Taipei City Government
Department Of Information Technology

政府資安的挑戰及未來

The Challenge and Future of Government Cyber Security

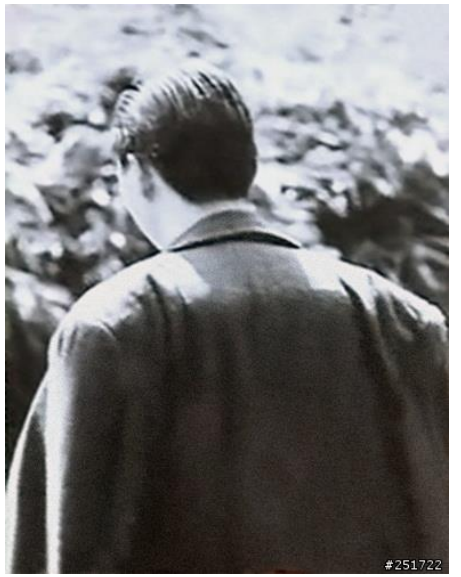
HITCON PACIFIC 2016

李維斌 教授
臺北市政府 資訊局 局長

Dec 2016

李維斌 (Wei-Bin Lee)

臺北市政府資訊局　局長
逢甲大學資訊工程學系　教授
臺北市智慧城市委員會　委員



雲端個人資料保護與應用、資通訊政策與安全管理、資訊犯罪與法律規範、資通安全鑑識與數位證據(ISO27037)

關於臺北市(政府)

- 台灣首都
- 12個行政區
- 2,696,319 市民
- 147 機關, 250 學校
- 65,086 員工
- 1000 系統 (at least)
- IT Budget 25 億 (NTD)

挑戰1: 最大的目標

關鍵基礎設施(CI, Critical Infrastructures)

- 捷運、醫院、水資源、交通號誌…

每月遭受的攻擊

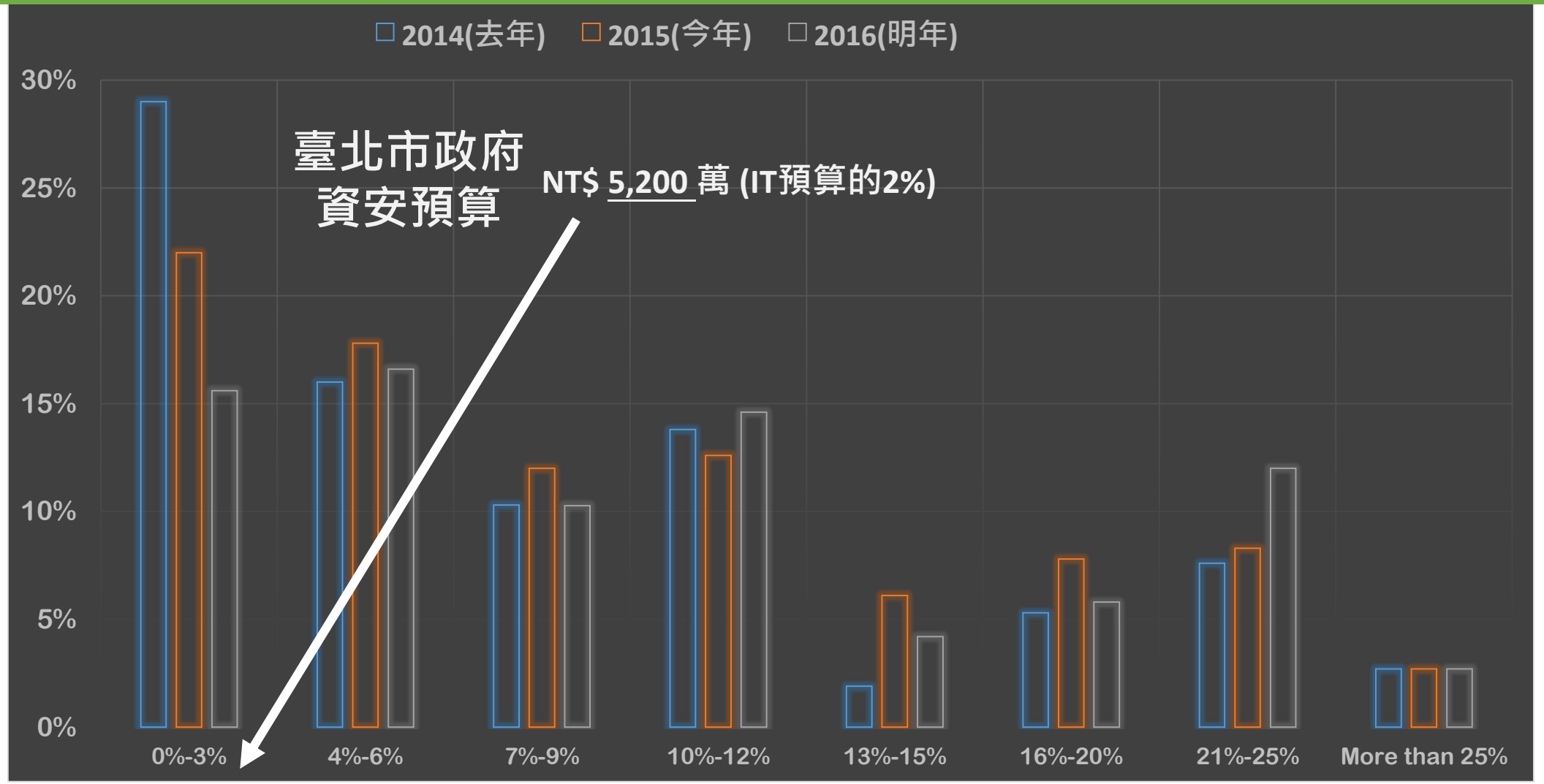
- 防火牆: 2,716,196,562
- 入侵偵測系統: 218,432
- 內容過率設備: 873,519
- 防毒軟體: 153 risks
- 郵件閘道器: 355,744 垃圾信 & 7,350 可疑郵件
- 應用程式防火牆: 11,987

挑戰2: 預算

- U.S: Obama is asking Congress for $19 billion (NT6,261億) in cybersecurity funding, a 35 percent increase.
- U.K: …”The UK will invest £1.9 billion(NT751億) over the next five years in a cybersecurity strategy that will include automatic defences to protect businesses and citizens..”
- Taiwan：
  - 行政院資安預算至少編列8億以上。
  - 2016年8月1日成立行政院資通安全處，首要任務訂定資安專法

挑戰2: 預算

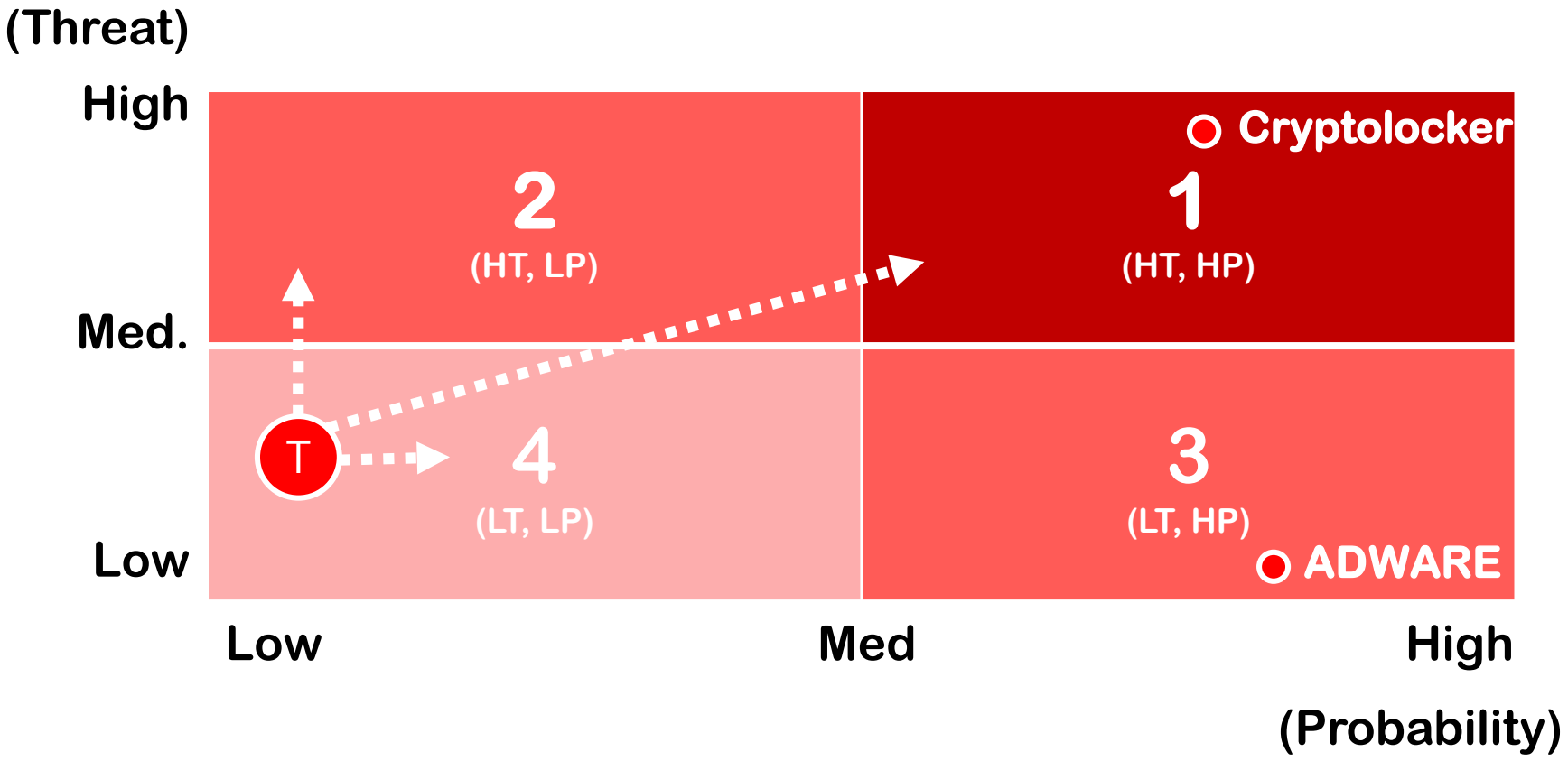
SANS Institute InfoSec Reading Room(2016), IT Security Spending Trends



挑戰3:持續變動的威脅

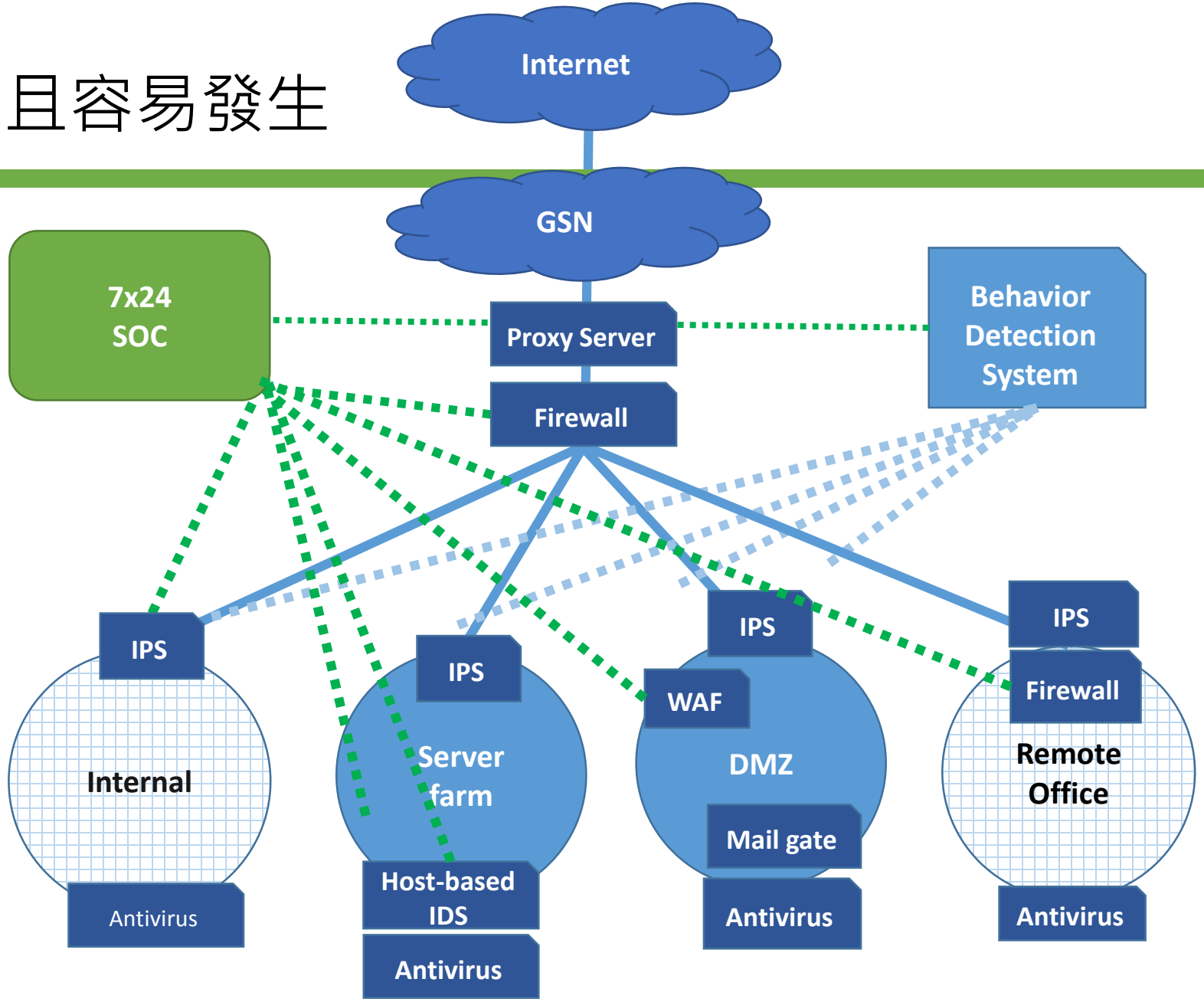
Risk Management

- Threat (Intelligence)x Probability x Asset

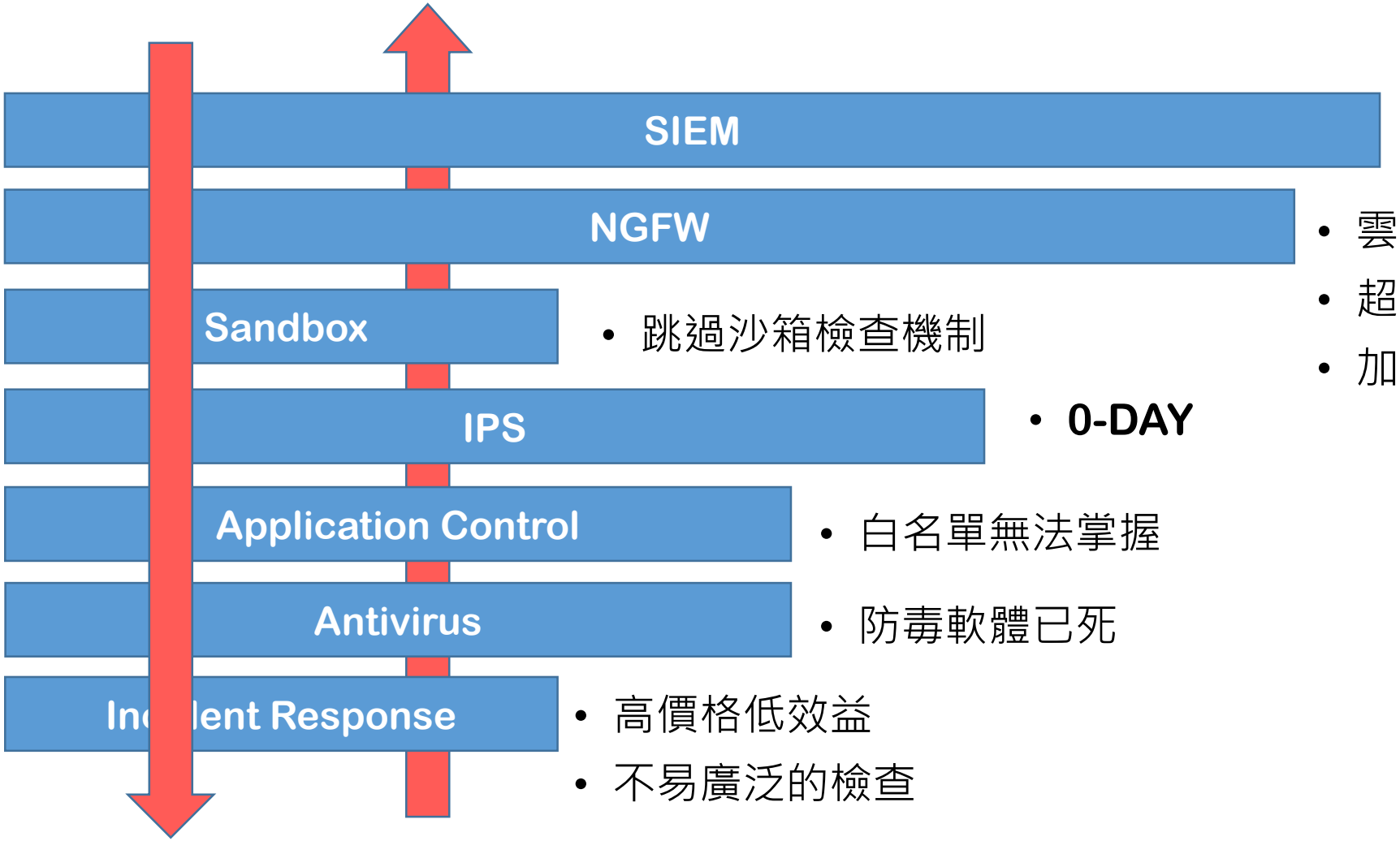


挑戰3.1:危險且容易發生

- 管理面
  - 機關資安等級分級
  - 資訊系統分級
  - ISO27001驗證
- 例行性工作
  - 滲透測試、資安健診
  - 社交工程演練
  - 資安事件通報演練
  - 弱點掃描
- 設備
  - 防火牆、入侵防護系統、APT防護工具

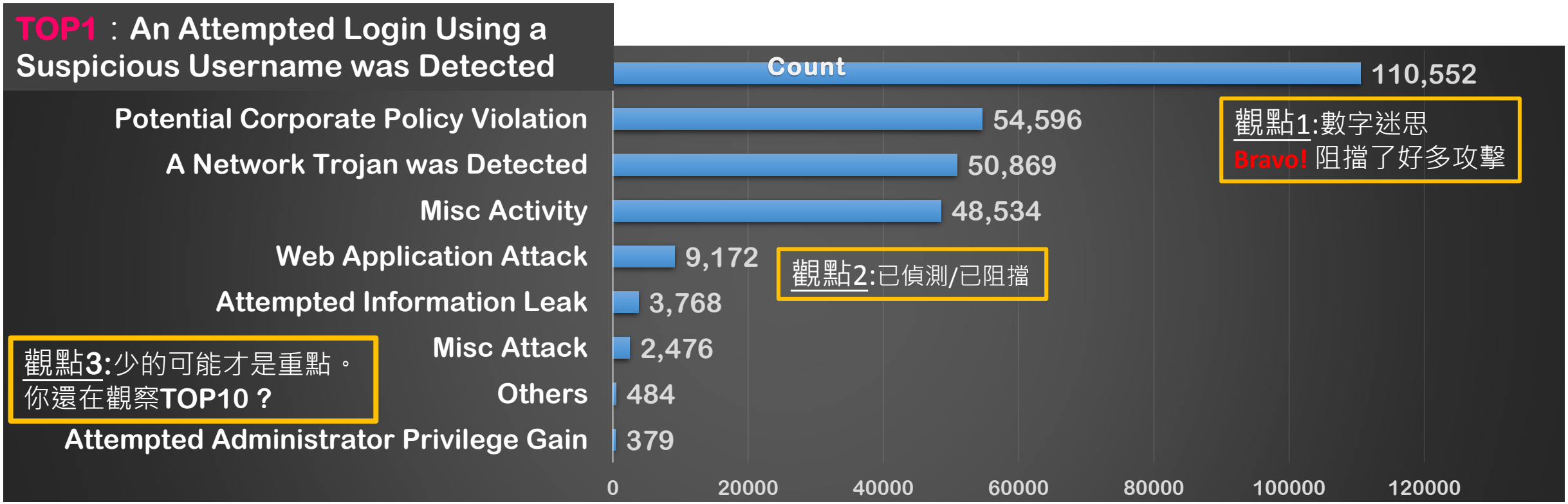


挑戰4: 資安設備各自為政的縱深防護



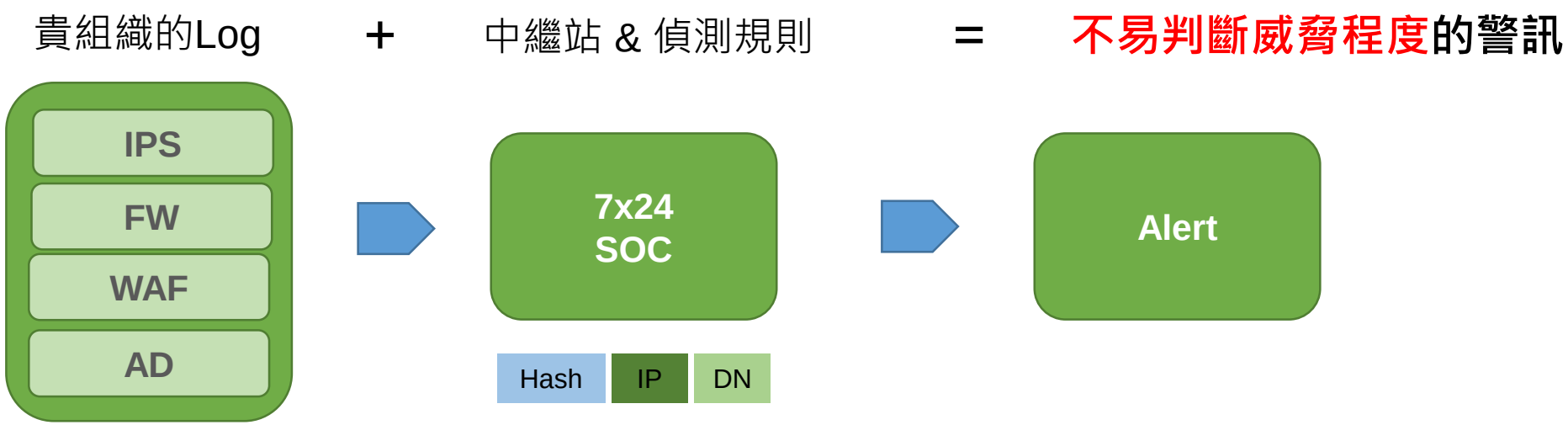
- 資料量過大
- 雲端服務無法管制?
- 超過 5000 條防火牆政策
- 加密流量
- 跳過沙箱檢查機制
- **0-DAY**
- 白名單無法掌握
- 防毒軟體已死
- 高價格低效益
- 不易廣泛的檢查

挑戰5: 大數據(誤)


TOP1：An Attempted Login Using a Suspicious Username was Detected
Count
110,552
Potential Corporate Policy Violation
54,596
A Network Trojan was Detected
50,869
Misc Activity
48,534
Web Application Attack
9,172
Attempted Information Leak
3,768
Misc Attack
2,476
Others
484
Attempted Administrator Privilege Gain
379
0
20000
40000
60000
80000
100000
120000
觀點1:數字迷思
Bravo! 阻擋了好多攻擊
觀點2:已偵測/已阻擋
觀點3:少的可能才是重點。
你還在觀察TOP10？

挑戰5.1: 監控中心

- SOC (Security Operational Center)



挑戰6: 人

- 考科
  - 共通科目：國文、英文、法學知識與英文
  - 專業科目：資通網路、程式語言、資料結構、系統專案管理、資料庫應用、資訊管理與**資通安全**。
- 擲筊
  - 職缺 **<>** 專長
  - 志願用名次決定
  - 進來看機關安排
- 我們有廠商(迷之聲:但只是想賺我們的錢)
  - 願意用多少價錢聘請一個專業資安人員**?**

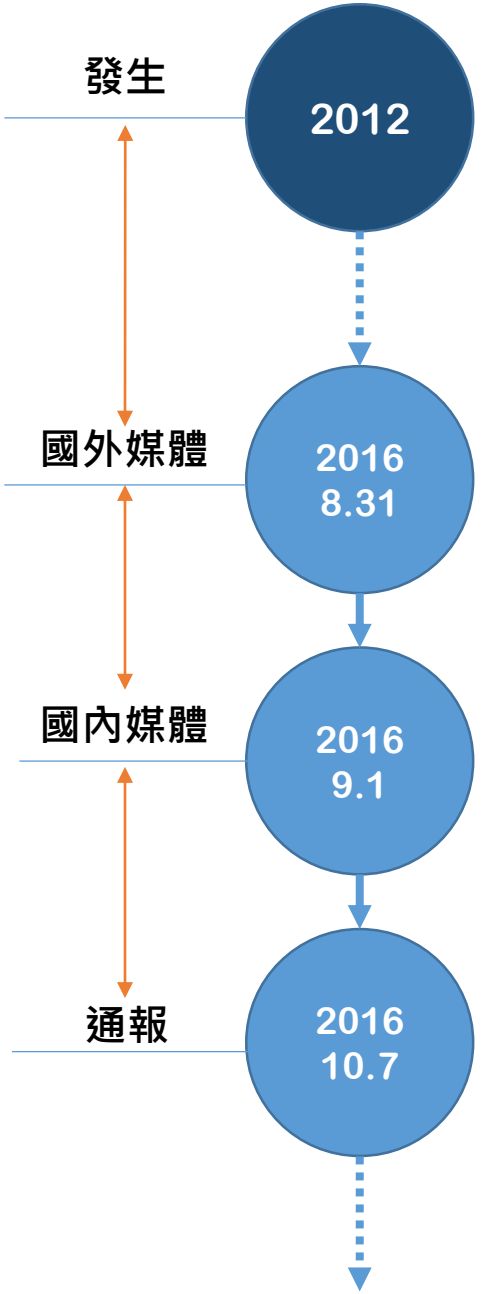
挑戰7: 跟時間賽跑

發現問題的時間，是判斷威脅程度的要件之一。

- **Mandiant:53**%外部通告入侵事件、**47**%內部發現入侵事件
- 外部通知約**320**天、內部探索**56**天

Dropbox hack leads to leaking of 68m user passwords on the internet

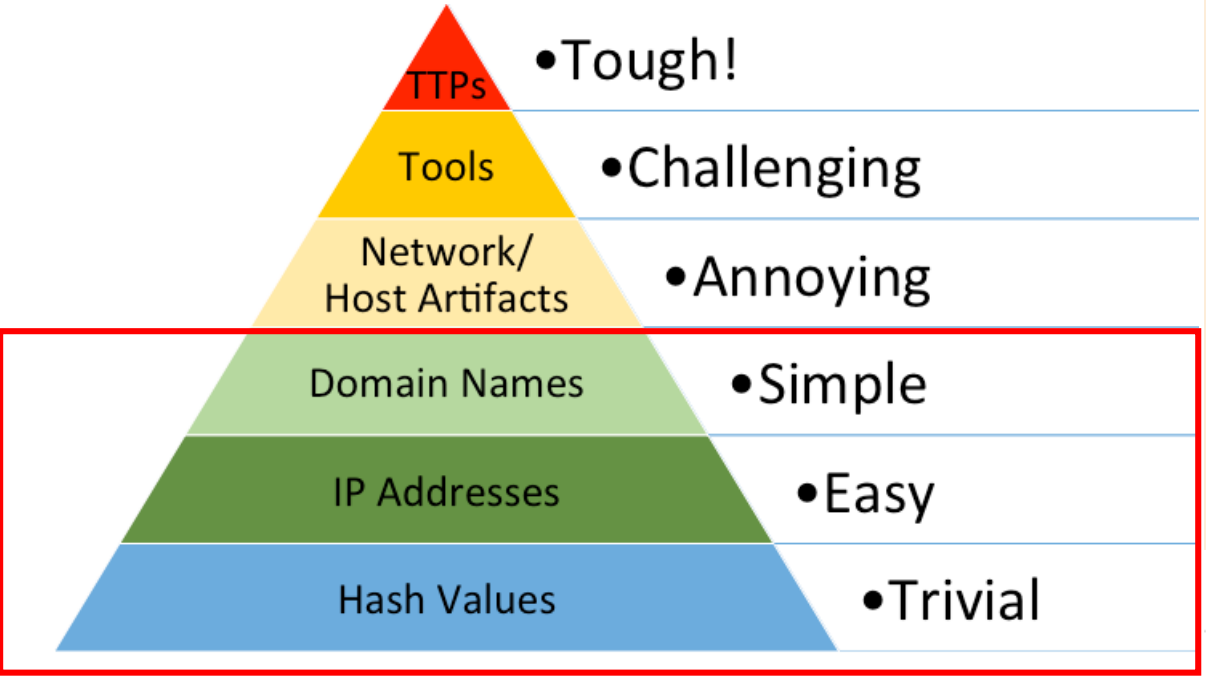
Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked



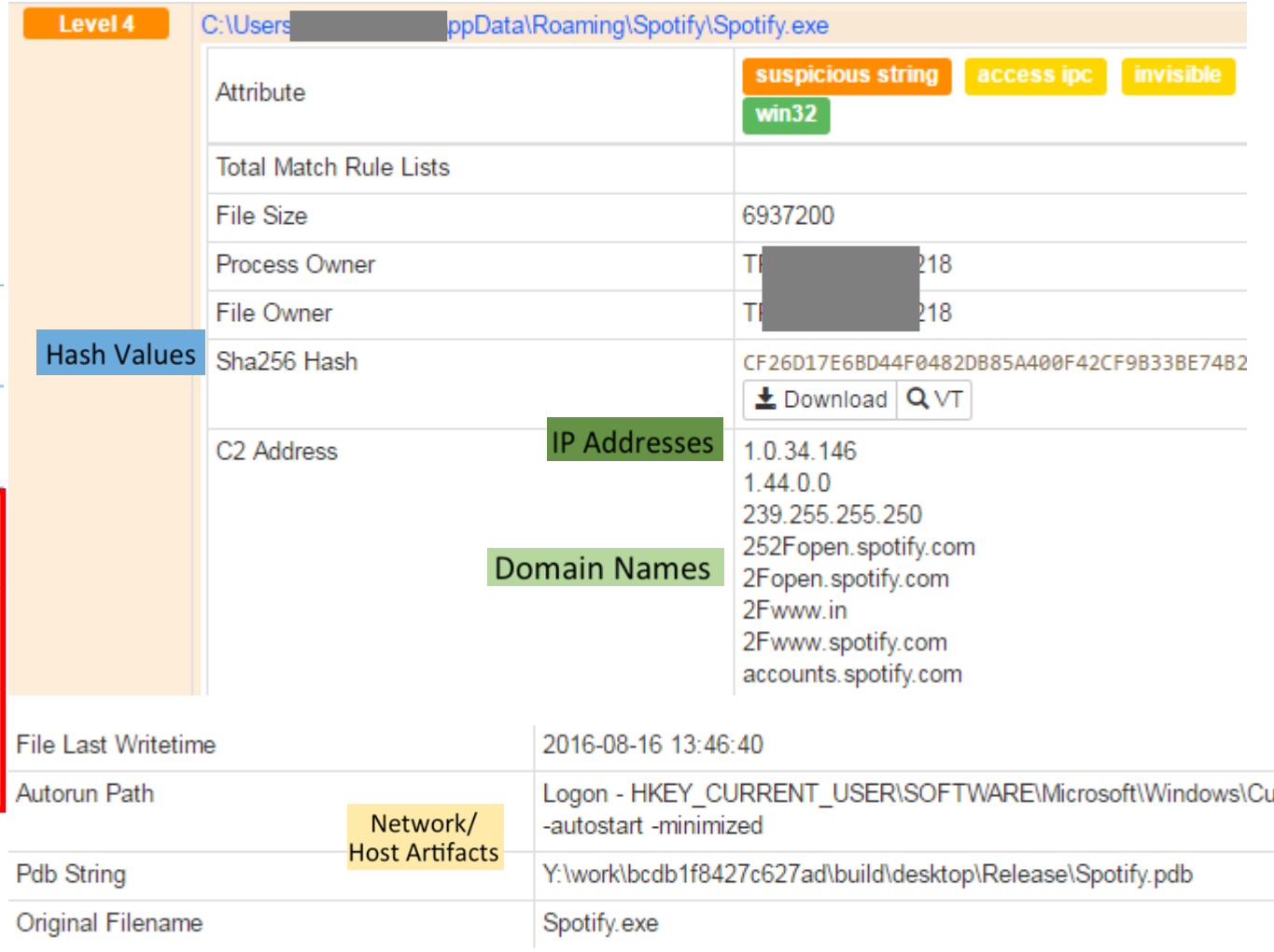
未來1: 最大的目標

- 機關資安等級分級已經將具備「關鍵基礎設施資訊系統」的機關列為A級。
  - 較多的應辦事項。
  - 較多的資安預算。
- 遭入侵已經無可避免，快速掌握問題，即時回應才是重點。

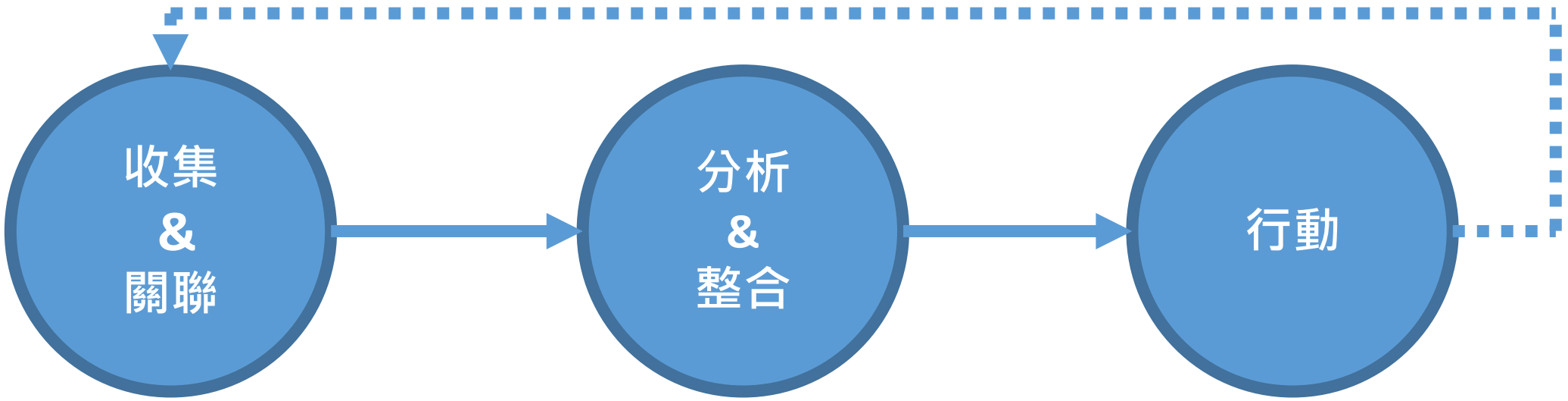
(駭客的)痛苦金字塔



Source: David Bianco, "The Pyramid of Pain," Enterprise Detection & Response, January 17, 2014 (detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html)



未來2:威脅情資分析



Hash IP DN

內部 + **外部**情資

- 資料格式
- 流量及端點可視性
- 社群情報

TTPs Tool

- **IR**分析
- 攻擊路徑
- 族群分析

- 策略層規劃
- 回應計畫
- **回饋規則**

建立屬於「自己」的情資

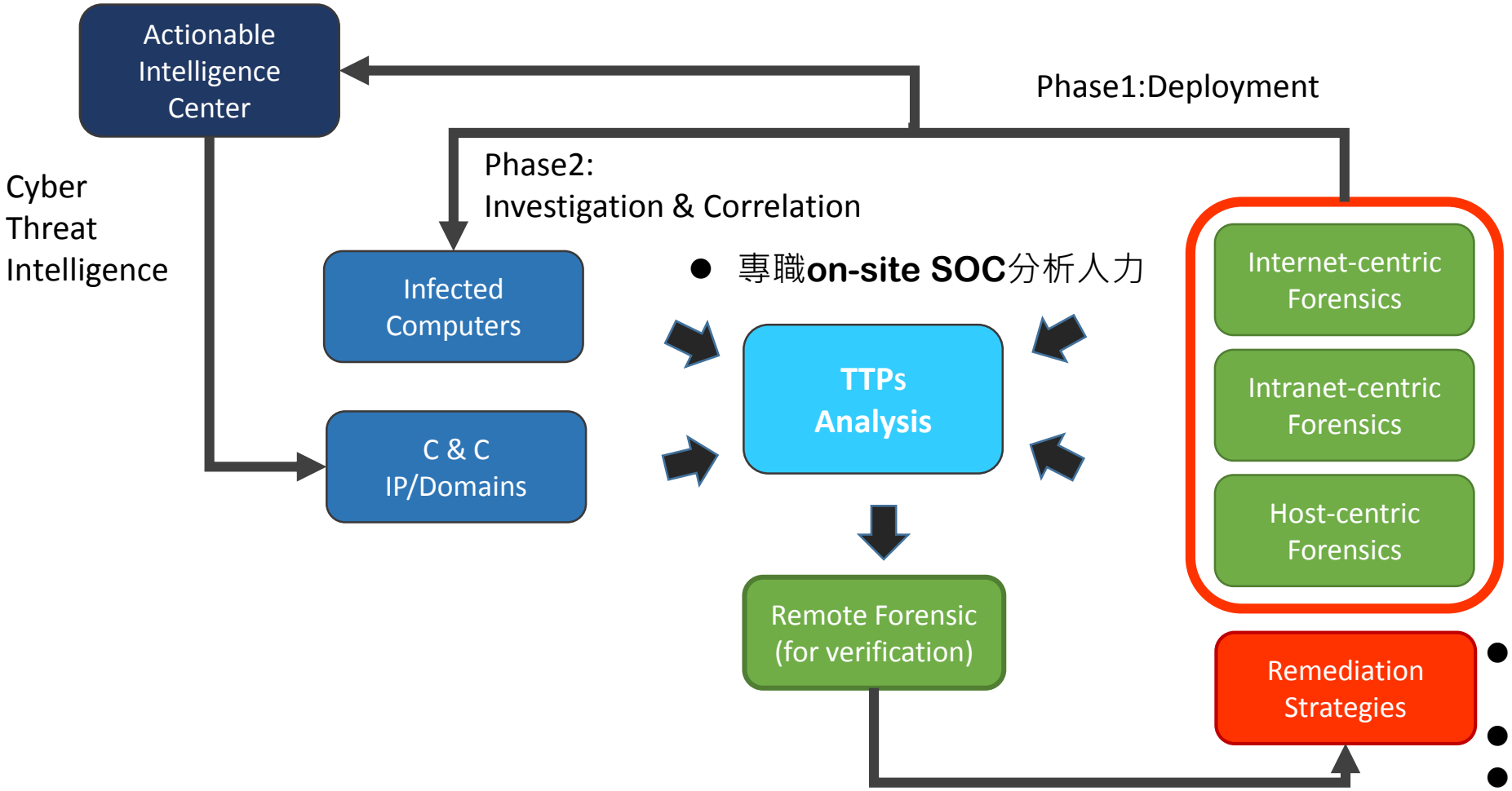
- 情資有「地區性」，別人的情資是借鏡 <>你的情資
- 情資的豐富性
  - 組織設備的Log OR 組織內的流量
  - 暗網的情報、媒體的情報、BitTorrent的監控
  - 內部資產的弱點資訊(版本)搭配即時的威脅
  - 惡意程式的分析報告
  - 自己威脅情資種子(DN、IP、HASH)
  - 中繼站的分類(廣告、過時的C&C、真正的APT)→決定處理的等級

未來3:預算、人

- 場域、橋樑、多贏
- 相信專業：增加專職資安駐點人力
- 給空間
- 多POC
- 多合作

結論

- 合作



- 濾掉不用看的流量，減少資安設備流量，降低成本
- 加密流量進行解密
- 彈性的網路架構

謝 謝