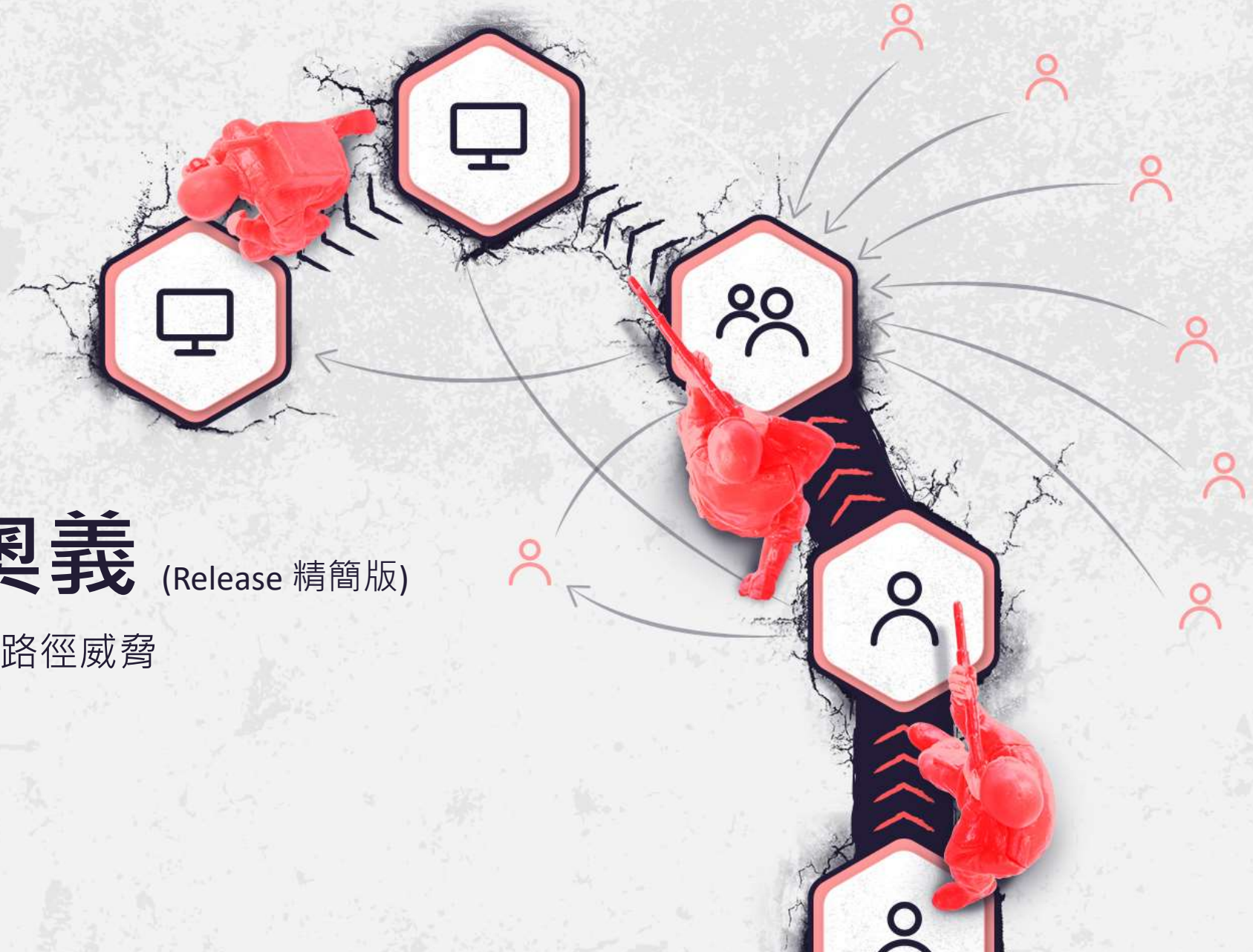
CYCRAFT
奧義智慧科技



AD 安全的奧義 (Release 精簡版)

量化 Active Directory 的攻擊路徑威脅

邱銘彰 / CyCraft

暗黑中的 AD

全公司 IT 最重要核心

駭客攻防的必爭之地

複雜難懂且漏洞一堆

AD 資安，是企業中無所不在威脅

> 現在的 AD 安全檢測，無法找出真正的問題點

傳統資安健診只為了合規，帳號來個點點名，列出密碼複雜度原則，無法反映 AD 真正的資安問題。

> 老生常談的資安政策與原則，不符合實務

資安政策，總在抽象地討論最小權限原則，並沒有把企業真實營運場景考慮進去，導致大部分原則都無法在實務上真正實現。

> 一堆檯面下隱匿的權限路徑，難以管理

AD 帳號間的關係，與可攻擊路徑才是該正視的問題，而資安人員缺乏對 AD 安全的可視性，且這些潛在攻擊路徑，正是駭客可以輕易橫向移動的主因。

- 86 % 的企業將增加 AD 防護預算

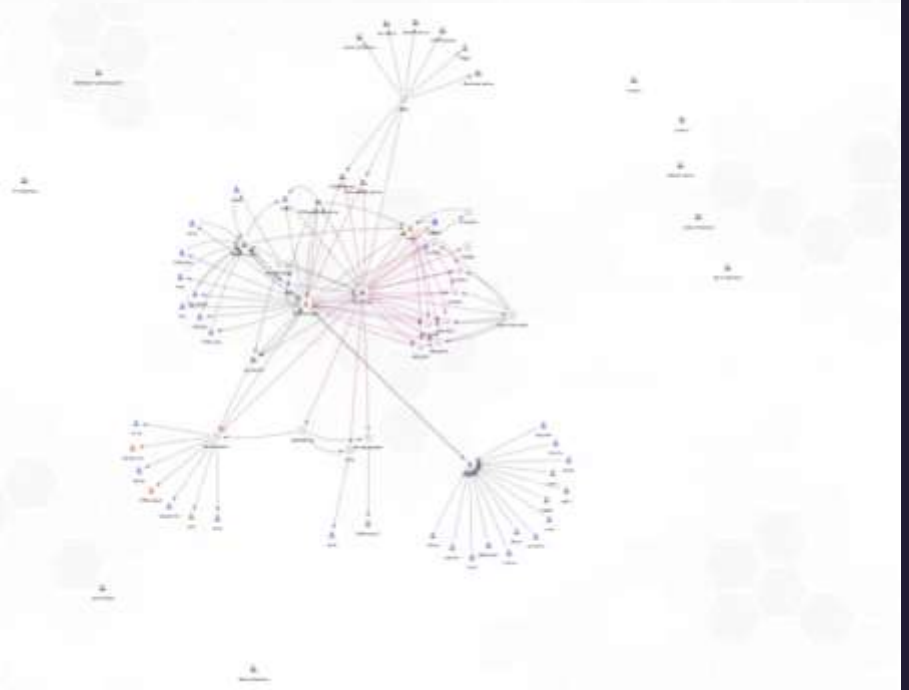
三大原因：

- 認為駭客間 AD 新攻擊手法正在流行
- 認為員工在家上班 (WFH) 越來越多
- 認為公司大量使用各種雲端服務

> 紅隊攻下 AD 的比例為 72 %

> 紅隊攻下 AD 平均是 11.5 天，最短 3 天

DEVCORE

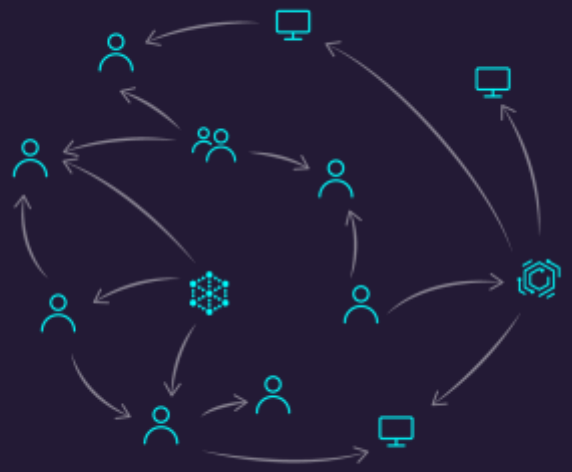


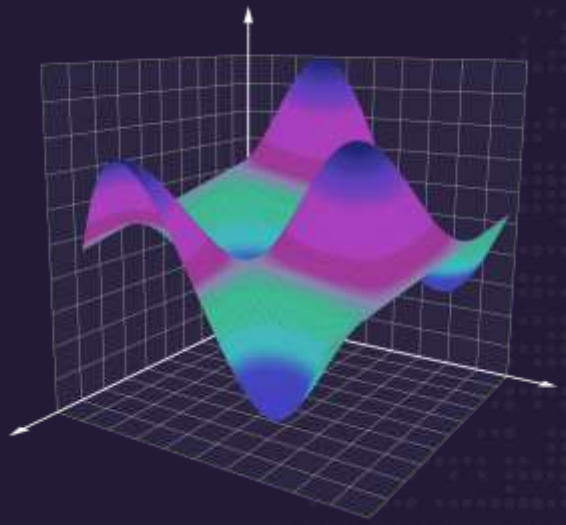
AD 攻擊路徑模擬評估服務

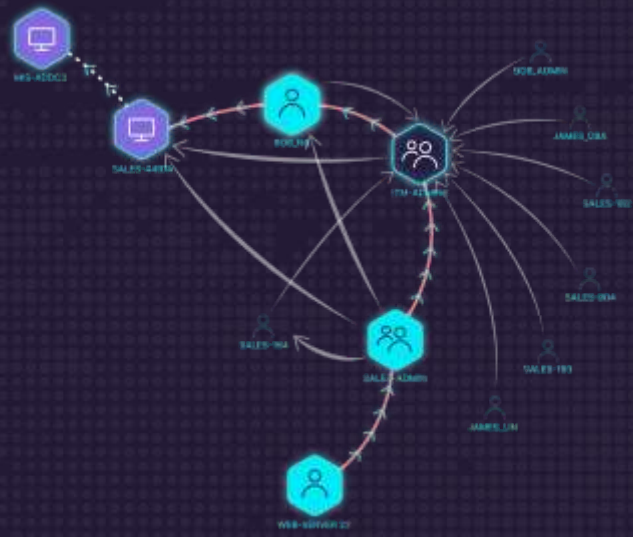
APA - Attack Path Assessment Service

- **創新科技**：整合 EDR 端點防禦與 AD 帳號分析
- **洞悉全貌**：可視化帳號關係與管理架構
- **智慧預測**：AI 模擬並預測各種條件的攻擊路徑
- **防禦評估**：量化威脅邊界與評估最佳攻擊斷點

創新的方法 Attack Path Simulation







Account Assessment

整合 EDR 的端點、 AD 的帳號資訊、與專家知識庫分析

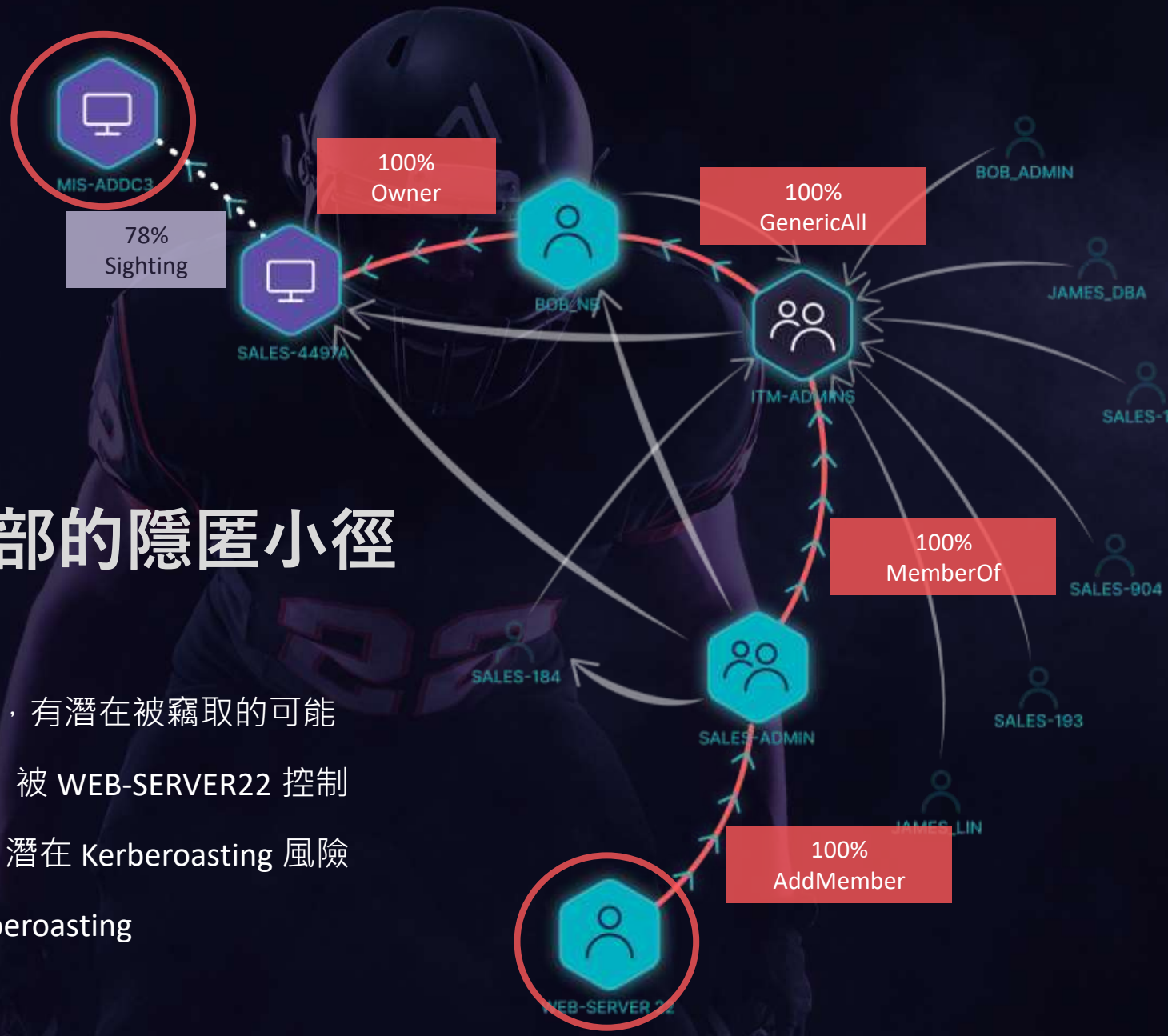
Attack Simulation

AI 計算控制權轉移機率，模型預測攻擊入侵點，攻擊成本計算

Attack Paths

推論可能的攻擊路徑，提供強化策略，縮小駭客攻擊面

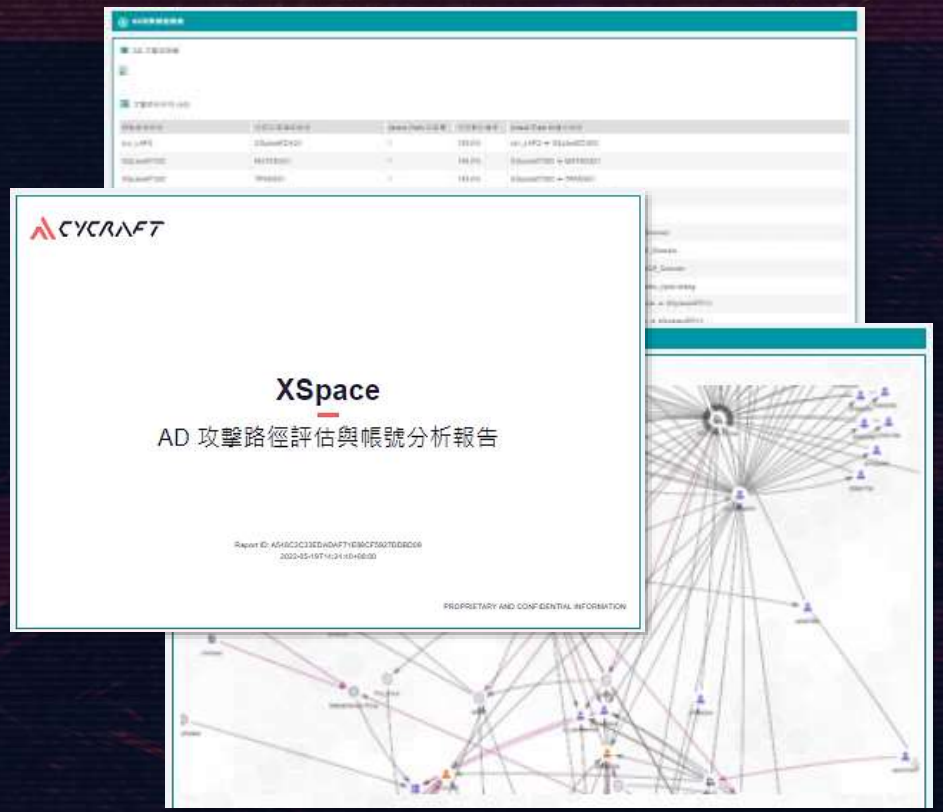
Attack Path 案例：
模擬攻擊，揪出公司內部的隱匿小徑



- AD 特權帳號 MIS-ADDC3 曾連到 SALES-4497A，有潛在被竊取的可能
- 而 SALES-4497A 可以間接透過 BOB_NB 帳號，被 WEB-SERVER22 控制
- WEB-SERVER22 是一個 Service User Account，潛在 Kerberoasting 風險
- T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting

洞悉 AD - 從量化到量測

Continuous Risk Measurement and Visualizations



> Attack Path Simulation

模擬駭客攻擊，智慧化計算所有可能攻擊路徑

可視化 AD 物件間的異常權限關係

> Account Assessment

盤點 AD 設定弱點與常見潛在安全問題

偵測潛在虛擬群組與隱匿的特權帳號

> Risk Rating and Mitigation Strategies

評估並量化 AD 環境整體資安風險

提供強化 AD 策略，限縮資安威脅邊界

CYCRAFT

分析功能與特色

AD Visualization	可視化 AD 物件關係圖，分析涵蓋各種 AD Object 包含 User、Computer、Group、OU、Container、GPO、MSI、Certificate Template
AD Security Posture	自動化量測 AD 場域帳號安全性，評估資安指標
EDR Integration	整合 Xensor EDR，彙整帳號在實際場域活動情況，並自動強化帳號防禦
Administrative Accounts	深度挖掘單位內潛在的網管 (Tier-0) 帳號，找出隱匿的權限管理問題
Attack Paths simulation	AI 演算法全面分析 AD 上的超過 40 種帳號與權限關係
Account Assessment	帳號權限分析：高風險屬性、服務帳號屬性、異常的群組與權限設定、少見的特殊權限、ADCS、LAPS、SPN、AS-REP Roasting、DCSync 等等

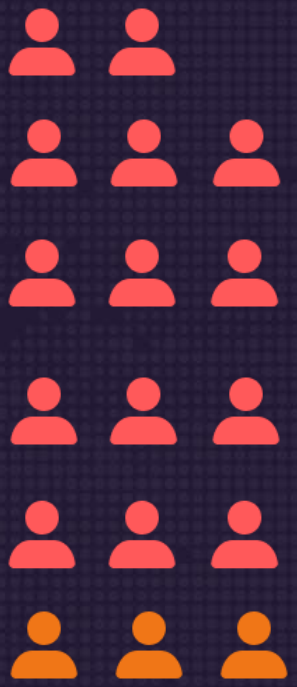
AD 網管有多少？

從我們分析過的案例中，統計了 AD 管理具規模且管理良好的上市公司客戶 (User Account 數量約 7 千至 6 萬)，往往都會發現許多客戶不知道的 AD Tier-0 的帳號 ...

實際的網管 (Tier-0) 帳號數量，
是客戶已知網管數的

5.8倍

客戶以為...



客戶實際

CYCRAFT

接下來，行動！

下一周你需要做：

- 熟悉自己單位內 AD 安全態勢，盤點已知的特權帳號
- 了解最新的 AD 安全問題，與常用的修補或是緩解策略

接下來三個月內你該做：

- 實施一次 Attack Path Assessment，以了解 AD 潛在網管帳號，找出不是網管，卻也能控制整個 Tier-0 的帳號
- 根據 APA Report 中的攻擊路徑，制定 AD 權限整治計畫，處理順序

六個月內你得做：

- 強化完成 AD 權限後，再實施一次 APA 以持續量測計畫成效

Don’t think.

Just do it.