

# 資訊安全面面觀

- 掌握趨勢、認識敵人、瞭解自己、迎戰未來

林峰正

GWAPT, ECSA, CEH, CHFI

2018/9/11



中華資安國際

CHT Security

# 大綱

- 掌握趨勢：資安威脅與觀察
- 認識敵人：從實際案例瞭解駭客
- 瞭解自己：盤點企業防護盲點
- 迎戰未來：化被動為主動迎擊

# 掌握趨勢

- 資安威脅與觀察



中華資安國際

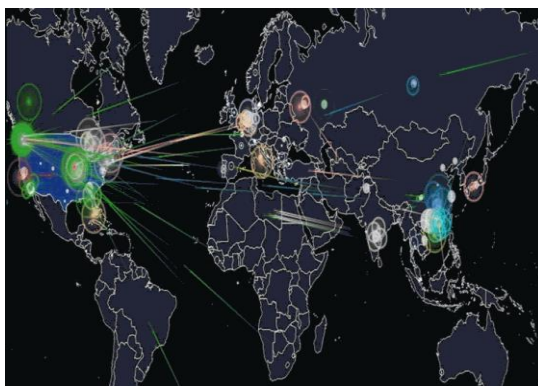
# 2018年台灣面臨的資安威脅



**勒索軟體、綁架挖礦**全球肆虐，  
<2017年攻擊次數增加了**90%**>  
<2018挖礦攻擊程式大增**1,189%**>



**ICS 工業控制系統**被駭威脅落地  
<關鍵基礎、高科技陸續遭駭>



**DDoS攻擊**癱瘓網路運作  
<攻擊次數較去年同期**成長4倍**>



**APT目標式**攻擊事件頻繁  
<1/131郵件夾帶惡意附件>

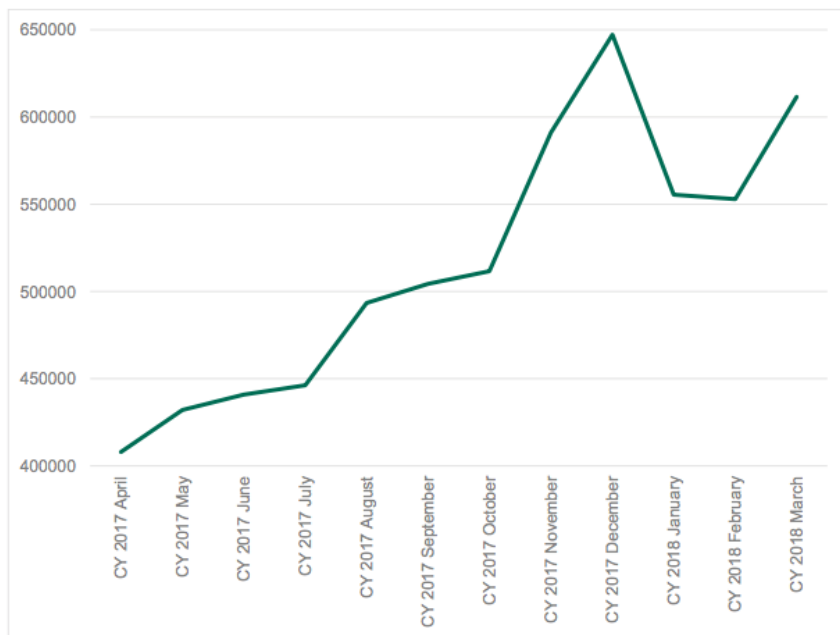


**IoT物聯網裝置**受駭頻傳  
<台灣裝置被駭數量為**亞太第4**>

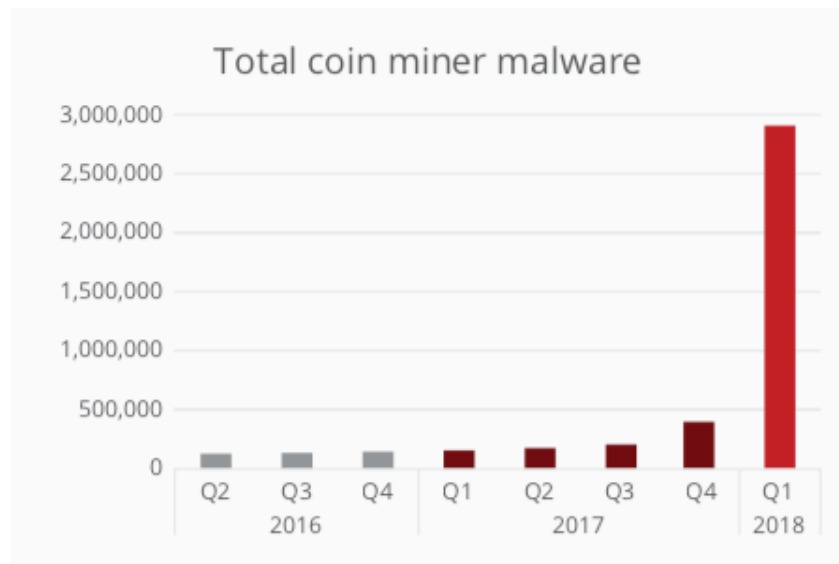


**網站仍最易被駭客攻破**  
<73%以上可被入侵>

# 挖礦惡意程式數量快速成長11倍



資料來源: Kaspersky Lab

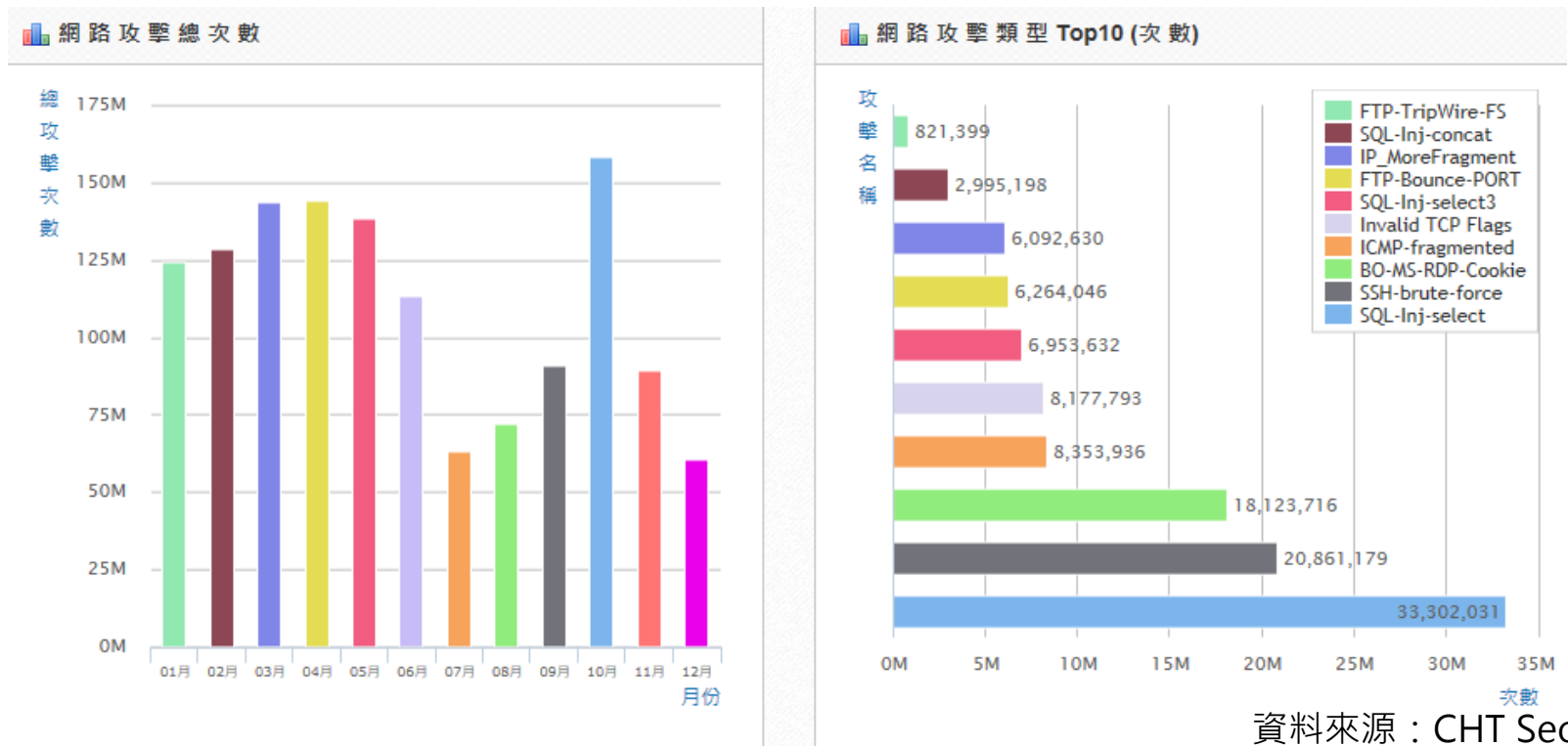


Source: McAfee Labs, 2018.

資料來源: McAfee Labs

- 勒索軟體已發展成為勒索軟體即服務(RaaS)商業模式，且攻擊目標多元-關鍵基礎設施、醫療、企業生產線等高價值產業
- 從2017/04至今挖礦惡意程式數量快速上升，2018年Q1的挖礦惡意程式新增比率高達**1,189%**
  - 因破壞力較低，使用者較難發現，讓駭客趨之若鶩，也呈現出近年來攻擊活動已經是以金錢獲利(Monetize)為導向的趨勢

# 網路攻擊樣態觀察



- 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**

# DDoS攻擊次數激增4倍

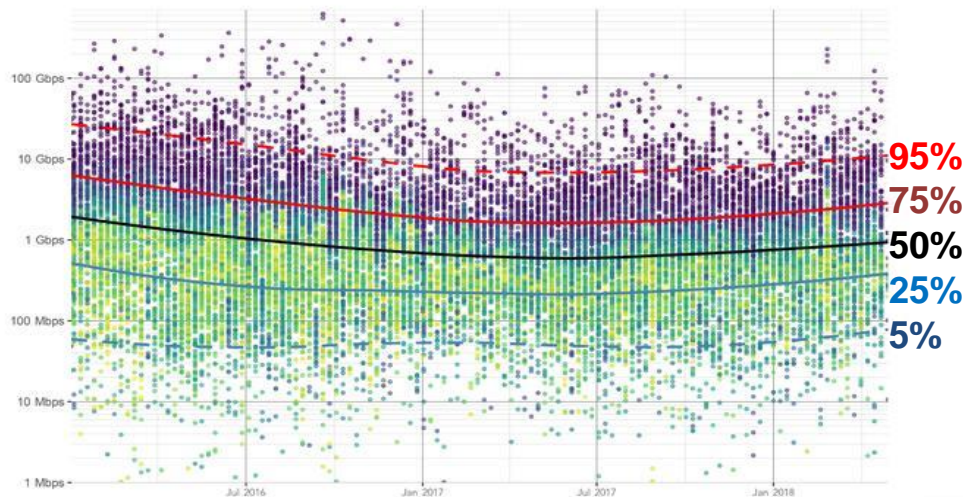
## 全球 DDoS攻擊趨勢(2018 Q2) :

- 受駭IoT設備形成的Mirai Botnet仍持續活動，衍生出許多變種惡意軟體
- 2018Q2攻擊次數增加(YoY增加**16%**)，最大攻擊流量達**1.7 Tbps**
- 新攻擊手法為Memcached UDP 反射放大攻擊，可將流量放大**萬倍**以上
- 高PPS(Packet Per Second)流量嚴重影響網路及資安設備效能，需注意此類攻擊手法

## CHT Security SOC 觀察(2018 Q2) :

- 國內2018 Q2 平均每天發生約**449次**攻擊，較2018 Q1 成長**491%**，為2017年Q2的**3.8倍**
- 最大攻擊規模為**101 Gbps**，**UDP Flooding**為大宗
- 攻擊對象偏重**資通信**、**製造業**、**政府機關**，其次為**遊戲業**、**學術教育業**、**金融保險業**等
- 2018/5 國內首家販售DDOS攻擊服務商「TWDDOS」網站，遭調查局法辦，查扣主機紀錄中發現，曾對國內外網站發動2萬餘次攻擊。

Attack Density Trends - Summer 2018

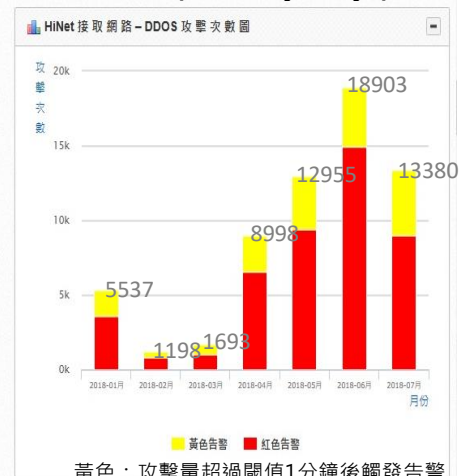


來源: Akamai Summer 2018 State of the Internet

HiNet DDoS最大攻擊流量  
(2018 Q1~Q2)



HiNet DDoS攻擊次數  
(2018 Q1~Q2)



黃色：攻擊量超過閾值1分鐘後觸發告警  
紅色：告警後2分鐘仍超過閾值



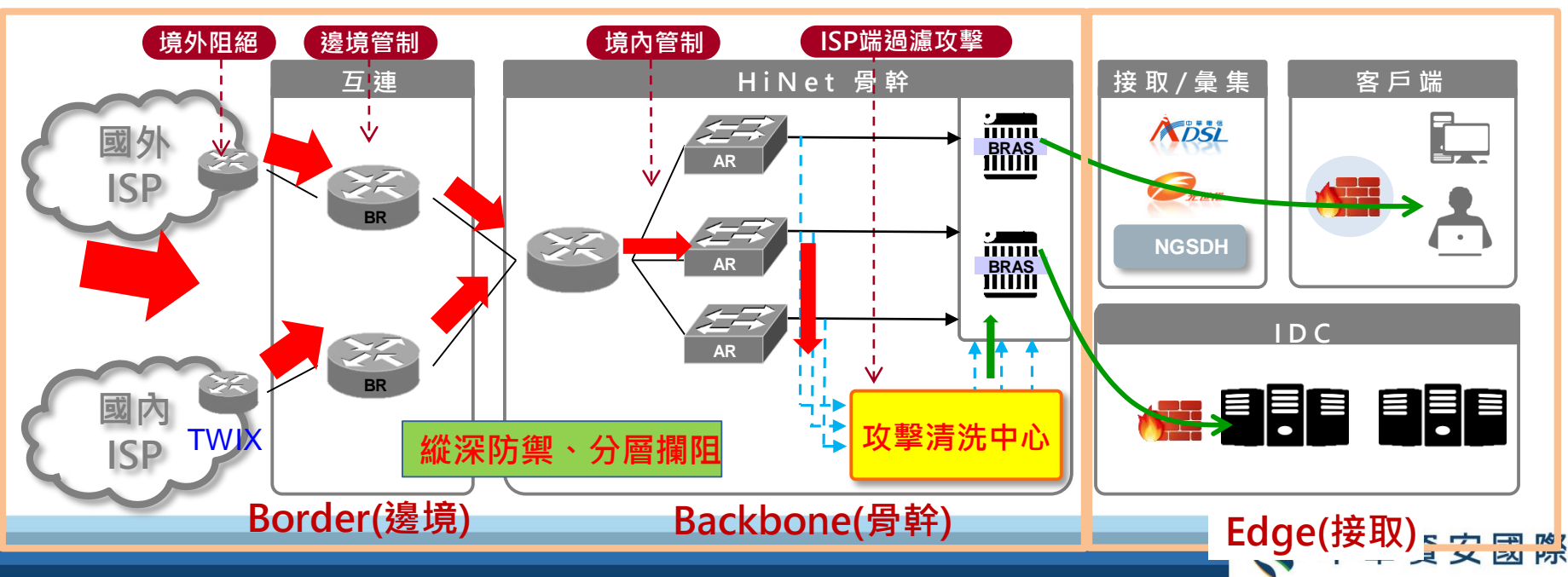
中華資安國際

# DDoS攻擊 – 因應之道

## 多層次阻擋/隔離/清洗來過濾攻擊

- ▶ **Border :**
  - ▶▶ 境外阻絕：呼叫Tier-1 ISP聯防，攔阻攻擊訊務於境外
  - ▶▶ 邊境管制：管制符合攻擊IP的訊務
- ▶ **Backbone :**
  - ▶▶ 骨幹管制：管制符合攻擊特徵IP的訊務
  - ▶▶ 隔離清洗：過濾攻擊訊務
- ▶ **Edge :**
  - ▶▶ 於企業端閘道/端點資安防護

1. 偵測異常訊務量
2. 辨識攻擊來源、攻擊手法
3. 啟動應變措施，多層次攻擊阻擋  
清洗過濾機制，迅速恢復服務
4. 定期演練，模擬攻擊、防禦應變





# 認識敵人

- 從實際案例瞭解駭客



中華資安國際

# 駭客的目的

金錢利益

政治意圖

商業機密

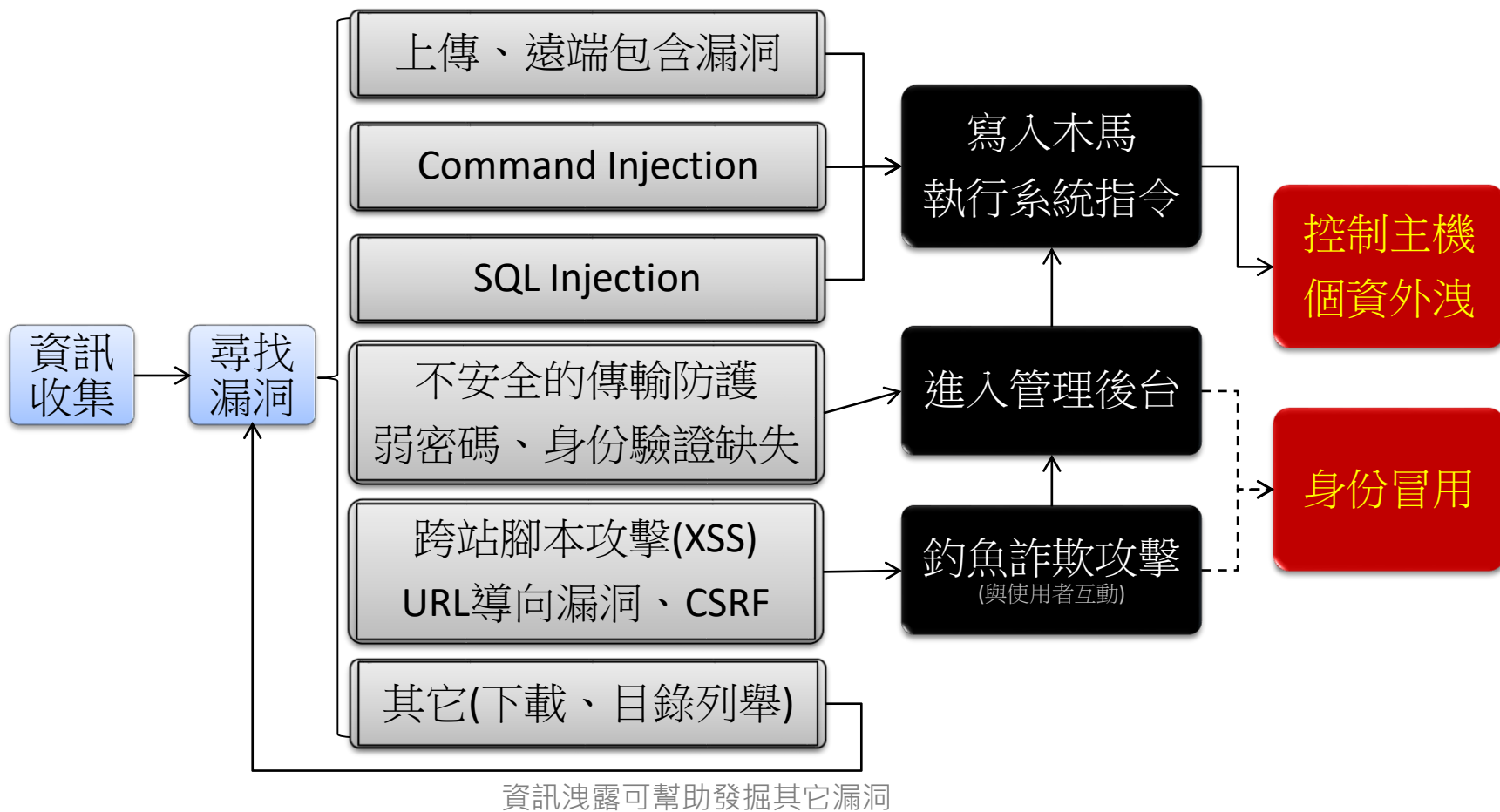
樂趣

練習

研究



# 一般伺服器入侵流程



# 高風險歷史排行榜

## 滲透測試高風險漏洞歷史統計

- 1 跨站腳本攻擊(XSS)
- 2 SQL注入攻擊
- 3 權限跨越
- 4 任意檔案上傳
- 5 弱密碼
- 6 下載弱點
- 7 IIS tilde 目錄列舉弱點
- 8 未經驗證的轉址與導向功能
- 9 目錄遍歷攻擊
- 10 敏感資訊洩漏

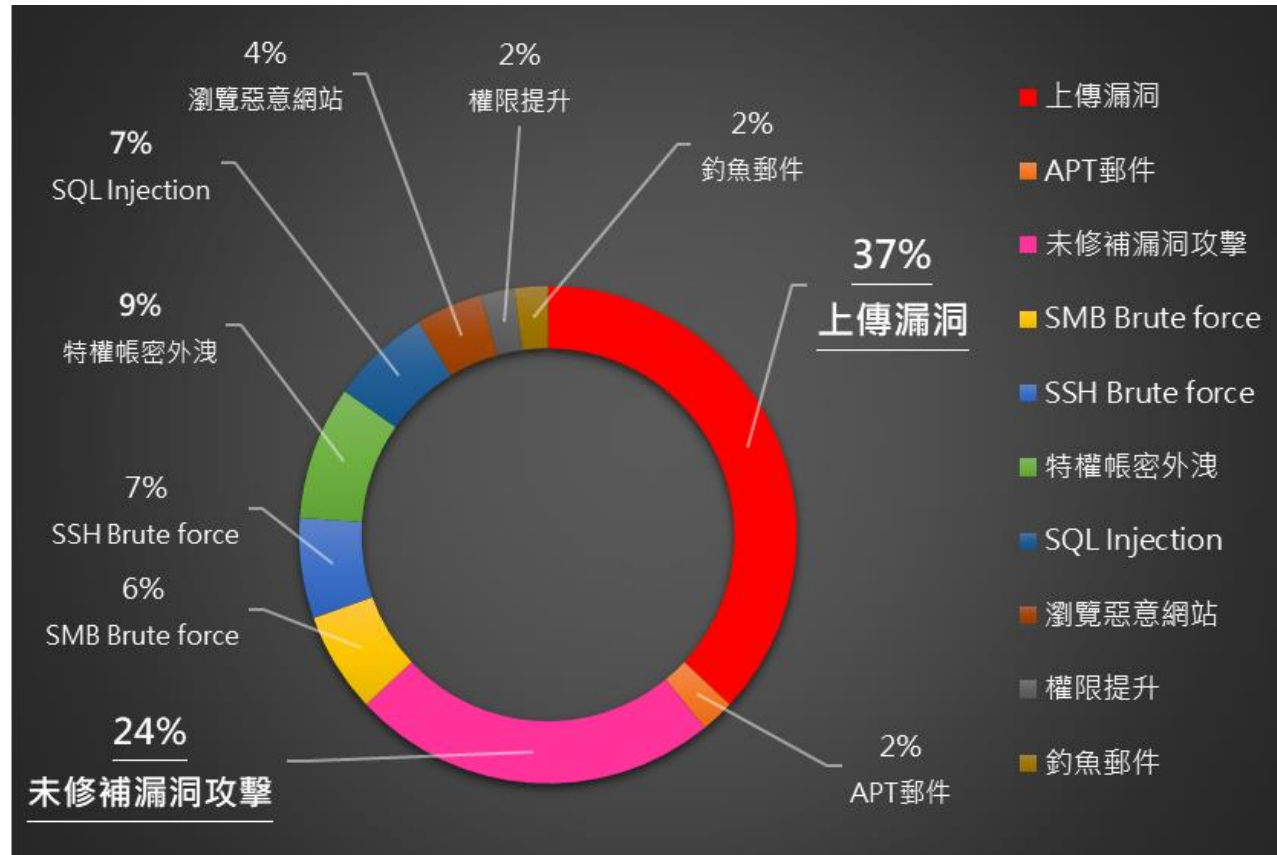
在所有受測系統中...

- ✓ **28%**的系統發現 跨站腳本攻擊
- ✓ **17%**的系統發現 SQL注入攻擊
- ✓ **13%**的系統發現 權限跨越
- ✓ **7%**的系統發現 任意檔案上傳



# 入侵管道觀測與分析

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

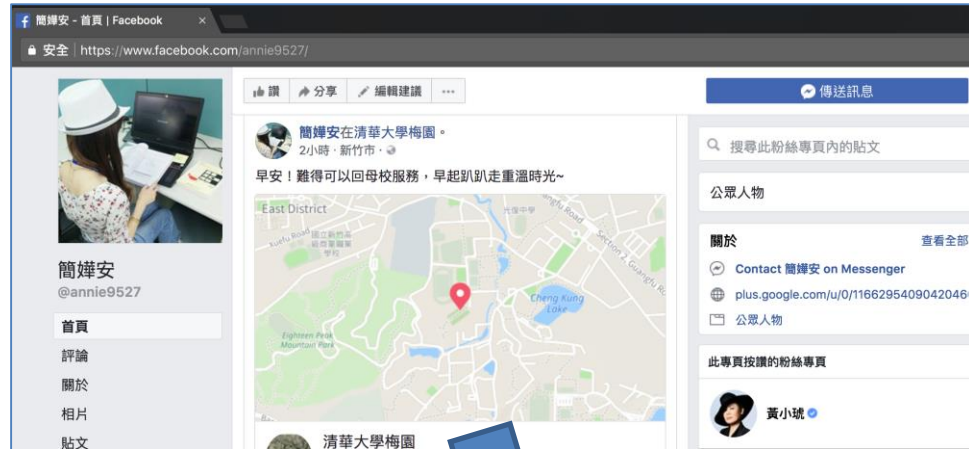
# 案例1、紅隊演練利用社交工程入侵

 中華資安國際  
CHT Security

 中華電信 關係企業

**簡燁安 Annie Jian**  
開發工程師 Development Engineer

中華資安國際股份有限公司 CHT Security Co., Ltd.  
TEL | +886 2 2343 1628 ext 9527 FAX | +886 2 2396 9527  
EMAIL | service@chtsecurity.com 統編 | 55765649



簡燁安 - 首頁 | Facebook  
安全 | https://www.facebook.com/annie9527/

簡燁安  
@annie9527

簡燁安在清華大學梅園。  
2小時 · 新竹市 ·  
早安！難得可以回母校服務，早起趴趴走重溫時光~

East District  
Cheng Kung Lake

清華大學梅園

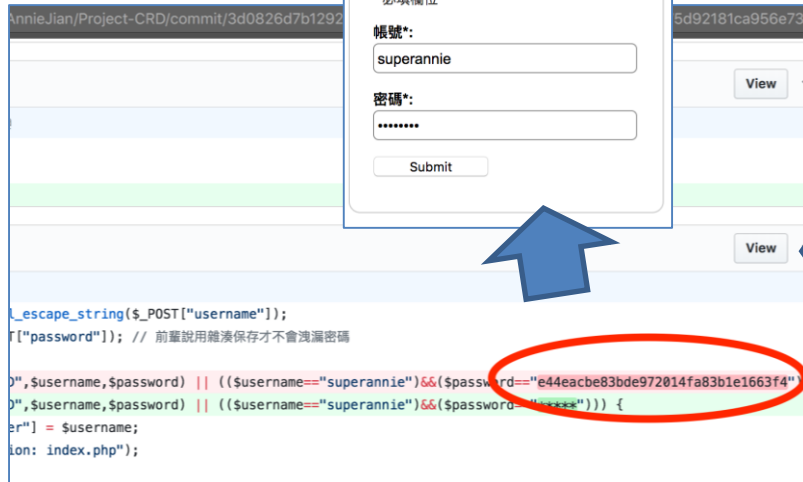
請輸入帳號密碼

\* 必填欄位

帳號\*:  
superannie

密碼\*:  
\*\*\*\*\*

Submit



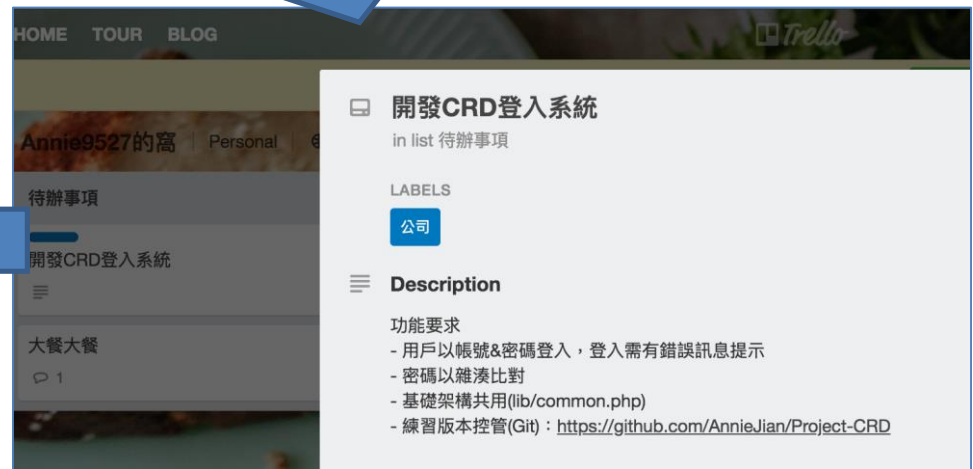
AnnieJian/Project-CRD/commit/3d0826d7b1292

5d92181ca956e73

View

View

```
_escape_string($_POST["username"]);  
["password"]); // 前輩說用雜湊保存才不會洩漏密碼  
), $username, $password) || (($username=="superannie") && ($password=="e44eacbe83bde972014fa83b1e1663f4"  
), $username, $password) || (($username=="superannie") && ($password=="*****")) {  
er"] = $username;  
ion: index.php");
```



HOME TOUR BLOG

Annie9527的高 | Personal

待辦事項

開發CRD登入系統

開發CRD登入系統

大餐大餐

1

開發CRD登入系統

in list 待辦事項

LABELS

公司

Description

功能要求

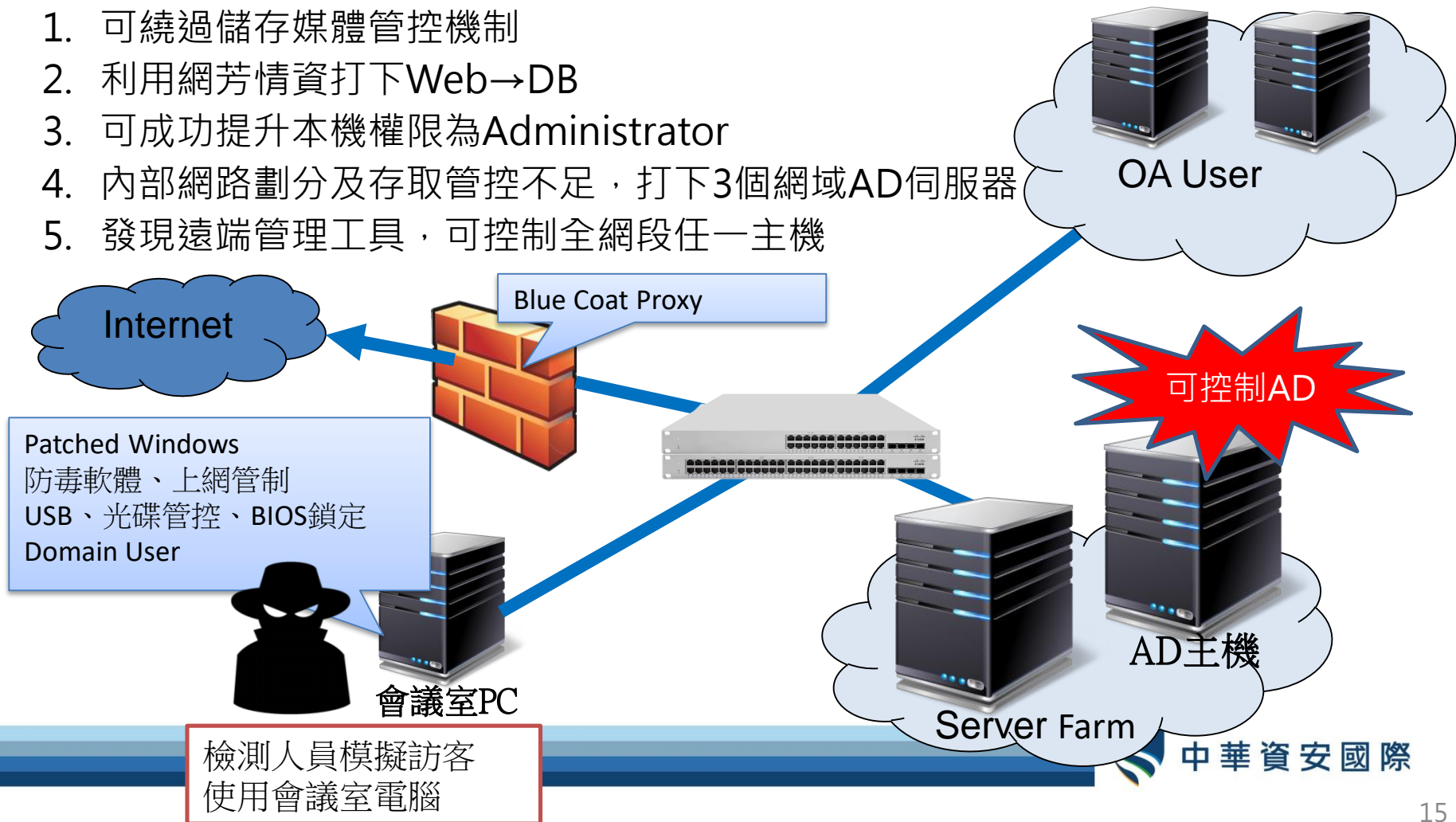
- 用戶以帳號&密碼登入，登入需有錯誤訊息提示
- 密碼以雜湊比對
- 基礎架構共用(lib/common.php)
- 練習版本控管(Git) : <https://github.com/AnnieJian/Project-CRD>

# 案例2、內網滲透演練服務

實測統計：內網滲透入侵成功率超過**90%**！

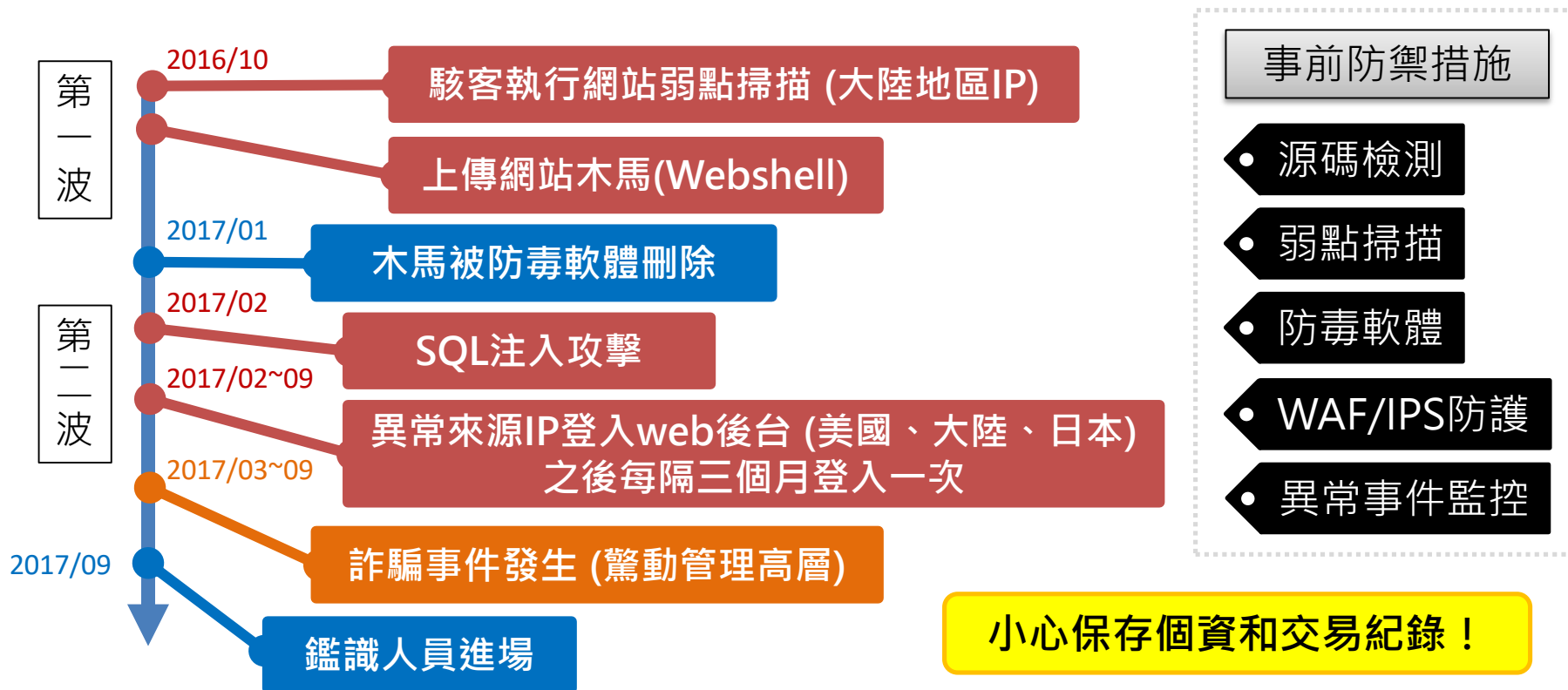
## 發現事項：

1. 可繞過儲存媒體管控機制
2. 利用網芳情資打下Web→DB
3. 可成功提升本機權限為Administrator
4. 內部網路劃分及存取管控不足，打下3個網域AD伺服器
5. 發現遠端管理工具，可控制全網段任一主機



# 案例3：銷售網站個資外洩事件

某銷售網站發生詐騙事件，但通報時間過久，消逝性證物已無法取得，鑑識人員分析日誌後發現，駭客先後利用上傳木馬、SQL注入漏洞，最後取得後台帳號密碼，大方從後台管理界面進出、取得消費者個資





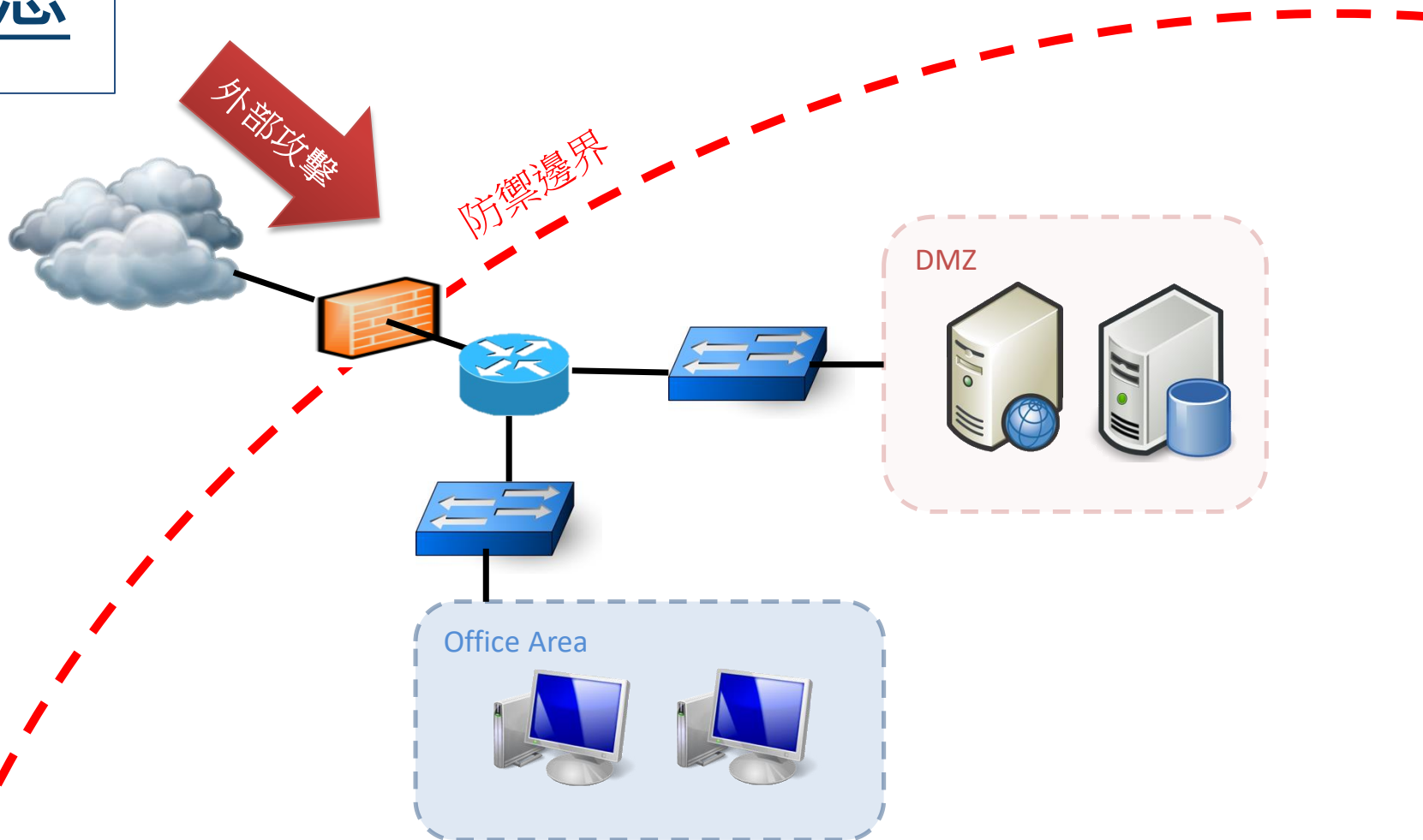
# 瞭解自己

- 盤點企業防護盲點



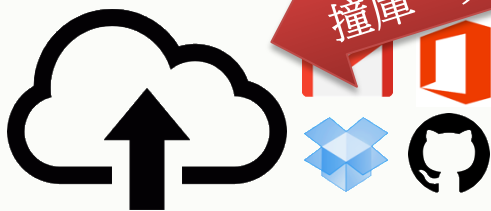
中華資安國際

# 理想



# 現實

Cloud Services



撞庫、資料外洩

DMZ

供應鏈污染



防毒更新  
維運監控  
基礎認證



測試環境  
閒置主機  
VM環境



外部攻擊

Work at home



社工釣魚、  
設備感染

惡意員工

釣魚攻擊

實體入侵

Hijacking

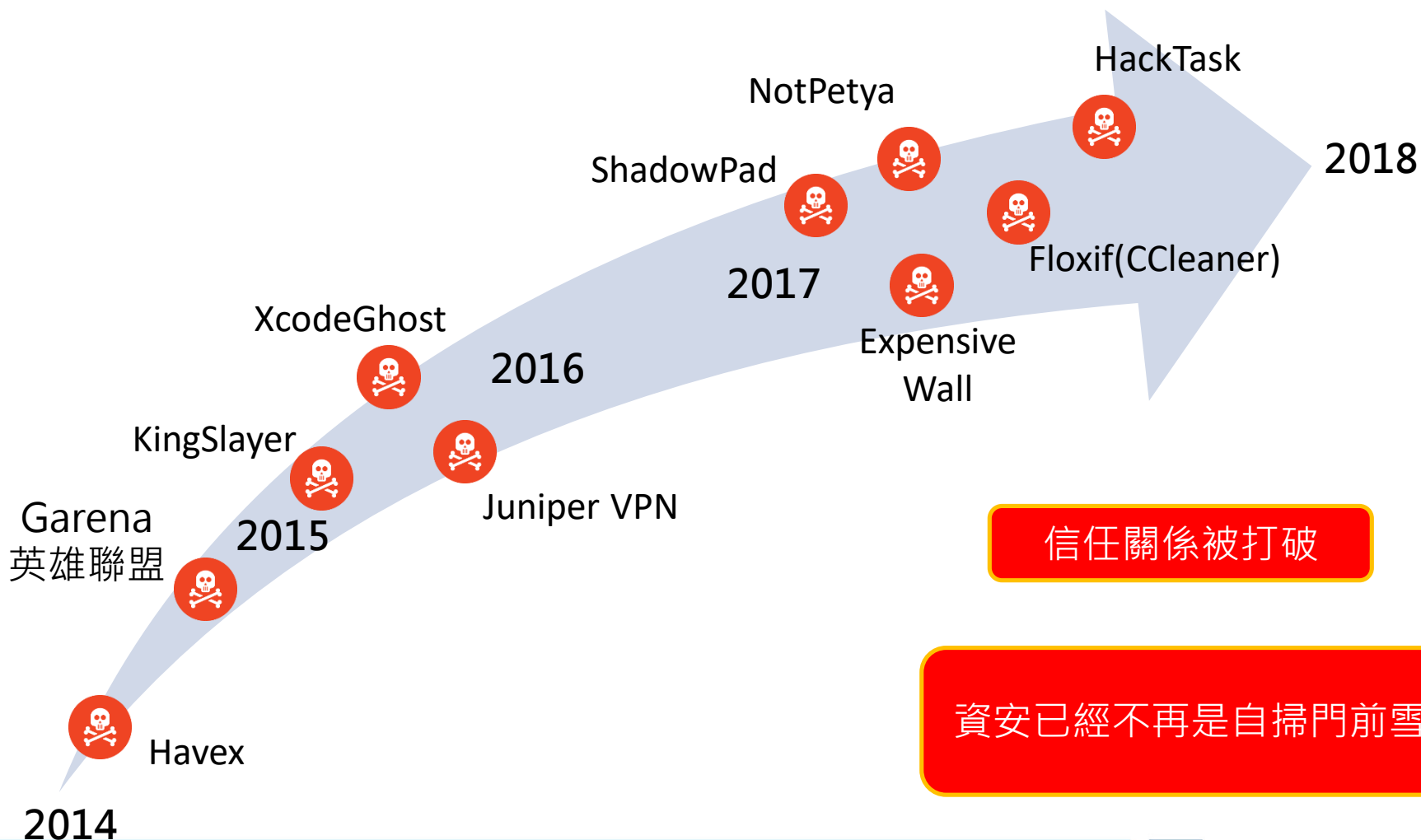
惡意App

感染、遺失

Office Area



# 軟體供應鏈攻擊事件大幅成長



信任關係被打破

資安已經不再是自掃門前雪



# 迎戰未來

-化被動為主動迎擊



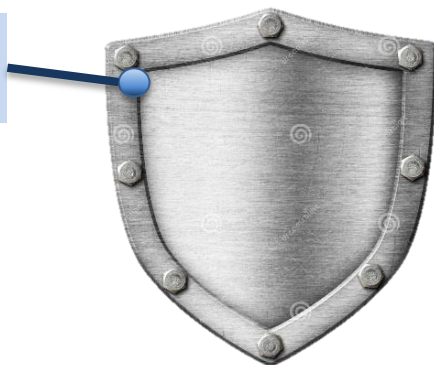
中華資安國際

# 攻防演練

## Blue Team

- 防火牆
- DDoS防禦系統
- IPS/IDS
- WAF
- APT防禦設備
- SOC監控中心
- 端點防毒/防駭

防：部署層層保壘，防範未知攻擊



攻：實際攻打系統，找出入侵管道

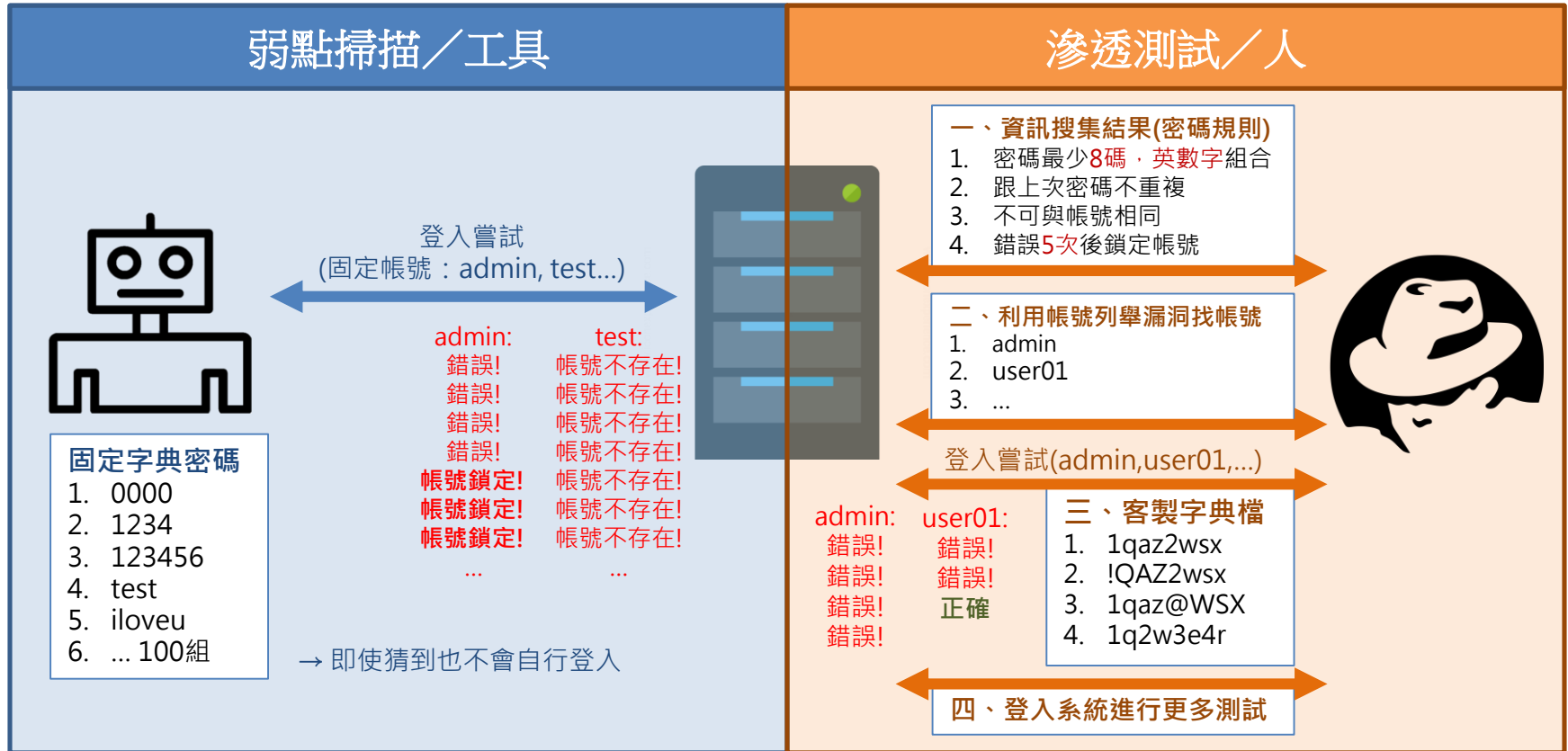
## Red Team

1. 滲透測試
2. 系統弱點掃描
3. 網站弱點掃描
4. 行動App檢測
5. IoT檢測
6. 社交工程



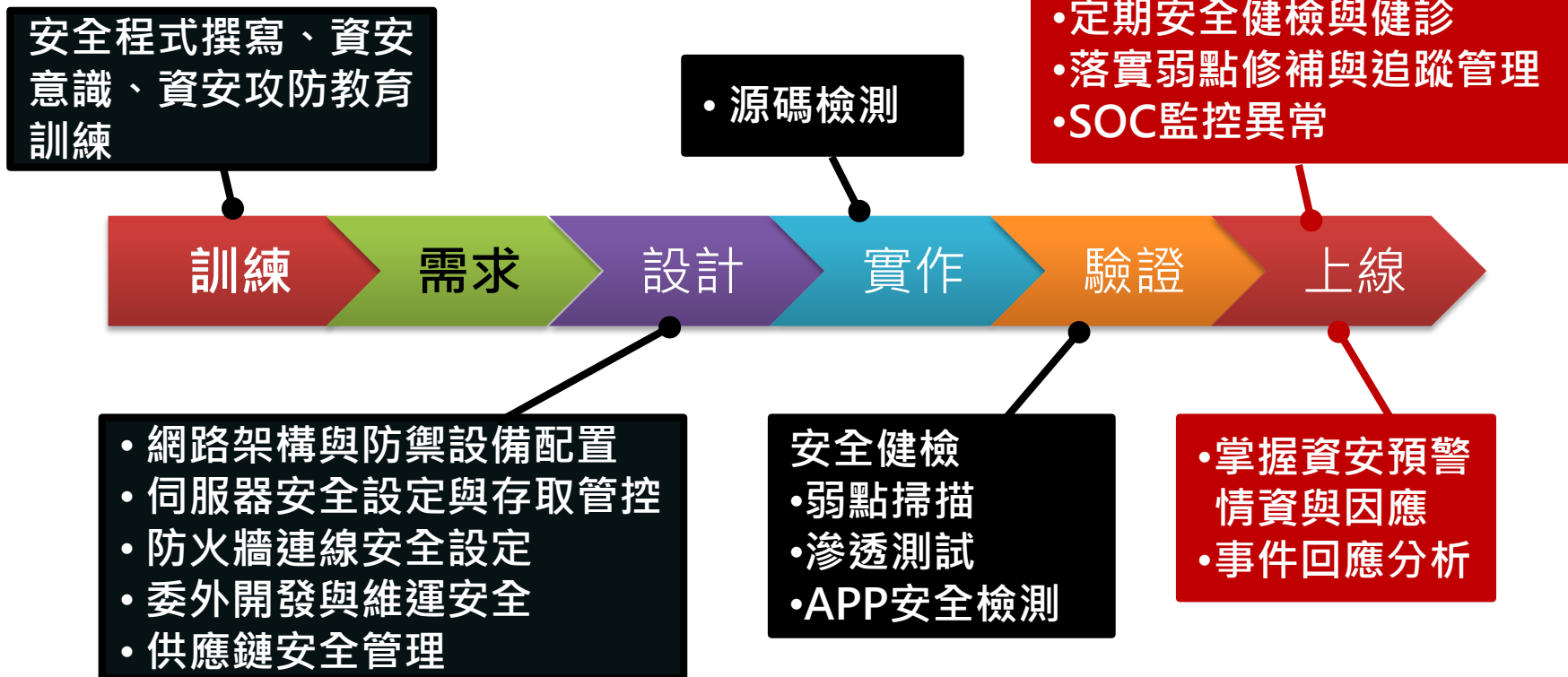
# 弱點掃描vs滲透測試的不同

- 以暴力猜解密碼為例



# 關鍵防護之鑰1 – 建立安全開發週期

## 建立安全開發及上線流程



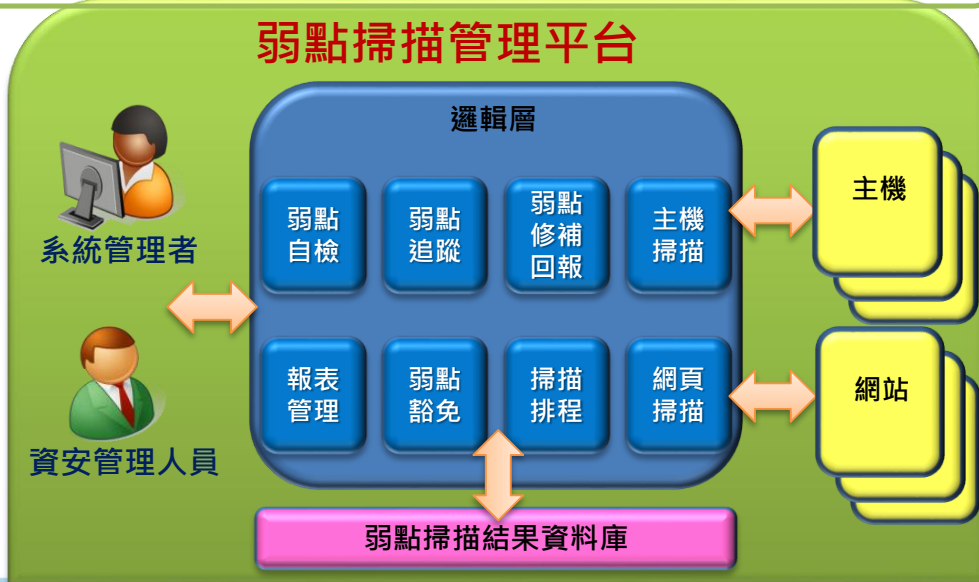
規劃適當的資安預算



# 關鍵防護之鑰2 – 落實資產與弱點管理

## 導入弱掃管理平台 – 落實弱點修補有效性

- 整合系統/網頁掃描商用軟體，**自動化排程弱點掃描**
- 系統化追蹤管理**各單位的弱點處理狀況，有效降低人力
- 可**自動複檢**落實弱點修補的有效性
- 系統管理者可**隨時自檢**，確認上線系統無已知弱點



### 弱點修補回報

透過平台查看弱點資訊

1. 點選要有哪台設備的弱點詳細資訊

2. 點選後，設備的弱點組項會顯示在下方表格

3. 查看弱點描述及處理方式

### 弱點掃描排程

時間、掃描政策、掃描標的

3

網頁弱點掃描可自訂掃描項目分類

可選擇All (所有掃描項目，包含 File Upload、XSS、Weak Passwords、Injection等)

可選擇只檢測XSS、Injection或高風險弱點

### 各式報表

依不同期別顯示統計資訊

你指定期間列表

弱點種類	弱點數量	已修補數量	已關閉數量	待修補數量	待關閉數量	待修補數量	待關閉數量
SQL注入	14	0	0	0	0	22	0
總和	14	0	0	0	0	22	0

依單位或是系統別顯示統計資訊

你單位列表

單位	弱點數量	已修補數量	已關閉數量	待修補數量	待關閉數量	待修補數量	待關閉數量
資訊室	0	0	0	0	0	0	0
業務發展部	0	0	0	0	0	0	0
資訊工程組	0	0	0	0	0	0	0

### 弱點豁免

弱點處理狀態修改為豁免或誤判之弱點經過審核後可排除

弱點系統：可選擇完成或退回

# 關鍵防護之鑰3 – 資安縱深防禦架構

## 資安縱深防禦架構

- 多層次防禦、管制，限制受駭範圍
- 組織可運用MSS資安服務，與ISP業者合作成為縱深一環，阻隔威脅於境外



威脅



Internet

CxO期待:

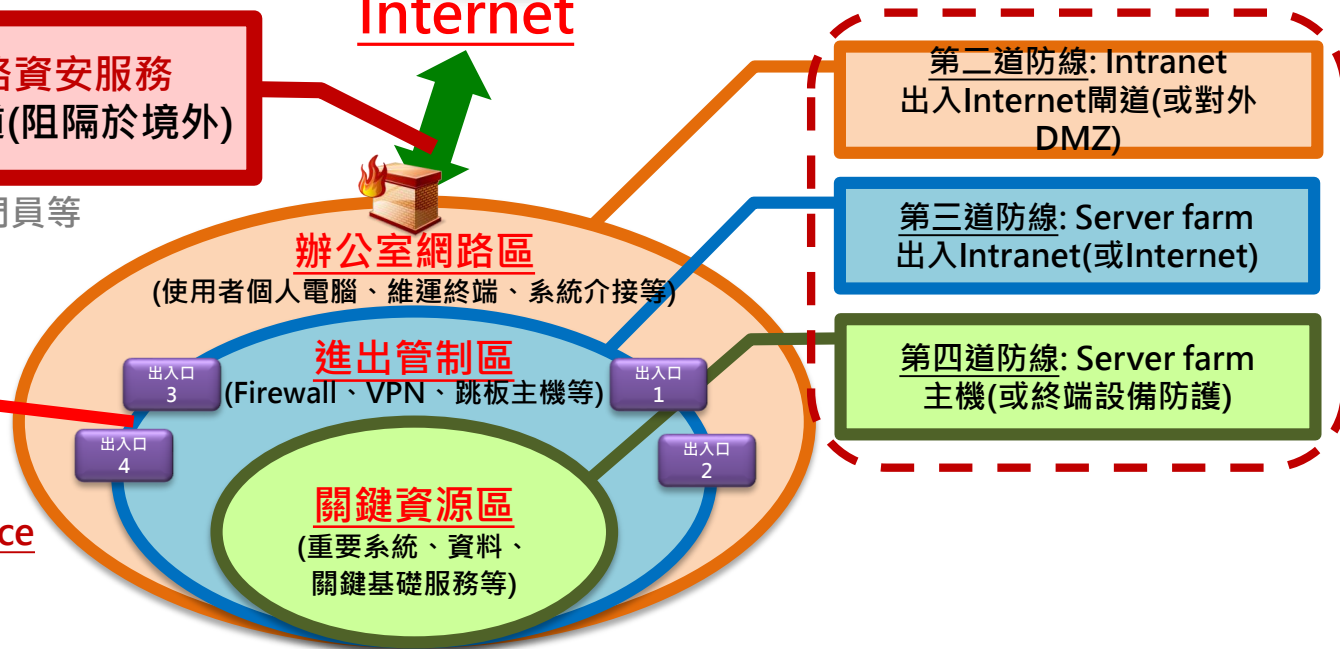
- 不要再發生資安事件
- 即使發生，也不能影響營運
- 即使影響營運，也要能快速回復！

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

例如: DDoS, IPS, 防駭守門員等

封閉、隔離，  
做好出入口防護

MSS: Managed Security Service



中華資安國際

# 關鍵防護之鑰4 – 終端自動化稽核

## 導入安全健診平台 – 快速檢測資安風險

### ▶ 多合1自動檢測風險

1. 惡意程式檢測(依IR經驗與技術自動檢測惡意程式，如：檢測開機時自動執行的程式、系統服務、工作排程等)
2. 安全性更新檢測(如：作業系統、Adobe、防毒軟體...等更新)
3. 安全性設定檢測(如：稽核原則、密碼原則...等設定)
4. 政府組態基準(GCB)符合度檢測

### ▶ 支援AD/資產管理軟體，派送檢測Agent快速檢測

### ▶ 提供Dashboard依IP呈現各類風險

### ▶ 操作介面簡單易學

### ▶ 自動產出報表



敬請指教



中華資安國際