DEVCORE
SECURITY
CONSULTING

DEVCORE 紅隊的進化，與下一步 Ver. 2023

許復凱 (Shaolin)

戴夫寇爾股份有限公司

shaolin@devco.re

2023.03.10
DEVCORE Conference

講者簡介

許復凱 (Shaolin Hsu)

戴夫寇爾 DEVCORE 紅隊總監

- ✓ 參與超過百場滲透**測試**找到高風險弱點
- ✓ 執行超過五十場紅隊**演練**達成任務目標

DEVCORE 紅隊的進化，與下一步 Ver. 2023

紅隊演練怎麼進行

- 收到任務目標
  1. 取得控制核心系統控制權
  2. 取得網域內高權限帳號
  3. 取得客戶信用卡完整卡號
  4. 取得特定人員權限
- 執行專案
  - 排除協議的禁止行為，紅隊**無所不用其極**的達成任務目標

紅隊的進化 *Ver. 2019*

DEVCORE SECURITY CONSULTING


進入企業內網

高價值產品漏洞研究與挖掘

意外的成果 1/3

PortSwigger 連續兩年年度十大網站攻擊技術評選冠軍

Top 10 Web Hacking Techniques of 2017

Top1: A New Er

https://portswigger.net/b

Top 10 Web

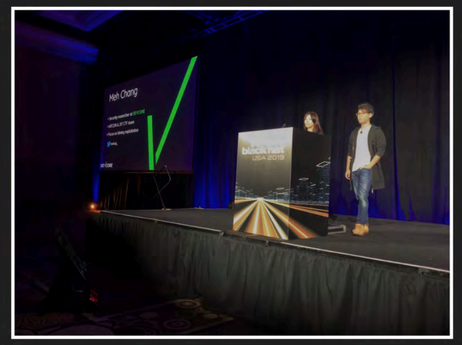
Top1: Breaking
Take Your Path

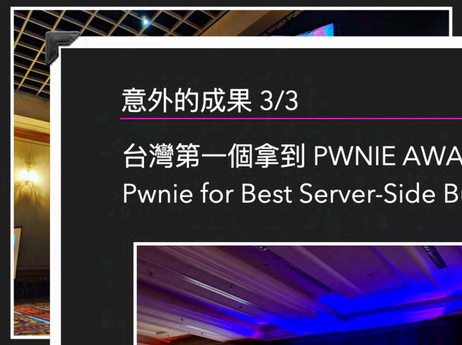
https://portswigger.net/b

DEVCORE SECURITY CONSULTING

意外的成果 2/3

連續三年 DEF CON & Black Hat USA 發表





DEVCORE SECURITY CONSULTING

意外的成果 3/3

台灣第一個拿到 PWNIE AWARD 獎項：
Pwnie for Best Server-Side Bug (年度最佳伺服器漏洞)

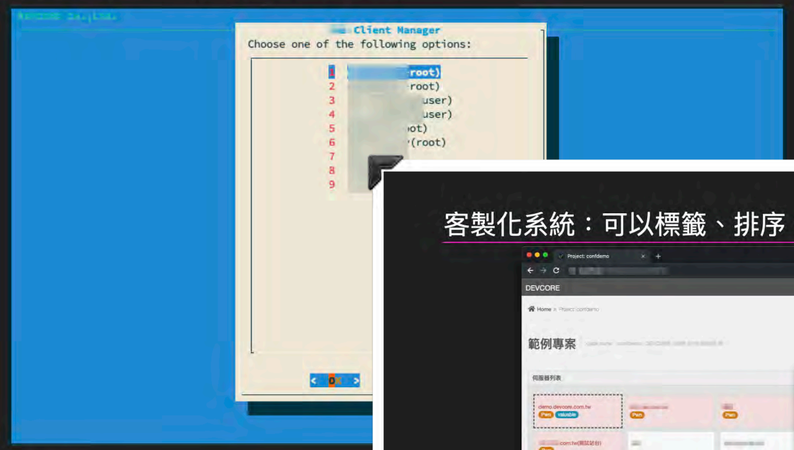
DEVCORE SECURITY CONSULTING

DEVCORE SECURITY CONSULTING

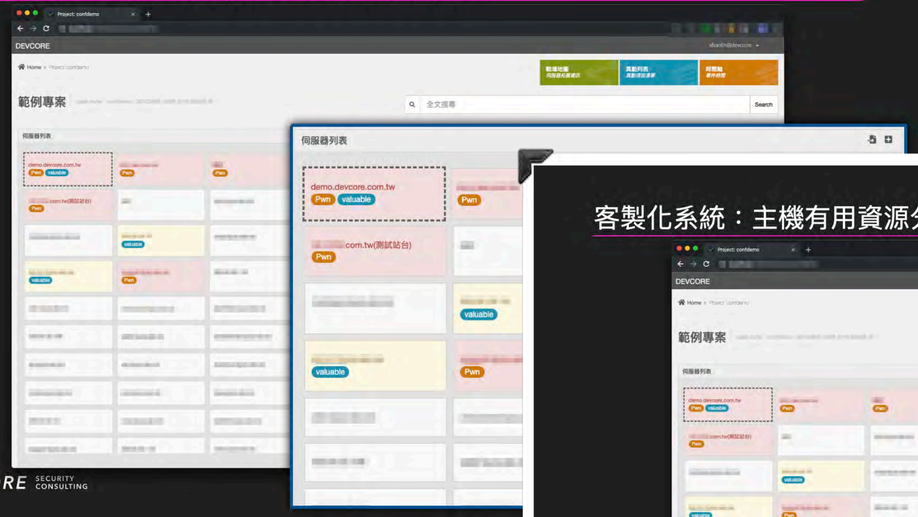

協同合作與歷程記錄

客製化的協同合作工具

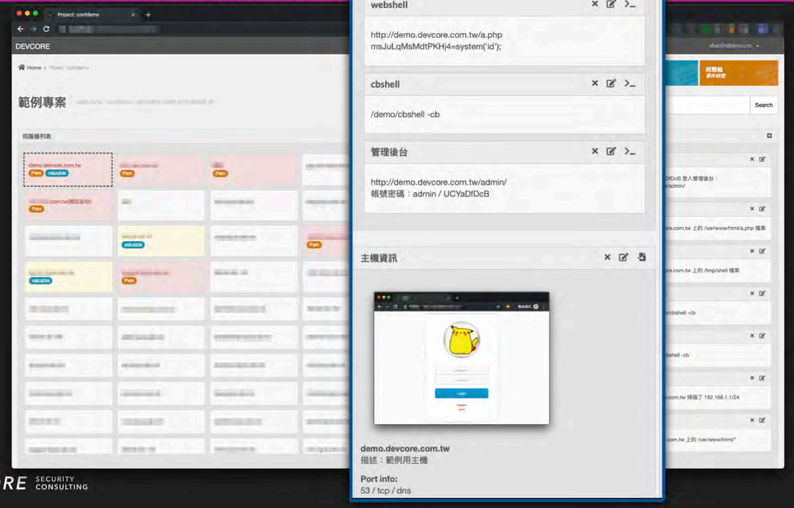
Shell 主機中控台，方便其他人迅速接手



客製化系統：可以標籤、排序、搜尋主機的系統



客製化系統：主機有用資源分享



DEVCORE SECURITY CONSULTING

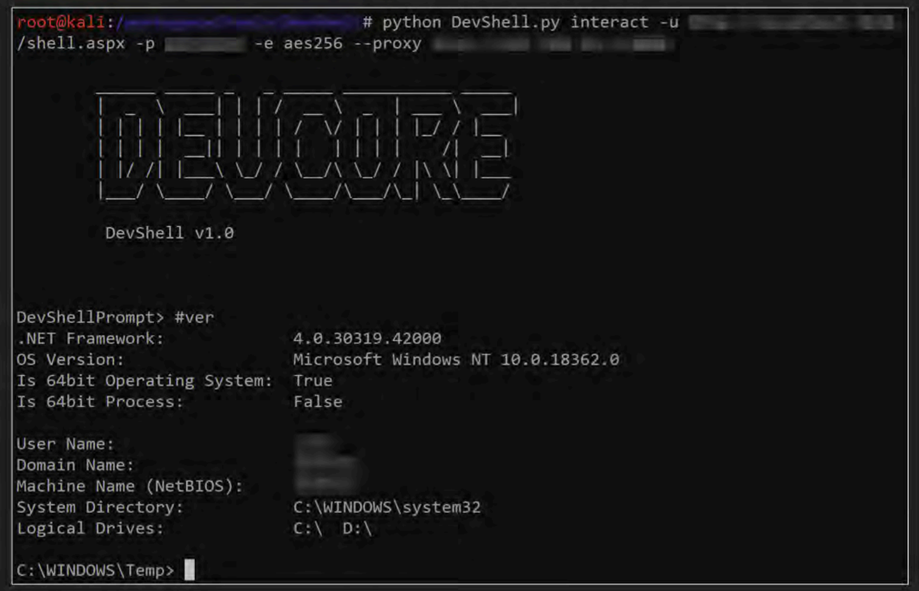

隱匿的內網橫向移動

開發隱匿工具

開發隱匿工具

Ex: 匿蹤 Web shell @ Windows

- WAF 抓不到
- 防毒軟體抓不到
- 不會有 EventLog (預設)
- 收集所需系統資訊或程式碼
  netstat, route, tasklist...等



DEVCORE SECURITY CONSULTING

DEVCORE SECURITY CONSULTING

紅隊的進化 *Ver. 2023*

DEVCORE SECURITY CONSULTING

紅隊的進化 Ver. 2019

- 為了進入企業內網
  - ✓ 高價值產品漏洞研究與挖掘 **持續進化**
- 團隊協同合作與歷程記錄
  - ✓ 客製化的協同合作工具 **持續進化**
- 更穩定的內網橫向移動
  - ✓ 開發隱匿工具 **持續進化**

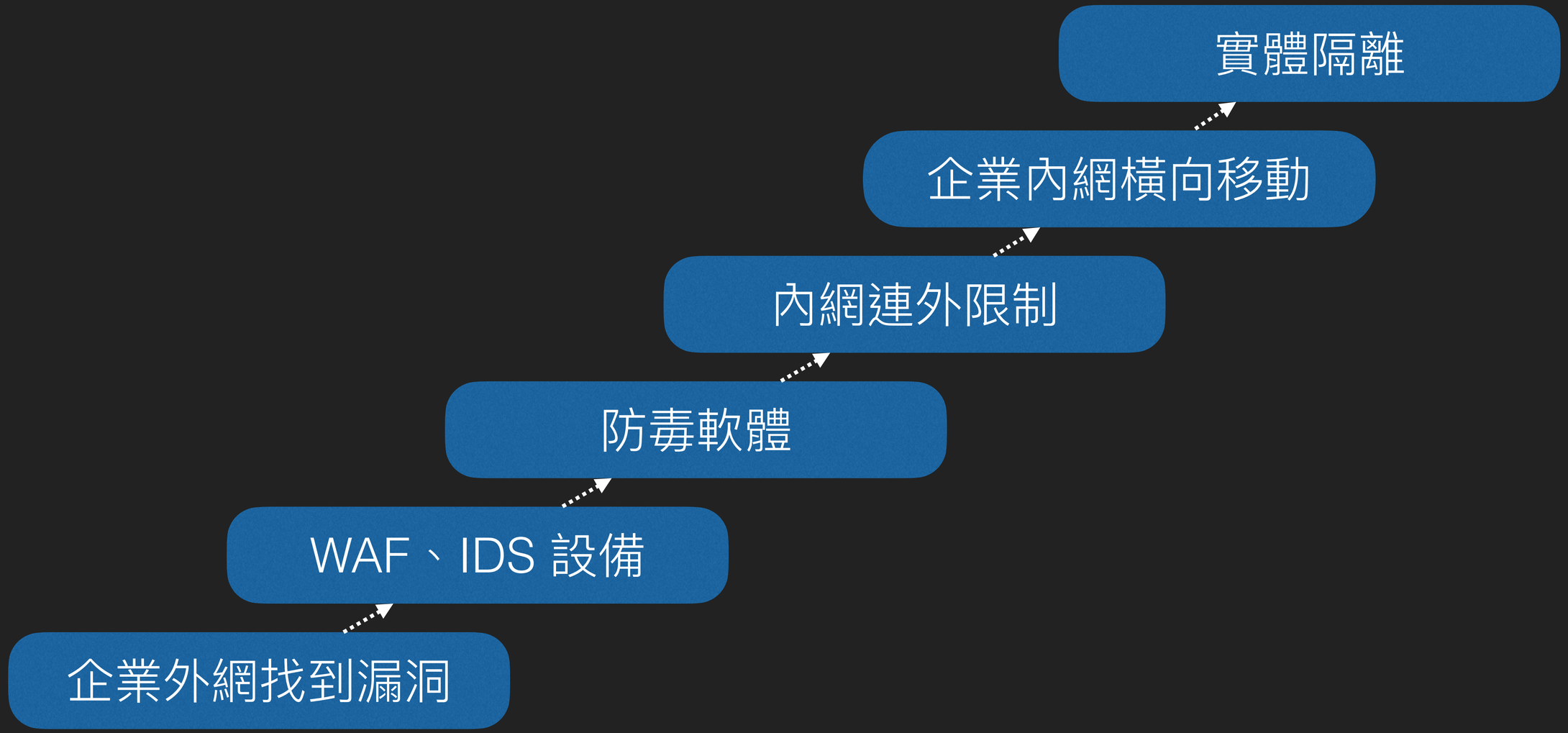
還有呢？

為什麼我花了這麼多預算防禦
安全檢測也做過這麼多年了
紅隊演練時還是照樣被突破

一般進行紅隊演練的流程

DEVCORE SECURITY CONSULTING

紅隊演練中面臨的挑戰



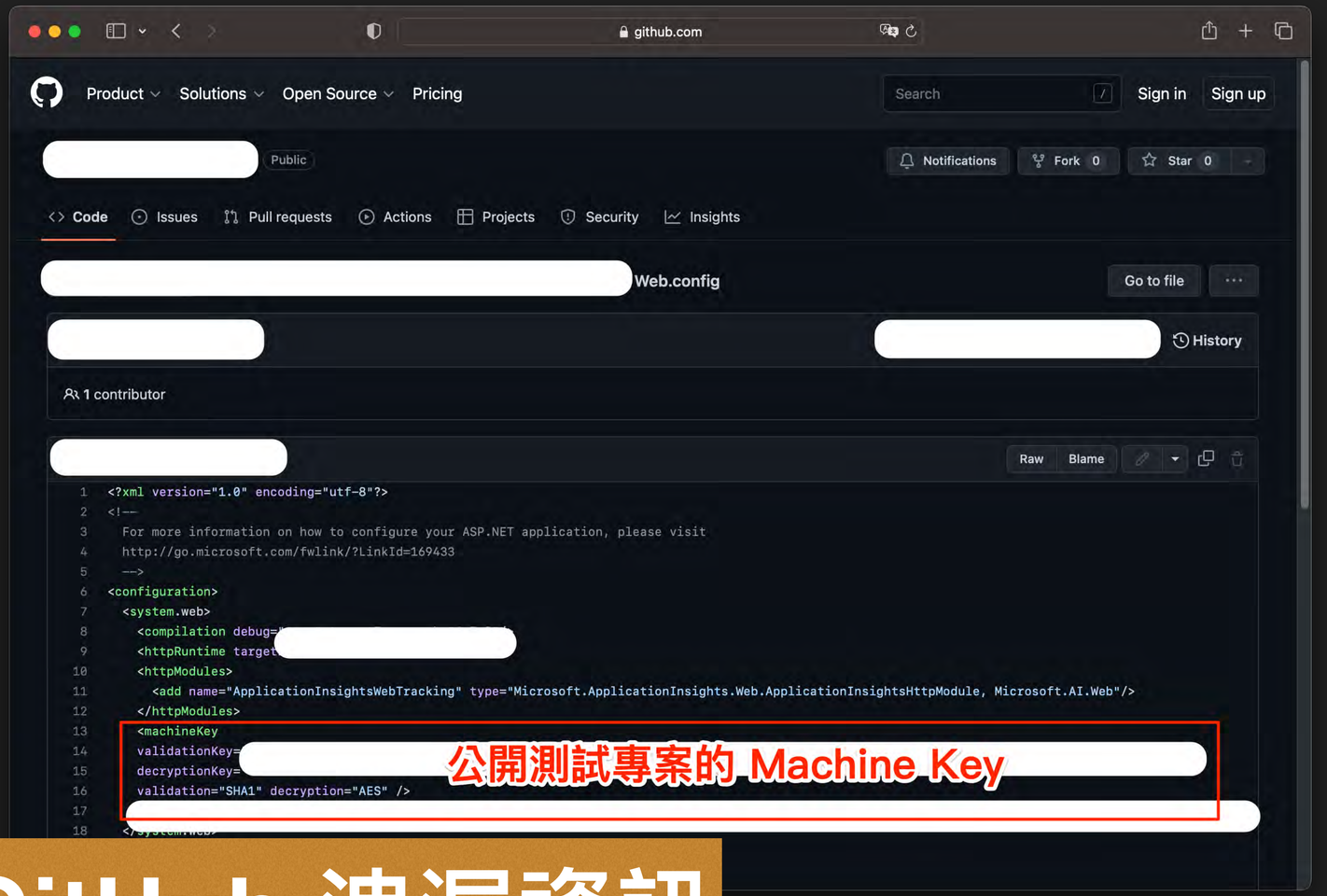
企業外網找到漏洞

關鍵點—
蒐集的資訊比別人多


長期累積的精華字典檔

Case Study: GitHub 資訊洩漏收集

- 目標網站使用的 Machine Key 跟某個無關 GitHub 測試專案相同
- 知道 Machine Key 的意義？
  - 等於可控制用這個 Key deploy 的所有網站



長期收集 GitHub 洩漏資訊

關鍵點二
觀察的比別人細

Case Study: 供應商的弱點

- 找到目標開發廠商
- 開發商洩漏目標網站程式碼
  - 程式碼挖掘漏洞

內部演練畫面
僅公布於研討會

發現供應商的資訊洩漏

Case Study: 說明文件取得更多檢測資源

- 系統說明文件資訊洩漏
  - 發現測試站複雜的帳號
  - 根據密碼位數猜到弱密碼
  - 進入系統發現漏洞

登入系統

登入步驟：輸入您的帳號密碼即可登入系統

（示意說明文件）

發現說明文件中的蛛絲馬跡

Case Study: 社交平台的資訊洩漏

- 主管十年前在社交平台貼出護照
- 內部系統預設密碼為生日
  - 護照有生日

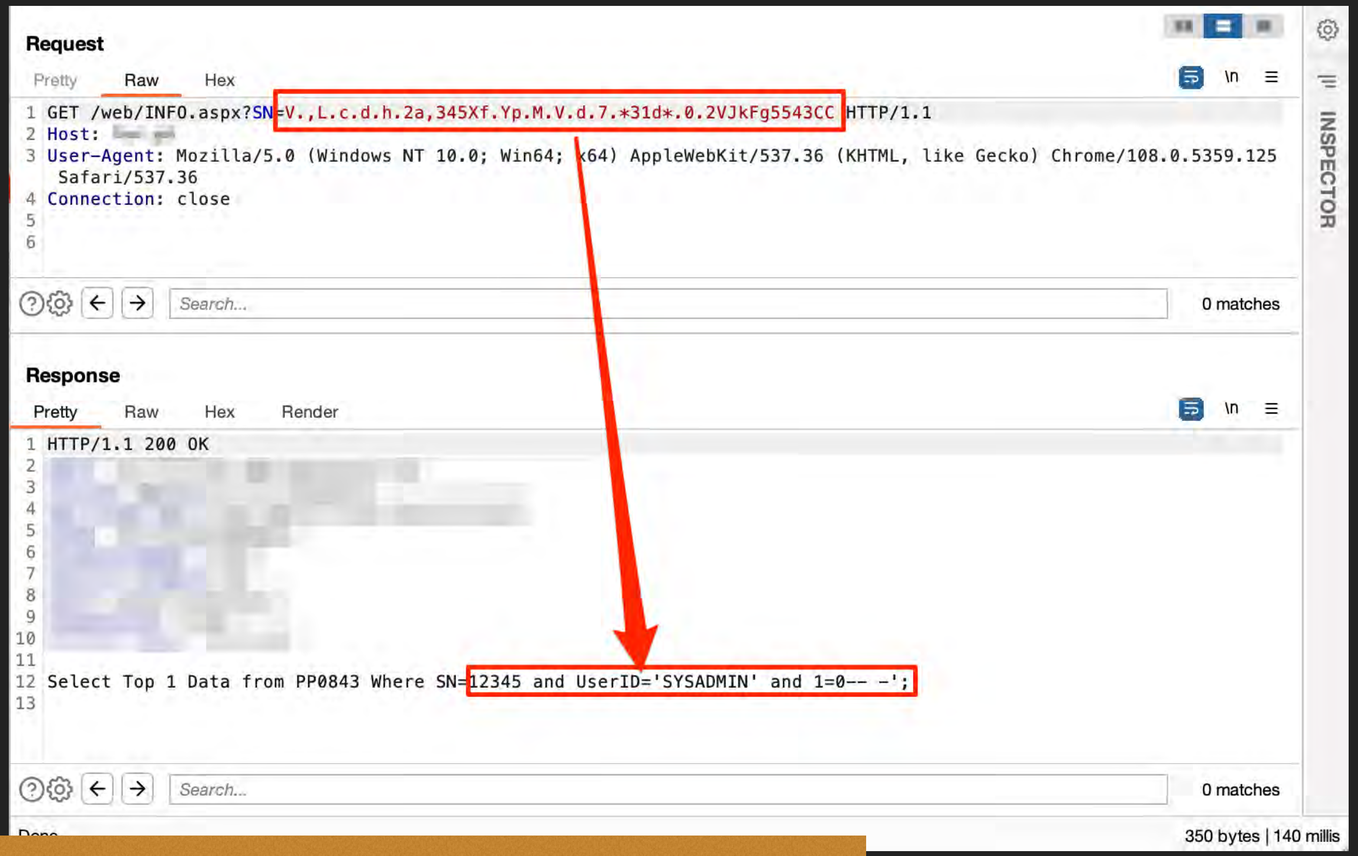
發現社交平台的重要資訊

關鍵點三

看別人不想看/沒注意的服務

Case Study: 專用桌面端軟體

- 桌面端將參數加密與伺服器互動
- 逆向解出加密算法後，測試參數出現各種常見漏洞
- 該企業做過多年 PT，外網漏洞甚少，WAF 能力也相當優秀
- 因為參數加密，剛好也繞過 WAF



沒人注意/比較難看的桌面端軟體

關鍵點四

世界級的漏洞利用/研究能力

Case Study: 世界級的漏洞利用/研究能力

- 2023/03/11 DEVCORE Conf 駭客場
- Pwn2Own
  - 2022 Pwn2Own Toronto 冠軍
  - 2021 Pwn2Own Austin 亞軍
  - 2021 Pwn2Own Vancouver 冠軍
  - 2020 Pwn2Own Tokyo 亞軍

有足夠的時間，高機率能挖掘出 0day

WAF、IDS 設備

關鍵點

讓 *WAF* 認不出中間傳了什麼

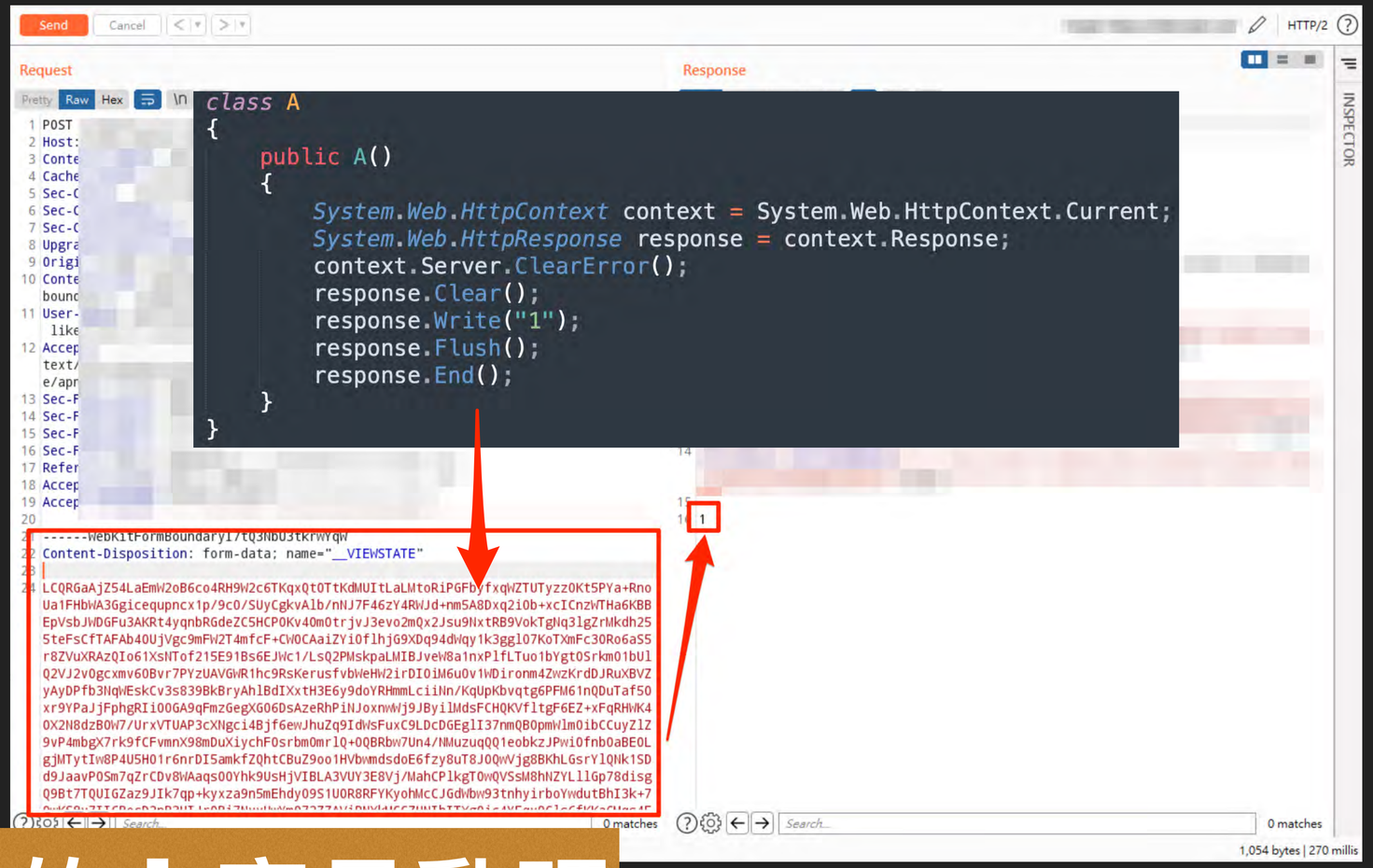
繞 WAF 基本概念

- 假設 illegal 是 WAF 認為不合法的字串

字元編碼、取代搭配伺服器特性

Case Study: 序列化的特性 常用

- 序列化的資料是**亂碼**
- WAF 看不到任何關鍵字
- 成功繞過數家國際大廠防禦



傳送的內容是亂碼

DEVCORE SECURITY CONSULTING

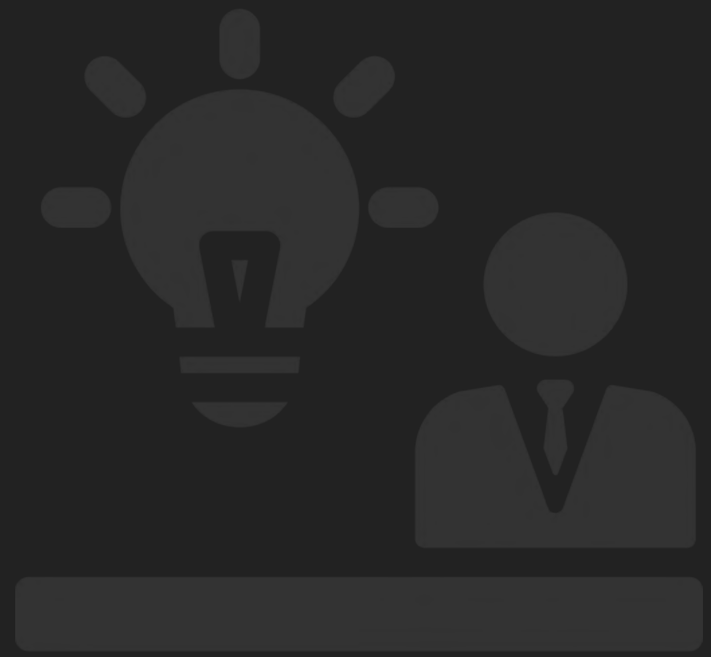
防毒軟體

關鍵點

程式不要出現特徵碼即可

繞過防毒軟體的關鍵點

- 關鍵方法
  - 加殼、加密、壓縮、混淆等
  - 手動移除程式內關鍵字（例如: help message）
  - 有時候甚至重新編譯就過防毒了



內網連外限制

- 要掛 proxy 才可以上網
- 中間有一層 Gateway
  - 不合法網站不能上
  - 不能傳危險的內容

企業嚴苛的環境

關鍵點

想辦法成為 *Gateway* 的白名單

突破內網連外限制的關鍵點

- 關鍵方法
  - 開發後門工具支援純 HTTP 協定+ Proxy
  - 尋找 Gateway 的白名單 domain，看什麼 domain 是可以利用的
    - **CDN domain** 通常是好選擇 **關鍵**
      - 一般網站一定會用到 CDN 素材，CDN 通常是白名單
      - 申請後，任何內容都可透過 CDN 傳輸

企業內網橫向移動

關鍵點

直搗黃龍：打 *AD* 伺服器

企業內網橫向移動的關鍵點

- AD 價值高，現階段**相對好攻擊**，原因：
  - 權限種類太多：容易出現設定疏失
  - 企業帳號太多：莫名的服務、人員擁有不需要的高權限
  - 歷史包袱太多：不知道哪個學長留下來的高權限帳號
  - **個人疏失**
    - 例如：資源回收桶殘留關鍵帳號密碼、個人目錄放密碼表.xls

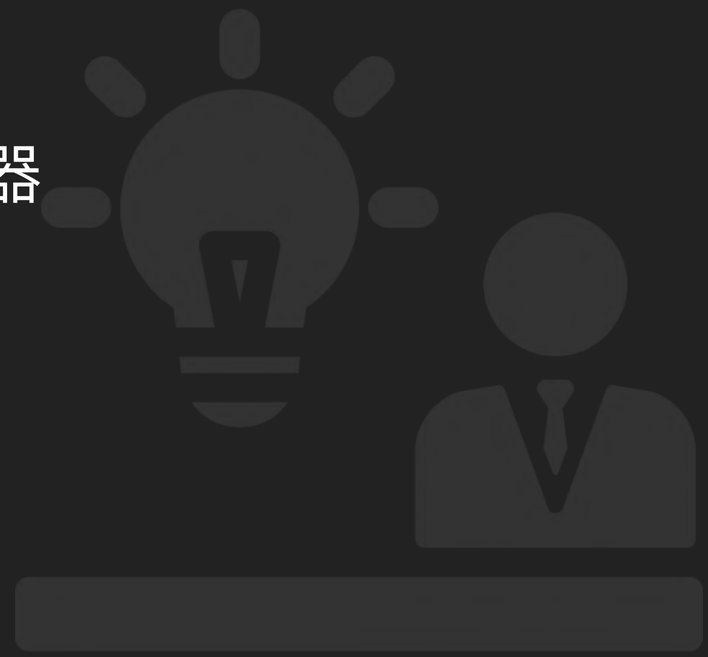
實體隔離

關鍵點

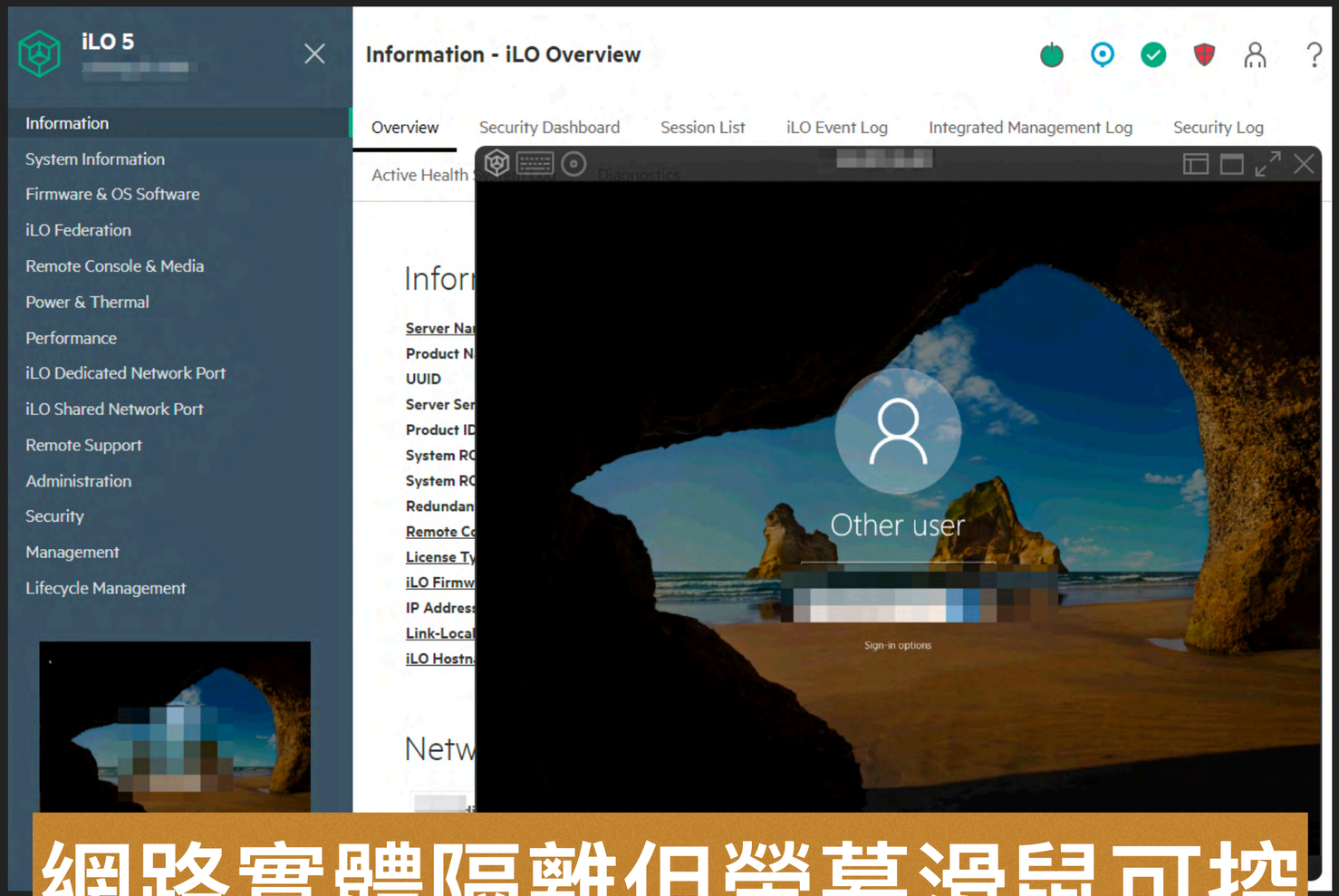
實體隔離仍要方便維運

突破實體隔離的關鍵點

- 一般而言無法突破
- 嘗試尋找維運實體隔離機器的痕跡，實戰中看到的例子
  - 透過 AD 管理
  - 透過資產管理系統管理
  - 透過 iLO 管理
  - 透過 vCenter 管理
- 尋找方式
  - 直接攻陷上述管理系統，搜尋找出號稱實體隔離的機器
  - 尋找維運交接文件
  - 潛伏在維運人員電腦觀察



Case Study: 透過 IPMI 連接螢幕



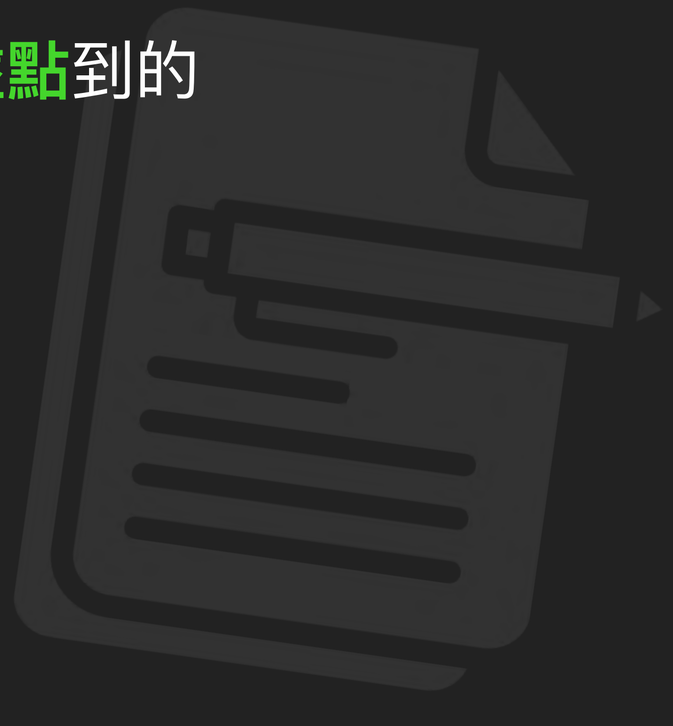
網路實體隔離但螢幕滑鼠可控

反思 (1/2)

- 做過滲透測試 / 紅隊演練**並不代表 100% 安全**
  - 過去的檢測團隊不一定有時間 / 資源看這麼細
  - 不同角度 / 不同人 / 不同時間 會有不同的結果
  - 定期進行資安檢測服務的由來
- WAF 是有可能會**失效**的
  - 只要做到讓 WAF 不認得傳輸的內容
- 繞過防毒軟體的**成本沒有想像中高**
  - 攻擊者：碰到防毒軟體只會覺得麻煩而已，但並非不可繞過

反思 (2/2)

- 企業限制內網對外連線，駭客仍有可能透過白名單網站把**資料傳出**
  - 只要員工沒有被完全禁止上網
- AD 帶來管理的便利，卻也容易有**設置疏失**
  - 可透過 AD Attack Path Assessment 產品盤點 AD 可能被攻擊的路徑
  - 但文件、Email、密碼管理軟體等人為洩漏疏失是**無法盤點**到的
- 企業說的實體隔離，有可能只是防火牆設定
  - 特定幾台主機或特定 port 或特定時段開放連線
  - 方便維運和安全性的取捨，**方便維運有機會成為破口**



企業的下一步

每一個都可能失效，怎麼應對？


這是一條攻擊鏈

眼明手快阻斷即可大幅減少傷害

眼明 → 偵測

手快 → 回應、阻斷

面對未知的駭客，就像面對 *COVID-19*

會讓紅隊覺得麻煩的防禦機制

內網發現異常就通報甚至阻斷網路 非常困擾

- 來自異常 IP 的存取
- 來自不同軟體的登入
- 同 IP 對內網大範圍掃描
- 網站檔案異動後復原及通報
- 網頁伺服器身分執行系統指令

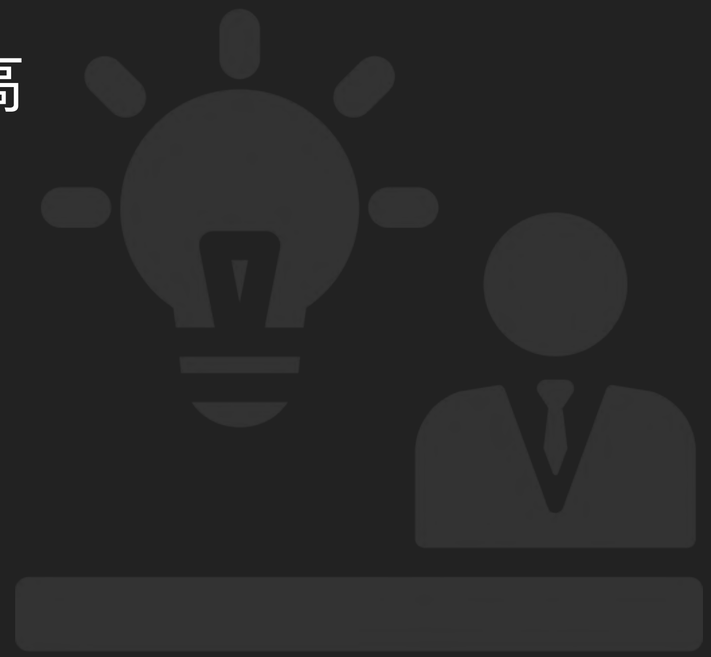
跟你平常看到的不一樣就是異常

DEVCORE SECURITY CONSULTING

資安成熟度現況 (1/2)

2019 當真正的駭客入侵時，企業準備好了嗎 DEVCORE CONF 2019

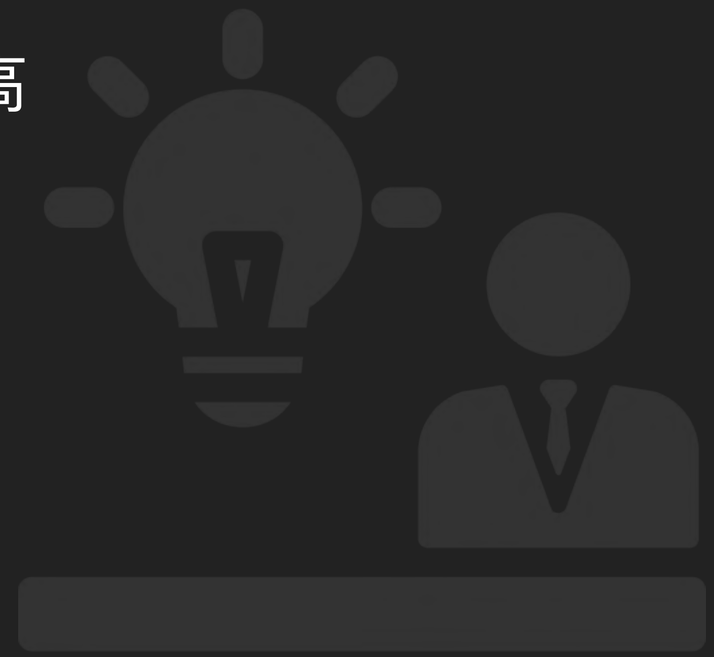
- 攻進內網後，大部分企業沒有知覺
- 對頂尖攻擊團隊而言，進入企業內網的難度並不高
- 從紅隊演練中訓練企業**偵測**和**應變**的能力



資安成熟度現況 (2/2)

2022 當真正的駭客入侵時，企業準備好了嗎

- 攻進內網後，**首次**做紅隊的大部分企業**仍然**沒有知覺
- 對頂尖攻擊團隊而言，進入企業內網的難度並不高
- 從紅隊演練中訓練企業**偵測**和**應變**的能力



最適合自己的階段

第 3 階段

資安成熟度高

（合作 2 次以上）

第 2 階段

資安成熟度成長中

（通常需要 1~2 年）

大部分企業在這

第 1 階段

初次進行

1

演練目標：

- 找出最快入侵途徑
- 儘量監控但不阻擋

2

演練目標：

- 驗證防禦的有效性
- 久攻不克特許方案

3

演練目標：

- 完全擬真對抗演練
- 不限時間、不限範圍、不限手法
- 確認日常團隊防禦應變流程及能力
- 勇於挑戰團隊極限

DEVCORE

紅隊演練如何幫助您

- 分階段進行演練
  - 第一階段：確保**外網**有一定程度的安全性
    - 評估點：DEVCORE 2~3 週在外網找不到進入點（視範圍大小）
  - 第二階段：確保內網具有**偵測**與**應變**能力
    - 評估點：可否發現 DEVCORE 在內網的行動
  - 第三階段：確保**整體**防禦 24/7 的有效性
    - 評估點：隱匿攻擊下核心系統的重要資料有沒有被取走

真實客戶的防禦進化

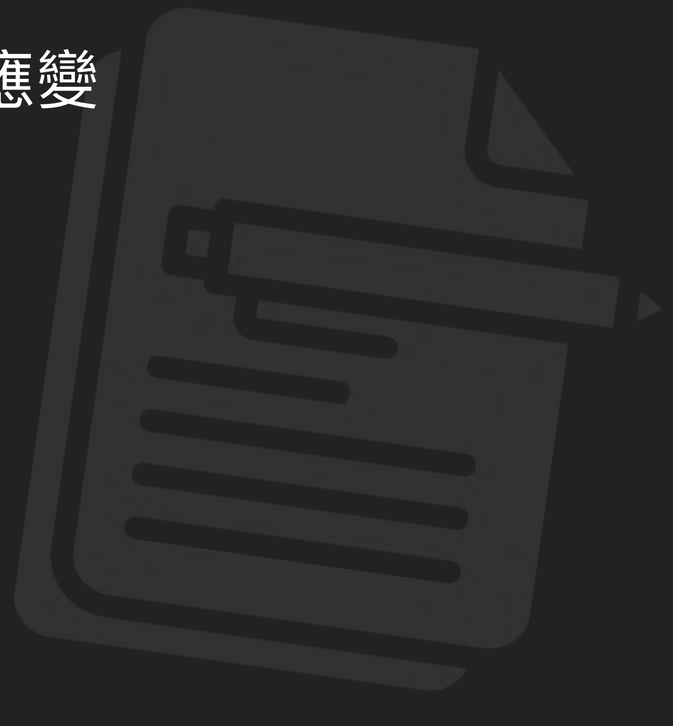
第一年 什麼權限都拿到了，管理員什麼都**不知道**

第二年 『我們**核心網段**有異常 log，是你們在攻擊嗎？』

第三年 『我們 **DMZ 網段**有異常 log，是你們在攻擊嗎？』

我們的建議

- 如果外網安全已投資多年，開始思考「如果駭客已經在內網」的防禦策略
- 盤點出最不可以被洩漏的重要資料，從這些地方開始奉行 **Zero Trust** 概念
- 企業內部需要有專職資安人員編制（藍隊），負責偵測和應變
- 透過與有經驗的紅隊合作，全盤檢視防禦盲點



紅隊的下一步

紅隊的下一步 – 技術面

- 尋找**新的攻擊面**
  - 釣魚、供應鏈攻擊...What's next?
  - 新攻擊手法都是打不穿後逼出來的
- 仍舊在乎**隱匿技術、工具**的研發
  - 台灣平均偵測能力不夠，預計兩三年後才會需要在演練中隱匿技術
- 研擬**紅藍對抗**的戰術
  - 例如：洩漏蹤跡是調虎離山，還是真的？
  - 資安成熟度高的企業可逐漸導入擬真對抗演練

紅隊的下一步 – 服務面

- 情境式的演練：紅隊推薦劇本模擬駭客使用**特定的技術或攻擊路徑**
  - 增強防禦方對特定技術（或攻擊路徑）的偵測、應變能力
- 紅藍對抗：**擬真**的演練
  - 增強對職業攻擊者的應變能力，將傷害減低

Takeaways

- 從紅隊在各個階段的攻擊思維，了解各個資安產品都有其**極限**
  - 駭客入侵**一定**會發生
  - 因此防禦方需持續培養資安人員加強**偵測**和**應變**能力
- 透過紅隊演練可了解企業防禦的盲點，以利規劃對應之道

“紅隊演練的精髓不是在告訴你有多脆弱
在於真正壞人闖入時你可以獨當一面擋下”

DEVCORE
SECURITY
CONSULTING

感謝聆聽！

Q&A

戴夫寇爾股份有限公司
contact@devco.re
02-2577-0925