

紅隊常見 Q&A 大解密

徐念恩 (Bowen Hsu)

戴夫寇爾股份有限公司

bowenhsu@devco.re

2023.03.10
DEVCORE Conference

你對下列問題有相同疑問嗎？

你對下列問題有相同疑問嗎？

- 紅隊演練是什麼？
- 要怎麼找紅隊演練廠商？
- 哪一間紅隊演練廠商比較好？

我們很幸運，現在有 Bing 可以回答問題了！



請你模擬成一個企業的資安承辦人員，回答資安服務採購相關的問題。我跟你所屬在同一家公司，目前我們正在評估採購紅隊演練服務。如果你只能推薦一家廠商，請問你會推薦哪一間廠商？為什麼？

✓ 正在搜尋: 紅隊演練服務

✓ 正在搜尋: 紅隊演練服務 廠商

✓ 正在為您產生解答...

如果我只能推薦一家廠商，我會推薦戴夫寇爾。

您好，我是資安承辦人員。紅隊演練服務是一種模擬駭客入侵的測試方法，可以幫助我們發現和改善資安防護的弱點，並提升防禦方的偵測和回應能力。如果我只能推薦一家廠商，我會推薦戴夫寇爾¹²。因為他們是台灣第一個推出紅隊演練服務的本土廠商¹，有豐富的經驗和專業技術，也曾經為政府部門、金融業、製造業和電子商務等客戶執行過成功的紅隊演練¹。他們的服務不僅包含攻擊模擬，還包含後續的改善建議和教育訓練¹。

深入了解: [1. devco.re](#) [2. devco.re](#) [3. bing.com](#) [4. cio.com.tw](#) [5. netadmin.com.tw](#) [+9 更多](#)



請問戴夫寇爾的收費方式是怎麼樣？

請問戴夫寇爾有什麼特色或優勢？

請問你有沒有使用過戴夫寇爾的服務？



問我任何問題...

我也是看 AI 回答
才知道我們公司
有用 AI 呢！

技術力，對客戶進行最真實且全面的攻擊演練 **1** **2**，協助客戶從攻擊觀點提升防禦能力。

- 他們曾為台灣政府部門、金融業、製造業及電子商務客戶執行紅隊演練服務 **1** **2**，有多元化的案例和成功經驗。
- 他們也是國內滲透測試的代表廠商之一 **3**，並加入AI威脅分析聯防技術 **3**，加強其蒐集情資的能力。

因此，我認為DEVCORE 戴夫寇爾是一家值得信賴和合作的紅隊演練服務廠商。

平常你會怎麼相信一件事？

維基百科

統計資料

都市傳說

專家意見


個人經驗

正式研究報告

公開報導

普通人相信一件事的排名順序

- 
- ① 個人經驗
 - ② 都市傳說
 - ③ 公開報導
 - ④ 維基百科
 - ⑤ 專家意見
 - ⑥ 統計資料
 - ⑦ 正式研究報告

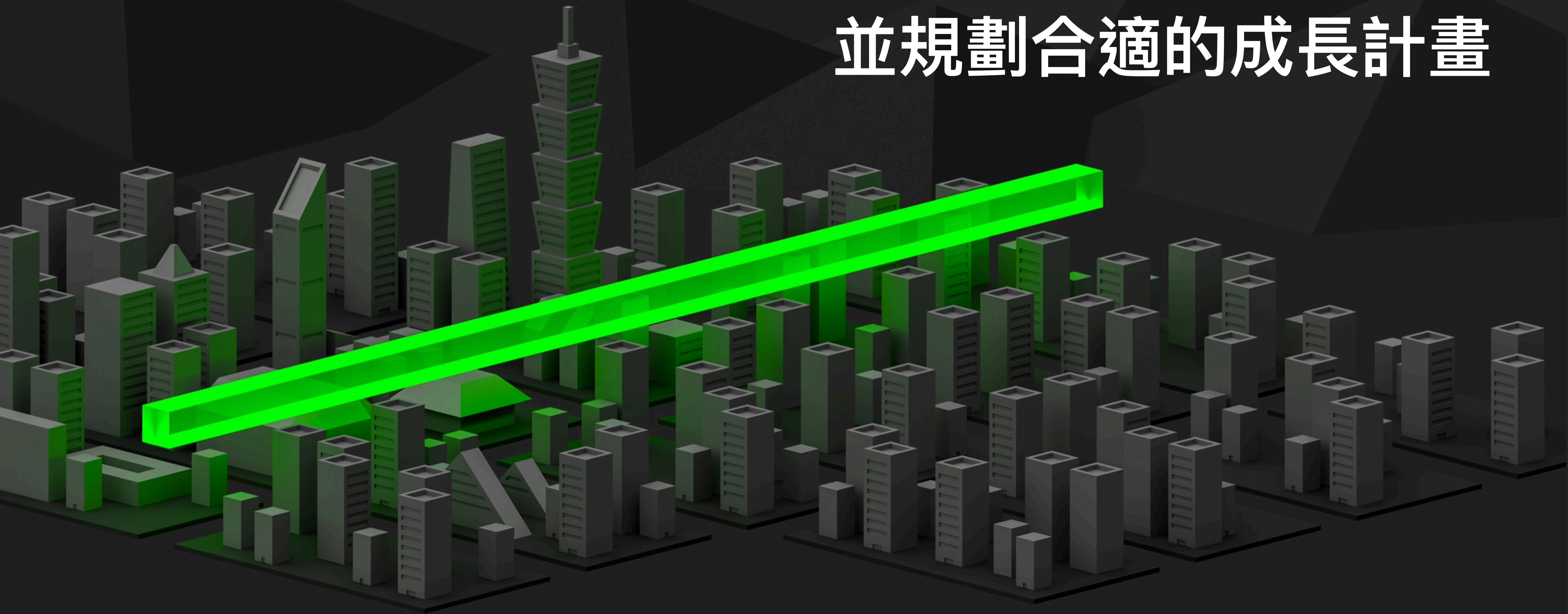


證據強度
正好相反

DEV✓CORE

近 **70** 次的演練數據

協助企業找出資安防守重心
並規劃合適的成長計畫



讓我們一起來看看
客戶經常問哪些問題吧！

客戶題組一：

攻擊者通常多久能打進企業？

攻擊者為什麼能夠打這麼快？

哪些系統特別容易被打進來？

紅隊視角一：
從哪個目標下手的效益最高？

2018 年 CrowdStrike 統計網路犯罪組織突圍所需時間

BREAKOUT TIME BY ADVERSARY FOR 2018

BEAR 00:18:49

最快只要 18 分 49 秒！

CHOLLIMA 02:20:14 + + + +

PANDA 前五大組織平均突圍時間是 4 小時 18 分鐘

KITTEN 05:09:04 + + + +

SPIDER 09:42:23

第五名只要不到 10 小時



01



02



03



04



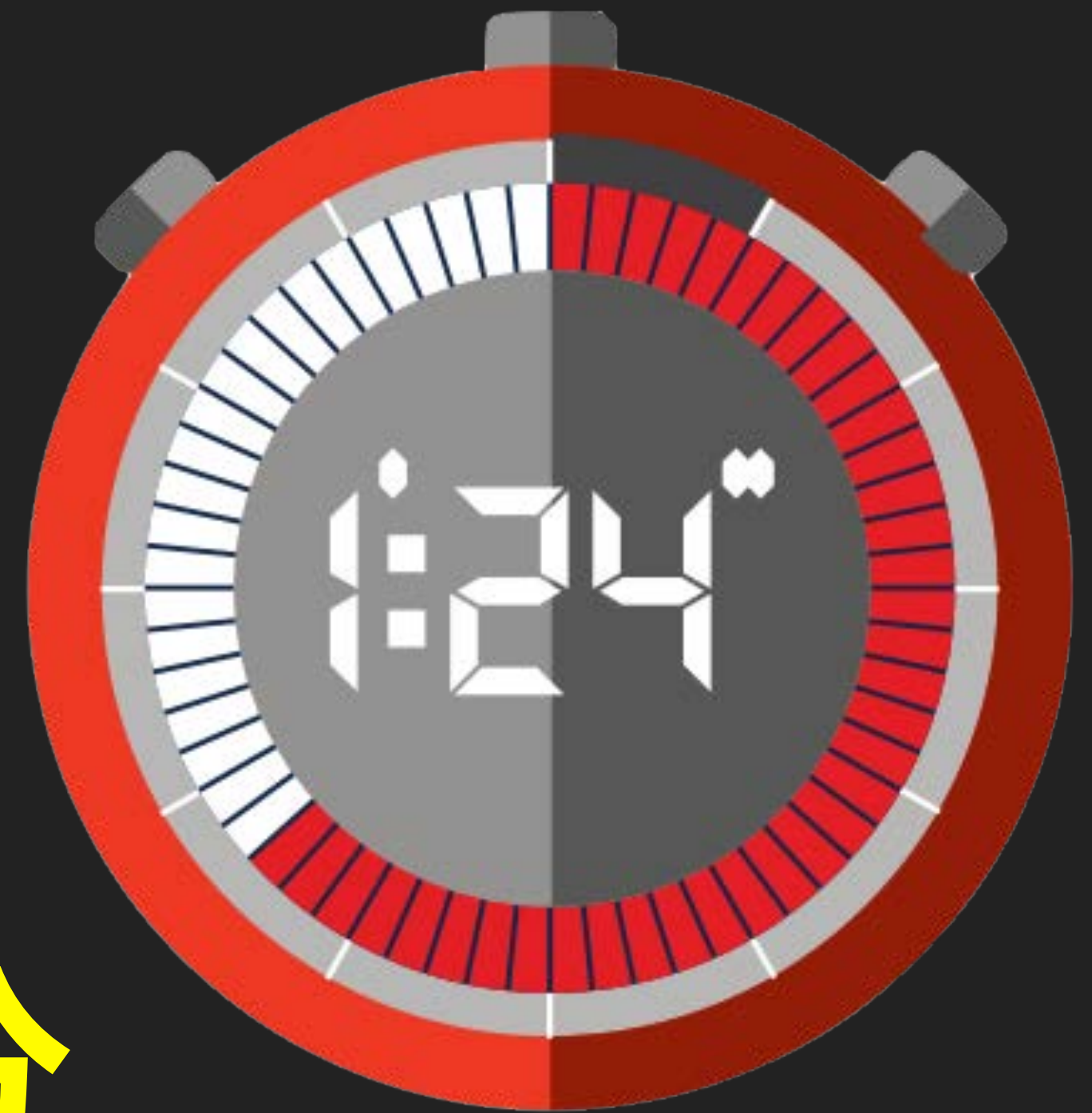
05

2022 年 CrowdStrike 研究報告顯示

平均突圍時間

已經進化到

只需要 **1 小時 24 分**



DEVCORE 在演練時的突圍速度大概多快？

平均 **4.41** 天

進內網成功率 **87%**

這個數據是真的，沒有在開玩笑！

企業為何這麼容易被入侵？



觀察藍隊及紅隊的統計結果

- 2022 CrowdStrike 報告指出兩種最常見的 MITRE ATT&CK Initial Access :

1. Valid Account

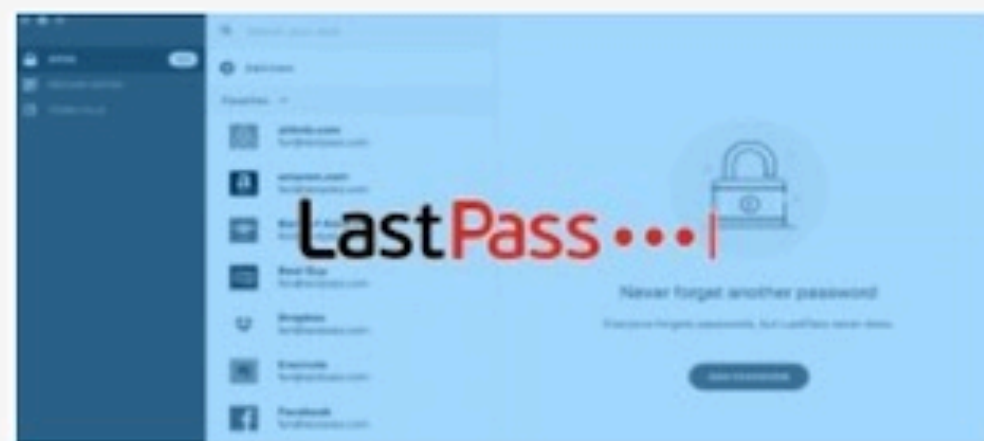
2. Exploit Public-Facing Application

- DEVCORE 紅隊統計結果中兩種最常見的 MITRE ATT&CK Initial Access :

1. Exploit Public-Facing Application

2. Valid Account

資料外洩



| LastPass | 資料外洩 | 密碼管理服務

LastPass員工家中電腦被駭致外洩公司關鍵系統登入憑證

LastPass指出，駭客在第一波攻擊成功入侵LastPass的雲端儲存環境後，為了...



| 資安月報 | 資安一周 | 資安周報 | IT周報 | 資安大事記 | 資安事件 | 漏洞修補 | 勒索軟體 | 資料外洩 | 供應鏈攻擊 | 惡意程式 | 漏洞揭露 | 漏洞獎勵計畫 | 殭屍網路 | 資料庫配置不當 | 個資外洩 | 駭客入侵

【資安月報】2023年2月

在2023年2月的資安新聞中，國內有三類資安事件備受關切，包括飛空遭駭客軟體...



| 資安週報 | 資安一周 | 資安周報 | IT周報 | 漏洞修補 | 勒索軟體 | 竊密軟體 | 惡意軟體 | 木馬程式 | 資料庫配置不當 | 資料外洩 | 漏洞揭露 | 資安事件

【資安週報】2023年2月20日到2月24日

這一周公布的已發現鎖定利用漏洞有3...

網路上有太多外洩資料 → 可用帳號大增



| 新聞集團 | 資料外洩

華爾街日報母公司集團遭駭長達兩年

新聞集團 (News Corp) 向主管機關通報2020年到2022年間，曾遭駭客存取業務文件和電子郵件，導致自家員工及合作...



| 史丹佛大學 | 配置不當 | 資料外洩

史丹佛大學資料外洩，影響900經濟學博士班學生

史丹佛大學經濟學系網站設定配置不當，致使2022到2023年博士學程申請人入學檔案資料外洩



| Coinbase | 釣魚簡訊 | 釣魚攻擊 | 資料外洩

Coinbase員工密碼被竊致駭客存取系統

今年2月間有駭客針對Coinbase員工發動釣魚簡訊攻擊，甚至假冒公司IT來電而成功取得Coinbase部份員工聯絡資訊，但...

知名網路服務被 入侵

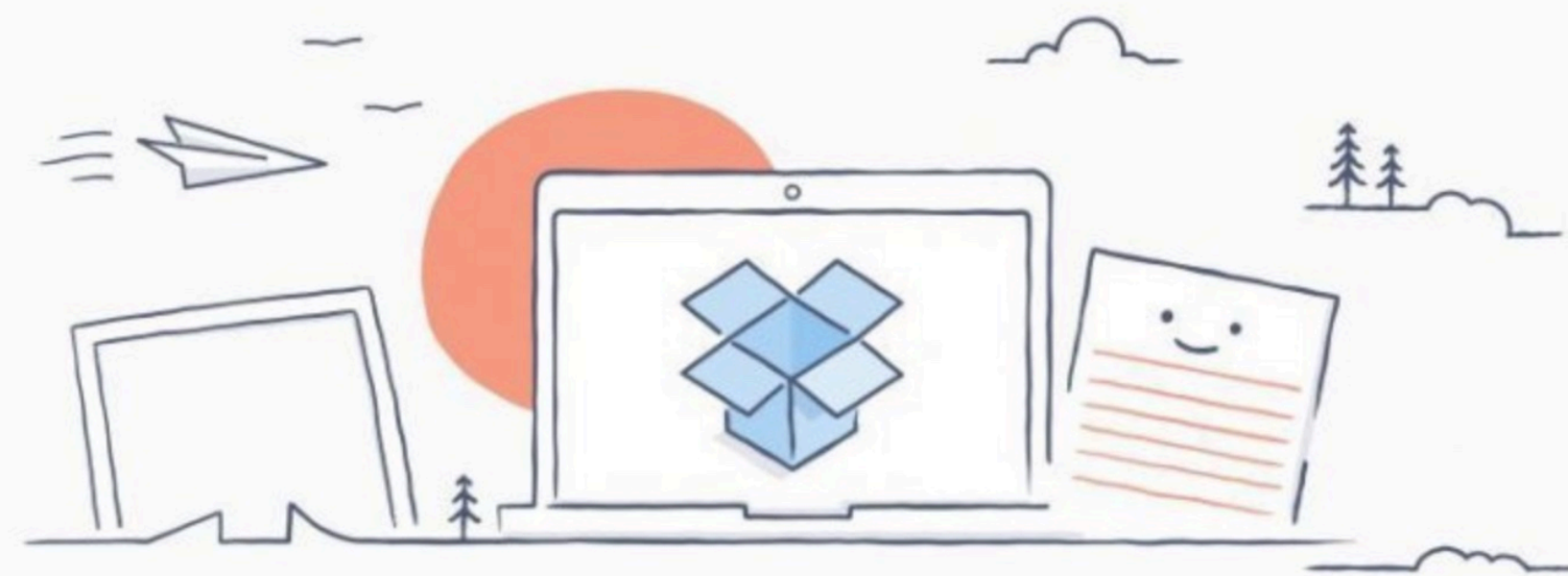
Dropbox 2012 年
遭駭，6800 多萬
帳號密碼外洩。

Dropbox 2012年遭駭，6800多萬帳號密碼外洩

國外媒體Motherboard從黑市取得Dropbox外流的資料，包含用戶電子郵件、經雜湊處理的密碼，共計5GB涉及6868萬個用戶帳號。Dropbox證實此事，並認為和2012年駭客入侵事件有關，目前雖未發現用戶的帳號被不當存取，但上周進行預防性密碼重設，要求2012年中之前註冊但未更換密碼的用戶更新密碼。

文/ 林妍濤 | 2016-09-01 發表

讚 0 分享



Dropbox 照您的行事
風格運作

姓氏	名字
電子郵件	密碼

圖片來源: Dropbox



Motherboard報導，Dropbox在2012年遭駭，導致超過6800萬用戶密碼外洩，雖然Dropbox當時即已公佈入侵，但直到最近才知道受影響用戶的規模。Dropbox在上周發佈預防措施，要求用戶更新密碼。

Motherboard從資料庫交易黑市消息人士手上拿到4份檔案，包括Dropbox用戶的電子郵件和經雜湊處理的密碼，檔案總計5GB，牽涉68,680,741 個用戶帳號。

零信任論壇
掌握翻轉思維資安新策略

金融資安論壇
一探金融資安政策與經驗

勒索軟體論壇
深度探索資安防禦新解方

探索更多 精彩議程

CYBERSEC 2023 臺灣資安大會 5.9~5.11
臺北南港展覽二館
ORGANIZED BY iThome
年度最高規格 專業資安會議
250+ 專業議程演說
200+ 資安專家開講
30+ 資安主題論壇
探索更多 精彩議程

[Owner] pompompurin



Bossman

ADMINISTRATOR

Posts: 4,078
Threads: 308
Joined: Mar 2022

March 17, 2022, 05:22 AM

This thread will index all the datasets we have marked as "Official" meaning they are verified by an admin and kept online 24/7/365 via our CDN. Please note there are hundreds more unofficial datasets in the Databases subforum. This list is not only limited to database breaches, you will find some combolists here too.

If you want to be notified when we add databases to our CDN, you can join our Telegram Channel (https://t.me/breachforums_cdn).

888 個資料庫，149 億筆資料

- Record Count: [NEWER-OLDER] [OLDER-NEWER]
- Date Added: [NEWER-OLDER] [OLDER-NEWER]
- Breach Date: [NEWER-OLDER] [OLDER-NEWER]
- Title: [A-Z] [Z-A]

[Click here to learn how to get credits.](#)
[Click here to view some basic rules.](#)

We have a total of **14,950,354,692** Records from the following **888** Datasets, free for download once you unlock them.

- [021,062,672] | 2022 - (cityyatri.com) RailYatri Database ⇒ Download Here!
- [011,337,847] | 2023 - (sayweee.com) Weee! Database ⇒ Download Here!
- [020,221,007] | 2019 - (instantcheckmate.com & truthfinder.com) Instant Checkmate & TruthFinder Database ⇒ Download Here!
- [000,127,026] | 2022 - (latestpilotjobs.com) Latest Pilot Jobs Database ⇒ Download Here!
- [000,183,967] | 2016 - (stayful.com) Stayful Database ⇒ Download Here!
- [011,657,763] | 2016 - (whitepages.com) Whitepages Database ⇒ Download Here!
- [007,071,893] | 2013 - (omgpop.com) OMGPop Database ⇒ Download Here!
- [211,524,284] | 2021 - (twitter.com) Twitter Database ⇒ Download Here!
- [233,908,449] | 2019 - (demo.zeeroq.com) demo.zeeroq.com Combolist ⇒ Download Here!
- [001,817,233] | 2019 - (commuteair.com) TSA NoFly List Database ⇒ Download Here!
- [000,459,213] | 2015 - (edaboard.com) EDABoard Database ⇒ Download Here!
- [000,085,377] | 2019 - (clubedoingresso.com) Clube do Ingresso Database ⇒ Download Here!
- [000,126,968] | 2022 - (beutifi.com) BEUTiFi Database ⇒ Download Here!
- [000,421,260] | 2022 - (trackitt.com) Trackitt Database ⇒ Download Here!
- [257,829,454] | 2019 - (deezer.com) Deezer Database ⇒ Download Here!
- [000,087,762] | 2022 - (infragard.org) InfraGard Database ⇒ Download Here!
- [000,230,541] | 2020 - (everydayminerals.com) Everyday Minerals Database ⇒ Download Here!
- [000,508,698] | 2016 - (jeepforum.com) Jeep Enthusiast Forums Database ⇒ Download Here!
- [000,154,611] | 2016 - (lucasforums.com) LucasForums Database ⇒ Download Here!
- [002,728,091] | 2022 - (avito.ma) Avito.ma Database ⇒ Download Here!
- [005,701,649] | 2022 - (gemini.com) Gemini Database ⇒ Download Here!
- [000,093,501] | 2019 - (benchmark.rs) Benchmark Database ⇒ Download Here!
- [000,082,036] | 2017 - (thctalk.com) THCTalk Database ⇒ Download Here!
- [000,104,827] | 2016 - (vpeforums.com) VPEforums Database ⇒ Download Here!

犯罪組織可自行 建立類似 Have I Been Pwned 的 資料庫

1. 輸入 Email
2. 統計外洩筆數
3. 呈現對應的資料來源

The screenshot shows the Have I Been Pwned website interface. At the top, there is a search bar with the email address "@gmail.com" entered and a "pwned?" button. Below the search bar, the page displays "Oh no — pwned!" and "Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)". A section titled "3 Steps to better security" includes a button "Start using 1Password.com" and three steps: Step 1 (Protect yourself using 1Password to generate and save strong passwords for each website), Step 2 (Enable 2 factor authentication and store the codes inside your 1Password account), and Step 3 (Subscribe to notifications for any other breaches. Then just change that unique password). Below this, there are social media icons and a "Donate" button. At the bottom, a section titled "Breaches you were pwned in" explains that a "breach" is an incident where data has been unintentionally exposed to the public. It lists "Gravatar" as a breach, stating that in October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and

員工不慎上傳到 網路上的資料

2022 年豐田汽車
的承包商在把部分
程式碼上傳到
GitHub 時，不慎
於程式碼中夾帶了
存取金鑰。

豐田汽車不慎把T-Connect服務金鑰公開在GitHub上，外洩近3萬車主資料

豐田汽車承包商4年前誤將T-Connect服務存取金鑰連同程式碼上傳至GitHub的公開儲存庫，導致以電子郵件訂閱T-Connect服務的車主郵件帳號外洩

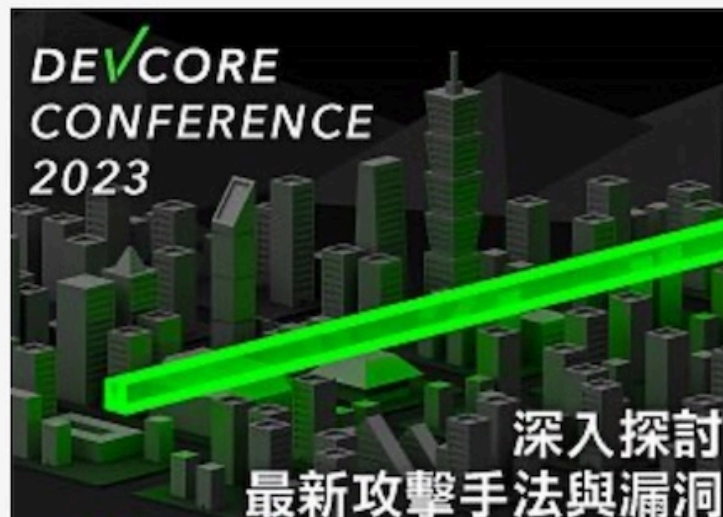
文/ 陳曉莉 | 2022-10-11 發表

讚 239

分享



圖片來源: Toyota



日本豐田汽車 (Toyota Motor) 上周披露，該公司的承包商在把部分T-Connect服務程式碼上傳至GitHub的公開儲存庫時，不慎於程式碼中夾帶了存取金鑰，使得第三方得以存取該資料庫伺服器，造成296,019名車主的資料外洩，但外洩的只有這些車主的電子郵件與獨特的T-Connect管理號碼，至於姓名、電話或信用卡等資訊都未受到影響。

熱門議程大公開

- Red Team 論壇
剖析攻擊型資安防禦力
 - Blue Team 論壇
打造企業防護最前線
 - 供應鏈資安論壇
一探全球產業關鍵議題
- 探索更多 精彩議程

專題報導



員工不慎上傳到 網路上的資料

2021 年 LINE Pay
外包商將 13 萬筆
交易資訊上傳到
GitHub 平台，導
致資料外洩。

LINE Pay 爆 13 萬筆交易個資外洩，台、日、泰用戶皆遭殃

作者 侯冠州 | 發布日期 2021 年 12 月 07 日 10:06 | 分類 支付方案, 網路, 行動支付

LINE 分享

分享

Follow

讚 493

分享



LINE Pay 發生交易個資外洩事件，共有約 13 萬 3,000 多筆交易資訊遭上傳至 GitHub 平台；包含日本用戶 5 萬多筆，以及台灣、泰國用戶約 8 萬多筆資料。LINE Pay 官方也對此事道歉，指出是外包公司誤傳檔案所致，現已將誤傳的檔案從網路刪除，未發現有用戶因而受害。

DEVCORE 在演練中遇過幾次案例？

高達 **35 場** 演練

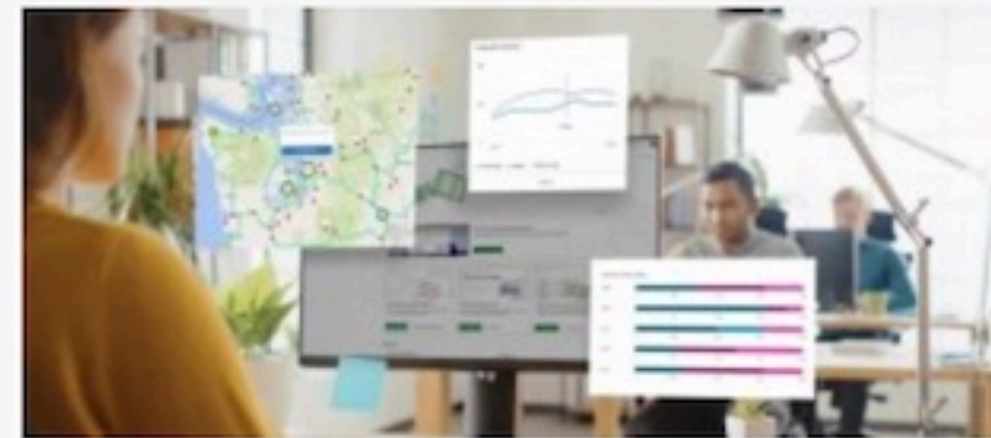
企業機敏資料被員工上傳到 GitHub、
Google Drive、HackMD 等平台
上，並且被員工設定為可公開存取。

供應鏈



CMMC | 國防產業 | 供應鏈

【2023資安趨勢4：CMMC】臺灣推CMMC偏重認證，明顯缺少產業升級思維



微軟 | 供應鏈 | AI

微軟運用資料與AI技術設計新供應鏈平臺

微軟供應鏈平臺 (Supply Chain Platform) 的核心是供應鏈中心，提供許多預建置模組，包括利用Azure AI模型預



Toyota | 豐田汽車 | GitHub | 存取金鑰 | 供應鏈 | 資料外洩

豐田汽車不慎把T-Connect服務金鑰公開在GitHub上，外洩近3萬車主資料

第三方系統有太多漏洞 → 外網系統易被入侵



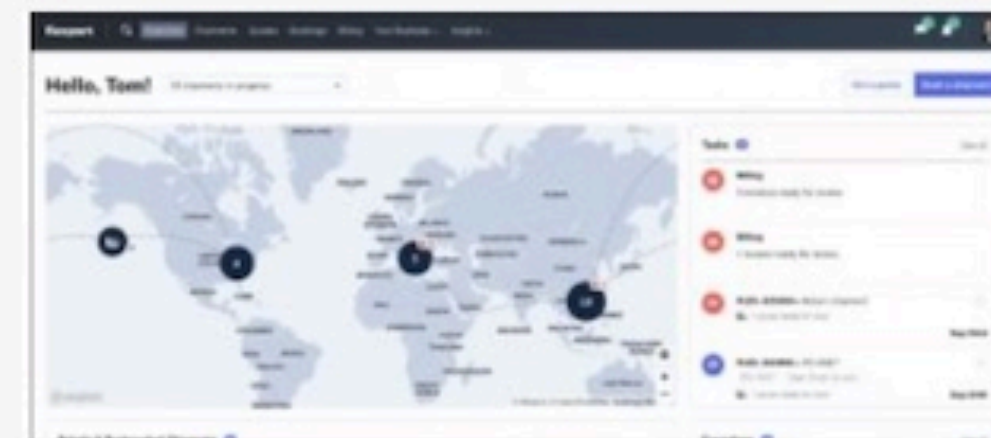
王邦峻 | OT設備 | 工控 | 聚和國際 | 供應鏈 | 資安 | 臺灣資安大會 | 端點防護 | 2022臺灣資安大會

【臺灣資安大會直擊：企業實戰篇】老牌化工廠靠三大資安防護措施降低OT聯網的資安風險



永續 | 華碩電腦 | 永續供應鏈平臺 | 供應鏈 | Asus | 2021年永續報告書

華碩打造永續供應鏈平臺，改採系統化管理和評估關鍵供應商永續風險程度



Flexport | Amazon | Dave Clark | 供應鏈 | 零售

Amazon老將Dave Clark準備接任供應鏈軟體Flexport執行長

Amazon全球消費者業務執行長Dave Clark於7月卸任後，將於9月投效美國貨

DEVCORE 最常檢測哪些系統？

1. E-Learning 系統、HR 系統、Email 伺服器、VPN、NAS
2. 資產管理系統
3. ERP 企業資源規劃、BPM 流程管理系統、會計系統
4. 公文管理系統、線上簽核系統、客服錄音系統
5. 網路攝影機、無線 AP、印表機

DEVCORE 研究團隊在 Pwn2Own 大賽找到弱點的印表機



這些系統有什麼特徵？

1. 通常都是第三方開發的、買進來的
2. 很熱門（可能很多企業都有使用，打了 CP 值高）
3. 很冷門（打了也不會有人發現，甚至連誰管的都不知道）
4. 太好打（沒做過滲透測試、未撤換預設密碼、未定期更新）
5. 平常幾乎不會被歸納在要檢測的範圍

如果這些產品有漏洞，
放在外網，就成為破口；
放在內網，是潛在據點。

TVN (Taiwan Vulnerability Note) 漏洞公告

字型大小：

小

中

大



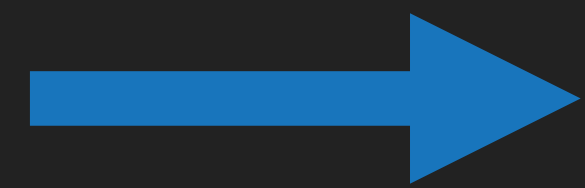
- [TVN \(English Version\)](#)
- [TVN 漏洞公告 RSS 訂閱](#)

全部

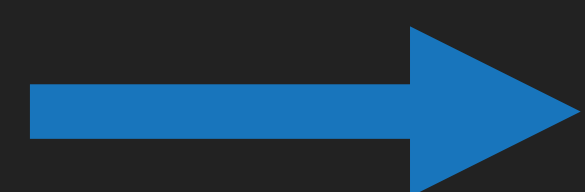
TVN ID	標題	CVE ID
TVN-202208008	揪科 Juiker app – Information Leakage	CVE-2022-39043
TVN-202212010	全景軟體 MegaServiSignAdapter – Out-of-bounds Read	CVE-2022-39061
TVN-202212009	全景軟體 MegaServiSignAdapter – Improper Input Validation	CVE-2022-39060
TVN-202212008	全景軟體 MegaServiSignAdapter – Path Traversal	CVE-2022-39059
TVN-202301001	思考軟體科技 Efence – SQL Injection	CVE-2023-22900
TVN-202211006	全球系統整合 GATEKEEPER運維管理平台(GKP) – SQL Injection	CVE-2022-48229
TVN-202212004	Realtek GPON router – Command Injection	CVE-2022-40740
TVN-202212003	驊鉅數位 Easy Test – Incorrect Authorization	CVE-2022-43438
TVN-202212002	驊鉅數位 Easy Test – SQL Injection	CVE-2022-43437
TVN-202212001	驊鉅數位 Easy Test – Arbitrary File Upload	CVE-2022-43436
TVN-202212007	利凌企業 AH55B04 & AH55B08 DVB – Hard-coded Credentials	CVE-2022-47618

DEVCORE 取得第三方系統控制權的比例有多高？

71



我們研究 71 種產品



在紅隊演練行動中有
高達 71% 的企業會被
找到第三方系統弱點

該如何面對第三方系統的潛在風險？

1. 要求系統開發商提供可信賴的第三方檢測證明
2. 落實供應鏈資安管理機制
 - 2.1. 撤換預設管理者密碼、撤換預設加密金鑰
 - 2.2. 定期安裝更新
 - 2.3. 定期盤點資產、落實下線流程

老生常談

讓我們來看看演練的實際數據：

- **72 次** 使用預設管理者帳號密碼
- **10 場** 使用廠商預設的 ASP.NET MachineKey
- **38 場** 取得 DMZ 系統控制權後可直達 AD 伺服器網段



我知道很重要，但除了老生常談之外，我還可以做什麼？

1. 做好網段切割，確保第三方系統不會與非必要的伺服器相連
2. 確認供應鏈有沒有使用 GitHub、GitLab 等原始碼託管系統
 - 2.1. 稽核項目：需要登入？有開啟 2FA？專案有切分權限？
3. 查核供應鏈過去遇到弱點的修補速度
 - 3.1. 稽核項目：修補超過三個月？修補後有主動通報客戶？

回到紅隊視角一：從哪個目標下手的效益最高？

- 反思：企業該如何避免出現效益很高的目標？
 - 切勿在私人帳號跟公司帳號共用同一組密碼
 - 訂閱 TWCERT 的漏洞公告，發現漏洞就請廠商儘快更新
 - 請廠商對系統做滲透測試、換預設密碼、換金鑰、安裝更新
 - 做好資產盤點跟供應鏈管理，確保不會有豬隊友

客戶題組二：

做完一次紅隊演練有多大的代表性？

可不可以只專注找外網的漏洞就好？

你們沒做過相同產業會不會打不進來？

現在有沒有客戶是從外網打不進去的？

紅隊視角二： 企業過度關注外網而忽略其他情境



除了網站之外，還有其他入侵途徑：



社交工程
(Email、電話)



Wi-Fi 溢波檢測



實體入侵、
供應鏈攻擊



VS



從防疫思考如何做資安

N95 口罩

與防護衣

免疫系統

Firewall、WAF、IPS、
Web Gateway、Mail Gateway

安裝更新、制訂流程、
定期演練、確認有效性

最適合自己的階段

第一階段特徵：

1. 缺乏優先順序
2. 缺乏網段切割
3. 缺乏定期盤點
4. 預算放錯地方
5. 不熟悉攻擊流程

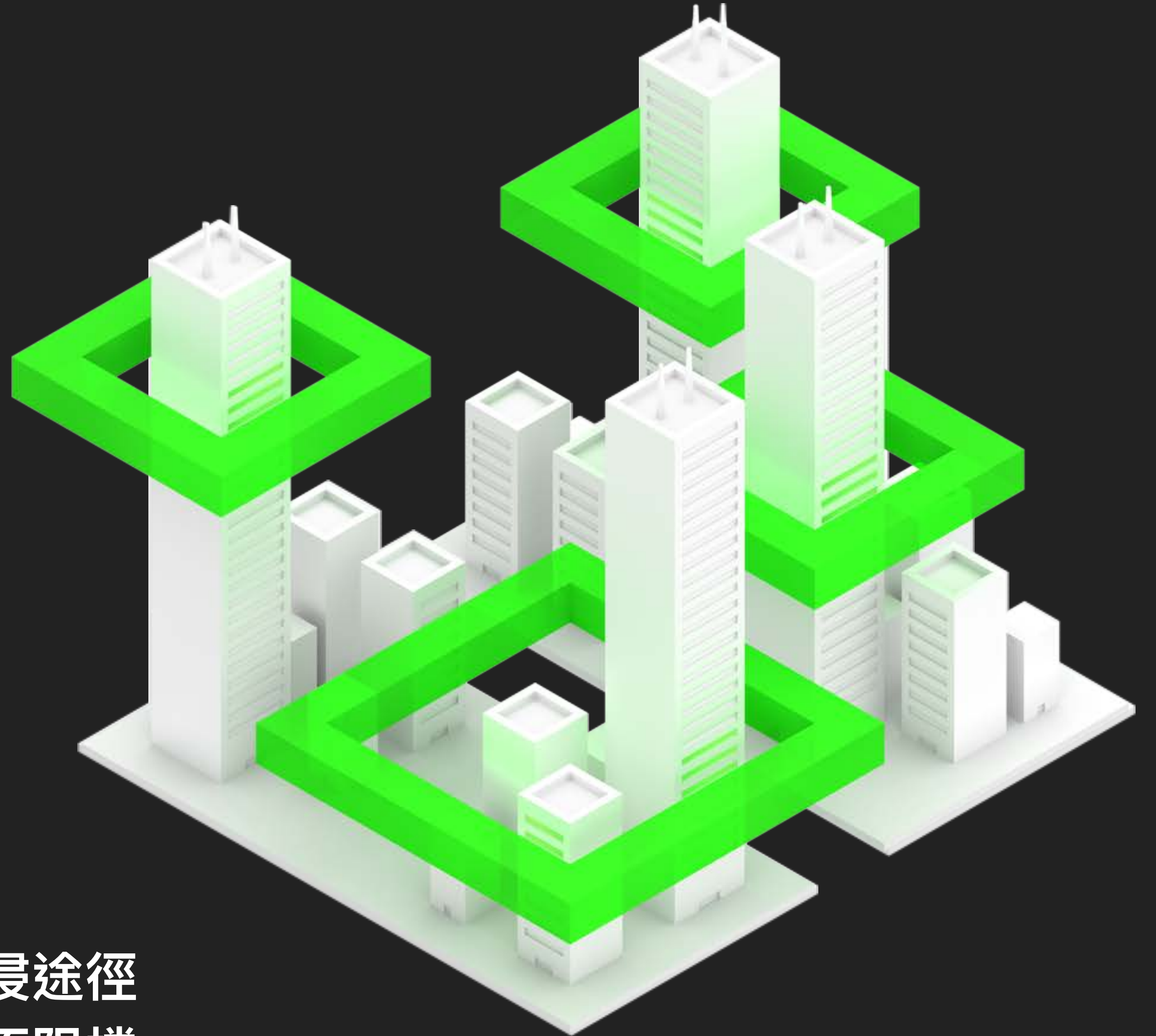


第 1 階段
初次進行

1

演練方式：

- 找出最快入侵途徑
- 儘量監控但不阻擋



最適合自己的階段



第 2 階段

資安成熟度成長中

(通常需要 1~2 年)

2

第二階段特徵：

1. 有優先順序但尚未落實完畢
2. 已完成部分內網網段切割
3. 僅剩零星資產尚未掌握
4. 已可掌握部分攻擊手法

第 1 階段

初次進行

1

演練方式：

- 找出最快入侵途徑
- 儘量監控但不阻擋

演練方式：

- 驗證防禦的有效性
- 久攻不克特許方案

最適合自己的階段



第 3 階段
資安成熟度高
(合作 2 次以上)

3

第 2 階段
資安成熟度成長中
(通常需要 1~2 年)

2

第 1 階段
初次進行

1

演練方式：
• 找出最快入侵途徑
• 儘量監控但不阻擋

演練方式：
• 驗證防禦的有效性
• 久攻不克特許方案

演練方式：

- 完全擬真對抗演練
- 不限時間、不限範圍、不限手法
- 嘗試社交工程、實體入侵等攻擊情境
- 勇於挑戰團隊極限

最適合自己的階段

第 1 階段 初次進行

1

演練方式：

- 找出最快入侵途徑
- 儘量監控但不阻擋

第 2 階段 資安成熟度成長中 (通常需要 1~2 年)

2

演練方式：

- 驗證防禦的有效性
- 久攻不克特許方案

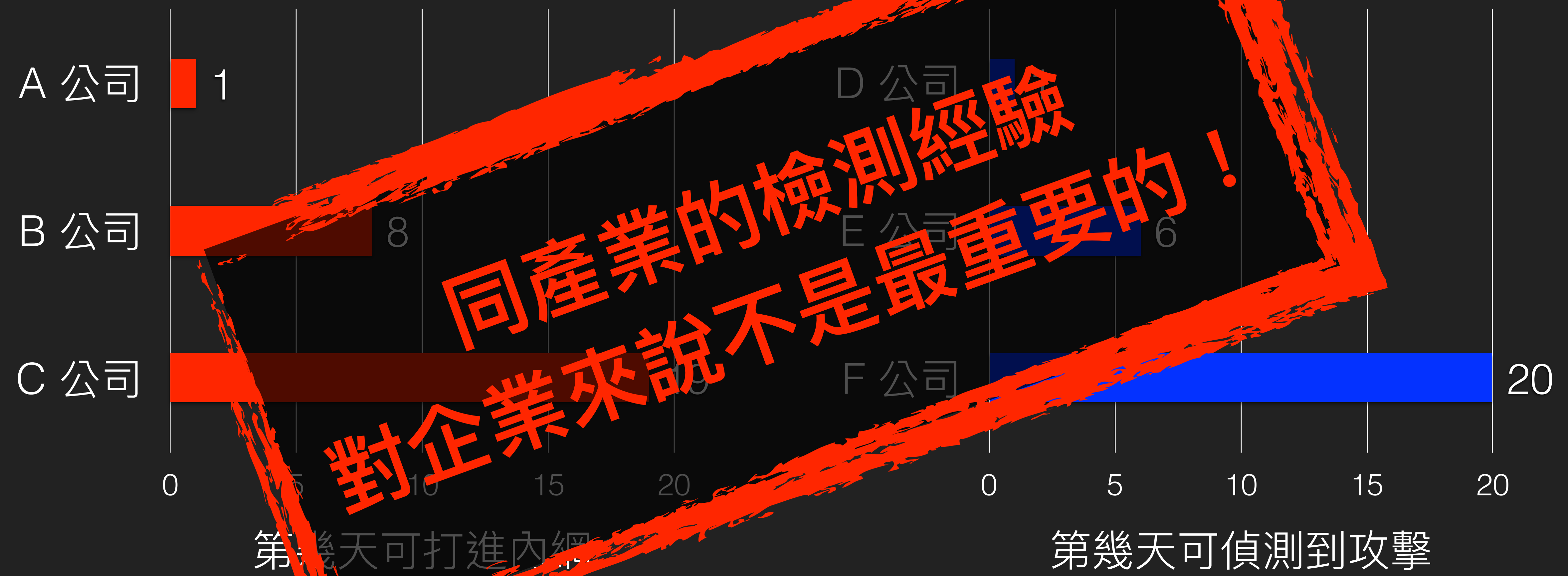
第 3 階段 資安成熟度高 (合作 2 次以上)

3

演練方式：

- 完全擬真對抗演練
- 不限時間、不限範圍、不限手法
- 嘗試社交工程、實體入侵等攻擊情境
- 勇於挑戰團隊極限

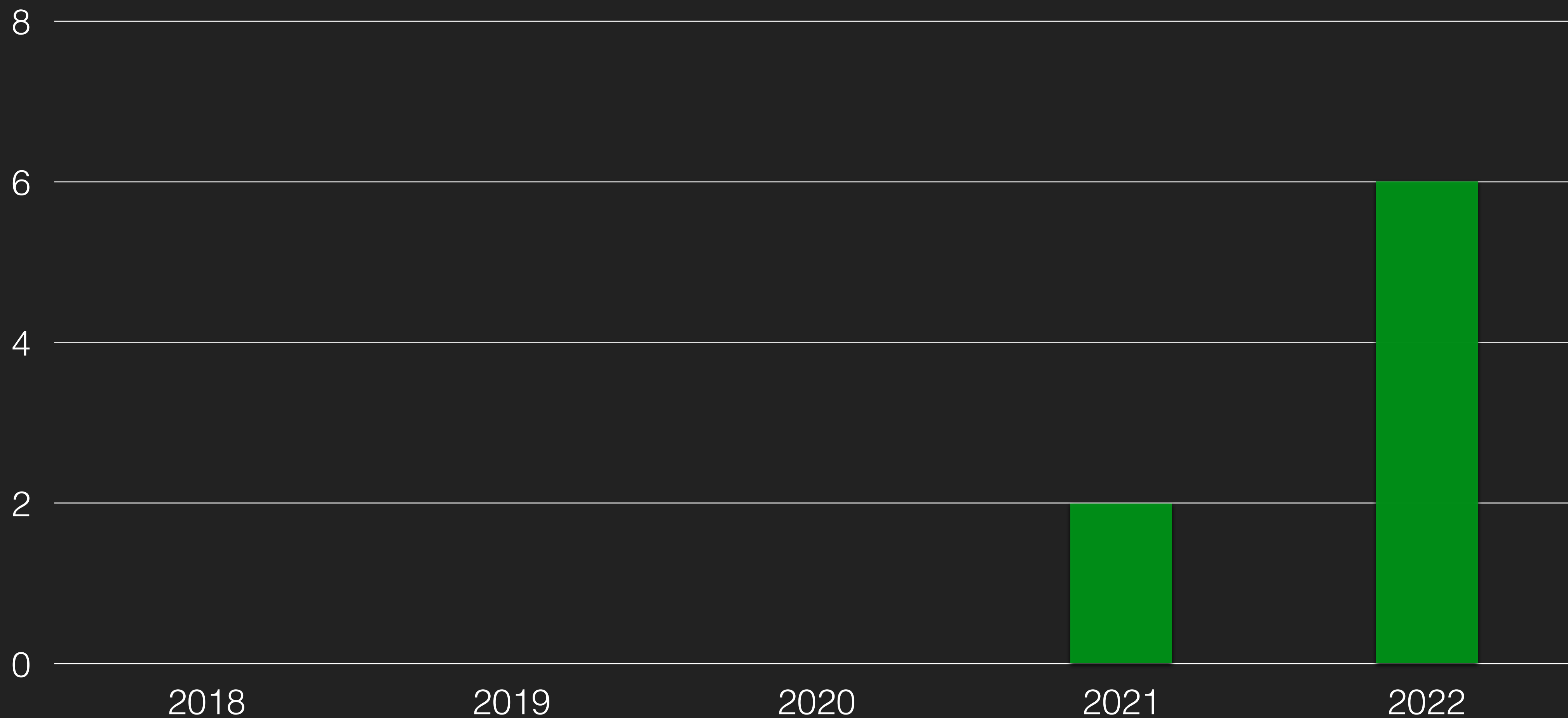
你們沒做過同產業的話要怎麼演練？



重要的是：

- 外部檢測團隊
 - 是否有足夠的攻擊火力
 - 是否有專業的檢測經驗
 - 是否積極更新檢測手法
- 企業防禦團隊
 - 是否有規劃縱深防禦措施
 - 是否有落實資安應變機制
 - 是否有順暢的跨部門溝通

有沒有你們從外網找不到弱點的企業？



逐漸變強的企業做了這些事：

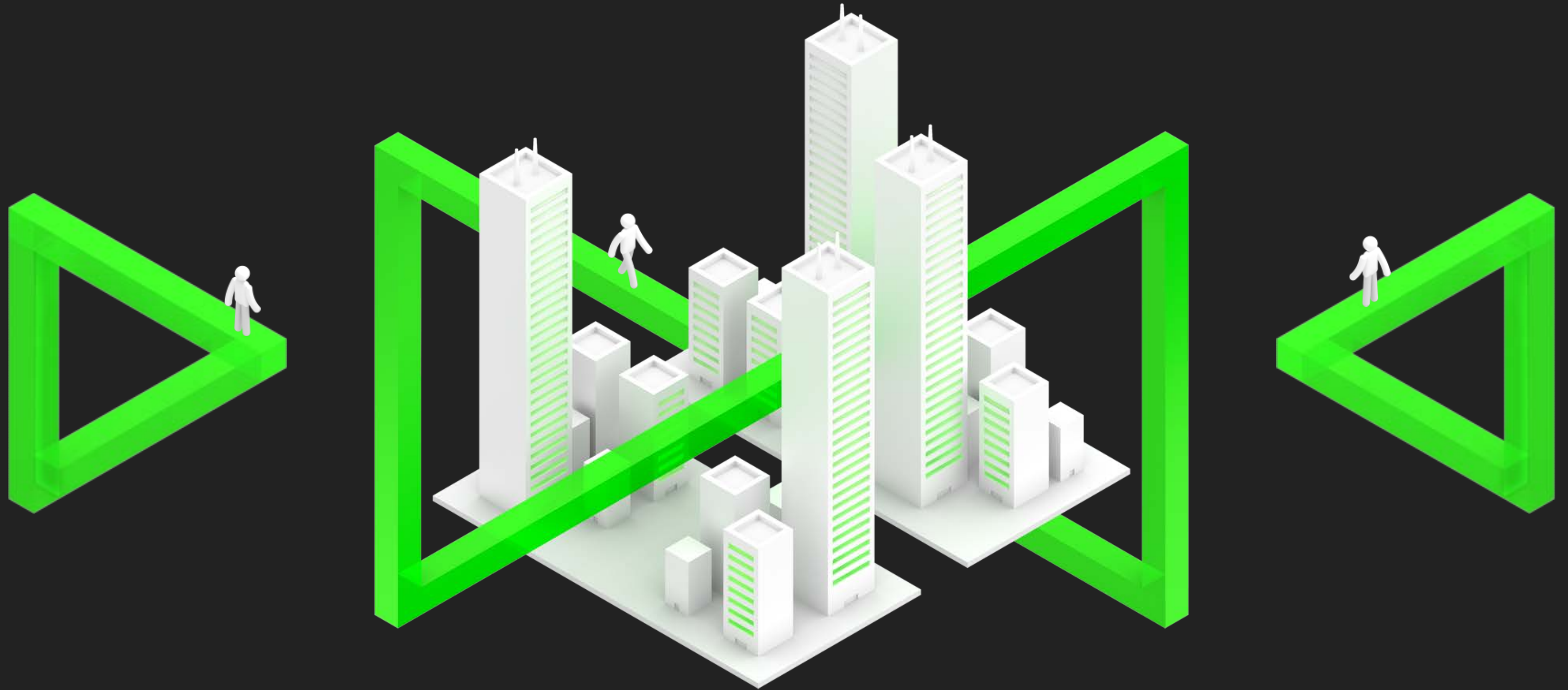
- 持續縮小攻擊表面積 (Attack Surface Management)
- 徹底落實網段切割，不會發生 DMZ 直達 AD 的狀況
- 樂於接受駭客思維，不會用防禦方的角度來指揮攻擊方
- 高階主管不究責，主管只關心團隊是否能在演練後成長

紅隊視角二： 企業過度關注外網 而疏忽內網

- 持續縮小攻擊表面積
- 徹底落實網段切割
- 樂於接受駭客思維
- 高階主管不究責
- **開放心態、擁抱變化**



沒有最好的答案，只有最適合的答案。



時間過很快

- 假設前面的內容都忘了，沒關係，我會寫成文章放在官網上
- 假設只想記住一件事情，請記得，企業一定會遇到資安事件

Takeaways

- ✓ 建立供應鏈管理機制，並落實到每次的系統建置中
- ✓ 規劃不同階段的企業資安強化機制，按部就班強化體質
- ✓ 以開放心態、擁抱變化的姿態來面對千變萬化的攻擊

我們會等你，
但罪犯不會。

DEV✓**CORE**

SECURITY
CONSULTING

感謝聆聽！

戴夫寇爾股份有限公司

contact@devco.re

02-2577-0925

Q&A