勒索軟體結合比特幣後大流行：

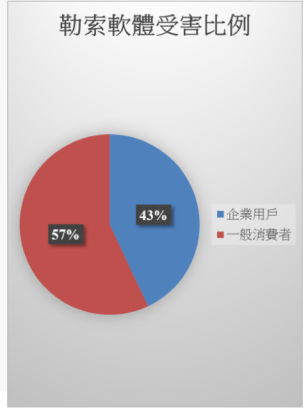
小心惡意軟體！每17人就有1人被勒索贖金 平均付22K

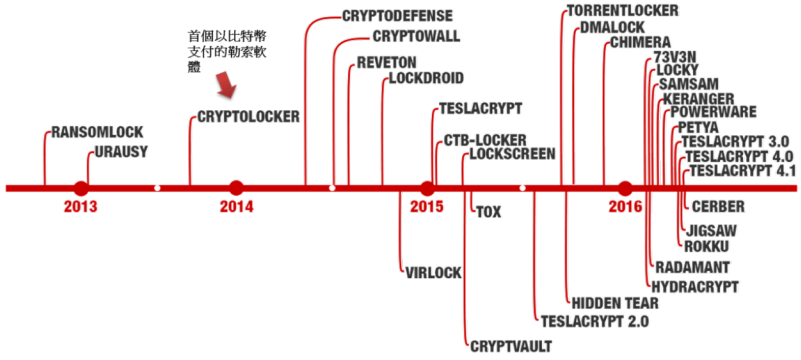
鉅亨網記者宋宜芳 台北 2016/08/18 11:08

臉書是最容易成為病毒攻擊的目標，近日臉書傳出「他看過的電影加了Atefub」病毒災情，當受害者點開惡意影片連結後，就會遭感染開始攻擊下一波目標，以致個資遭竊取。近年來，除了社群媒體惡意程式攻擊外，「加密勒索軟體」更成了駭客最有效的犯罪獲利模式，根據賽門鐵克勒贖軟體調查報告顯示，2016 年 3 月受勒贖軟體感染的數目甚至激增至 56000 個案例。而為了解除勒索軟體的威脅，平均每人支付的贖金，更從 9498 元，躍升至 21946 元。

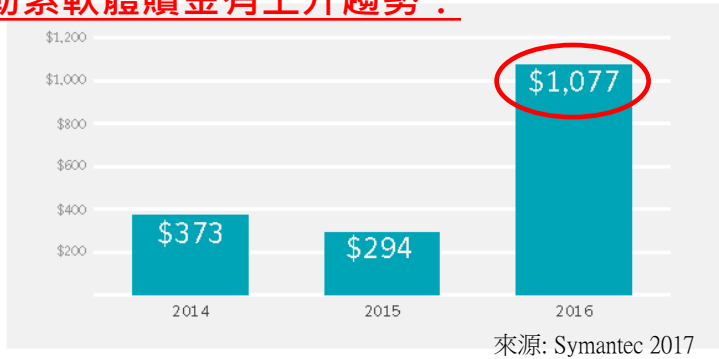
賽門鐵克網路安全調查報告重要訊息發現，平均 17 個用戶中就有一個人被勒索軟體威脅，勒贖軟體犯罪集團成長因素不外乎為，加密軟體取得容易、有效的感染媒介、先進攻擊技術等，甚至利用勒贖軟體作為服務開始企業化經營，提供下游分潤機制吸引更多人一同犯罪。

常見的勒贖手法有，使用「網路描述語言」躲避防毒軟體偵查，例如 JavaScript、PHP 等程式語言，「附加元件功能」像是 Cerber 新增殭屍病毒，讓中毒者發動 DDoS 攻擊；「勒贖新增威脅語言」言語脅迫使用者交出贖金，市面上還出現了「限時解鎖」勒贖軟體，要讓消費者在時間壓力下無法思考而衝動上當。





勒索軟體贖金有上升趨勢：



來源: Symantec 2017

駭客透過DDoS攻擊勒索比特幣：

來源: iThome 2017

駭客嗆後天攻擊 勒索券商10元比特幣

2017年02月05日

來源: 蘋果日報 2017

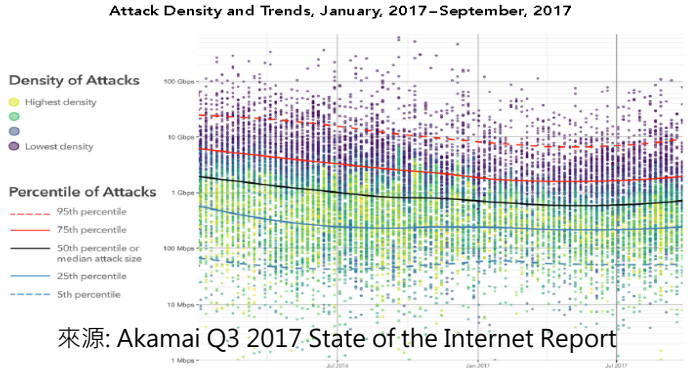
【劉文淵/台北報導】網路攻擊無所不在，國內多家證券商本月初遭到國際駭客從羅馬尼亞發動分散式阻斷服務攻擊（簡稱DDos），意圖癱瘓券商電子下單系統，駭客還要求支付10元比特幣（bitcoin；約新台幣31萬元），若不從將會在後天再度發動攻擊，刑事局已介入偵辦。警方表示券商已加強網路安全系統，駭攻並未癱瘓券商，且當日股市未開市，沒有造成損失，應是詐騙集團手法。

DDoS分散式阻斷攻擊觀察

CLOUDSEC2018 Freedom to Connect

全球 DDoS攻擊趨勢(2017/1-9月)：

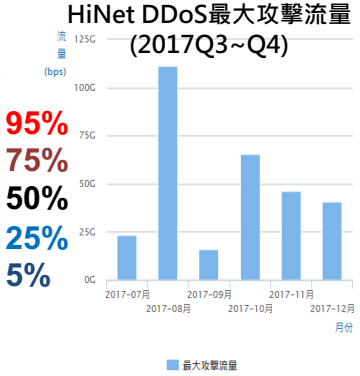
- 由受駭IoT設備形成的Mirai Botnet仍持續頻繁活動， 2017Q3出現過109Gbps的ACK Flood 攻擊
- 2017Q3攻擊次數增加(較Q2增加**8%**)，遊戲業占大宗(**86%**)
- 近期攻擊以反射放大洪水式為大宗(佔49%)：常見的有 DNS(16%) NTP(12%) CLDAP (8.84%)等
- 行動設備逐漸成為DDoS攻擊來源， 2017 年8月再度出現用來DDoS的Mobile Botnet “WireX”

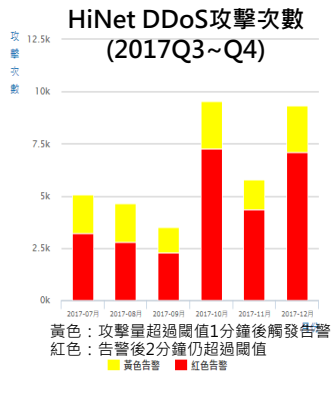


來源: Akamai Q3 2017 State of the Internet Report

SOC觀察(2017Q4)：

- 國內2017Q4 HiNet**平均每天發生約268次**攻擊，較Q3成長**187%**，為2016年的**3倍**
- 最大攻擊規模為**65 Gbps**，**UDP** Flooding為大宗
- 攻擊對象偏重**資通信**、**製造業**，其次為**遊戲業**、**學術教育業**、**金融保險業**等
- 2017/8 出現2家**證券商遭駭客DDoS**





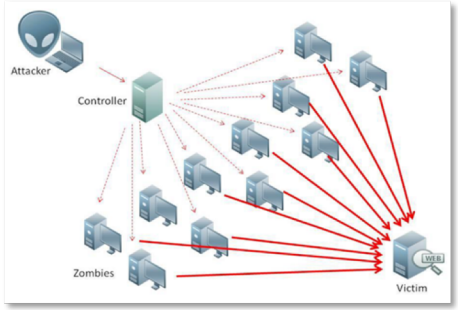
資料來源：CHT Security

#cloudsec

IoT設備遭駭，當成攻擊武器

CLOUDSEC2018
Freedom to Connect

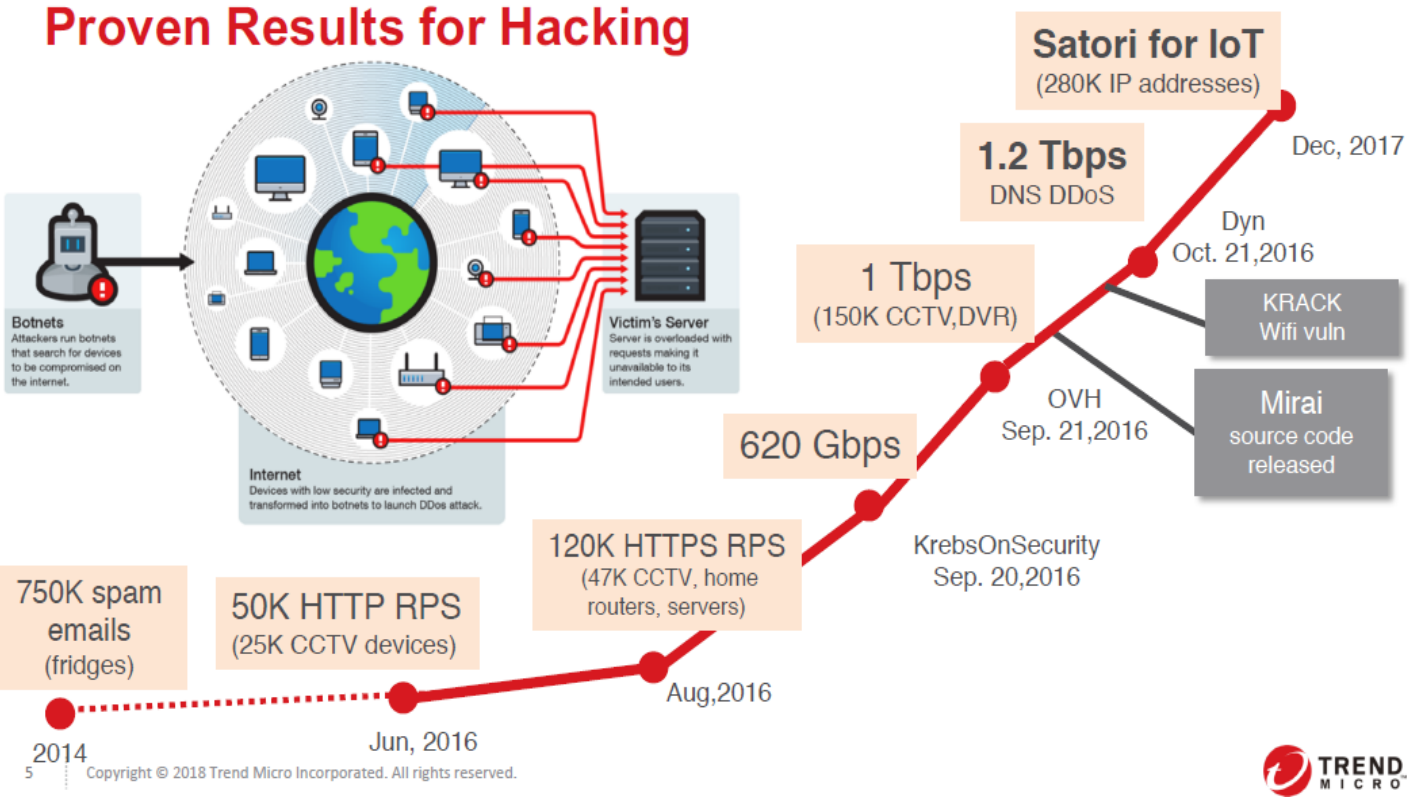
IoT設備DDoS攻擊



- **萬物皆聯網導致萬物皆可駭**
  - ✓ 2016年10月21日知名網路服務 Dyn 遭受殭屍網路發動三波巨大規模 DDoS 攻擊，世界各大網站服務皆因為此攻擊而中斷，包括 Amazon、Twitter、Github、PayPal 等大型網站都因此受到影響。
  - ✓ **利用 IPCAM、CCTV、DVR、IoT 裝置等系統進行 DDoS 攻擊**
- **網路安控系統使用者關鍵問題**
  - ✓ IoT設備使用弱密碼
  - ✓ **未進行適當的權限劃分與管理**
  - ✓ 容易開啓攻擊者寄送的惡意連結，導致被 XSS、CSRF 等手法攻擊
  - ✓ **未限制連入 IP 位址，導致安控系統可從外網任意存取**

資安管控
網路隔離
資安管控
使用管理

IoT Hacking is Growing

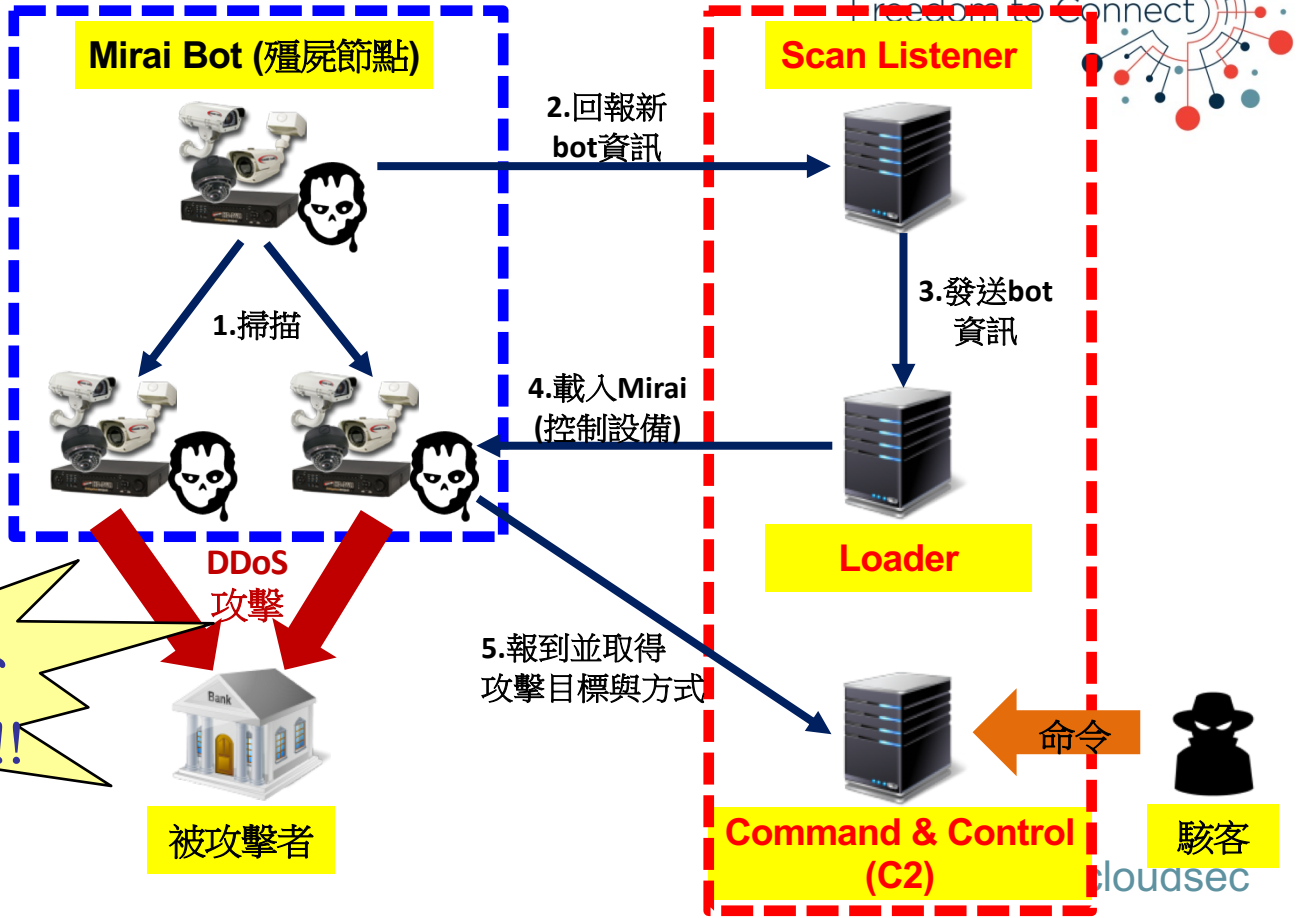


Mirai – 模組化、系統化架構設計

1.裝置預設/弱密碼

2. N-day 攻擊
(IoT裝置很少上patch)

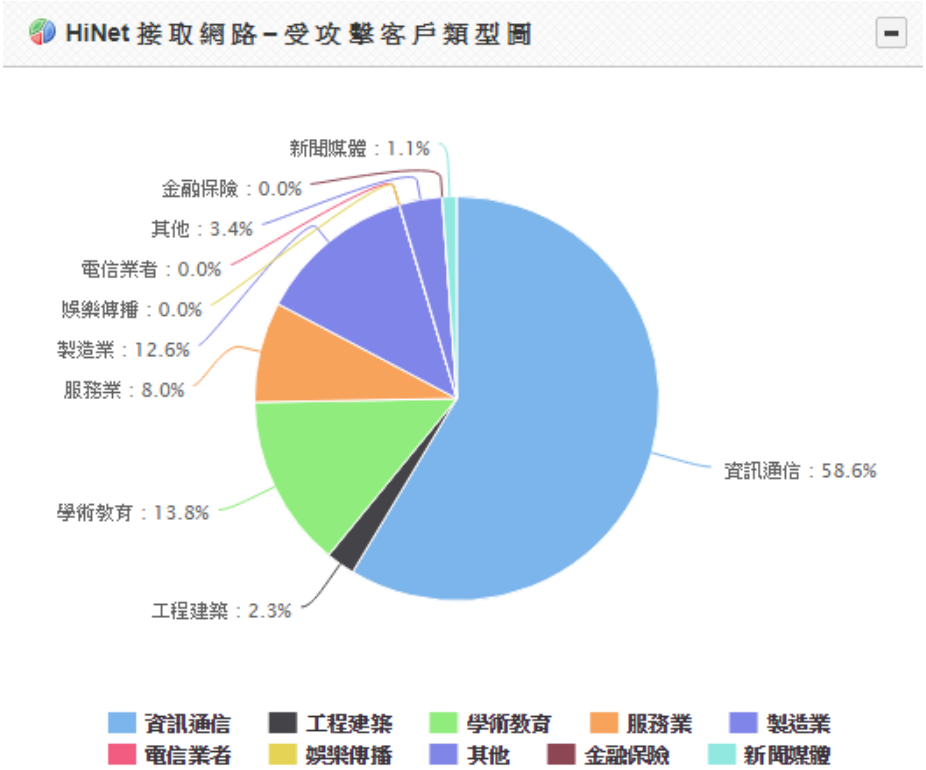
3. 0-day 攻擊
(掃到就開打!)



數量成長驚人、攻擊腳本可換!!

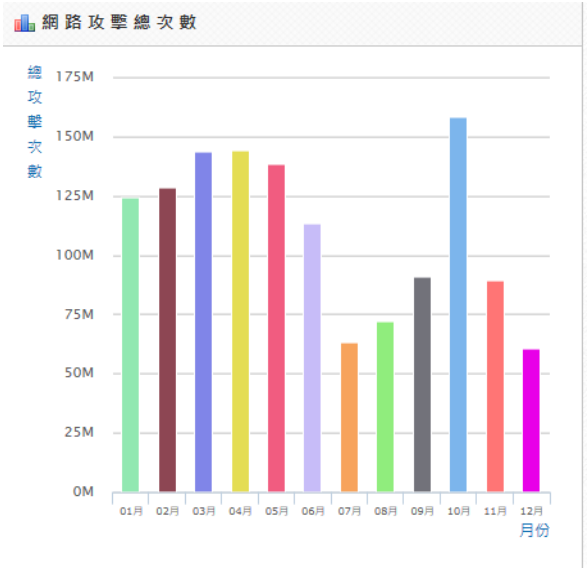
2018年Q1的攻擊產業分析圖

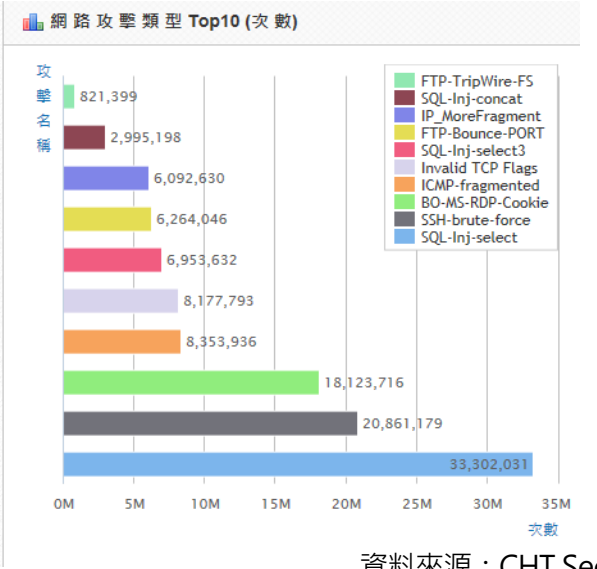
CLOUDSEC2018
Freedom to Connect



資料來源：CHT Security #cloudsec

網路攻擊樣態觀察





資料來源：CHT Security

- Internet攻擊防護
  - 協助客戶阻擋外部攻擊**平均每月1億5千萬次**
  - SQL injection、SSH Brute-force與RDP buffer overflow佔攻擊手法前三名
- 防駭守門員
  - 協助客戶阻擋連線惡意網域/網站**平均每日1萬5千次**

駭客肆虐日趨嚴重，勒索、挖礦、間諜程式及各種網路攻擊防不勝防

CLOUDSEC2018
Freedom to Connect

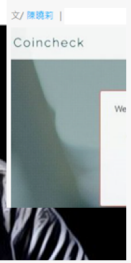
【犯罪事件】駭客癱瘓美國亞特蘭大市，勒索$51,000美元贖金

by Moore, S. T. —2018/3/24

2018/3/09

日本虛擬貨幣交易商Coincheck遭駭餘波盪漾，2家交易商被停業1個月

Coincheck遭駭後，日本金
Coincheck等7家業者祭出



勒索軟體Petya再襲全球，車諾比核設施、WPP廣告集團都受駭

資安業者指出Petya變種勒索軟體至少利用了Eternal Blue感染受害者的
300美元比特幣，遭會竄改主開機紀錄，受害者包括海運公司、石油公司

文/ 陳文霞 | 2017-06-28 發表

Petya勒索軟體的新
府，包括全球最大
(AP Moller Maersk)

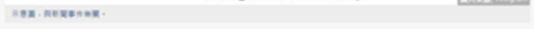
根據資安公司(Syman
微軟(Microsoft)的MS
電腦，感染Petya的
Petya還會竄改被感
求約等值300美元的比特幣作為
補了這個漏洞，但駭客還可能
卡巴斯基(Kaspersky)估計，在
遭到攻擊。

2018/2/14

挖礦攻擊無孔不入，Telegra

駭客以偽裝的檔名誘騙使用者按下「執行」鍵後即會下載真正的攻擊程式，有可能下載挖礦程式，利用受害者
的電腦挖礦，也有可能下載後門程式，讓駭客取得遠端控制權。

文/ 林妍溱 |



新聞

勒索軟體變種超快，ShurL0ckr竟能穿越Google和微軟Office雲端內建的木馬偵測機制

不過，研究人員於2/7再以VirusTotal檢查防毒軟體對ShurL0ckr的偵測能力時，已有50%可辨識該勒索軟體

文/ 陳曉莉 | 2018-02-09

新聞

去年勒索軟體肆虐誰是最大受害者？Sophos：醫療保健業

儘管金融與醫療保健業者擁有重要的資料，但金融服務業只有45%遭勒索軟體攻擊，居所有受害產業的最末位，而醫療保健業者因IT系統較為老舊、缺乏足夠的安全防護，成為駭客攻擊的首選。

文/ 陳曉莉 | 2018-02-07

新聞

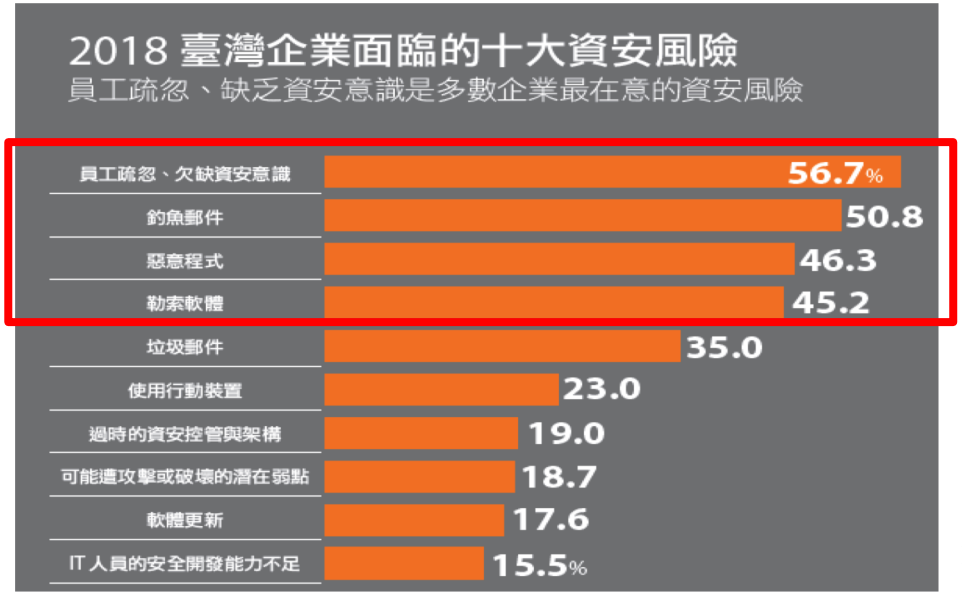
醫療IT服務商Allscripts遭勒索軟體攻擊，拖累醫院被迫關門兩天

勒索軟體綁架了Allscripts北卡羅萊州羅利市和夏洛特市的資料中心，數個系統受到影響，其中專業電子病歷系統和管制藥物處方箋系統，兩個系統花了5天恢復運作。

文/ 李建興 | 2018-02-06

企業資安風險排名

CLOUDSEC2018
Freedom to Connect

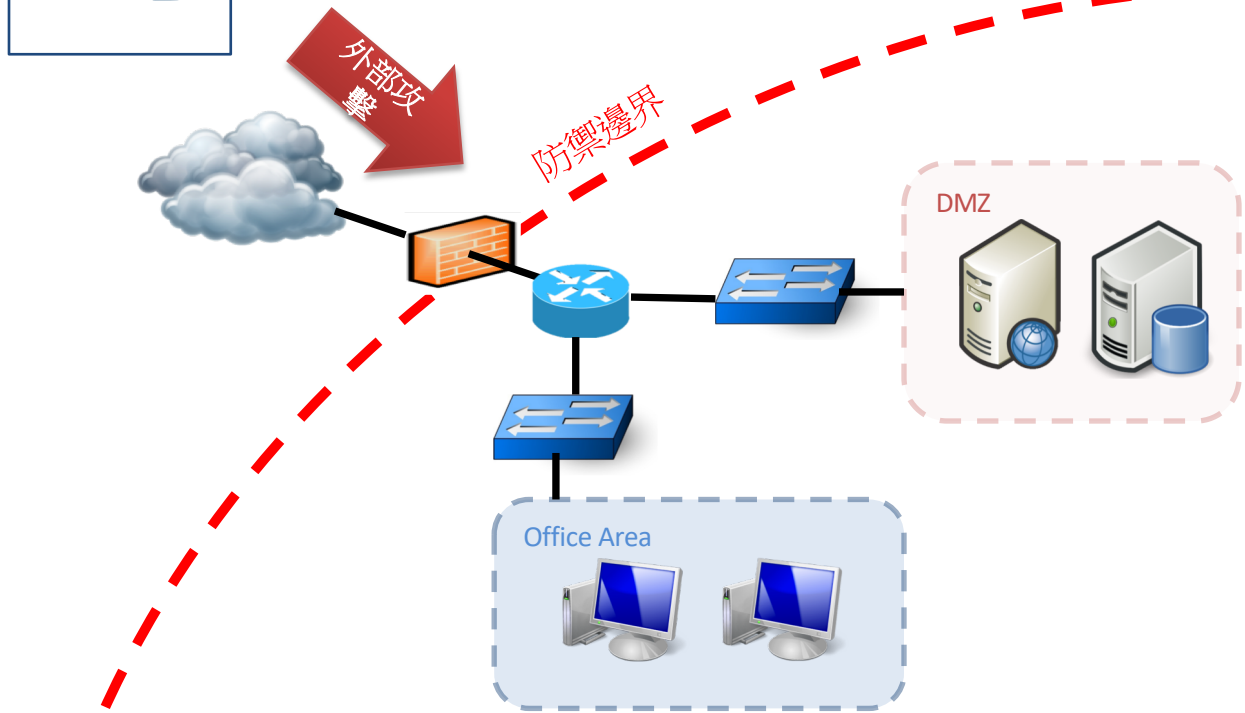


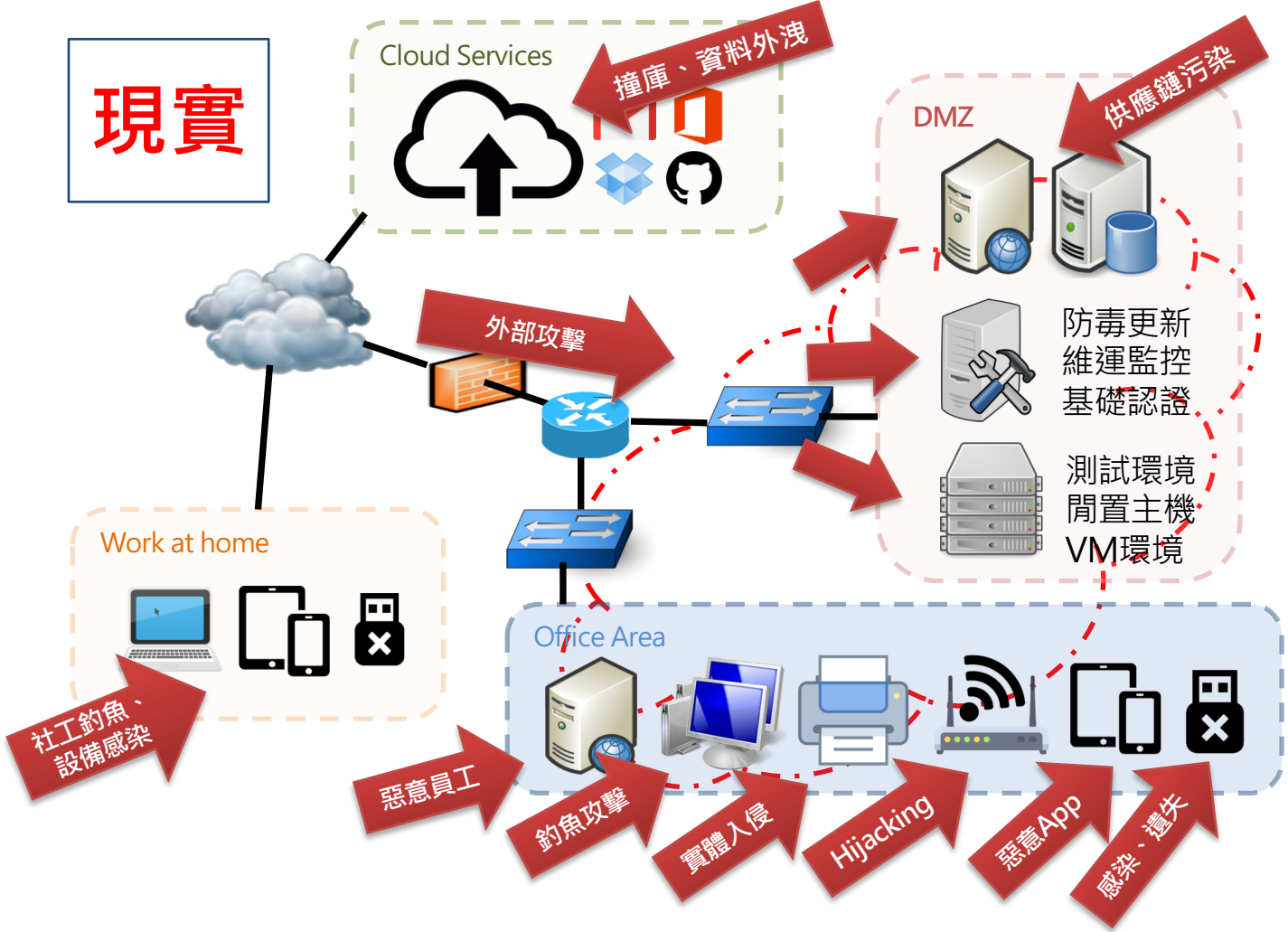
資料來源：Ithome
2018/4/07

- 員工疏忽、欠缺資安意識、釣魚郵件、惡意程式及勒索軟體為企業所面臨前四大風險，占比均超過4成5
- 資安事件對企業所帶來的衝擊，造成災害復原時間增加、員工生產力下降...等，導致營運成本增加、商譽受損...等嚴重損失

企業面臨資安風險的困境

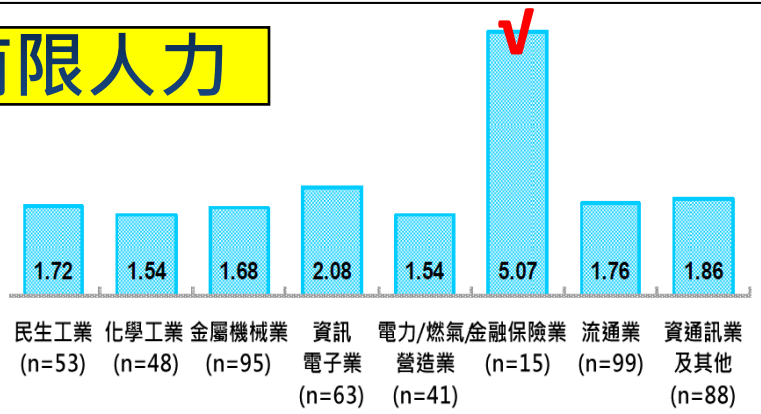
理想



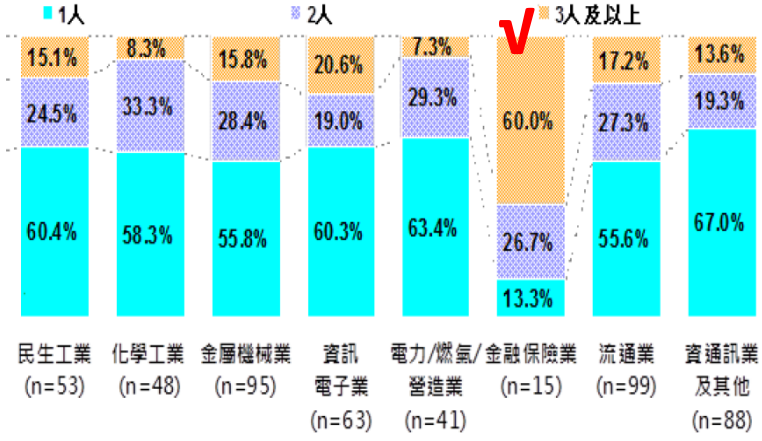

現實
Cloud Services
撞庫、資料外洩
DMZ
供應鏈污染
外部攻擊
防毒更新
維運監控
基礎認證
測試環境
閒置主機
VM環境
Work at home
Office Area
社工釣魚、
設備感染
惡意員工
釣魚攻擊
實體入侵
Hijacking
惡意App
感染、遺失

有限人力

十、2016 年企業平均資安人力數量（產業別）

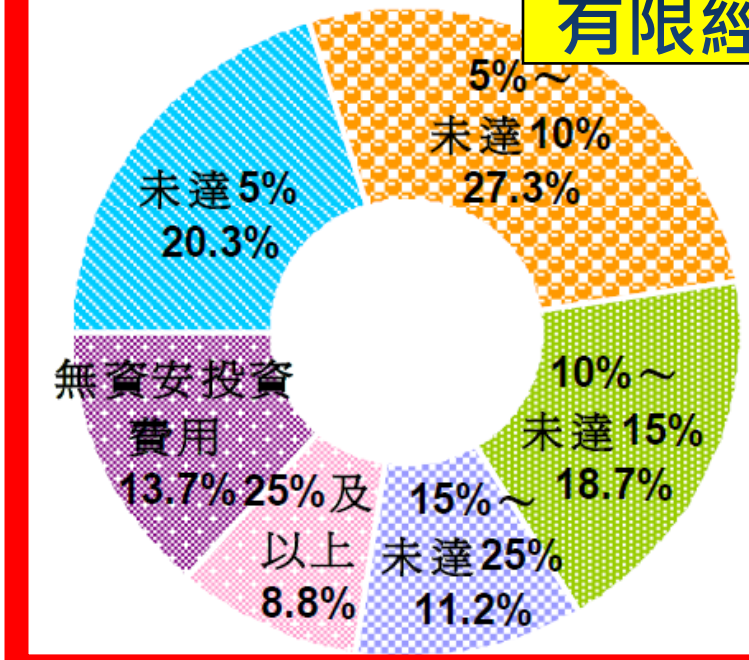


九、2016 年資安人力數量（產業/家數比）



有限經費

圖三、2016 年資安投資佔 IT 投資比例（家數比）



需有資安夥伴，掌握威脅情資、建構防衛體系

備註：N=500

資料來源：MIC，2016 年 5 月

建立資安防護新認知

CLOUDSEC2018
Freedom to Connect

巨大流量癱瘓服務
IoT殭屍網路+反射式攻擊
創造1Tbps以上攻擊量

勒索攻擊盛行
以DDoS攻擊癱瘓服務或勒索軟體
綁架資料要求贖金

已知漏洞修補不完
公開1年內仍會被駭客利用，
若未及時上Patch會受駭

0時差攻擊/APT
利用尚未被公布之系統或產品弱點
進行攻擊，成功率高

Shadow IT
網路服務(如Dropbox、AWS)
不受IT部門管理，33%事件由此造成

企業網路邊界消失
需將不屬自己管理的雲端/網路服務
也納入資安防禦範圍

駭客目標持續擴大
一般認為安全的裝置(如影音設備、
印表機、ATM)也成為攻擊目標

人的問題始終存在
私自使用不受IT管理的網路服務、
貪圖方便、社交攻擊開啟惡意檔案

企業內網
未必安全 !!

獨力防禦
極為困難 !!

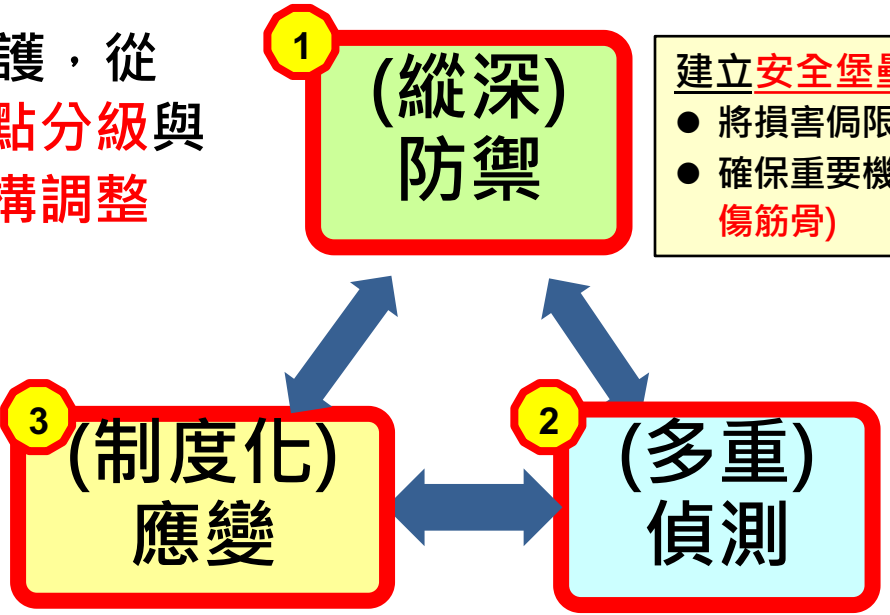
需重新思考
防護戰略 !!

#cloudsec

資安防護戰略 – 防禦/偵測/應變

CLOUDSEC2018
Freedom to Connect

最好的防護，從
1.資產盤點分級與
2.網路架構調整
開始！



建立安全堡壘、多層分艙防護機制
- 將損害侷限在一定範圍
- 確保重要機敏資料不流出(小傷、不傷筋骨)

結合大數據分析工具，快速回溯偵測隱匿行為
- 鑑識快篩、回溯式分析快速收斂與控制受駭範圍(緊急處置)
- 挖掘受駭根因回饋調適防禦機制(鑑識分析)

多重偵測與自動化關聯，即時發覺異常行為
- 透過偵測、於第一時間洞察已被攻擊
- 爭取重大損害發生前之黃金應變時間

#cloudsec

1 建立安全堡壘，佈署縱深防禦網路架構

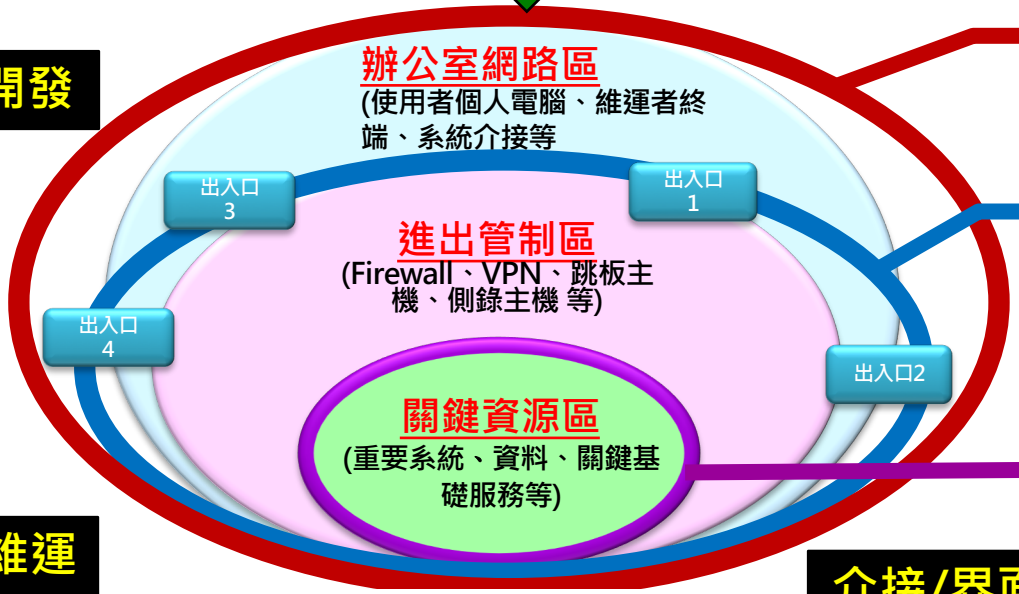
CLOUDSEC2018 Freedom to Connect

第一道防線: MSS 網路資安代管服務
企業網路的資訊安全閘道(阻隔於境外)

例如: HiNet 資安艦隊 IPS入侵防護、
DDoS, APT, email GW

Internet

CxO期待:
- 不要再發生資安事件
- 即使發生，也不能影響營運
- 即使影響營運，也要能快速回復!



系統開發

遠端維運

第二道防線: Intranet
出入Internet閘道(或對外DMZ)

第三道防線: Server farm
出入Intranet(或Internet)

封閉、隔離，
做好出入口防護

內部系統防護
內網東西向隔離

介接/界面

MSS: Managed Security Service

#cloudsec

1 從ISP網路機房端切入之資安防護

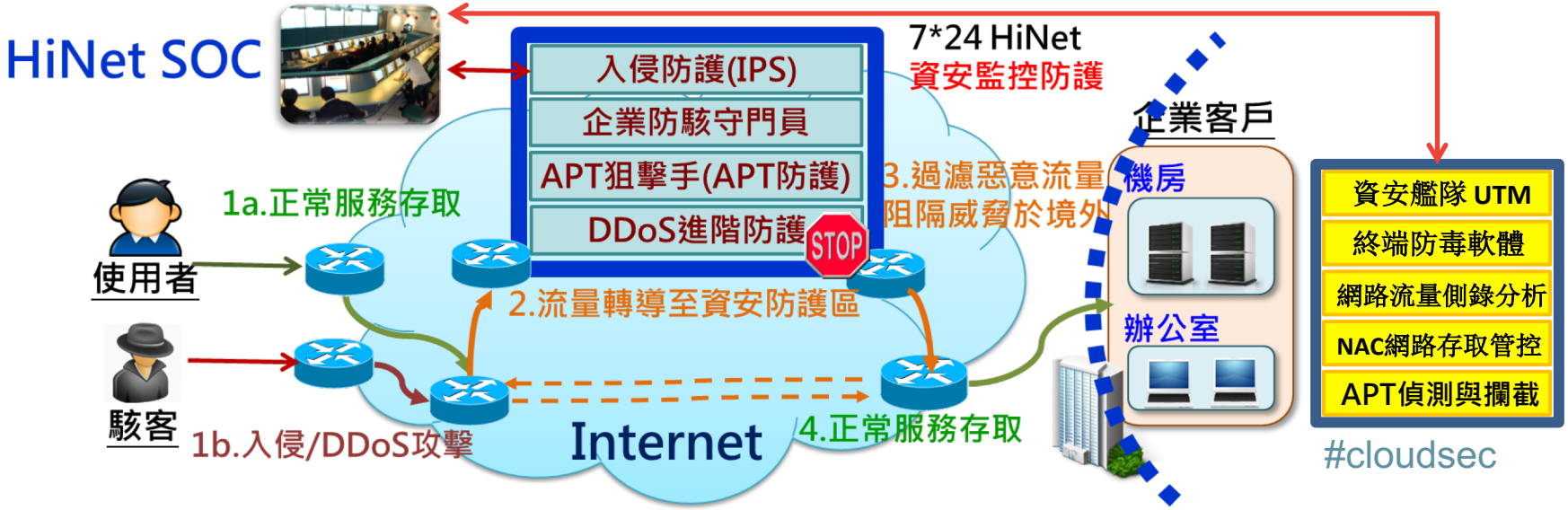
CLOUDSEC2018 Freedom to Connect

■ MSS資安服務

- 入侵防護(IPS)：阻擋駭客攻擊與病毒等威脅
- 企業防駭守門員：惡意連線阻擋、端點檢測排除
- APT狙擊手：阻擋APT流量及惡意郵件附檔
- DDoS進階防護：防護網站不受大流量攻擊癱瘓

■ 中華電信與同業差異

- 於HiNet資安防護區過濾，於企業外阻隔威脅
- 以領導廠牌設備(如Gartner推薦)提供防護，配合HiNet資安專家調校，確保防治最新攻擊
- 客戶無須安裝設備與投入人力管理，節省成本



DDoS 多層次縱深防禦

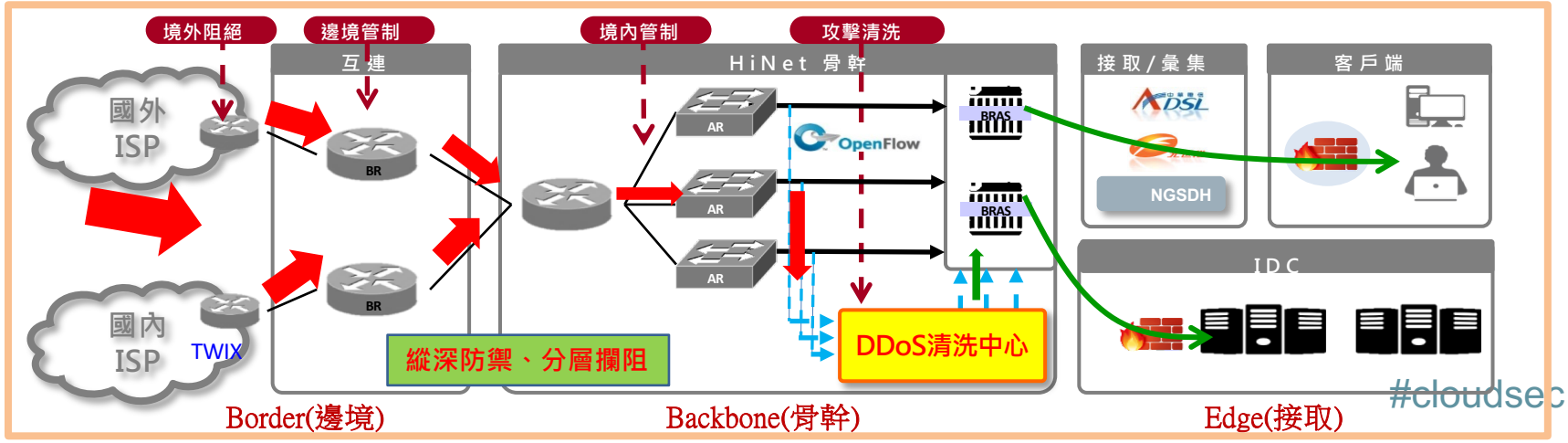
縱深防禦

CLOUDSEC2018 Freedom to Connect

- 多層次阻擋/隔離/清洗來緩解攻擊，可選:
  - Border：
    - 境外阻絕：利用遠端驅動工具，呼叫Tier-1 ISP聯防，攔阻攻擊訊務於境外
    - 邊境管制：利用網路存取控制工具，管制符合攻擊IP的訊務
  - Backbone：
    - 骨幹管制：利用境內管制符合攻擊特徵IP的訊務
    - DDoS隔離清洗：利用專屬網路/資安設備，過濾攻擊訊務
  - Edge：
    - 於客戶網路端部署資安設備防護

中華電信與同業差異

1. 全台最大ISP與網路骨幹，可承受大量攻擊封包
2. 獨家多層次攻擊緩解、防堵機制，迅速恢復服務
3. 延遲最小，將資安防護內化於網路服務中
4. 資安專家具有豐富網路資安防護技術與經驗
5. 提供演練服務，可模擬遭攻擊時應變程序與能力
6. 另提供國際清洗中心，可滿足跨國企業需要



Gartner 建議 DDoS防護架構

Featuring Research from Gartner

- SOURCE : Hype Cycle for Threat-Facing Technologies, 2017
- User Advice: DDoS mitigation services should be a standard part of business continuity/disaster recovery planning, and they should be included in all internet service procurements when the business depends on the availability of internet connectivity. Most enterprises should look at detection and mitigation services that are available from ISPs or DDoS security-as-a-service specialists. To defend against complex, application-based attacks, a mix of local protection (on-premises DDoS appliances) and cloud-based mitigation services is a strong option. The content delivery network (CDN) approach to DDoS protection is also a valid approach, particularly when the organization is already using a CDN for content distribution to improve the performance of its website. However, the CDN approach only protects websites. It does not protect against attacks aimed at nonweb targets (for example, corporate firewalls, VPN servers and email servers).

1. 大多數企業都應向ISP或DDoS防護服務商尋求DDoS偵測與緩解方案
2. 企業端在地端設備結合網路端DDoS緩解服務，是防禦DDoS的最佳解決方案

HiNet新世代防火牆服務服務簡介

縱深防禦

CLOUDSEC2018 Freedom to Connect

- 於HiNet機房端建置Palo Alto Networks 新世代防火牆(NGFW)，阻擋來自Internet攻擊、並提供客戶上網流量過濾
- 基本版功能：
  - 防護：過濾外對內(Internet->企業客戶)的入侵攻擊
  - 防護：隔絕網路病毒、阻擋惡意連線
  - 管控：管控內對外5大類別網站連線，如：惡意網站、違反善良風俗、降低生產力、影音播放、其他分類 (2018 Q4提供)
- 全能版可加購以下功能：
  1. 阻擋黑名單連線（IP address/URL/Domain；共50組/每月）
  2. 控管應用程式 (25個類別應用程式，如：傳輸、遊戲、影音、加密通道、視訊語音…)
  3. 控管國別流量（放行或阻擋國別流量；10組/每月）
  4. 控管檔案傳輸（120種以上檔案類型）
  5. 提供沙箱行為分析與報告

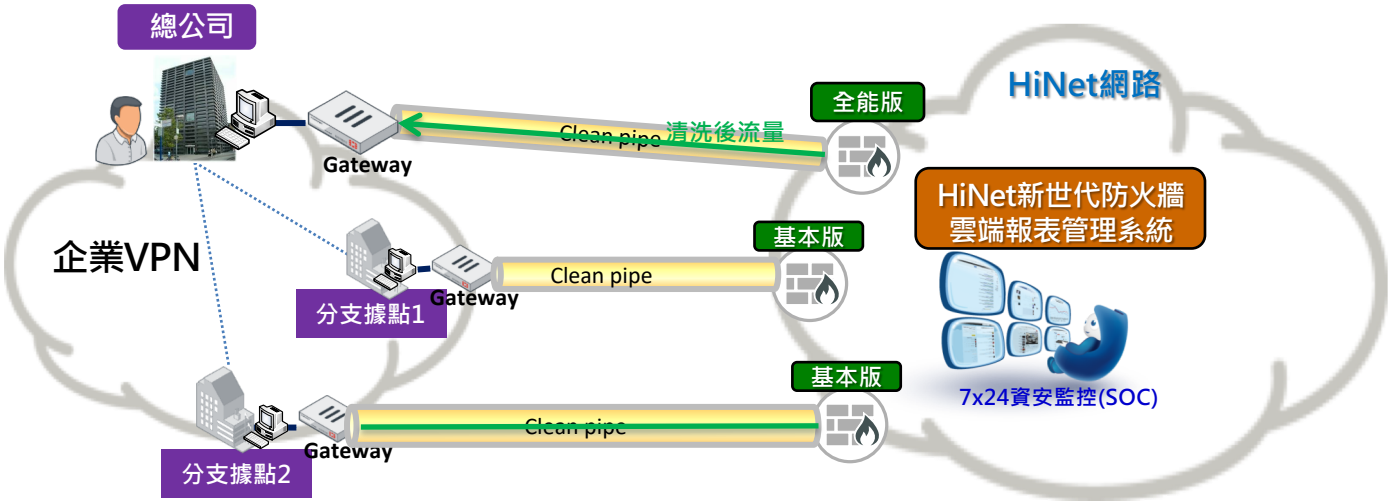
「模組化」選購，讓企業在「功能」與「價格」中取得最佳的平衡點

服務架構示意圖 - 阻絕攻擊於企業外，過濾惡意流量

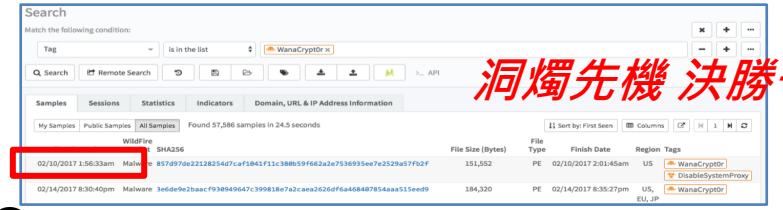
CLOUDSEC2018 Freedom to Connect

全能版：基本版 + 強化資安管控模組
1. 結合企業內部自有資安管控與外部電信機房端防護，雙管齊下
2. 產製資安威脅報表，知彼知己，預防勝於治療

基本版
1. 適合無網管/IT人員的SME、大型公司各地據點申辦
2. 分支據點資安防護快速部署，省時省力



以WannaCry 勒索病毒為例說明



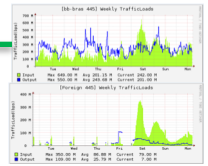
洞燭先機 決勝千里

Cyber Threat Alliance(CTA)

1 2017/2/10 WannaCry 情資

paloalto NETWORKS
Palo Alto 全球威脅情資

中華資安國際 CHT Security
CHT Security 台灣在地情資



2 2017/2/10 情資更新

情資資料庫

3 2017/5/13 大幅感染日

Internet

惡意攻擊流量

清洗後流量

HiNet新世代防火牆

Gateway

HiNet Customer

新世代防火牆-資安防護儀表板(1/2)

新世代防火牆-資安防護儀表板(2/2)

CLOUDSEC2018
Freedom to Connect

新世代防火牆-攻擊統計分析報表

CLOUDSEC2018
Freedom to Connect

■ 阻擋網站連線排名

no	目的主機名稱	次數
1	update.googleapis.com	1.23K 23.33%
2	settings-win.data.microsoft.com	960.00 17.72%
3	login.live.com	690.00 12.74%
4	v10.vortex-win.data.microsoft.com	549.00 10.13%
5	iecvlist.microsoft.com	452.00 8.34%
6	curs.microsoft.com	328.00 6.05%
7	watson.telemetry.microsoft.com	243.00 4.49%
8	armmf.adobe.com	186.00 3.43%
9	sls.update.microsoft.com	184.00 3.4%
10	go.microsoft.com	47.00 0.87%

■ 攻擊事件排名

no	事件	次數
1	THREAT url ssl: (9999) block-url	3.42K 39.51%
2	THREAT url google-base: (9999) block-url	1.28K 14.76%
3	THREAT spyware sip: SIPVicious SIP Auditing Tool Activity(18088)	1.14K 13.17%
4	THREAT vulnerability unknown-udp: Netis/Netcore Router Default Credential Remote Code Execution Vulnerability(39587)	1.09K 12.62%
5	THREAT url web-browsing: (9999) block-url	331.00 3.74%
6	THREAT url ms-update: (9999) block-url	209.00 2.36%
7	THREAT vulnerability portmapper: RPC Portmapper DUMP Request Detected(32796)	111.00 1.25%
8	THREAT url soap: (9999) block-url	42.00 0.47%
9	THREAT vulnerability ypserv: Sun Solaris rpc.yupdated Command Injection Vulnerability(31247)	18.00 0.2%
10	THREAT spyware ssl: Suspicious TLS Evasion Found(14978)	17.00 0.19%
11	THREAT vulnerability rpc: Sun Solaris sadmind RPC Request Integer Overflow(32803)	16.00 0.18%

■ 應用服務連線排名

no	應用服務	次數	Session	packet	byte
1	ssl	3.45K 39.9%	0.00	0.00	0.00
2	google-base	1.28K 14.76%	0.00	0.00	0.00
3	sip	1.15K 13.26%	0.00	0.00	0.00
4	unknown-udp	1.11K 12.88%	0.00	0.00	0.00
5	web-browsing	466.00 5.26%	0.00	0.00	0.00
6	ms-update	209.00 2.36%	0.00	0.00	0.00
7	unknown-tcp	192.00 2.17%	0.00	0.00	0.00
8	smtp	162.00 1.83%	0.00	0.00	0.00
9	portmapper	118.00 1.33%	0.00	0.00	0.00
10	rpc	67.00 0.76%	0.00	0.00	0.00
11	soap	54.00 0.61%	0.00	0.00	0.00

#cloudsec

縱深防禦

CLOUDSEC2018
Freedom to Connect

企業內部網路2.0: 強調管理

- 管理誰在使用你的網路: IP實名制
- 管理網路使用的範圍
- 管理網路使用的時段
- 管理網路使用的的內容
- 管理網路使用的訊務是否需加密
- 進行非法使用訊務進行的側錄

商用IP+MAC管控設備限制

- 利用SNMP/Telenet進行蒐集資料
- 缺點: 只能看，發生障礙時無法作為 (且不即時)

議題	NetSecure
1. 無法即時阻擋	• 因利用SNMP讀取Router ARP Table是週期性的(5分鐘或10分鐘)，會有空窗期，導致無法即時阻擋 • 無法防治ARP偵測其他設備的IP/MAC資料
2. 有誤判情形及錯誤阻擋	• Router的ARP Table會被Spoofing(欺騙)，當Spoofing發生時，NetSecure會誤判認為諸多IP/MAC均有誤，而封鎖大片交換器的Port，導致錯誤阻擋 • ARP Table及MAC均是學習來的，容易被駭導致錯誤學習
3. 封鎖後的開通，會影響其他正常設備	被封鎖的Ethernet Switch埠再次被開通時，被阻擋的設備若未被修正，可能影響其他正常設備

第二代企業內部網路: CHTNet 2.0

CLOUDSEC2018 Freedom to Connect

強化網路安全、易管理、自動化

	CHTNet 1.0	CHTNet 2.0
設計原則	• 容易連線及使用(Default開通)，隨插隨用 • 單一VPN網路 • 增購防火牆進行接取管理 • 網路24小時全開通	• 網路嚴格管理(Default不通)，沒有申請即無法使用 • 多個VPN網路 • 網路設備進行接取管理 • 上班時段網路開通，非上班時段需申請
安全	• 無內部防護機制 • 可布建防火牆進行網段隔離 • 可加購資安設備	• 特定網段/特殊連線(業務會議)可進行隔離 • 無法用ARP偵測其他設備的IP/MAC資料 • 可加購資安設備
供裝維運	• 人工操作 • 個別設定 • 人員異動須人工作業網路設定	• 資訊系統自動供裝設定 • 統一GUI集中設定/管理 • 人員異動由資訊系統自動變更
設備來源	• 商用解決方案	• 商用解決方案 • CHT TL客製化

企業內部網路解決方案
中華電信 EyeLAN產品

CLOUDSEC2018
Freedom to Connect

ICT Month Innovative Elite 2017 百大創新產品獎

106資訊月 百大創新產品 Innovative Products

下載百大創新產品參選須知
下載百大創新產品報名步驟說明

獎項資訊 About | 最新消息 News | 聯絡主辦單位 Contact

歷年創新產品回顧 | 首頁 | 報名

讚 分享 趕快註冊來看看朋友對哪些內容按讚。

中華電信 中華電信研究院 系統整合、工具軟體、應用設備類 編輯

EyeLAN企客網路解決方案

產品介紹

「EyeLAN 企客網路解決方案」 是針對企業內網提供網路集中管理、彈性設置與安全存取管控的智慧網路解決方案。

目前的企業網路架構常使用L2/L3網路設備 (如 Ethernet Switch 與 IP Router) 來建構隨插即用 (Plug & Play)、網網相連 (Anything Connected) 的企業內網，網管人員需採購大量的資安設備與網路管理設備進行資安防護與網路

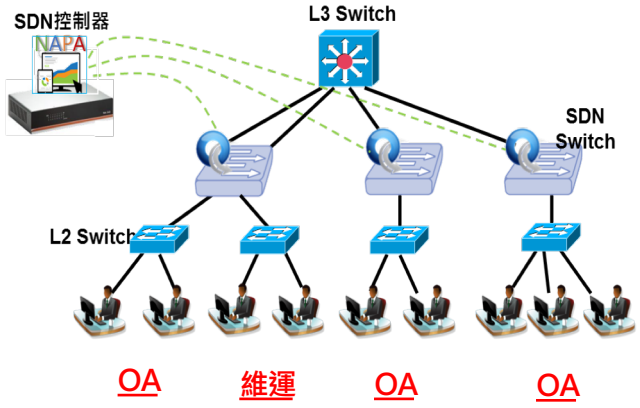
... 更多

產品圖片

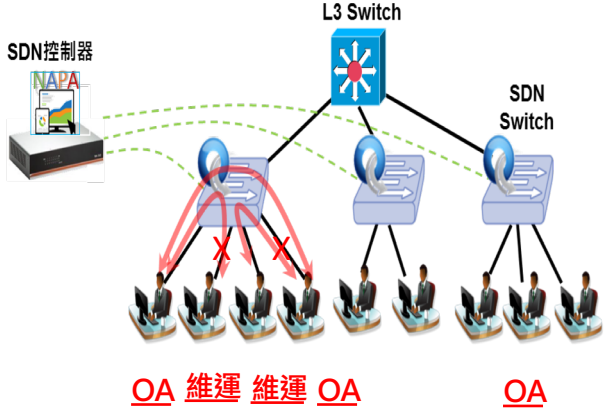
#cloudsec

EyeLAN網路架構建議

- 架構1
  - L2 Switch當成Openflow switch的延伸
  - L2 Switch不能混用
  - 無法防治ARP偵測其他設備的IP/MAC資料
  - 無法徹底隔離



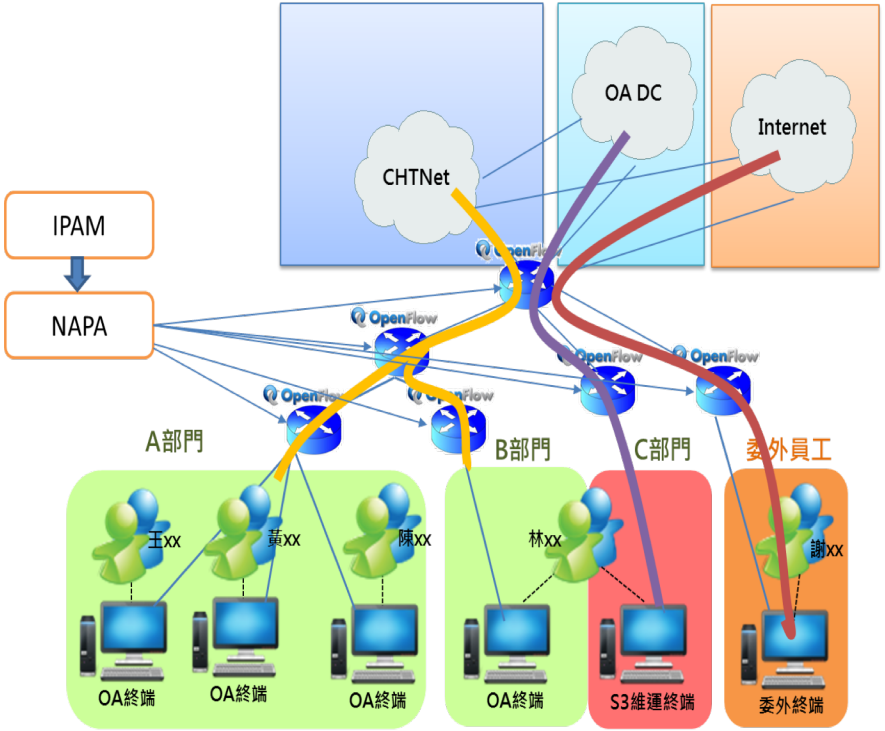
- 架構2 (CHT 總公司)
  - 終端直接接入SDN Switch，系統可管控終端設備連線，終端設備彼此不互通，安全性更高
  - 可達到CHTNet 2.0需求



以CHT 總公司大樓內部網路當範例

效益

- 由資訊系統(IPAM)管理網路的使用者
- NAPA依據屬性將設備導到不同路徑，彼此隔離
- 網管人員透過NAPA管理網路
- 骨幹網路確實隔離(各自有路由器)
- 資訊系統可動態調整設備屬性，網路接收指令自動調整設定(無人工介入)



EyeLAN管理系統功能簡介

- GUI操作
- 終端設備管理
- 網路拓璞
- 訊務監控
- 政策與網路存取管理(ACL)
- 網路設定(DB)備份與回復
- 路徑建立操作
- 網路障礙查測

GUI操作畫面

- Dashboard

終端設備管理

CLOUDSEC2018
Freedom to Connect

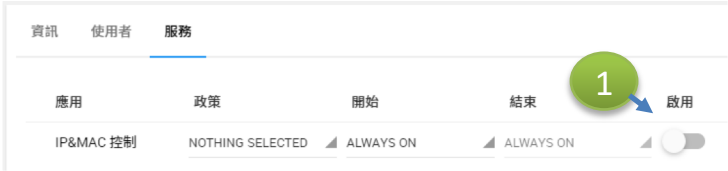
- 終端上網管控
- IP實名制

❖ 終端上網管控

1. 一鍵啟動IP+MAC控制

❖ IP實名制

2. IP實名制
   - 紀錄使用者與狀態



網路拓樸

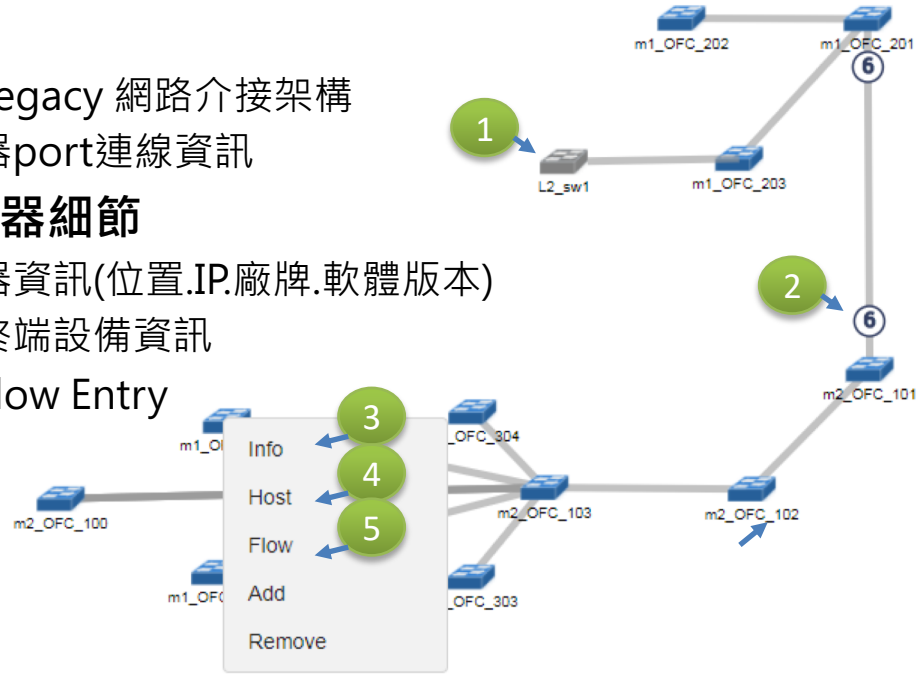
- 網路拓樸
- 右鍵顯示交換器細節

❖ 網路拓樸

1. 可顯示與Legacy 網路介接架構
2. 顯示交換器port連線資訊

❖ 右鍵顯示交換器細節

3. 顯示交換器資訊(位置.IP.廠牌.軟體版本)
4. 查詢介接終端設備資訊
5. 查詢設備Flow Entry



政策與網路存取管理(ACL)

- 網路政策
- 網路存取管理
- 物件集合

- **集合式設計**
  - 物件集合與政策
- **網路政策**
  1. 對象集合
  - 黑名單/白名單設計
  2. L4存取限制，可搭配存取埠(80,443...)
- **網路存取控制**
  - 集中管理
  - 同時可新增多筆ACL清單

網路設定(DB)備份與回復

CLOUDSEC2018
Freedom to Connect

- 資料庫備份
- 資料庫回復

❖ 資料庫備份

- 一鍵備份
- 可輸入自定義註解

❖ 資料庫回復

- 一鍵回復

#cloudsec

訊務監控

- 連接埠訊務
- 指定訊務

❖ 連接埠訊務

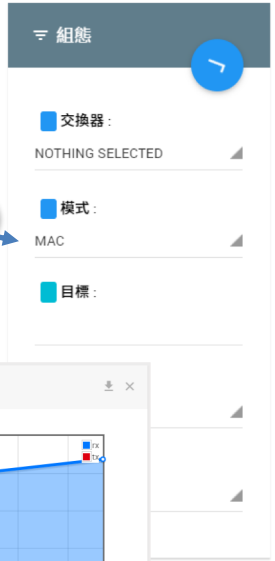
- 針對交換器上的連接埠
- 即時訊務與歷史訊務

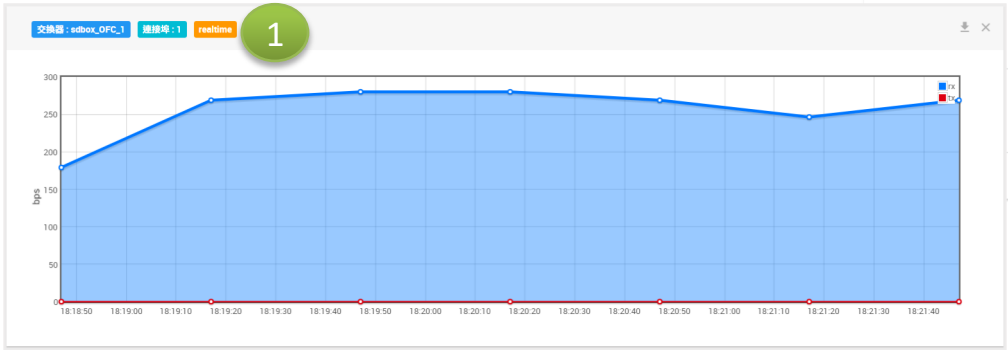
1

❖ 指定訊務

2

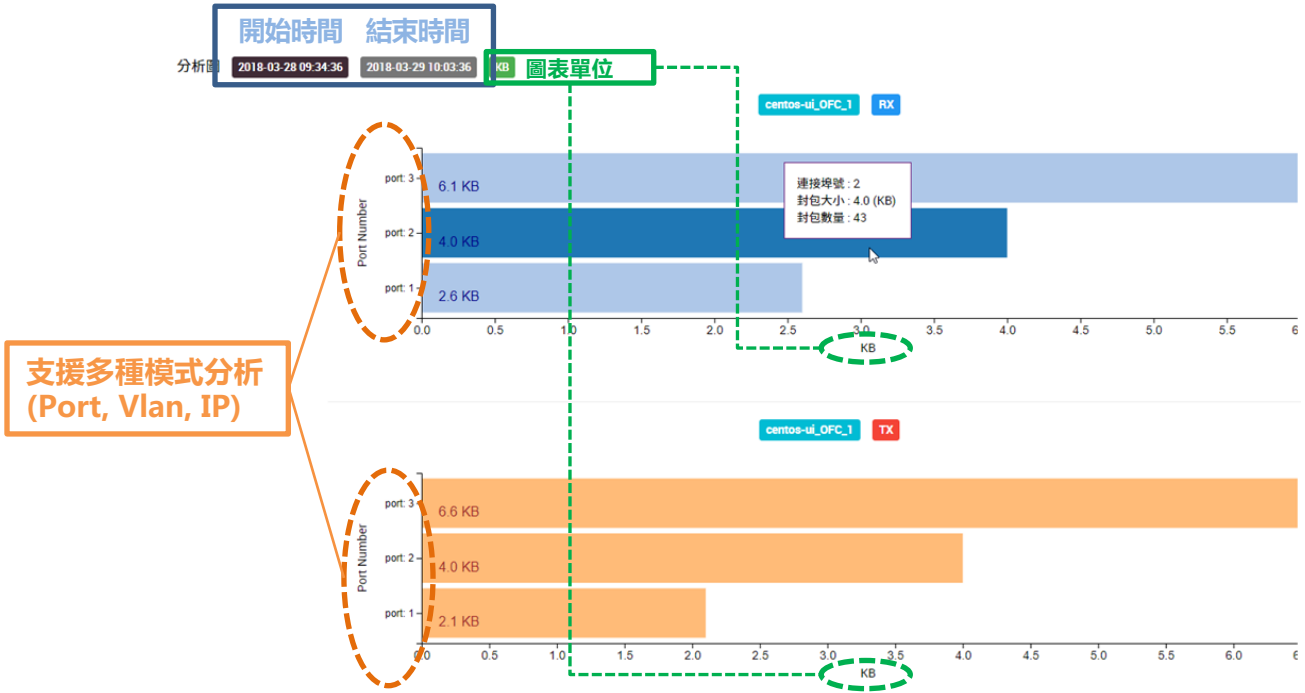
- 可選擇IP、MAC或VLAN
- 即時訊務與歷史訊務





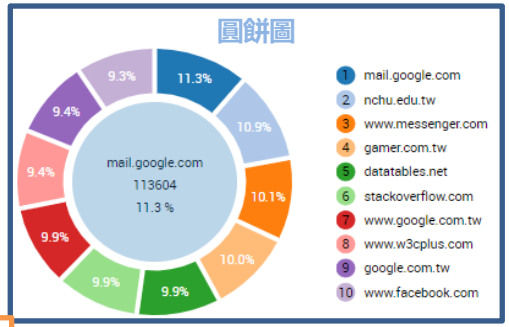
Top-N 流量分析

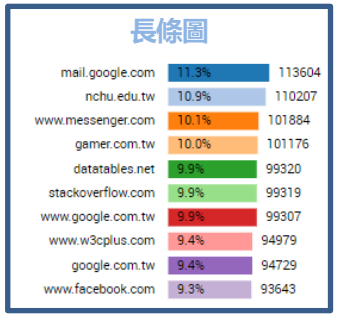
- 即時分析
- 支援多種分析模式(Port, Vlan, IP)
- 圖表單位無需自行換算 (Bytes, KB, MB, GB)
- 精確的時間範圍



Top-N 網址分析

- 即時訊務分析
- 提供圓餅圖、長條圖兩種模式圖表，可依照喜好切換
- 動態供裝DPI服務，可適吞吐量調度服務至小型box或大型伺服器中
- 高乘載能力，視硬碟寫入能力，吞吐量可達3~4Gbps





圖表下方有更詳細的表格

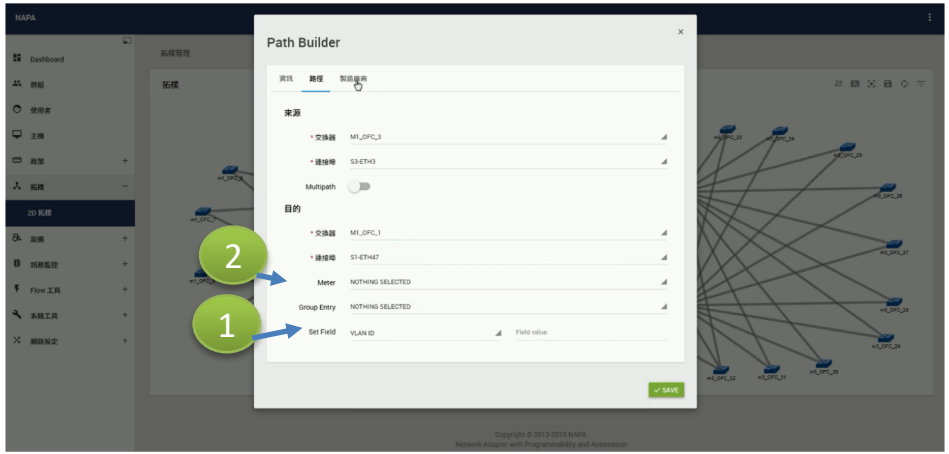
點擊

端對端路徑建立

- 建立Port-to-Port路徑

建立端對端路徑

- 自動計算可行路徑(全部or最短)
- 可套用 VLAN
- 可套用 group entry 和 meter entry



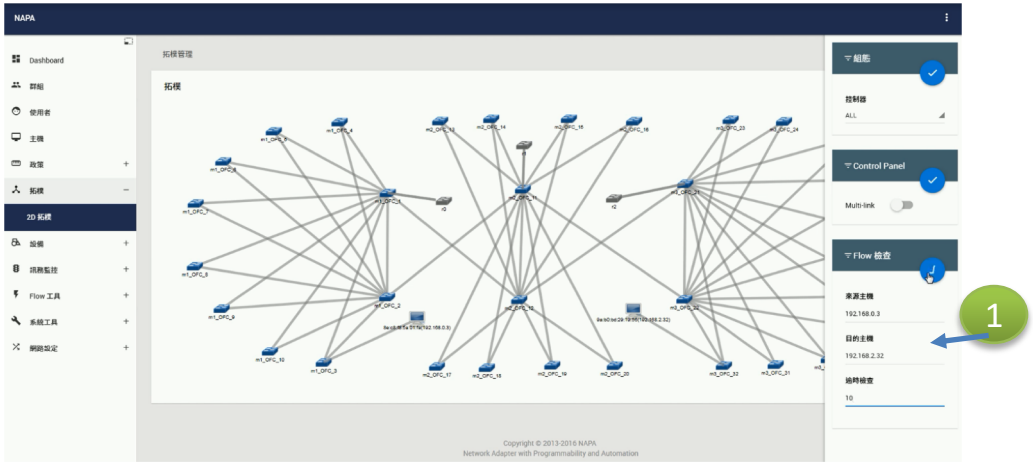
網路障礙查測

- 點對點即時障礙查測

❖ 點對點即時障礙查測

1

- 查測兩終端設備間的障礙發生點
- 透過真實封包傳遞



2 建立多重偵測與監控即時告警機制

CLOUDSEC2018

偵測及警覺隱匿攻擊行為

- 研發多維度關聯分析與巨量資料分析技術，找出發掘緩慢、持續且隱密的控制活動
- 找出攻擊擴散的活動

結合SIEM + 巨量資料分析

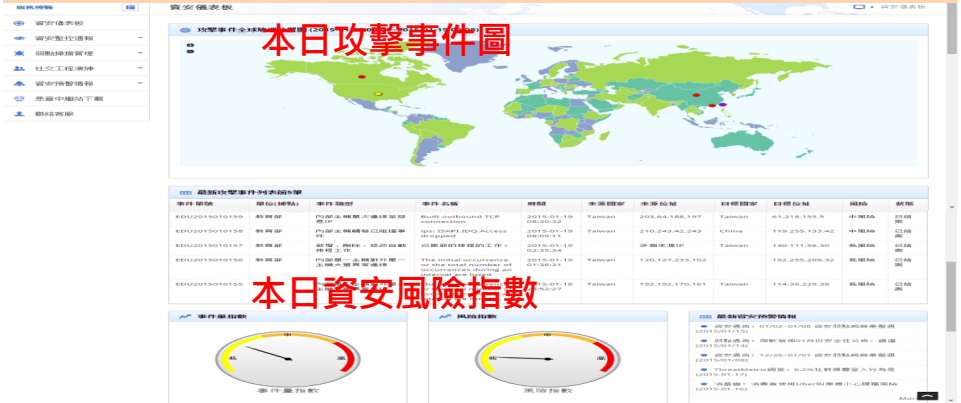
快速回溯偵測

- 當發生國內外重大資安事件時，可在幾分鐘內快速確認半年內是否有相似的攻擊行為

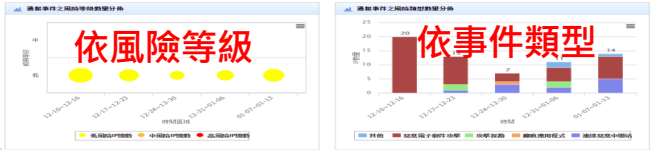
回饋與調適

- 學習長時間日誌資料，自動推薦關聯規則水位，視覺化分析平台
- 依據使用端變更、外部情資與鑑識發現回饋與偵測結果，智慧化地適應運作環境

● 資安風險指數



● 通報事件統計



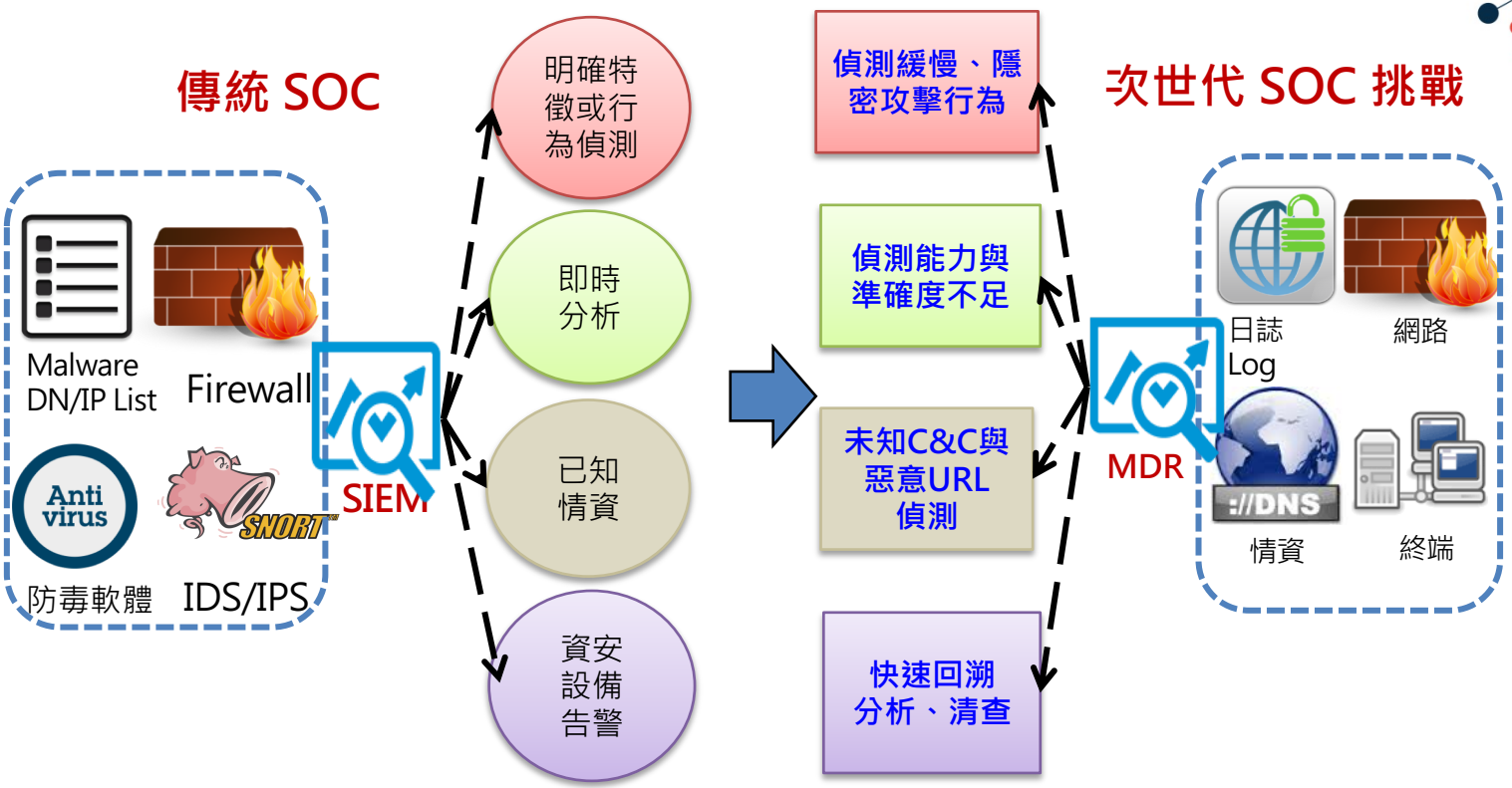
● 通報事件清單

#cloudsec

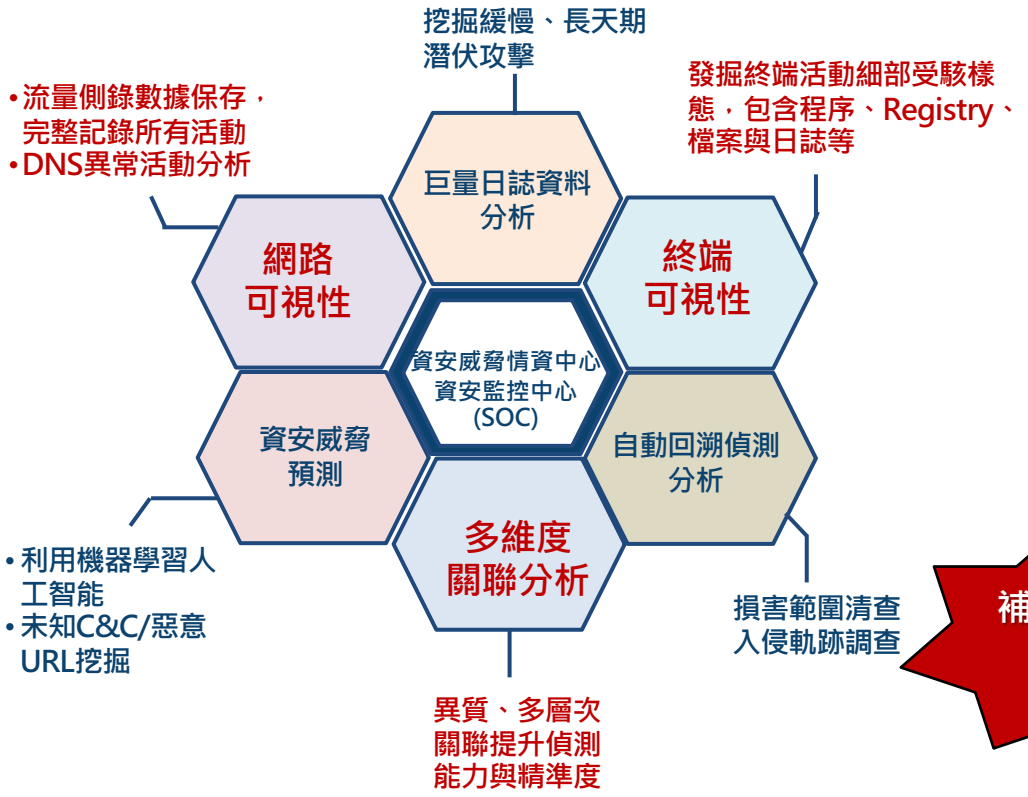
傳統 SOC vs. 次世代SOC

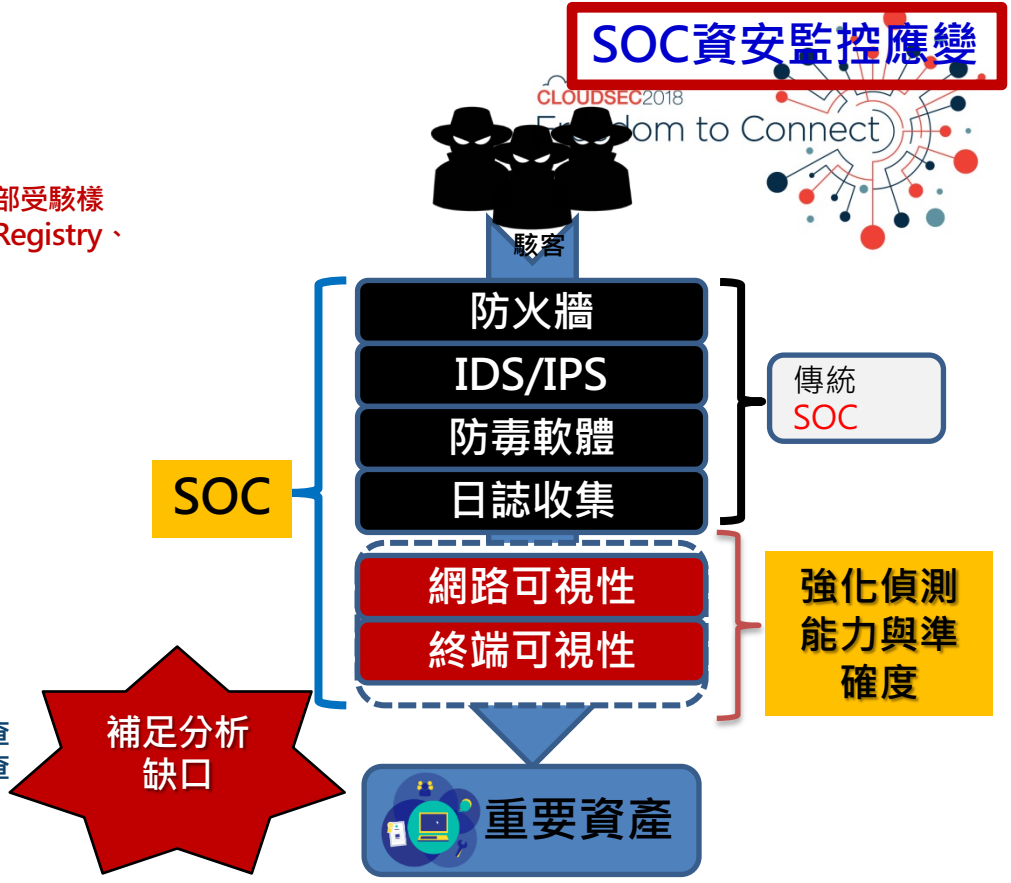
SOC資安監控應變

CLOUDSEC2018 Freedom to Connect



次世代SOC技術



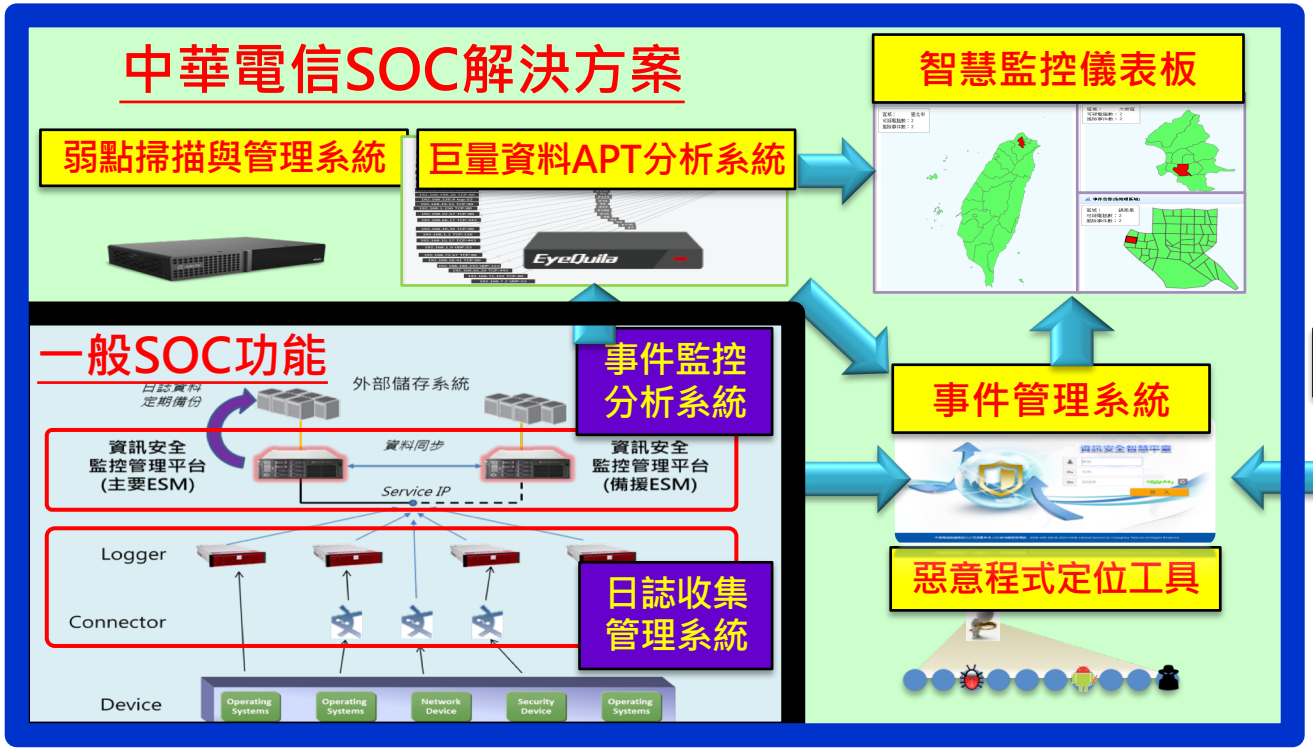


#cloudsec

HiNet SOC資安監控中心

CLOUDSEC2018
Freedom to Connect

■ 除一般SOC功能外，中華電信還提供多項自有資安工具，結合HiNet SOC的經驗、情資與關連規則智慧，協助企業做好資安監控處理



HiNet SOC

7x24資安監控

資安專家
遠端/到場處理

全球預警情資中心

資安鑑識中心

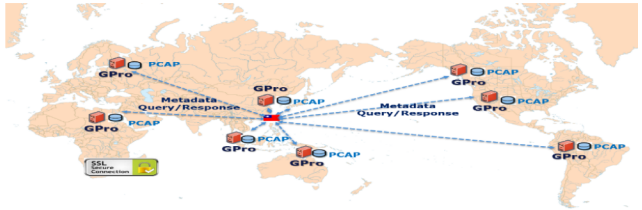
#cloudsec

網路流量側錄分析系統GPro -網路威脅分析儀

資安防禦從被動轉為主動，快速掌握內網安全威脅，從點、線、面全面掌握內網可疑活動，完整歸納資安事件的來龍去脈。

自主研發

- **基礎數據完整收容**
  - 記錄完整網路閘道活動軌跡
  - 提供彈性調閱與檢索機制
- **惡意行為即時感知**
  - 即時監控網路安全狀態
  - 情資導向設計理念，即時標記惡意活動
- **網路流量主動分析**
  - 自動化萃取與分析網路流量
  - 數十項惡意檔案特徵比對模型，建構分群與分類機制
- **機器學習威脅預測**
  - 獨有惡意特徵數學模型
  - 利用機器學習取得未知威脅與疑似受害電腦清單



彈性佈署、集中控管

流量側錄 數據保存 → 人工智能 威脅分析 → 交叉分析 威脅驗證 → 情資共享 區域聯防

核心價值：監控、分析、情資、聯防

GProBox	GProMalwr	GProML	CTIS
巨量網路流量資安分析系統	惡意程式自動化分析系統	資安威脅預測機制	自主性資安威脅情資中心

已部署於**國安單位、政府機關與金融機構**等從事機敏業務單位

#cloudsec

APT潛伏威脅的偵測系統 EyeQuila

- 中華電信**自主研發**的資安產品，專注在**偵測進階持續威脅(APT)與未知威脅**
- 透過網路與資安設備**日誌**分析可能的潛在風險
- 可提供軟硬體整合版本 或 軟體版本產品，可快速擴展的專屬硬體設計

- 使用者可自定搜尋條件
- 智慧搜尋語法提示，快速輸入搜尋條件
- 自動保存歷史搜尋條件，重覆使用重要搜尋目標

長天期巨量資料機器學習

獨家開發的機器學習行為偵測引擎，分析長天期網路活動數據補捉變化緩慢、難以察覺的攻擊行為

自動化回溯偵測機制

EyeQuila自動回溯分析保存的歷史軌跡能清查出曾經遺漏或是過去未曾發現的新型未知威脅

多面向威脅情資整合

可自主擴增情資，介接外部黑名單(開源與商業資安情資來源)

視覺化整合分析統計

視覺化整合，將可疑行為找出攻擊關聯性及範圍，掌握資安威脅的起源及受駭範圍

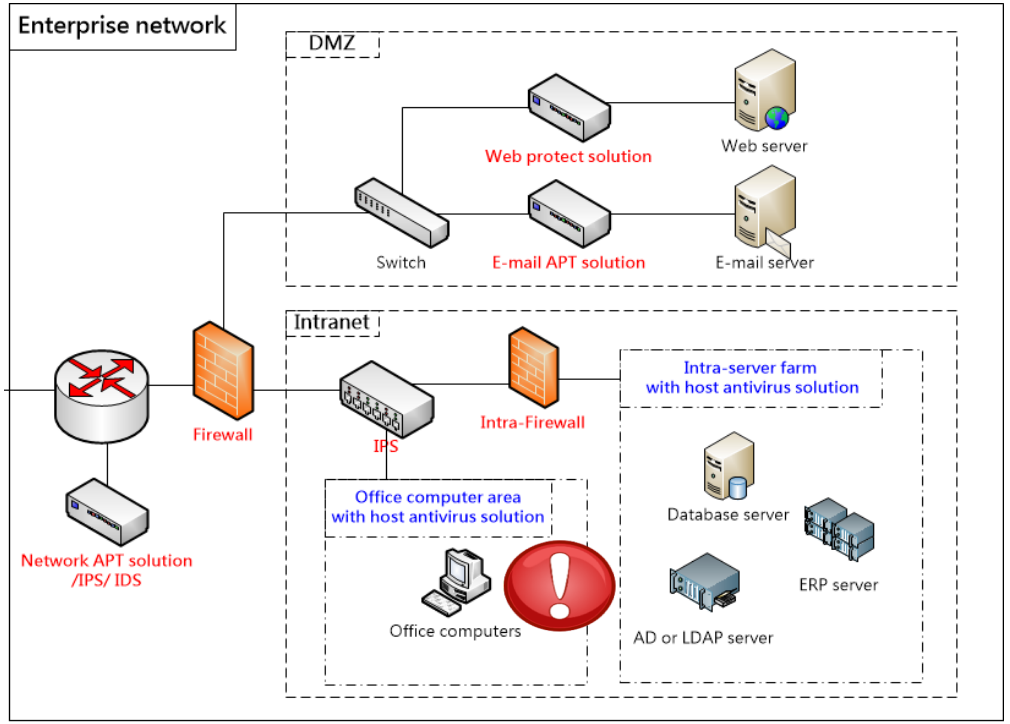
#cloudsec

3 事件發生時，能快速應變處理控制

CLOUDSEC2018 Freedom to Connect

1. **應變與鑑識團隊進場**
2. 分二組平行處理：
   - •收集及確認背景資料
   - •部署監控設施
3. **評估事件可能範圍**
4. 快速篩檢
5. 第一階段控制
6. **深入分析**
7. 第二階段控制
8. 應變與鑑識團隊退場

一天內完成緊急處置、三天內完成範圍控制、
一週內完成整個應變流程，避免延遲導致影響範圍擴大

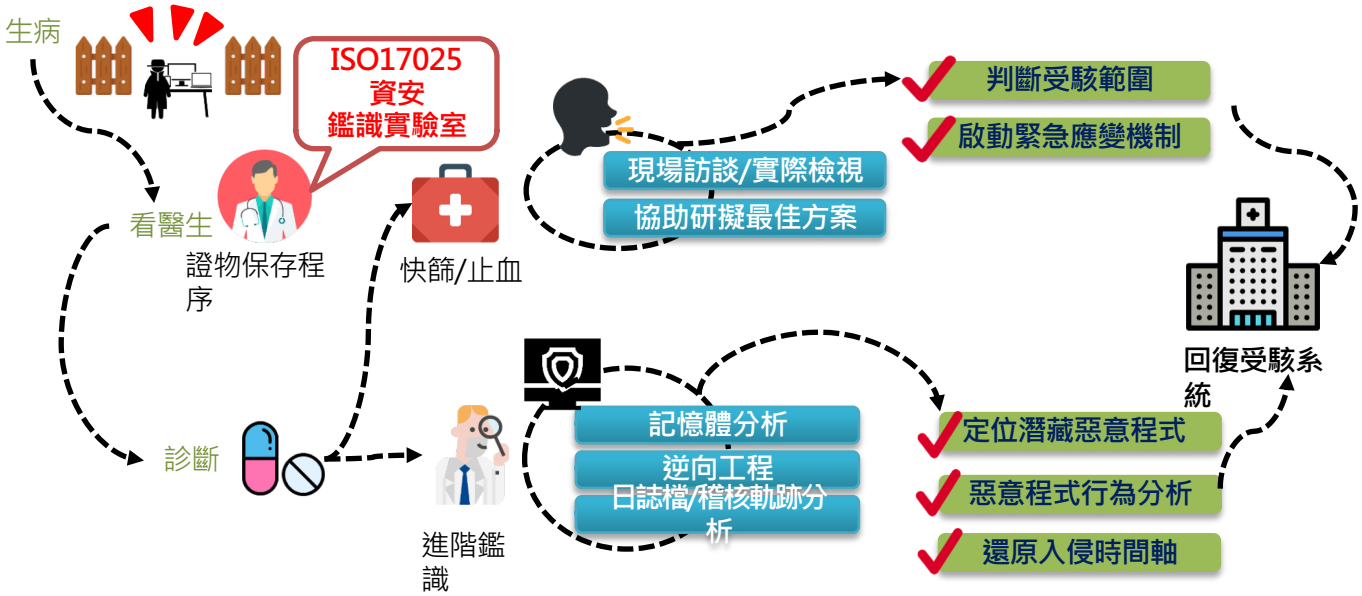


- Red : Common enterprise network security deployment
- Blue : Common enterprise host security deployment

#cloudsec

資安事件處理與鑑識服務

資安事件處理與鑑識是屬於在【資安事件】發生後提供的服務，主要目的是在協助客戶緊急應變、定位入侵管道、評估受影響範圍及回復受駭系統



資安鑑識關鍵能力

自行開發採證工具

- 網路流量檢測工具
- 惡意程式檢測平台
- 各式軌跡蒐證工具

主導多起重大駭客入侵事件調查

- 政府檢調單位委託合作
- 政府機敏單位資安事件
- 金融/高科技業受駭事件

技術能量

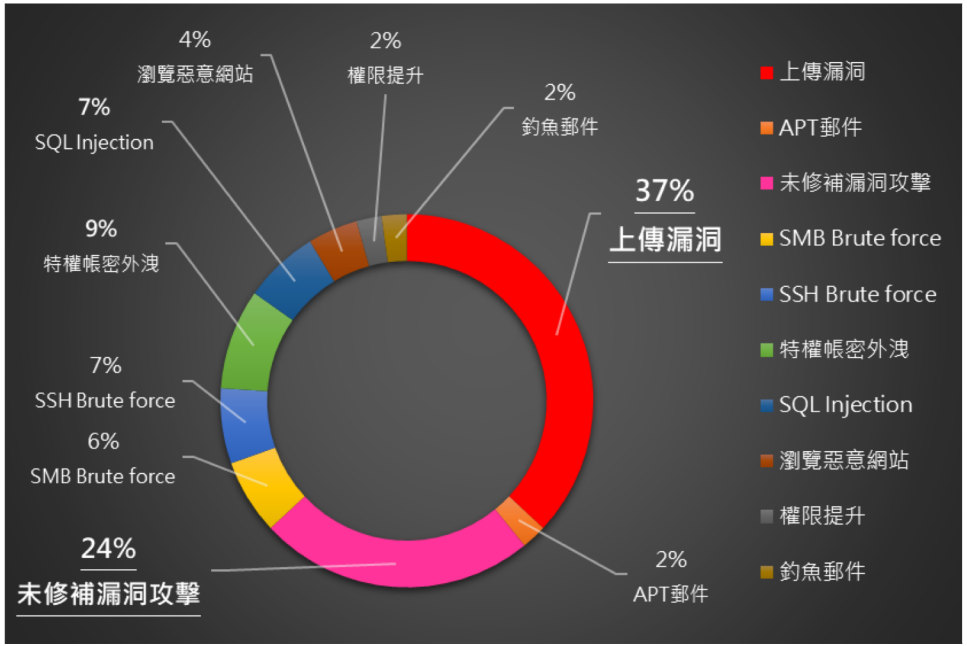
- 逆向工程/惡意程式定位/惡意程式行為分析/記憶體鑑識/軌跡資料分析
- 事前資安事件應變教育訓練
- 受駭系統復原/災後教育訓練
- 實驗室建置輔導/顧問諮詢

ISO 17025 資安鑑識實驗室

- 鑑識結果符合司法調查要求
- 保證證物之完整性

資安事件鑑識統計：入侵管道分析

事故鑑識處理發現入侵管道，自行撰寫或採用第三方套件的檔案上傳功能限制寬鬆，以及未修補漏洞是導致受駭2大主因



統計日期：2017/1/1~2017/12/31

資料來源：CHT Security forensic Team

鑑識案例 -網頁伺服器攻擊事件調查結果

透過日誌檔/OS軌跡分析，確認：
該單位的一台IIS6.0 Server(對外服務網站)為最早受駭主機

透過逆向工程，確認共有連線至3個惡意中繼站：

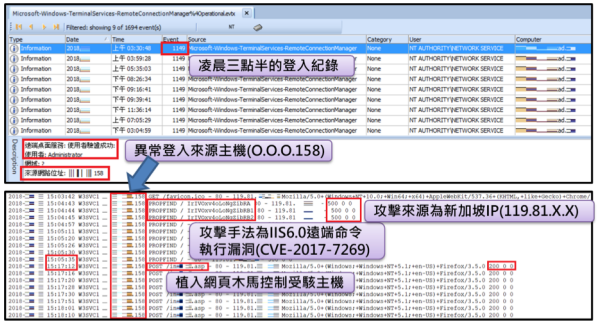
- alibaba[###].wikaba.com
- alibaba[###].zzux.com
- alibaba[###].dynamic-dns.net

透過快篩檢測及日誌軌跡分析發現駭客共打下126台內網主機，並植入惡意程式

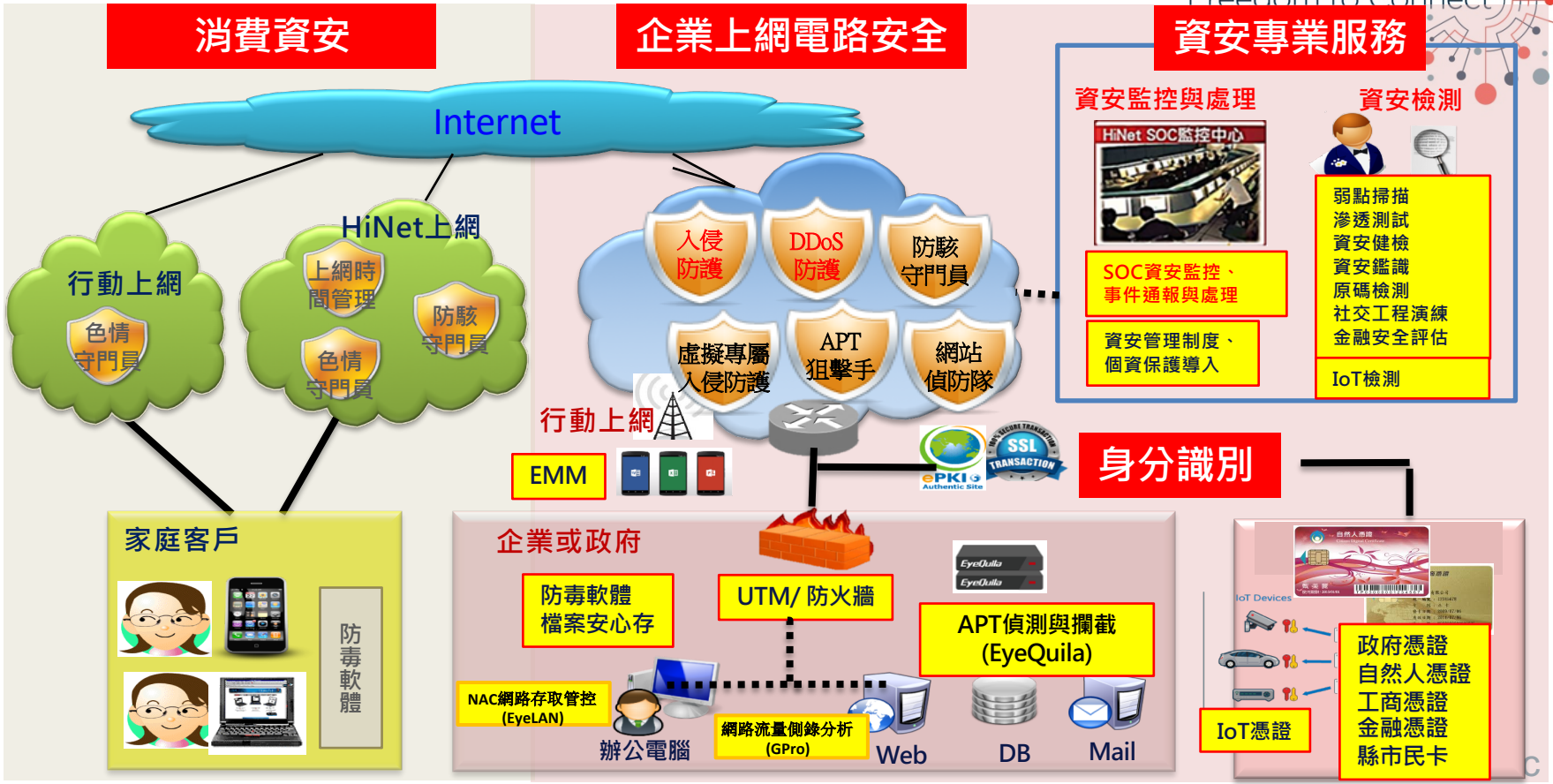
透過記憶體鑑識，發現最早受駭的IIS Server被開啟隱藏的TCP Port 3900

入侵管道:
IIS6.0遠端命令執行漏洞
(CVE-2017-7269)

攻擊來源：
新加坡IP：119.81.X.X



中華電信 – 不只是電信公司，也是專業資安服務公司



CLOUDSEC2018
Freedom to Connect

THANK YOU

王信富 資深資安架構規劃師
中華資安國際