DEVCORE

以戰代訓 – 透過攻防不斷進化資安團隊

翁浩正 (Allen Own)

戴夫寇爾股份有限公司
allenown@devco.re

CYBERSEC 2025 | 2025.04.17

講者介紹

翁浩正 (Allen Own)

戴夫寇爾 DEVCORE 執行長

台灣駭客協會 HIT / HITCON 理事長

TiEA 協會 理事及資安小組負責人

SEMI 國際半導體產業協會 資安委員會

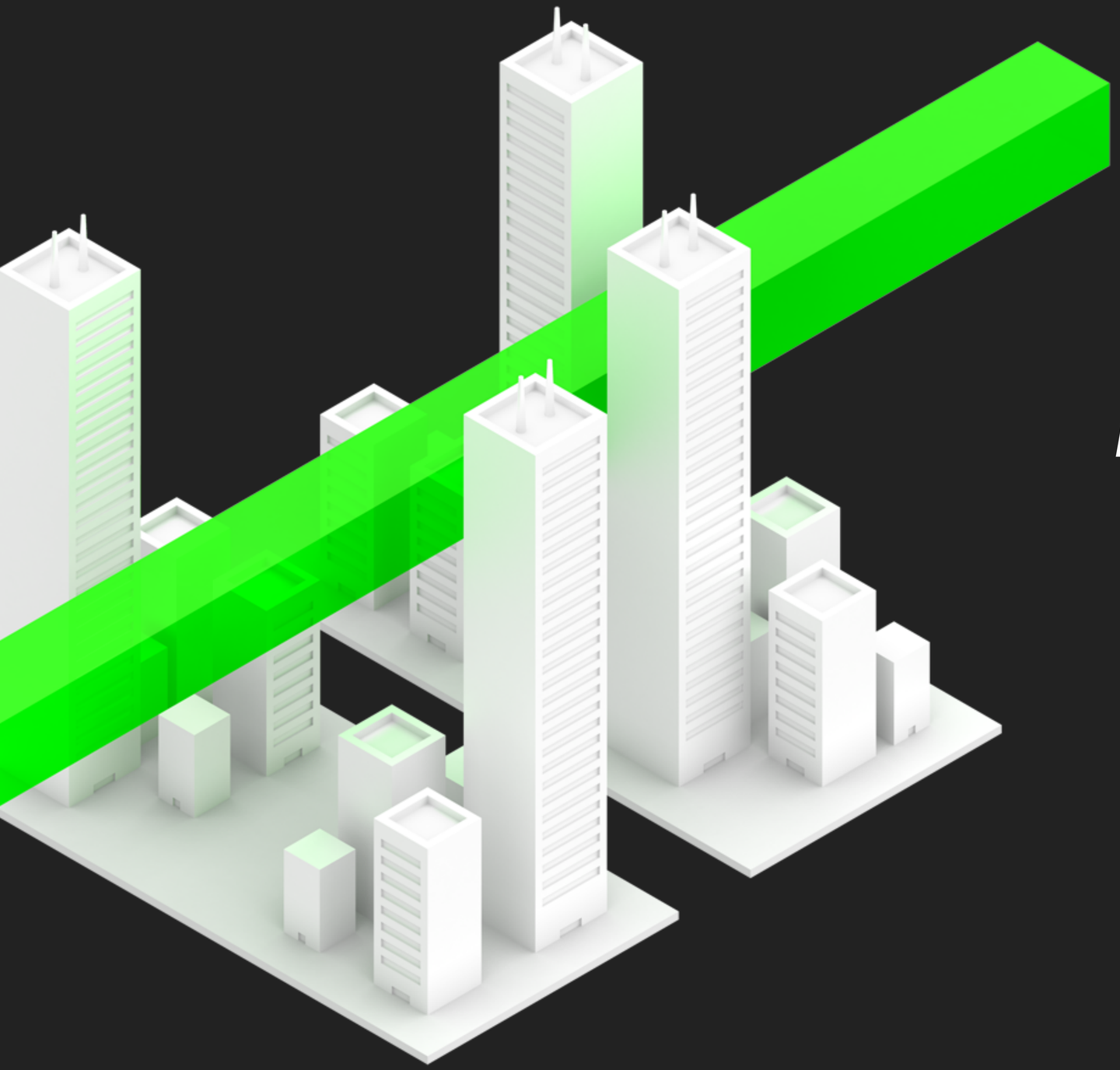
台灣數位信任協會 理事

DEVCORE

DEVCORE
SECURITY
CONSULTING

DEVCORE 成立於 2012 年，團隊由**具備駭客思維及技巧的專家組成**。專注於**世界級攻擊手法研究**，具豐富的檢測及真實資安風險評估經驗。以對資安的熱情與專業，為企業建立堅強的資安後盾。

- 國內紅隊演練及滲透測試領導廠商
- 客製化攻擊工具的能力
- 發現世界級產品 0-day 漏洞能力
- 熟悉最新的攻擊技巧



DEVCORE

最專注攻擊的資安公司


資安的最大困境是什麼？


是團隊不夠強！
是敵人太強！
是我們疲於奔命抵禦敵方全力的進攻！

#REDTEAM

對紅隊疑問 TOP 3

1 我到底安不安全
有沒有進步

2 未來後續規劃
該怎麼進行

3 打不進去
是不是就畢業了

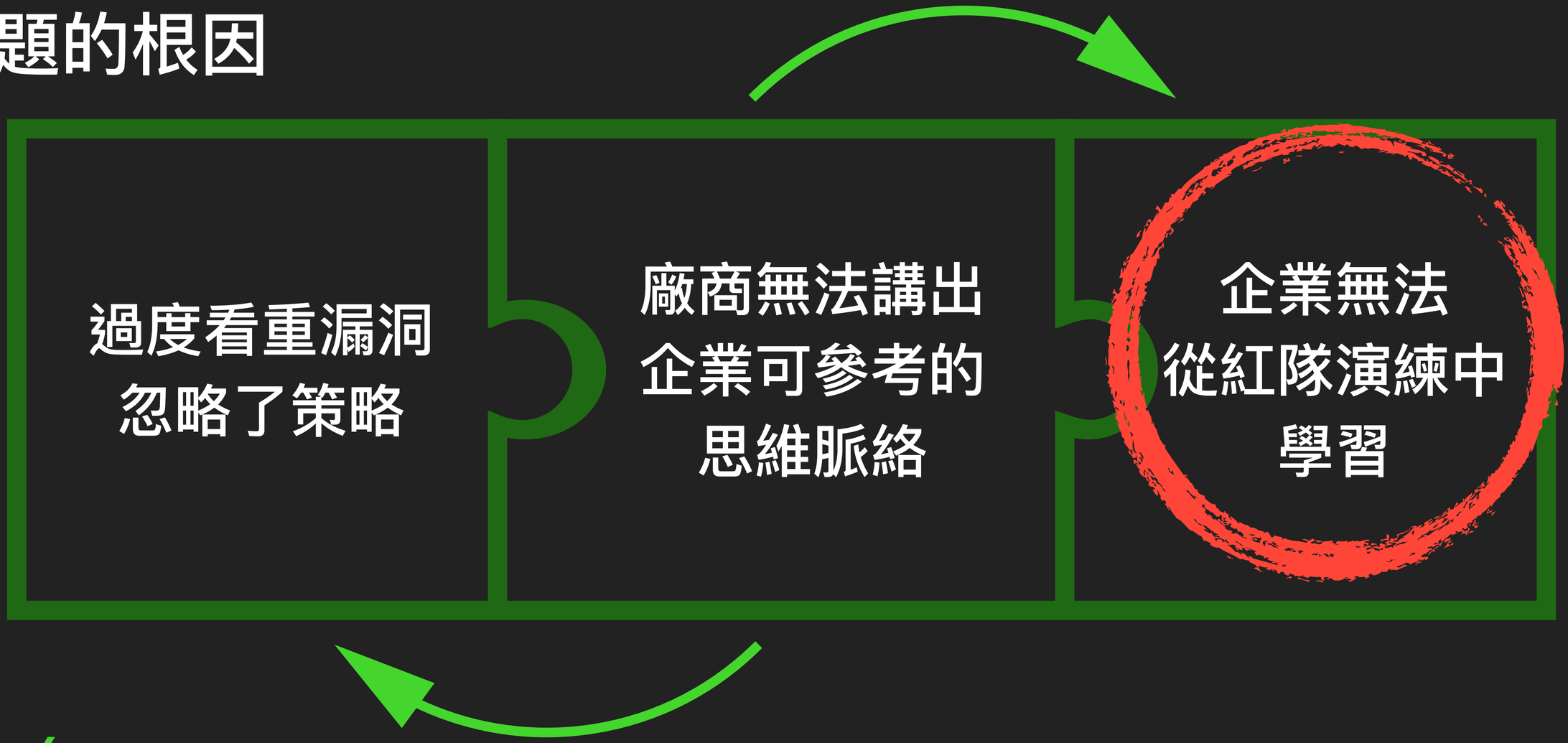
問題的根因是什麼

CYBERSEC 2024

DEVCORE

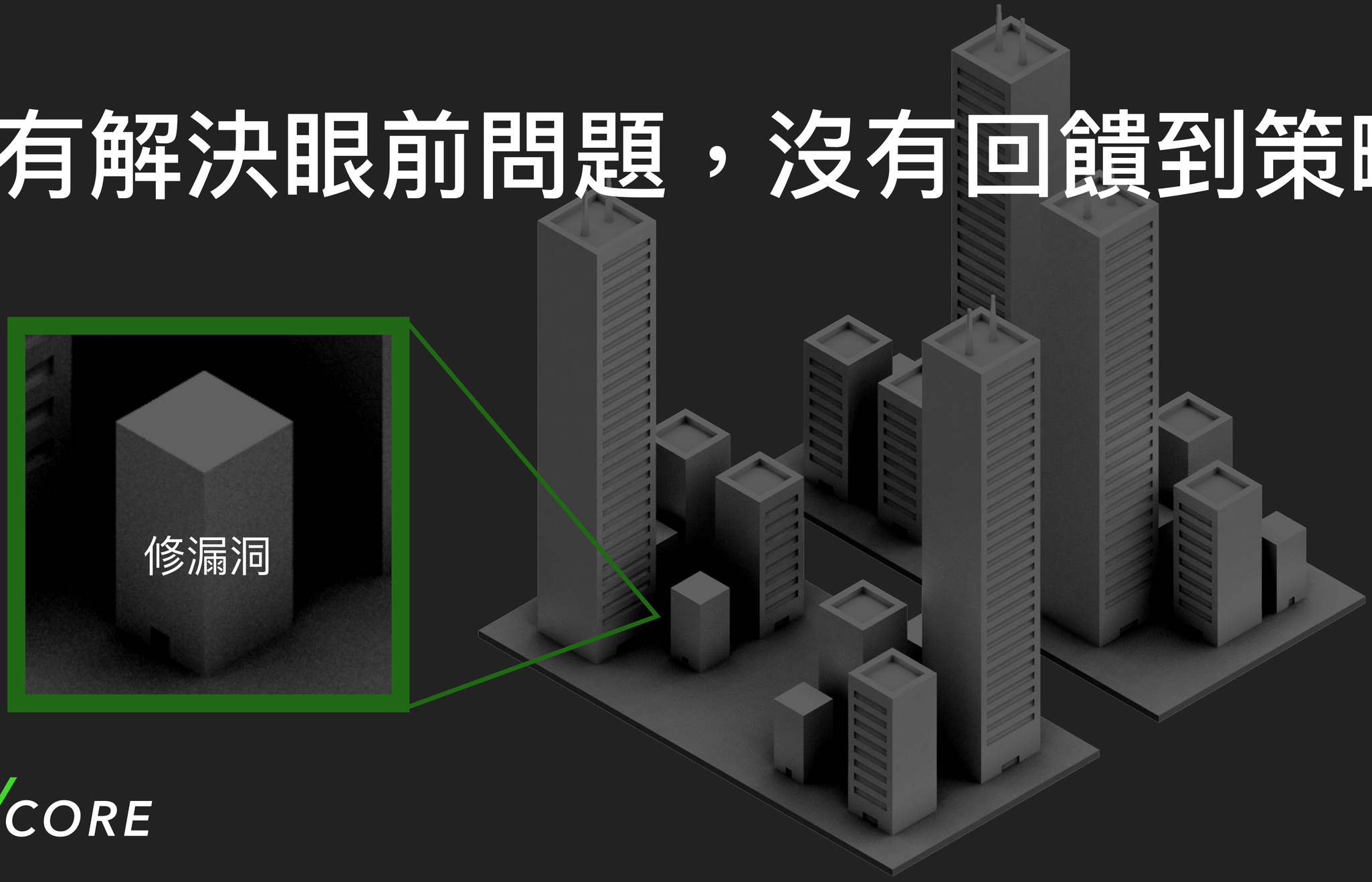
#紅隊的疑問

問題的根因



DEVCORE

只有解決眼前問題，沒有回饋到策略

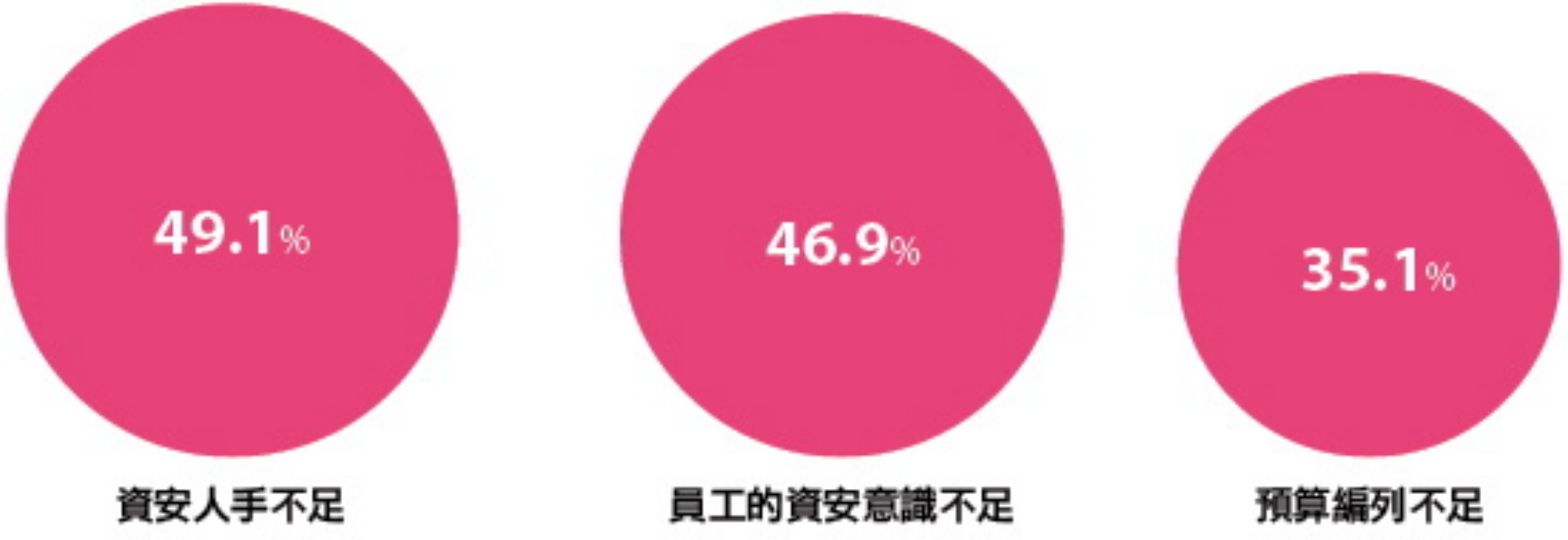


DEVCORE

2024 年企業資安三大阻礙

半數企業苦於資安人手不足和員工資安意識不足

iThome
2024
資安大調查



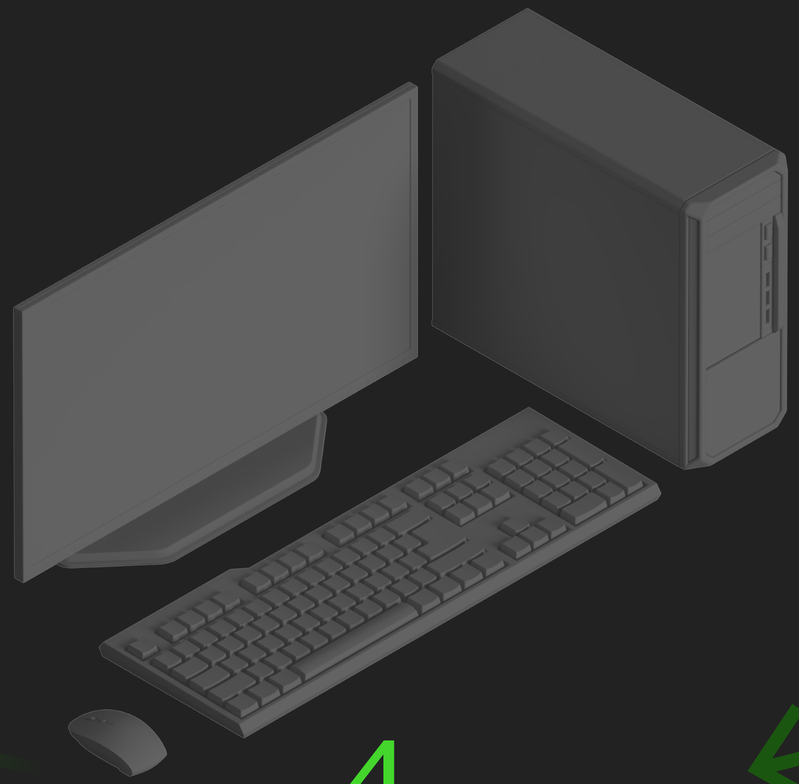
說明：百分比為將該項列為資安阻礙（無法做好資安的痛點）的企業比例
資料來源：2024 iThome CIO大調查，2024年5月

https://www.ithome.com.tw/article/163450

消極防禦循環

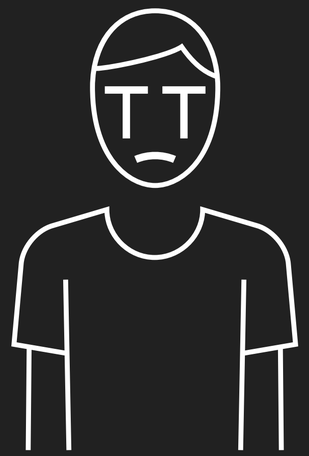
DEVCORE

2.
事件應變



3.
修補 & 調查

1.
攻擊事件



4.
檢討（挨罵）

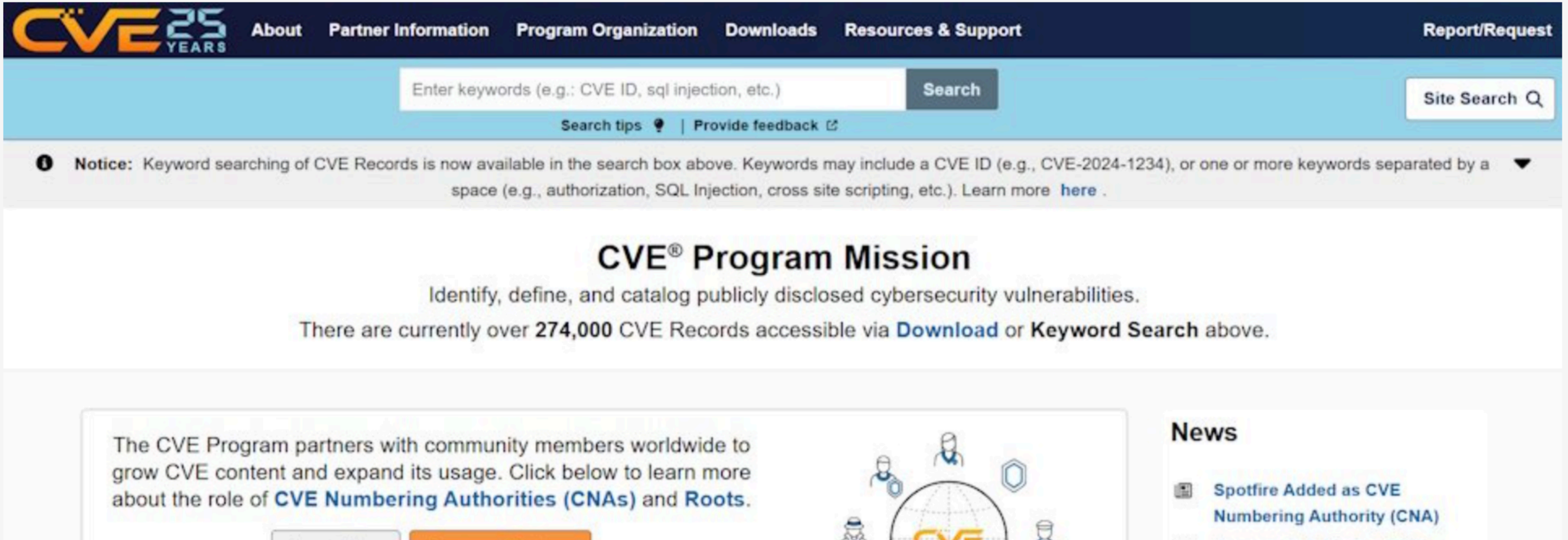
不過，昨天有人跟我說，
資安圈終於出現令人振奮的新聞

新聞

川普大砍行政預算，CVE與CWE專案的合約本周到期

美國國土安全部委託非營利組織MITRE進行的CVE與CWE專案合約在4月16日到期，外界猜測應是川普大砍美國行政預算所導致

文/ 陳曉莉 | 2025-04-16 發表



US funding running out for critical cyber vulnerability database, manager says

By **A.J. Vicens** and **Raphael Satter**

April 16, 2025 7:06 AM GMT+8 · Updated a day ago

WASHINGTON, April 15 (Reuters) - The defense and research-focused nonprofit MITRE Corporation says funding from the U.S. government runs out on Wednesday for it to maintain a critical database of cyber vulnerabilities used by security researchers and digital defenders the world over.

MITRE manages the Common Vulnerabilities and Exposures (CVE) database which aims to identify, define and catalog publicly disclosed cyber weaknesses, enabling IT administrators to quickly flag and triage the myriad different bugs and hacks discovered daily.

今天...

他罕見的早上就倒了一杯威士忌

CVE Program Funding Reinstated—What It Means And What To Do Next

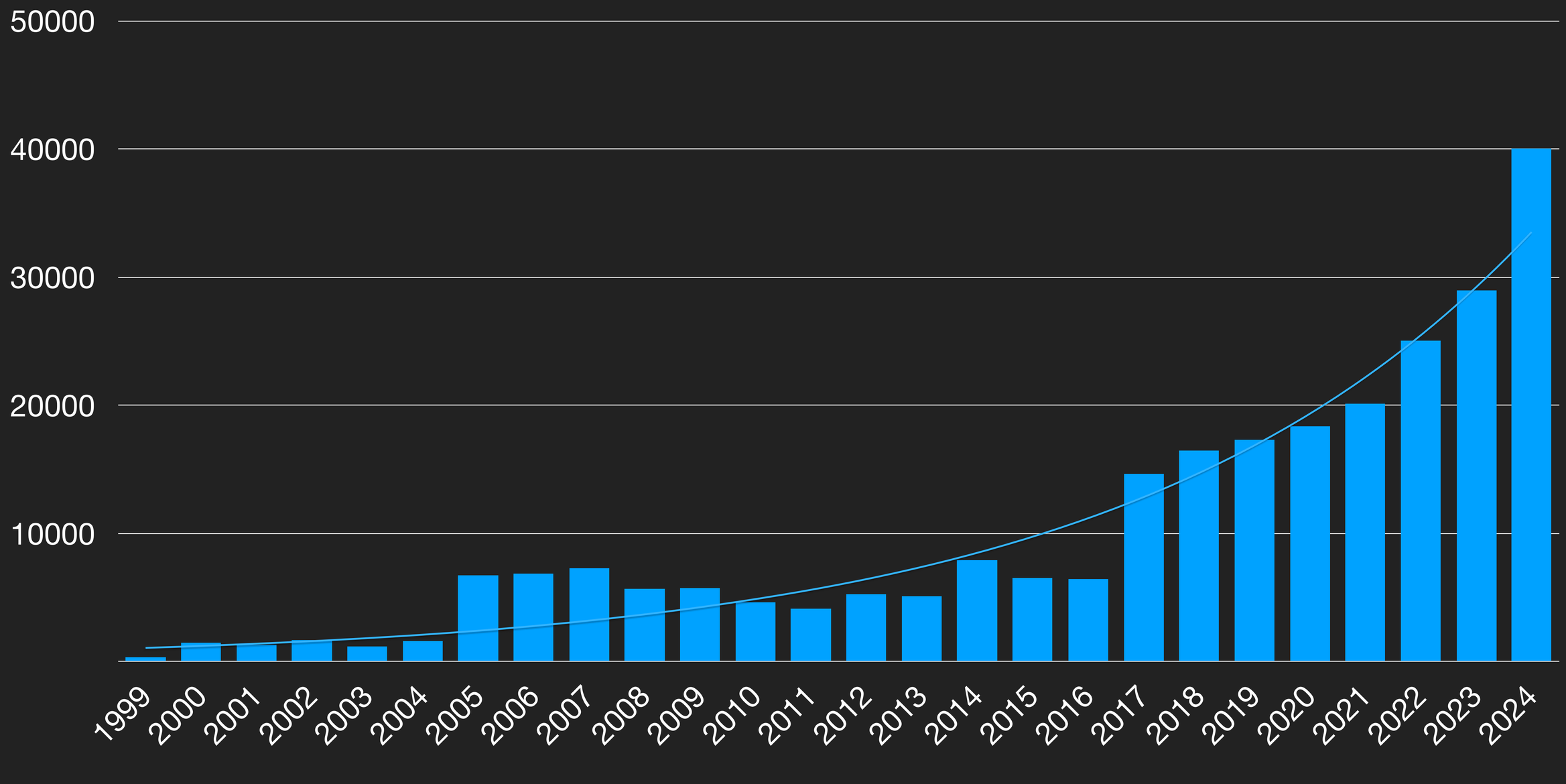
By Kate O'Flaherty, Senior Contributor. Kate O'Flaherty is a cybersecurity an...

Follow Author

Apr 16, 2025, 11:08am EDT

U.S. President Donald Trump has cut funding for the global database of security flaws, the Common ... More
GETTY IMAGES

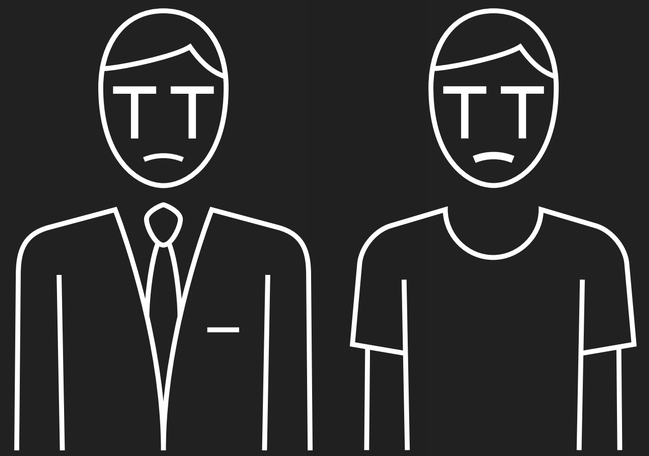
CVE 每年公開漏洞總數量



現今資安團隊疲於奔命的真相

DEVCORE

- 事件處理時間黑洞：全球平均資安事件發現時間 **194 天**（※1）
- 修補漏洞永無止境：2024 年 CVE 漏洞編號共公開 **40077 個**（※2）
- 警報疲勞：平均每天處理超過上百則告警，但**忽略率高達 50%**
- **不斷應對資安事件卻缺乏主動成長的機會**



※1: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry
※2: https://www.cve.org/about/Metrics

傳統教育訓練為何失效

DEVCORE

- 知識與實戰脫節：

  課堂理論與實際攻擊手法差距大

- 訓練頻率不足：

  每人每年僅安排 3 – 12 小時專業訓練

- 內容更新緩慢：

  課程內容平均比最新攻擊手法晚 6 – 12 個月

TIPS

變強

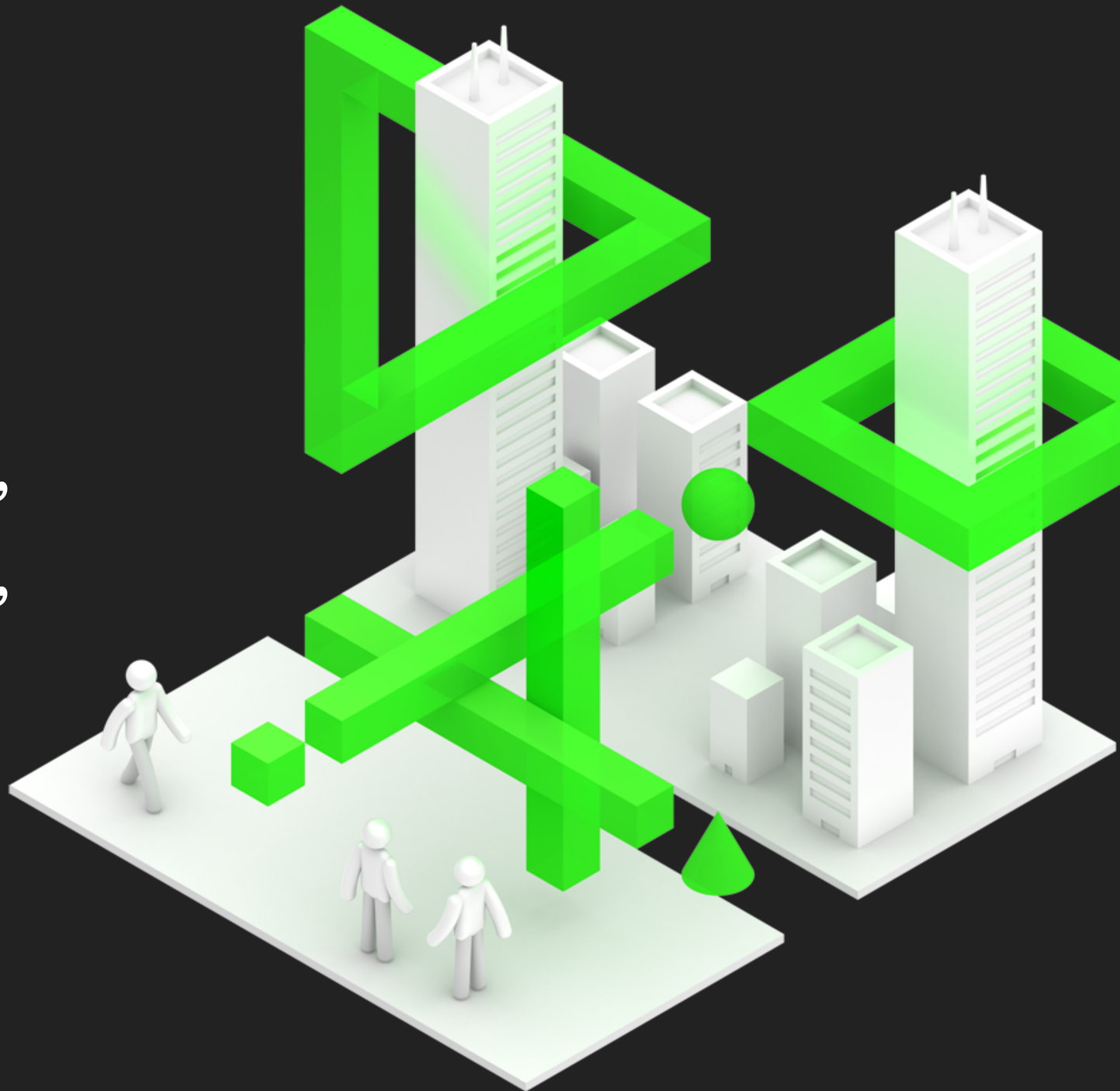
DEVCORE

最完善的防禦
從了解攻擊開始

DEVCORE

以戰代訓

以實戰或模擬取代傳統訓練，
讓團隊在接近真實的環境下，
鍛鍊作戰技能與應變能力



DEVCORE

為什麼實戰對學習更有效

DEVCORE

情境學習理論

在真實環境中學習效果提升 80%

壓力幫助記憶

適度的壓力能夠促進記憶的鞏固
（腎上腺素如皮質醇）

為什麼實戰對學習更有效

DEVCORE

回想記憶最深刻的資安經驗，是來自課堂還是實際事件？

情境學習理論

在真實環境中學習效果提升 80%

壓力幫助記憶

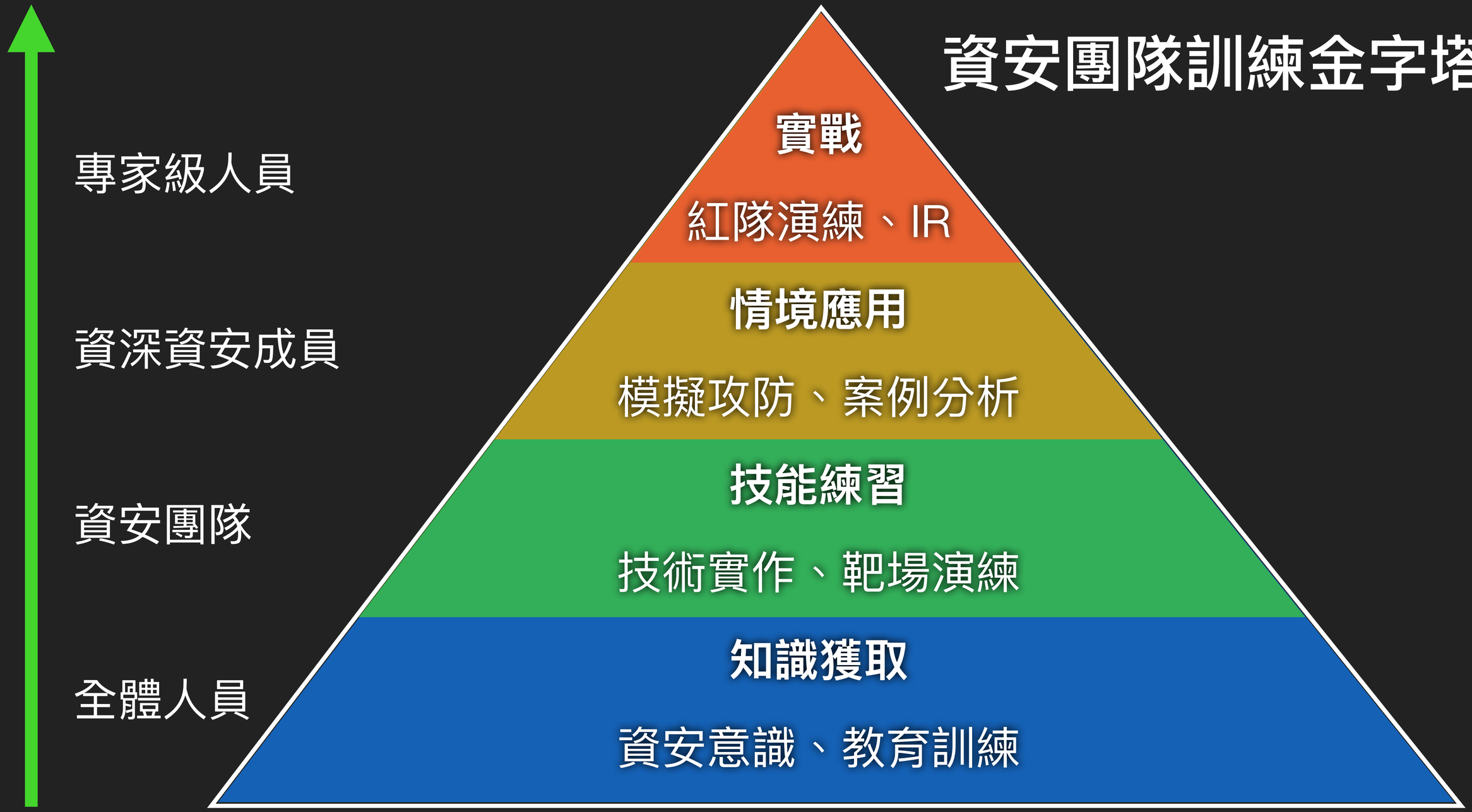
適度的壓力能夠促進記憶的鞏固
（腎上腺素如皮質醇）

資安訓練方法的演進

- 訓練方式隨著威脅演進而進化
- 除了「教育訓練」之外，
  資安服務也都該有訓練團隊的本質
- 就連資安事件的處理，
  也都應成為資安團隊的重要養分

DEVCORE

資安團隊訓練金字塔


專家級人員
資深資安成員
資安團隊
全體人員
實戰
紅隊演練、IR
情境應用
模擬攻防、案例分析
技能練習
技術實作、靶場演練
知識獲取
資安意識、教育訓練

同仁 A

走啊！我們一起去報這堂教育訓練課！

同仁 B

哇你這麼上進喔？我事情已經做不完...

同仁 A

當然是可以溜出去逃離辦公室囉...

同仁 B

算我一份。

資安人的迷惑行為

傳統教育訓練

DEVCORE

- 建立資訊安全的基本理論框架，形成團隊之間溝通的標準語彙。
- 優點：基礎知識建立、標準化、易於執行、大規模實施
- 缺點：缺乏實戰經驗、無法模擬真實攻擊、知識轉化率低

DOs **建構系統化知識，幫助碎片化學習歸檔**

DON’Ts **消化上課時數、逃離辦公室**

知識建構

同仁 A

(認真盯著螢幕...)

同仁 B

欸你這一題會解嗎？老師講的我聽不太懂。

同仁 A

成功了！台積電我 850 掛到了！

同仁 B

.....看盤？

資安人的迷惑行為

線上學習與認證

DEVCORE

- 培養自主學習與國際認證能力，對齊基礎知識與證照標準，同時為職涯加值。
- 優點：系統化學習、教材更新較即時
- 缺點：缺乏與講師的實體互動、語文問題

DOs **建構系統化知識、探索資安各領域自我定位**

DON’Ts **消化上課時數、掛機看股票**

自主學習

虛擬靶場 (Cyber Range)

DEVCORE

- 在模擬企業環境中訓練攻防技能，適應真實場域中的壓力與系統複雜性，熟悉團隊協作及分工方式。
- 優勢
  - 不同攻擊情境腳本
  - 安全可重複的訓練環境
  - 即時回饋與評估
  - 量化技能學習

模擬實戰

DOs **練習工具、訓練團隊合作、展現能量**

DON’Ts **照抄別人的做法、以為這是 CTF**

同仁 A

這個弱點掃描報告修補完了嗎？
下週一主管要看。

同仁 B

我很多東西看不懂啊！報告也沒有說該怎麼修。

同仁 A

不用看懂啊！我們分工合作，我去改 PDF 把風險改低，你重新產一份沒漏洞的複測掃描報告。

同仁 B

這種分工合作嗎？！

資安人的迷惑行為

弱點掃描 (VA)

DEVCORE

- 學習掃描工具與漏洞評估，理解漏洞本質與成因，並根據風險進行資源配置與修補，規劃優先順序。
- 優勢
  - 操作簡單、人力介入少
  - 系統性理解弱點分類
  - 掌握修補優先順序
  - 協助資產盤點、漏洞盤點

風險盤點


DOs **驗證漏洞成因、盤點系統漏洞**


DON’Ts **全盤接受，不管我只修漏洞**

同仁 A

快稽核了，這次要年度滲透測試，麻煩你去產生掃描報告。

同仁 B

我們還沒找廠商耶，是要從詢問既有掃描廠商能不能做滲透嗎？

同仁 A

把原本的弱點掃描專案，名稱改成「滲透測試暨弱點掃描」，然後請他們一樣出原本的掃描報告。

同仁 B

我怎麼感覺哪裡怪怪的....

資安人的迷惑行為

滲透測試 (PT)

DEVCORE

- 透過駭客思維思考系統弱點，理解真實攻擊路徑與防禦弱點。
- 如何訓練
  - 從外部視角審視防禦
  - 理解攻擊鏈與路徑
  - 發現防禦盲點
- 學習循環
  - 結果分析與歸納：漏洞成因、系統架構
  - 防禦策略調整：針對漏洞強化防禦
  - 團隊能力強化：盤點團隊技能
  - 知識庫建立：知識系統化

DOs **學習駭客思維、驗證漏洞成因、學習 Secure Coding**

DON'Ts **當成弱點掃描處理、每年例行的麻煩作業**

攻擊思維

同仁 A

我們這次買了紅隊演練工具 BAS 來掃描！

同仁 B

我記得 Allen 說這好像不一樣？

同仁 A

一樣啦！都說是攻擊模擬了。掃描出報告，成本又低。掃看看伺服器有沒有哪些 CVE。

同仁 B

我好像都掃不出來...

資安人的迷惑行為

入侵及攻擊模擬 (BAS)

DEVCORE

- 定期模擬攻擊手法，自動驗證防禦產品是否能正確阻擋並產生警報。
- 優勢
  - 自動化定期驗證防禦設備
  - 協助調整防禦控制措施

自動化驗證

DOs **驗證防禦措施有效性，學習針對脆弱點持續監控調整**

DON’Ts **當作一般掃描，當作找漏洞，不做任何調整亂掃描一通**

DEVCORE

您認為組織中
最難有效防禦的攻擊途徑是什麼？

紅隊演練

DEVCORE

- **最接近實戰的訓練**，找出企業立即入侵風險及防禦措施有效性，測試企業資安能力在真實壓力下的反應與協作機制。
- 紅隊演練 vs. 滲透測試
  - 目標導向 vs. 單一系統
  - 持續性 vs. 一次性
  - 隱蔽性 vs. 協同性
  - 綜合戰術 vs. 單一技術

驗證防禦

紅隊演練的技術層次

1. 初級

已知漏洞利用、
基本權限提升

2. 中級

防禦規避、
持久性植入、橫向移動

3. 高級

客制化攻擊工具、
0-Day 利用、APT 攻擊

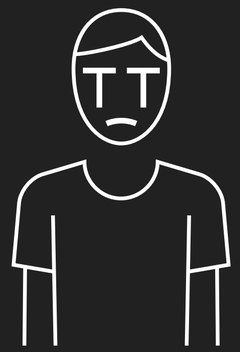
DEVCORE

紅隊演練時企業常見錯誤心態

DEVCORE

- 把紅隊當外包稽核
  - 覺得紅隊只是來「找洞」，結果交給紅隊，自己不必參與
  - 影響：錯失學習與流程最佳化機會，內部團隊無成長

- 怕丟臉、怕被打穿、怕被究責
  - 擔心紅隊結果太難看會影響評鑑或對外觀感
  - 影響：惡性抵抗、限制演練範圍、抑制攻擊路徑，無法暴露真正風險



客戶 A

請提供紅隊會使用的 IP 區段。

DEVCORE

好的，我們是 xxx.xxx.xxx.xxx。

客戶 A

(把 xxx.xxx.xxx.xxx 全擋掉)

DEVCORE

？？？

真人真事 1

客戶 A

我們想確認 OOO 是否你們的演練行為，我們只是掌握不會阻擋。

DEVCORE

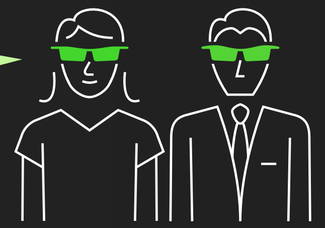
是的，我們在 2025/04/17 16:15 進行的行為，會再進一步滲透。

客戶 A

好的。
（轉頭）擋掉。

DEVCORE

？？？

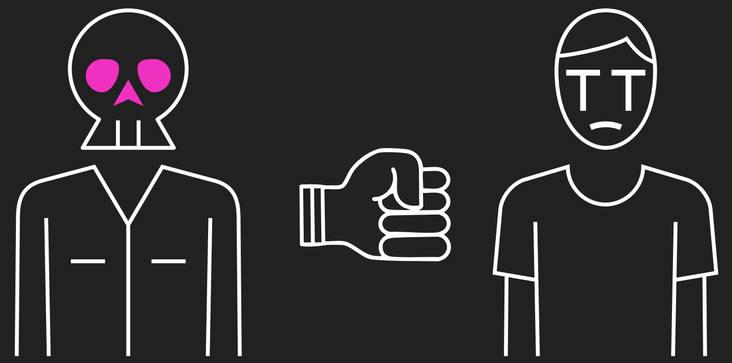


真人真事 2

紅隊演練時企業常見錯誤心態

DEVCORE

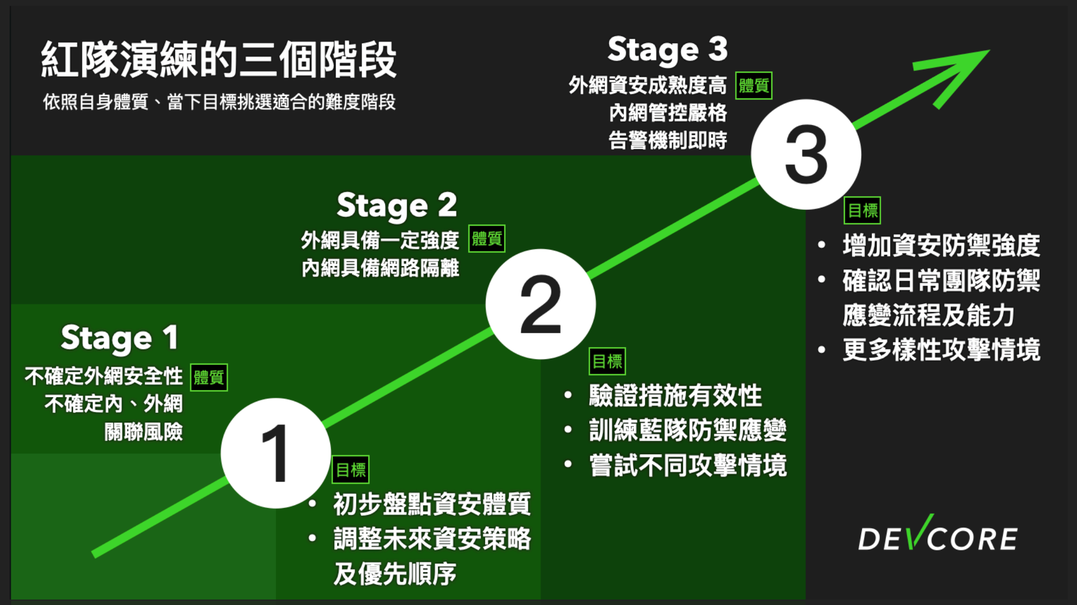
- 只看結果報告、忽略過程
  - 紅隊報告當成一份交辦作業，只修補列出的漏洞
  - 影響：忽略系統性問題（例如流程缺口、監控盲點、跨部門機制失靈）
- IT 部門與資安部門脫節
  - 入侵滲透點經常在 IT 管理面，但 IT 不參與演練或抗拒修正
  - 影響：資安成果難落實，持續產生結構性風險



紅隊演練時企業常見錯誤心態

DEVCORE

- 防禦團隊事後才參與
  - 紅隊打完後，藍隊看報告才知道內容，無法互動學習
  - 影響：無法培養團隊實戰經驗，也無即時回饋可用於學習



紅隊演練的三個階段

依照自身體質、當下目標挑選適合的難度階段

Stage 1

不確定外網安全性
不確定內、外網
關聯風險

體質

1

目標

- 初步盤點資安體質
- 調整未來資安策略及優先順序

Stage 2

外網具備一定強度
內網具備網路隔離

體質

2

目標

- 驗證措施有效性
- 訓練藍隊防禦應變
- 嘗試不同攻擊情境

Stage 3

外網資安成熟度高
內網管控嚴格
告警機制即時

體質

3

目標

- 增加資安防禦強度
- 確認日常團隊防禦應變流程及能力
- 更多樣性攻擊情境

DEVCORE

紅隊演練的三個階段

依照自身體質、當下目標挑選適合的難度階段

Stage 1

不確定外網安全性 體質
不確定內、外網
關聯風險

1

目標

- 初步盤點資安體質
- 調整未來資安策略及優先順序

Stage 2

外網具備一定強度 體質
內網具備網路隔離

2

目標

- 驗證措施有效性
- 訓練藍隊防禦應變
- 嘗試不同攻擊情境

Stage 3

外網資安成熟度高 體質
內網管控嚴格
告警機制即時

3

目標

- 增加資安防禦強度
- 確認日常團隊防禦應變流程及能力
- 更多樣性攻擊情境

DEVCORE

紅隊演練期間的最佳實踐做法

1. 明確定義紅隊目標與成功條件
   - 與紅隊合作前，內部要明確界定**「訓練」 vs「驗證」**的目標
   - 是否以打穿為主？還是觀察藍隊反應？或演練某類情境？
2. 建立內部觀察與學習機制
   - 指派內部資安人員與紅隊互動，觀察攻擊流程
     （如 TTP、繞過邊界、防守反應）
   - 紅隊期間不參與防守阻擋，但監控觀察可用於事後教育訓練

DEVCORE

紅隊演練期間的最佳實踐做法

3. 同步進行藍隊觀察與事件回應
   - 觀察是否能從 SIEM、EDR 中發現異常行為，訓練事件調查與判斷
   - [第三階段] 鼓勵藍隊「照常」防守，但不事先告知演練細節
4. 紅隊結束後安排專案說明及內部檢討會議
   - 由紅隊逐步說明攻擊邏輯、使用工具、繞過技巧，讓團隊理解攻擊者思維
   - 除了閱讀演練報告，內部應召開「攻擊流程重現」會議

DEVCORE

紅隊演練期間的最佳實踐做法

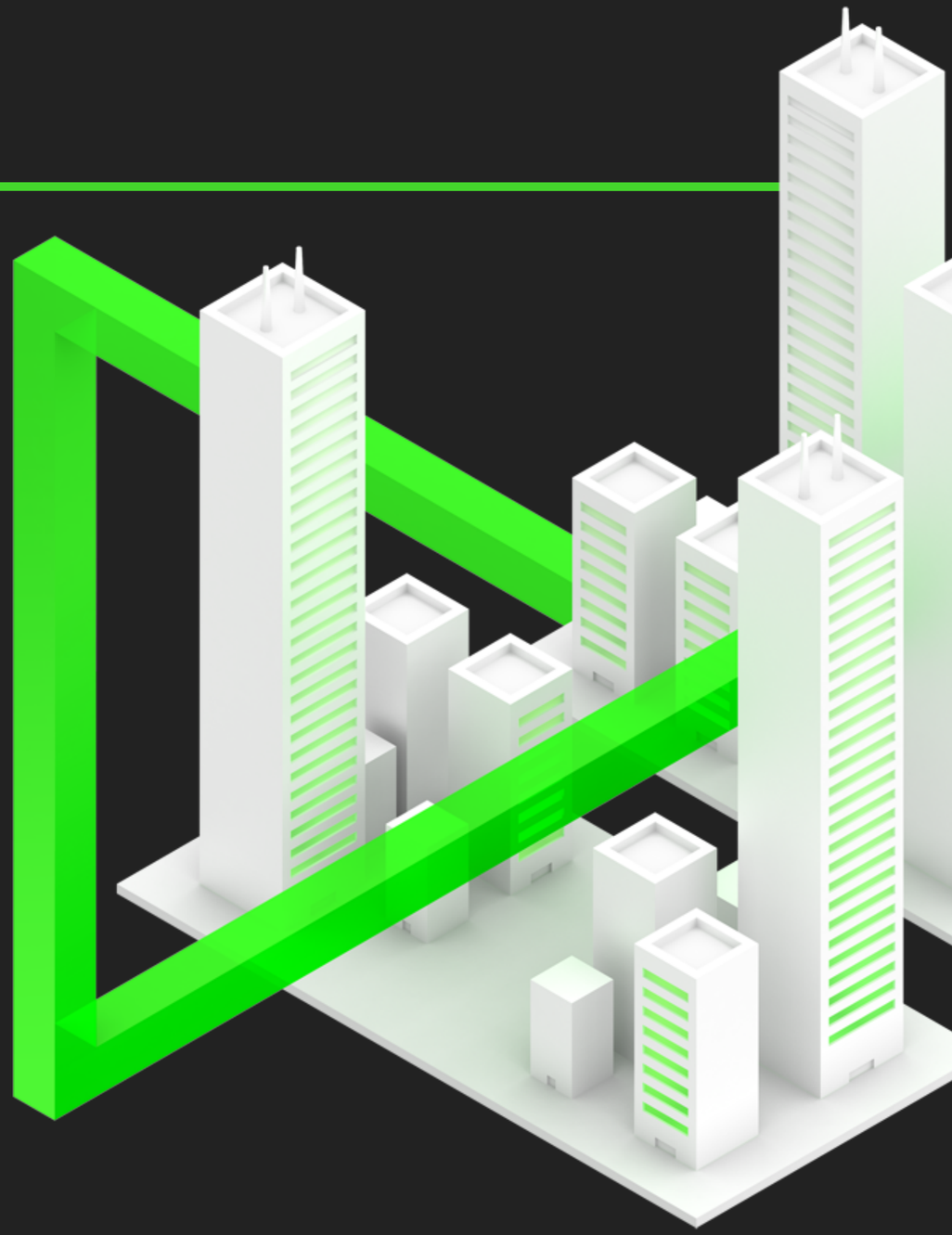
5. 建立「導入成果→訓練內容→改善追蹤」閉環

- 將紅隊演練中揭露的問題，

  分類為**技術/流程/人員**

- 問題對應不同改善方案
- 指派負責人並列入季度追蹤
- 隔年紅隊演練啟動時，

  優先追蹤前次項目，確認並驗證改善情況



DEVCORE

紅隊演練時藍隊該做什麼

DEVCORE

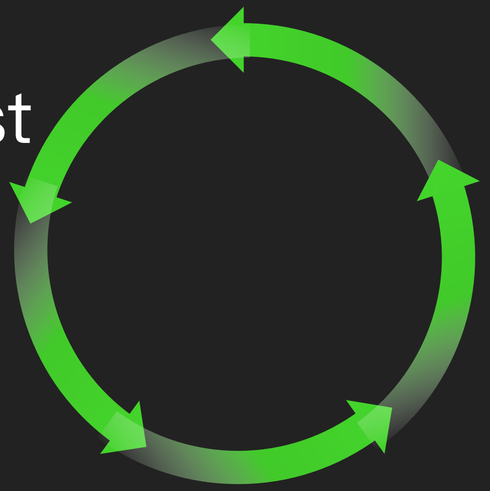
- 藍隊核心能力培養
  - 威脅檢測策略制定
  - 事件分類與優先順序判斷
  - 證據軌跡收集與保存
  - 根因分析與復原計劃
  - 事後改進與防禦最佳化

有效運用紅隊演練成果

DEVCORE

- 紅隊成果轉化為訓練素材：
  - 攻擊路徑分析練習
  - 防禦措施失效點 & 有效性評估
  - 技術與流程改進點識別
  - 攻擊技術解析
  - 對抗技術實作 Lab
  - 團隊協作環節優化
- 建立知識庫：

  將演練經驗系統化保存與應用
  - 攻擊技術分類 (ATT&CK)
  - 防禦最佳實踐
  - 事件回應手冊
  - 事件應變 Checklist



真實資安事件處理

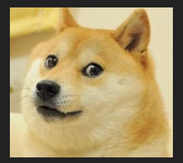
DEVCORE

- 在混亂與不確定下決策與行動，
  提升跨部門協作與事件通報、處理、復原的整體韌性。
- 資安事件的學習框架
  - 事件時間軸重建與分析
  - 攻防對抗關鍵點識別
  - 防禦失效原因歸納
  - 未來防禦改進規劃
- 從事件中提取訓練素材
  - 真實案例教學
  - 團隊自我評價
  - 流程與技術優化
  - 創建團隊知識庫

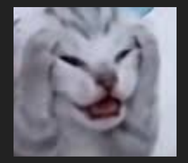
「最好的訓練素材來自於真實事件」

現實有這麼美好嗎？

老闆

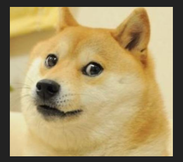


Allen 說團隊要學習，我怎麼看你們都不像是會學習的樣子。

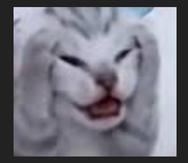


報告老闆，沒時間啊... 每天忙著工作開會，根本沒時間學習啊！

老闆

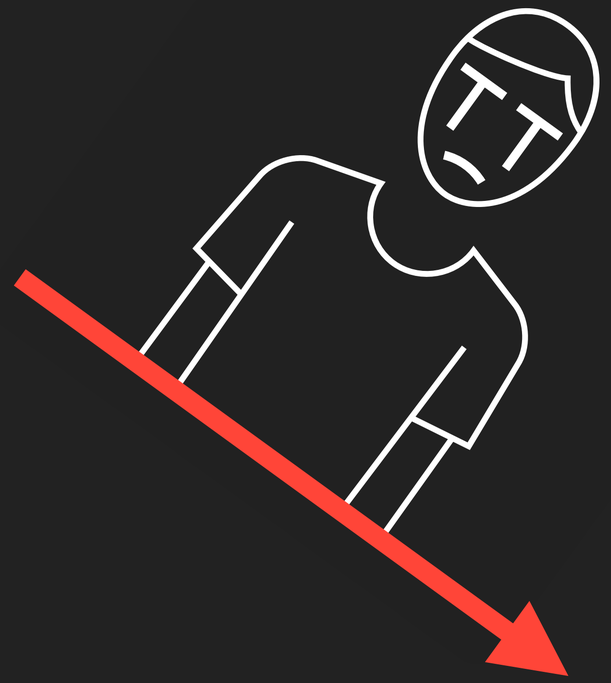


都是藉口！



人家資安都是完整系統化學習，就只有我們的時間支離破碎...

甲方資安人員常見的學習困境



時間碎片化，學習中斷

- 工時長、常臨時支援 IT/稽核/專案、學習**時間被切割**。
- 假日想進修卻**疲憊無力**，導致只看資料但無深入吸收。

任務導向導致技術片段化

- 每天在處理事件、配合部署新工具、寫報告，學到的都是**局部知識**。
- 沒有餘裕完整了解底層原理（如只會跑 Nessus，卻不懂風險評分邏輯）。

沒有學習地圖，迷失方向

- **學習目標模糊**，只能跟著需求走，沒有主線任務，不知為何而做

缺乏討論與社群回饋

- 公司缺資安團隊，可能整個部門**只有你一人**，也沒有 mentor，難以驗證知識對錯或交換觀點。

現實與理想落差

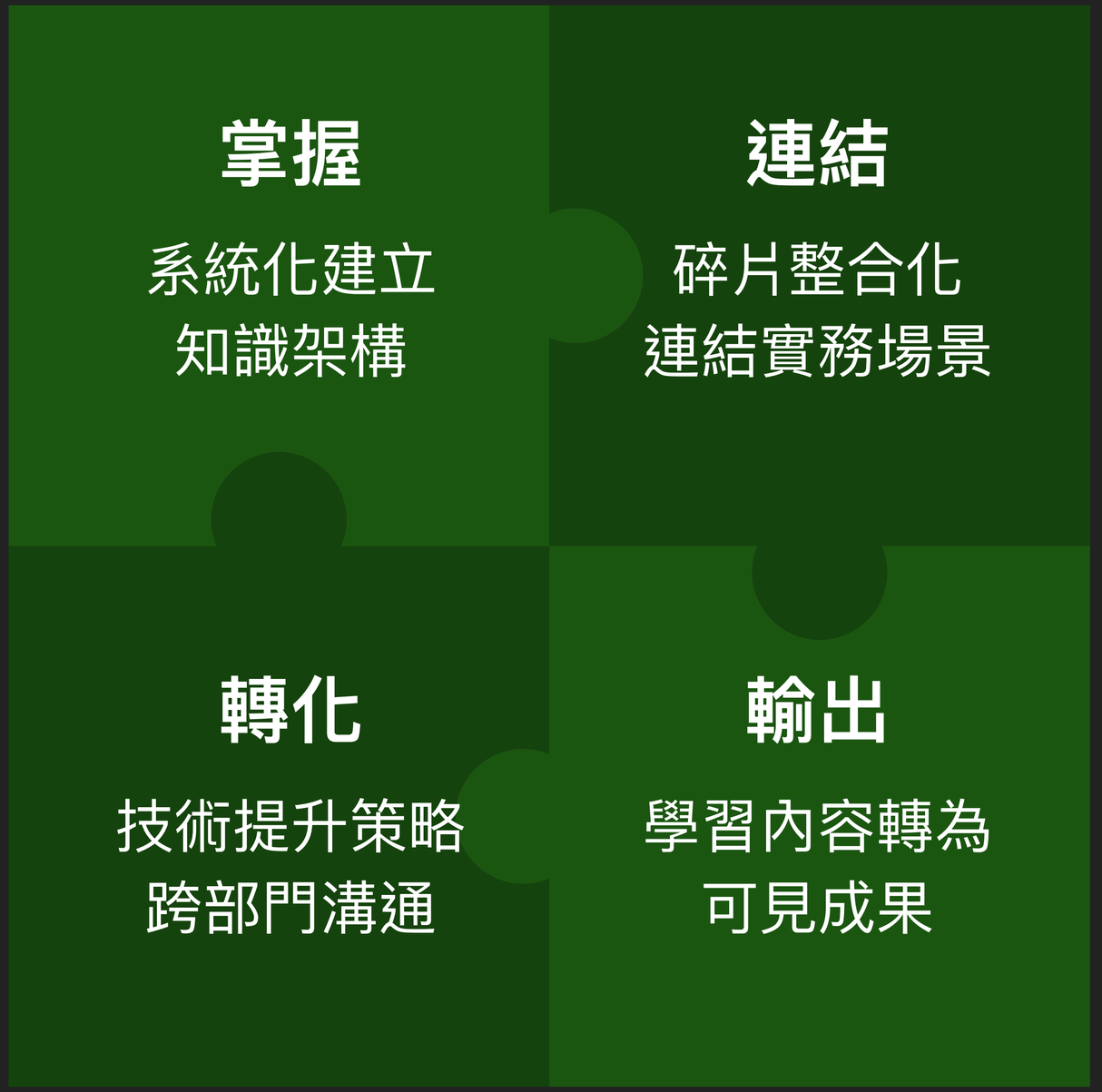
- 學到的理論（如 CSF）很完美，實際上卻**無法導入**（預算不夠、IT 不配合、C-Level 不懂資安風險）。

#變強的秘訣

策略性學習

- 定位資安職能地圖
- 設定學習主線架構，避免瞎忙
- **系統化打基礎，碎片化學習連結映射**
- 建立輸出的習慣就是最強的學習方式

（輸入輸出 **3:7**），如報告、內訓



DEVCORE

現實學習目標

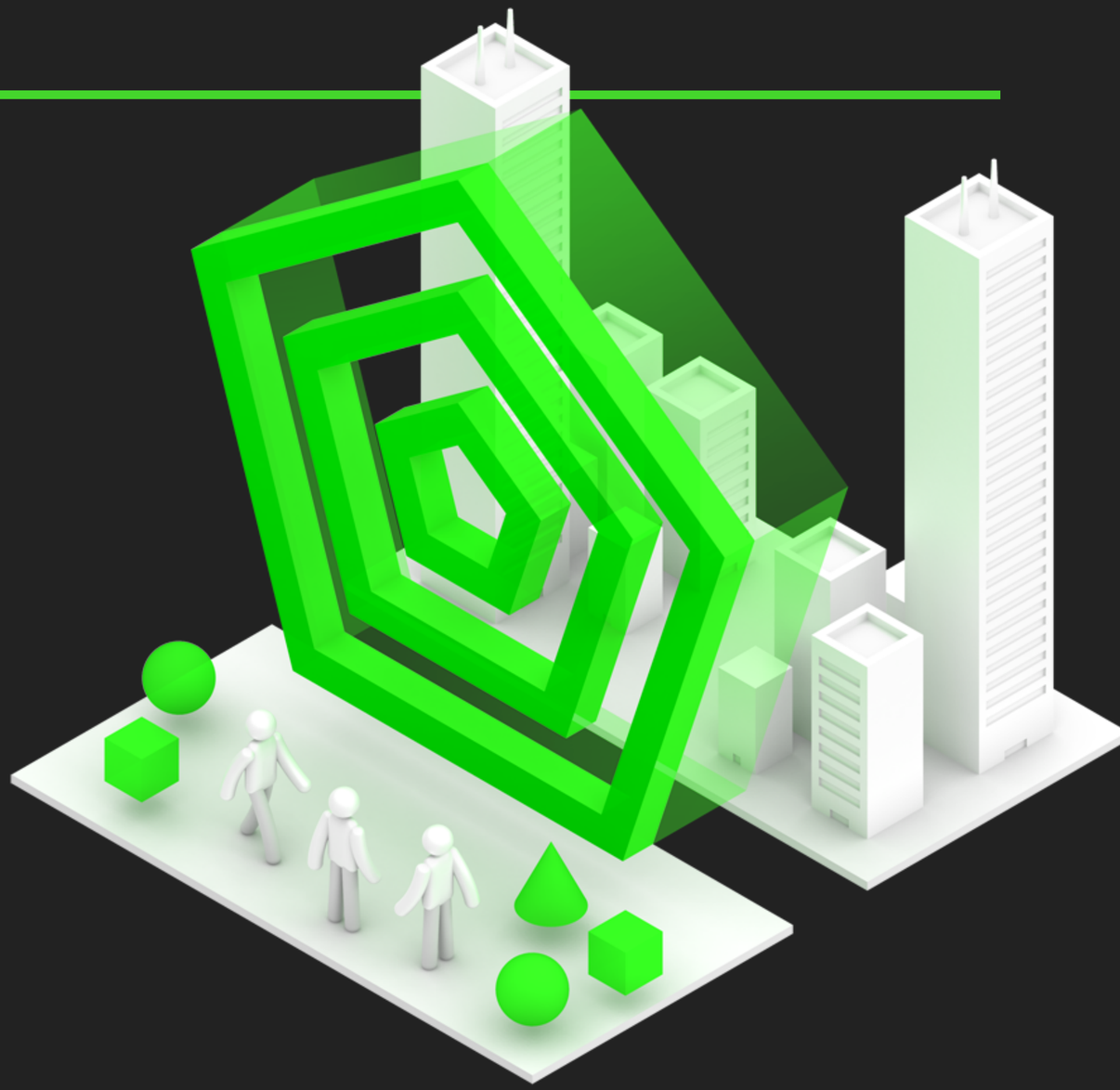
DEVCORE

- 資安人員面臨的不是技術瓶頸，而是「**職涯倦怠與動能耗損**」。
- 克服目標
  - 有成就感（不只是修補漏洞）
  - 有掌控感（不是被動支援，而是主導策略）
  - 有成長路徑（知道三年後的自己會變得更強、更值錢

現實學習目標

DEVCORE

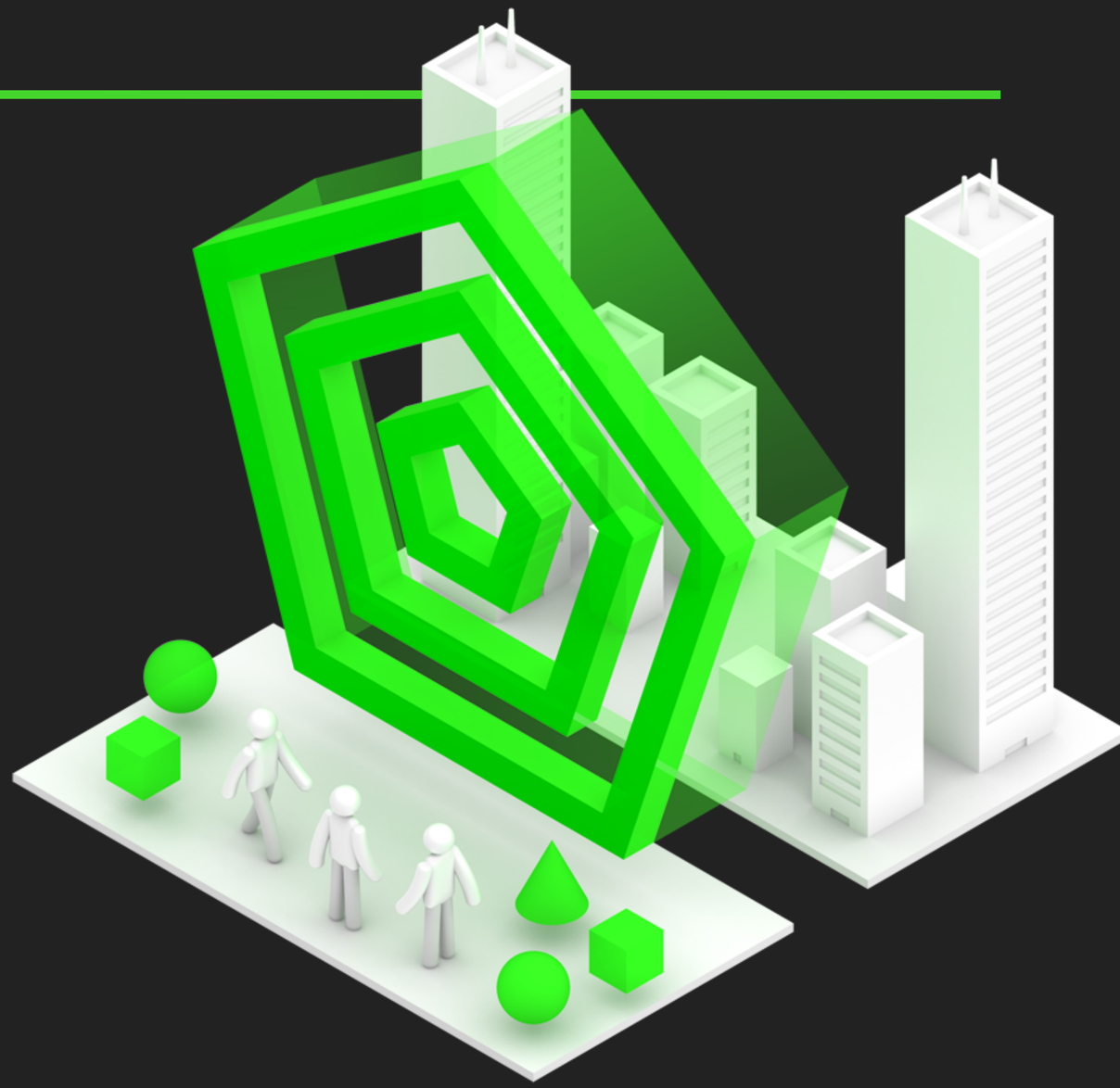
- **第一年 — 建立掌握度、強化基礎**
  - 盤點資產與風險，增加掌握度
  - 理解攻擊鏈與手法，建立對應文件
- **第二年 — 技術深化、整體感建立**
  - MITRE ATT&CK / NIST CSF
  - 資安架構設計
- **第三年 — 策略制定、資安顧問化**
  - 參與資安策略與提案
  - 評估優先順序，包含成本與風險的平衡



現實學習目標

DEVCORE

- 第四年 — 被挖角（？）



SUMMARY

Takeaways

DEVCORE

Takeaways

DEVCORE

- 真正的資安挑戰是人才而非技術
- 實戰是最有效的學習，活用資安服務學習
- 知識系統化是持續變強的關鍵，有效連結破碎化知識
- 攻防融合是未來資安團隊的常態，
  讓「以戰代訓」成為組織文化的一部分

DEVCORE

Q&A

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