DEVCORE
SECURITY
CONSULTING

紅隊紅隊，
多少服務假汝之名而行！

鍾澤華 (Aaron Chung)

戴夫寇爾股份有限公司

contact@devco.re

2023.3.10
DEVCORE Conference

講者簡介

Aaron Chung

DEVCORE 商務發展總監

工作：售前接洽、售後管理顧問。研究對企業有幫助攻擊產品跟服務。

經歷

- 擔任金融、交通、製造業紅隊演練資安管理顧問
- HITCON、CYBERSEC、上市櫃公司資安講師
- 曾任大型組織資安主管，負責資安事件處理、資安政策規劃、資安防禦架構維運管理
- 半導體製造業 IT 工程師

DEVCORE SECURITY CONSULTING

DEVCORE 的 10 年

2012.11 創立
提供滲透測試
及資安顧問服務

2014.08
PT 無法完整解決企業問題
開始做更廣更真實的檢測

2016
累積大量滲透攻擊經驗
研究企業整體安全議題

2017.11
推出 Red Team Assessment
正式命名為「紅隊演練」

2018.08
紅隊演練首次揭露
政府資料外洩於地下網站販售

2019.02
入選 Red Team Summit 2019 分享
RED TEAM IN TAIWAN: ZERO TO ONE

2019.08
SSL VPN 研究獲得 Black Hat USA
Pwnie Awards Best Server-Side Bug

2019.09
DEVCORE Conference
2019

2019.11
DEVCORE 資安獎學金

2021.03
Microsoft Exchange Server
回報漏洞研究 ProxyLogon

2021.04
首度獲得 Pwn2Own 冠軍

2022.01
DEVCORE 實習生計畫

2022.12
獲得 Pwn2Own Toronto 冠軍

2023.03
DEVCORE Conference
2023

DEVCORE SECURITY CONSULTING

紅白演練

紅藍演練

紅軍演練

網路攻防演練
Cyber Offensive and Defensive Exercise

紅人演練 (註：這是一個梗，說笑的)
Red Bull Assessment

弱點掃描
Vulnerability Scanning

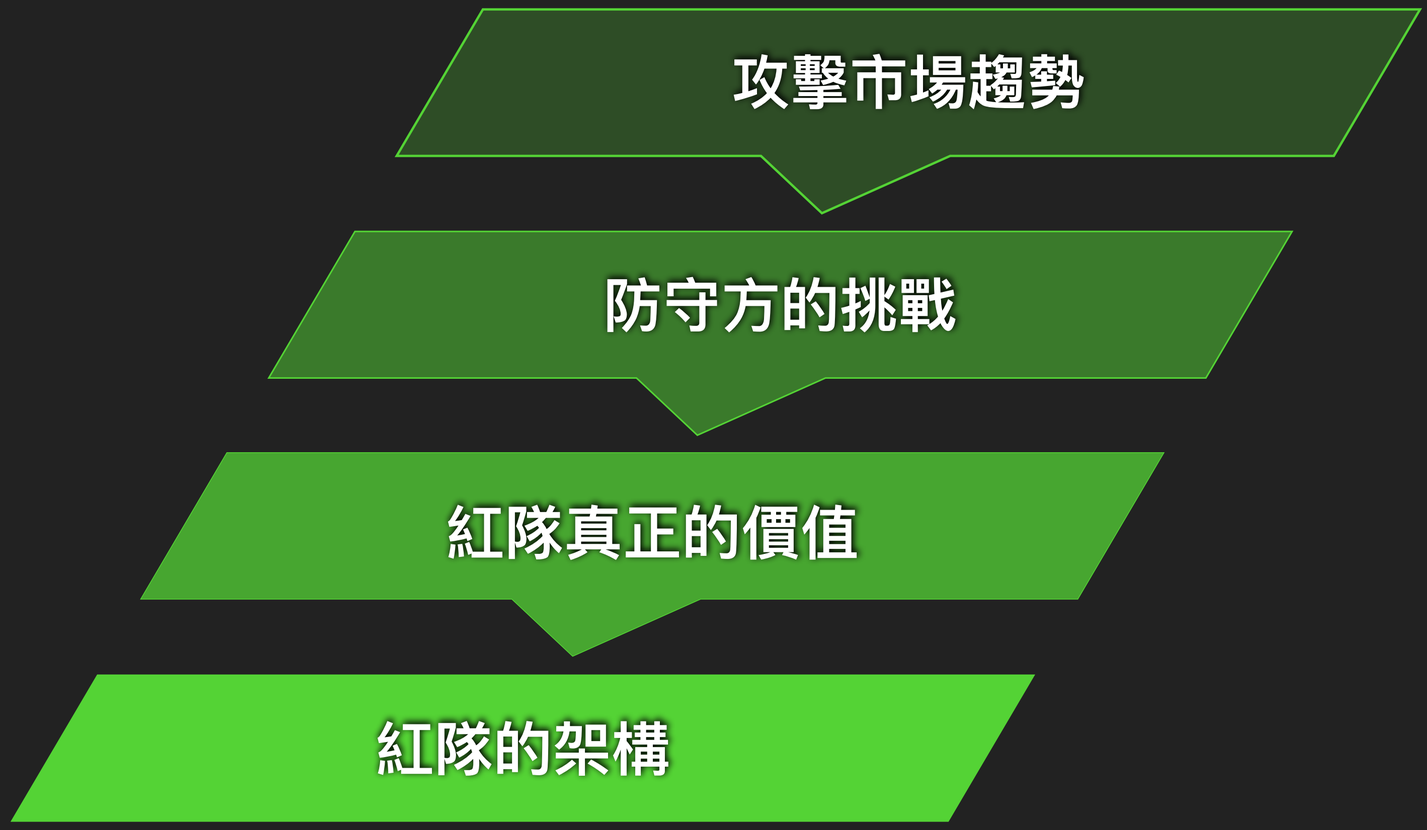
滲透測試
Penetration Testing

弱點評估
Vulnerability Assessment

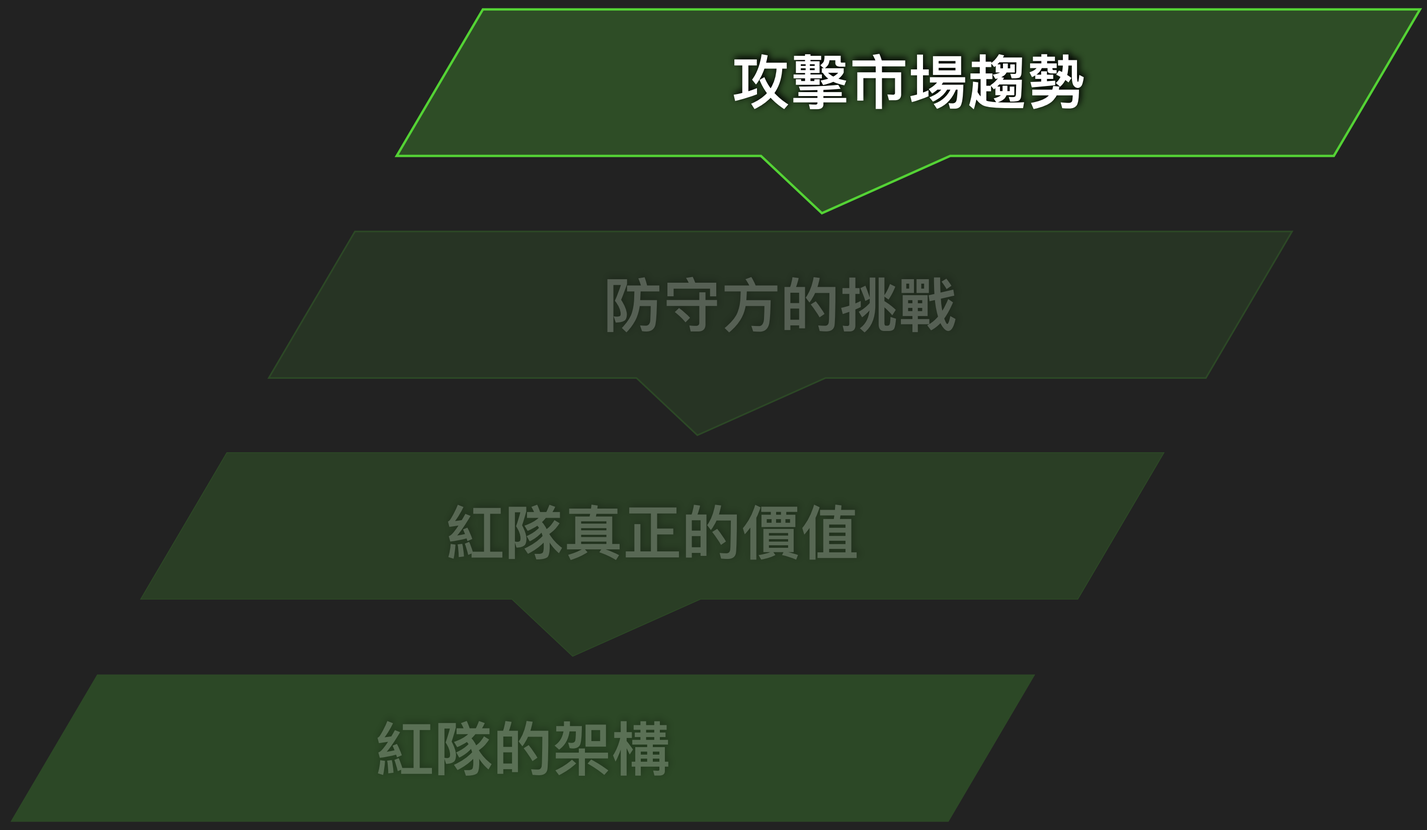
攻擊與入侵模擬工具
Breach and Attack Simulation

網路資安風險管理系統
Attack Surface Management

簡報大綱



簡報大綱



DEVCORE SECURITY CONSULTING

趨勢一、攻擊型產品市場急速增加

DEVCORE SECURITY CONSULTING

未來 6 年攻擊型產品的市場每年將以 11% 以上成長

The global Cybersecurity, ***Red Teaming and Penetration Testing*** *market size was valued at USD 120695.13 million in 2021 and is expected to* ***expand at a CAGR of 11.59% during the forecast period,*** *reaching USD 233045.88 million* ***by 2027****.*

360ResearchReports

The ***Penetration Testing Market*** *Size is Anticipated to Hit USD 8.13 Billion* ***at a CAGR of 13.5% by 2030.***

MARKET RESEARCH FUTURE

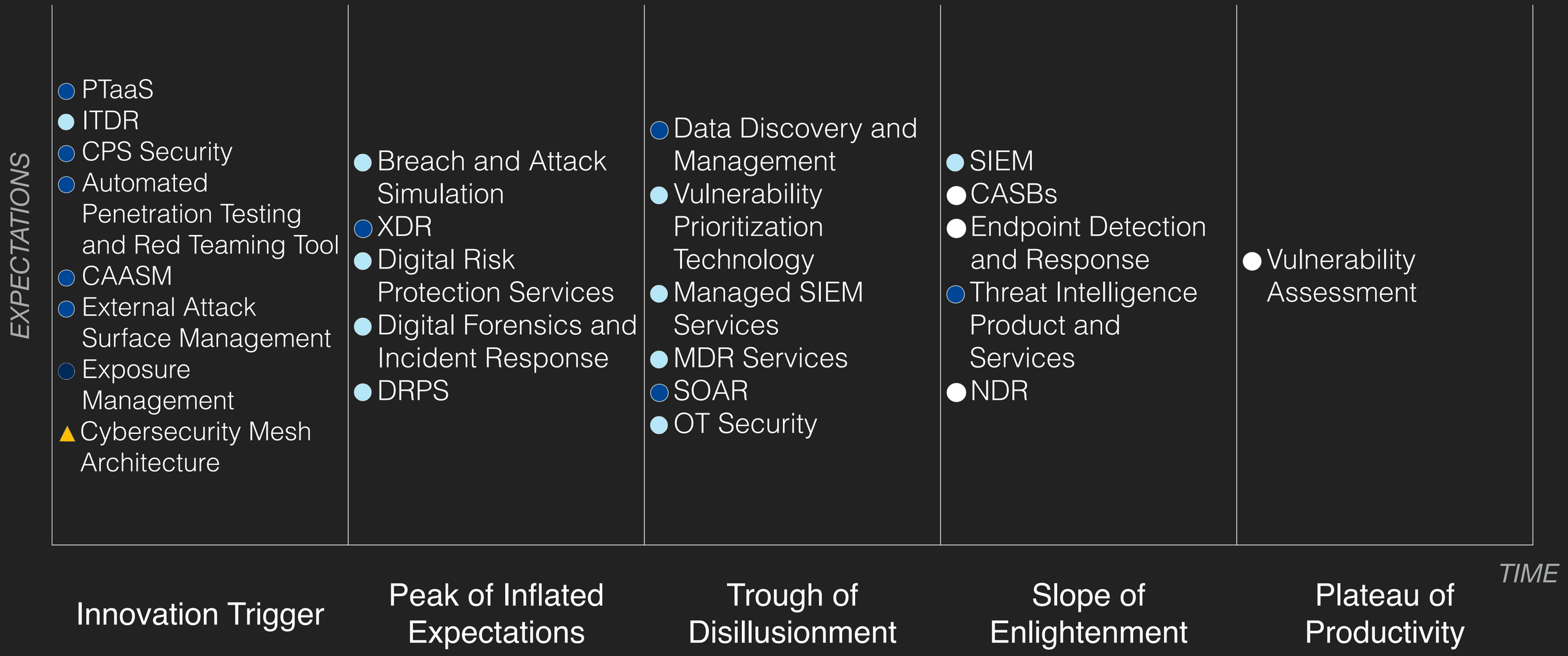
The ***Penetration Testing Market*** *is expected to reach $4.05 billion by 2029,* ***at a CAGR of 12.5% during the forecast period of 2022-2029.*** *The growth of this market is driven by a surge in the need to identify cybersecurity threats and risks across enterprise networks, adherence to regulatory compliance and laws for the implementation of penetration testing solutions and services, and the growing demand for web application firewalls.*

MARKETSANDMARKETS

從資安產品的角度

DEVCORE SECURITY CONSULTING

Gartner Hype Cycle for Security Operation 2022

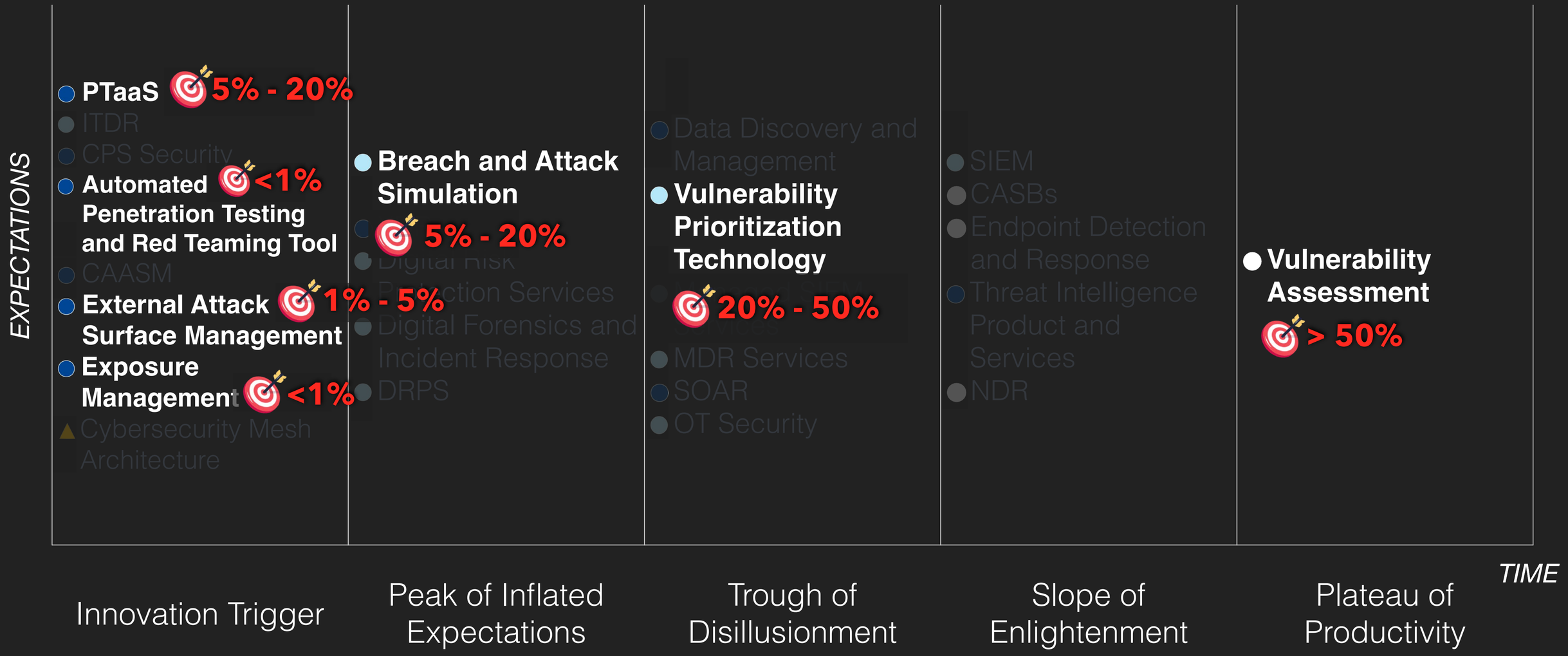


DEVCORE SECURITY CONSULTING

Plateau will be reached： < 2 yrs. 2-5 yrs 5-10 yrs >10yrs


在
2022 Gartner
Hype Cycle for
Security Operation
中，
1/4
攻擊型產品佔了
DEVCORE SECURITY CONSULTING

Gartner Hype Cycle for Security Operation 2022



DEVCORE SECURITY CONSULTING

Plateau will be reached： < 2 yrs. 2-5 yrs 5-10 yrs >10yrs

DEVCORE SECURITY CONSULTING

攻擊型服務及產品的演進

已知漏洞
從被動識別到積極管理

- Vulnerability Scanning
- Vulnerability Analysis and Notice System
- Vulnerability Assessment
- Vulnerability Prioritization Technology

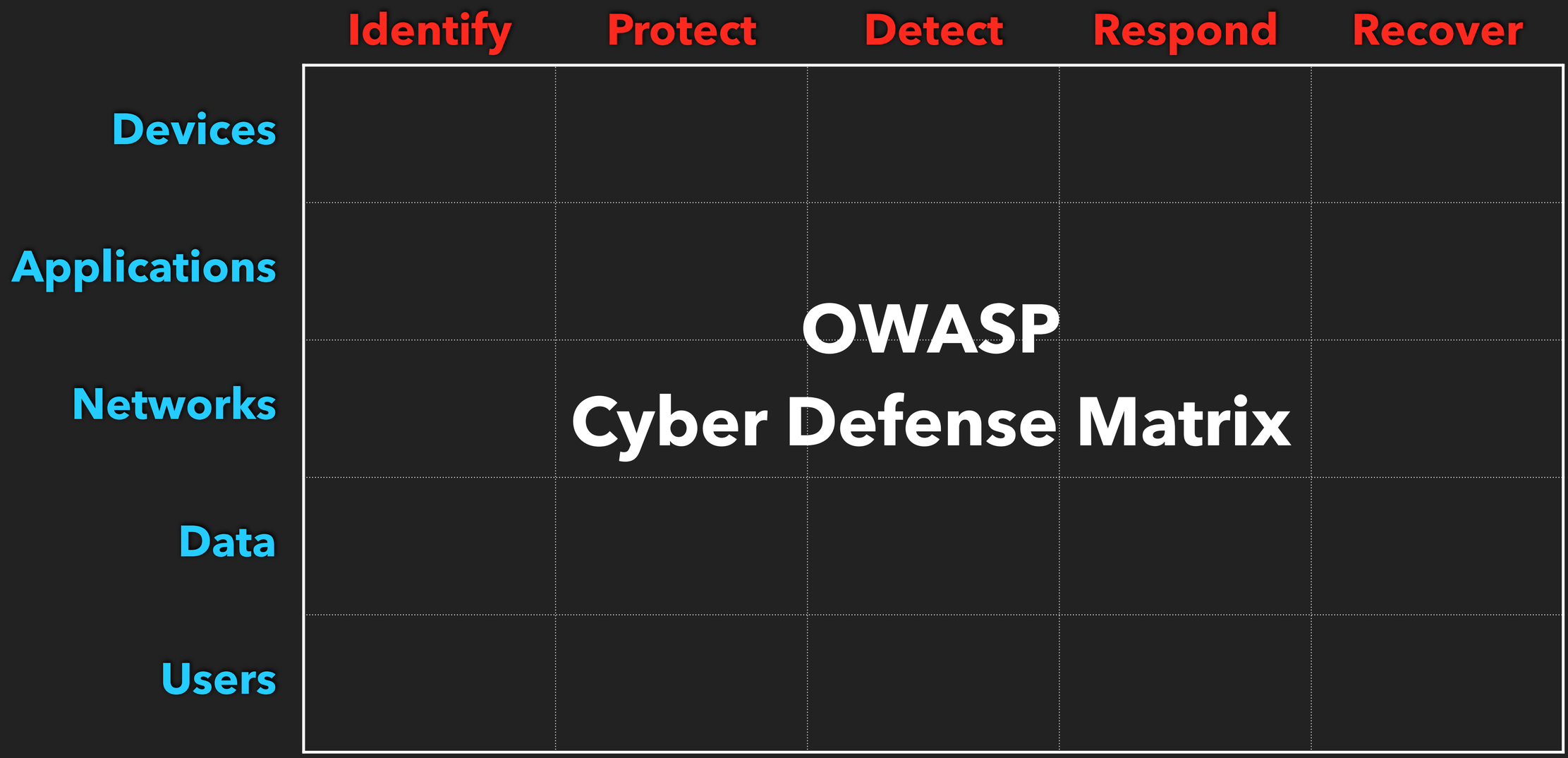
未知漏洞
Web 服務、產品到目標導向

- Web Penetration Testing
- Network Penetration Testing
- Physical Penetration Testing
- Full-Stack Assessment
- Threat Intelligence Red Team Assessment
- Red Team Assessment

執行頻率
每年定期掃描到持續檢測

- Vulnerability Scanning
- External Attack Surface Management
- PTaaS
- Breach and Attack Simulation
- Security Assessment
- Exposure Management

DEVCORE SECURITY CONSULTING



DEVCORE SECURITY CONSULTING

DEVCORE SECURITY CONSULTING

簡報大綱

DEVCORE SECURITY CONSULTING


挑戰一、漏洞不只推陳出新，
嚴重程度也難以評估。
DEVCORE SECURITY CONSULTING

- 至 2025 年全球將有 750 億個物聯網裝置
- 截至今年 2 月底，全球有超過 196,843 個 CVE 編號
  - 10.1%、19,974 個 **極高風險漏洞**
  - 18.8%、36,895 個 **高風險漏洞**
  - 13.3%、26,229 個 **低風險漏洞**

DEVCORE SECURITY CONSULTING

2023/03/11（六） **11:30 — 12:00**

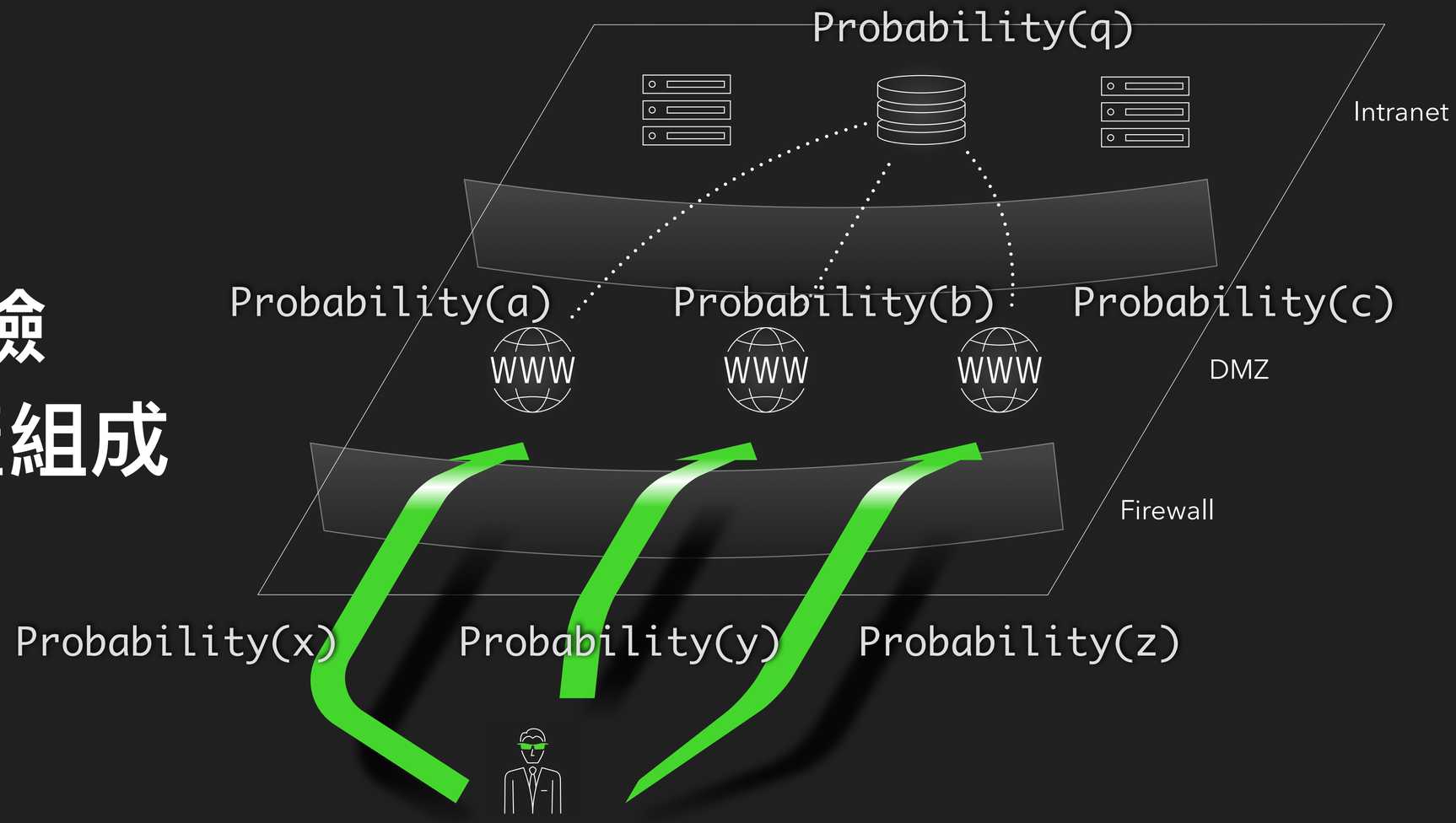
黑魔法、大壞蛋得崩，讓四個臭蟲變成漏洞吧！

Cyku & Crystal ｜ 職位：DEVCORE 資深紅隊演練專家 & 技術專案經理

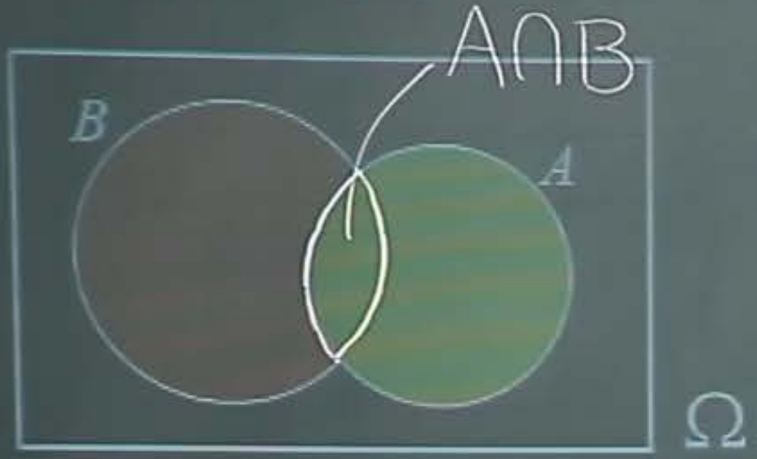
再廢的低分漏洞也有春天！雞肋般的弱點，對紅隊而言還有任何利用價值嗎？低風險、利用機會也低的小漏洞，企業真的可以置之不理嗎？DEVCORE 資深紅隊演練專家 Cyku 及 技術專案經理 Crystal 將透過實際案例，分享攻擊者如何將四個 CVSS 幾乎 0.0 分的廢洞化腐朽為神奇，串成 RCE 漏洞。

DEVCORE SECURITY CONSULTING

企業的風險
由一連串資產組成



條件機率



$$P(B|A) = \frac{P(A \cap B)}{P(A)}$$

例題

有一家庭有兩個小孩，若已知兩個小孩至少有1個男孩，求兩個均為男孩之機率？

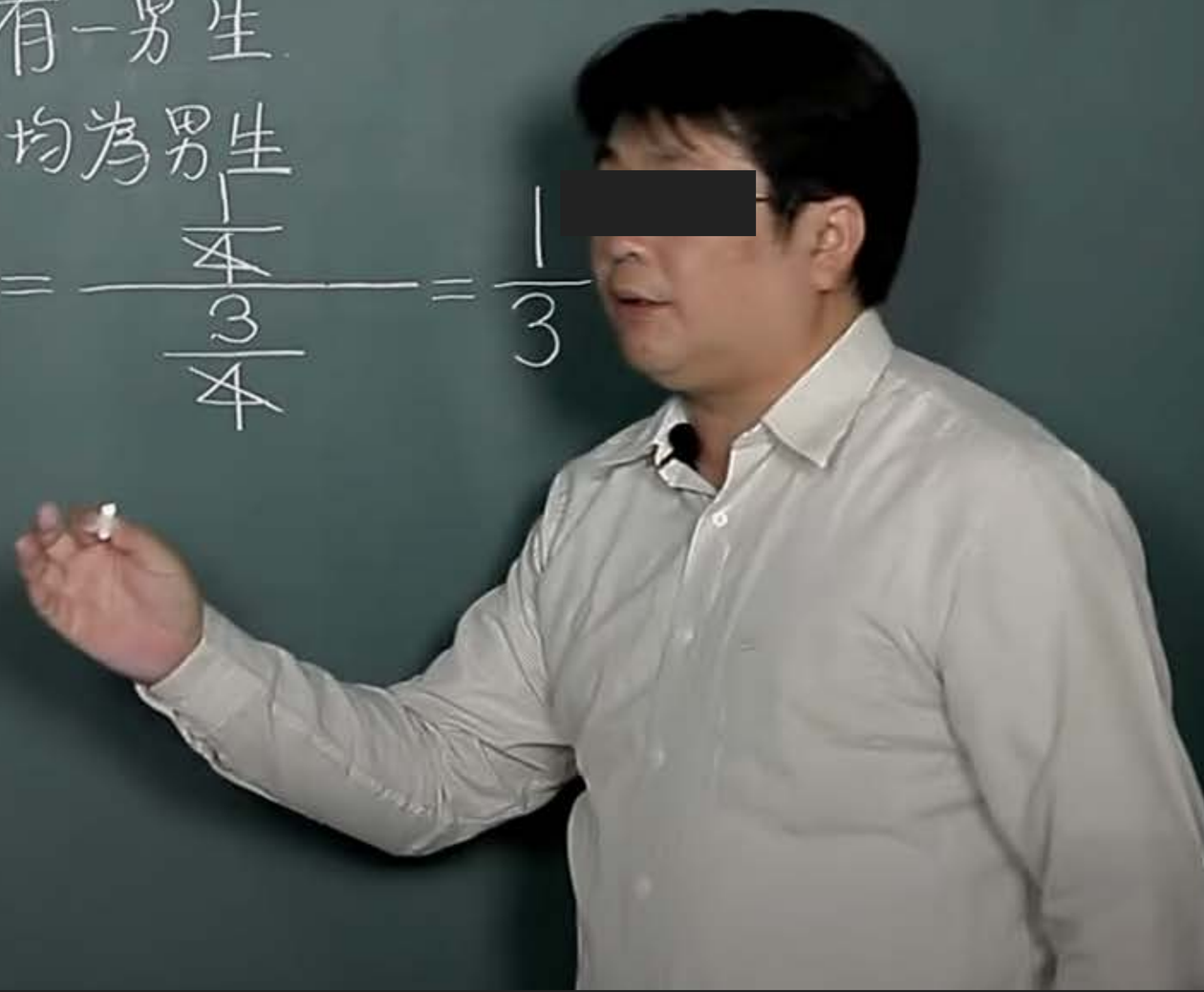
(男,男),(男,女),(女,男),(女,女)

Ans: $\frac{1}{3}$

A：至少有一男生

B：兩個均為男生

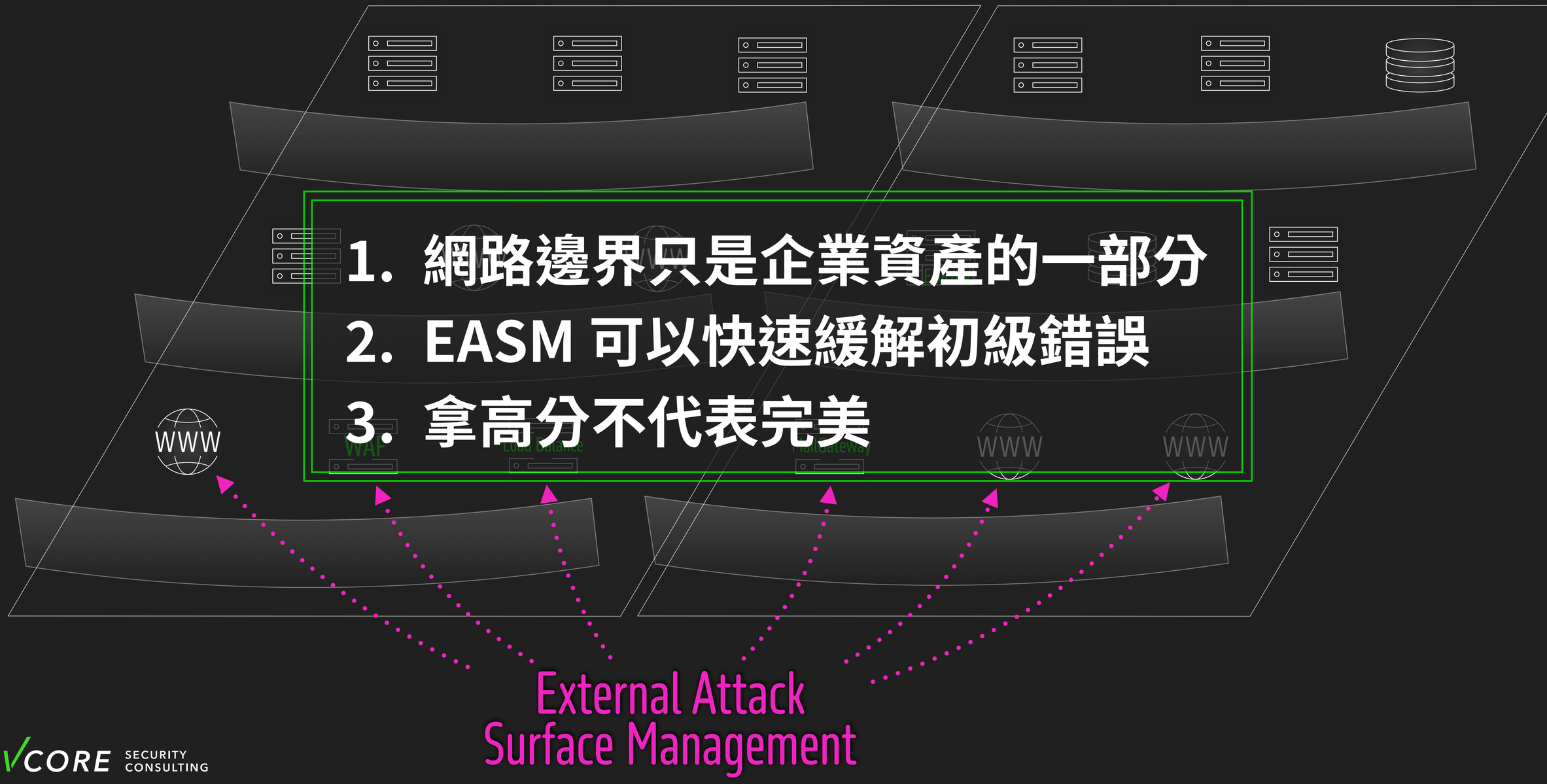
$$P(B|A) = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}$$



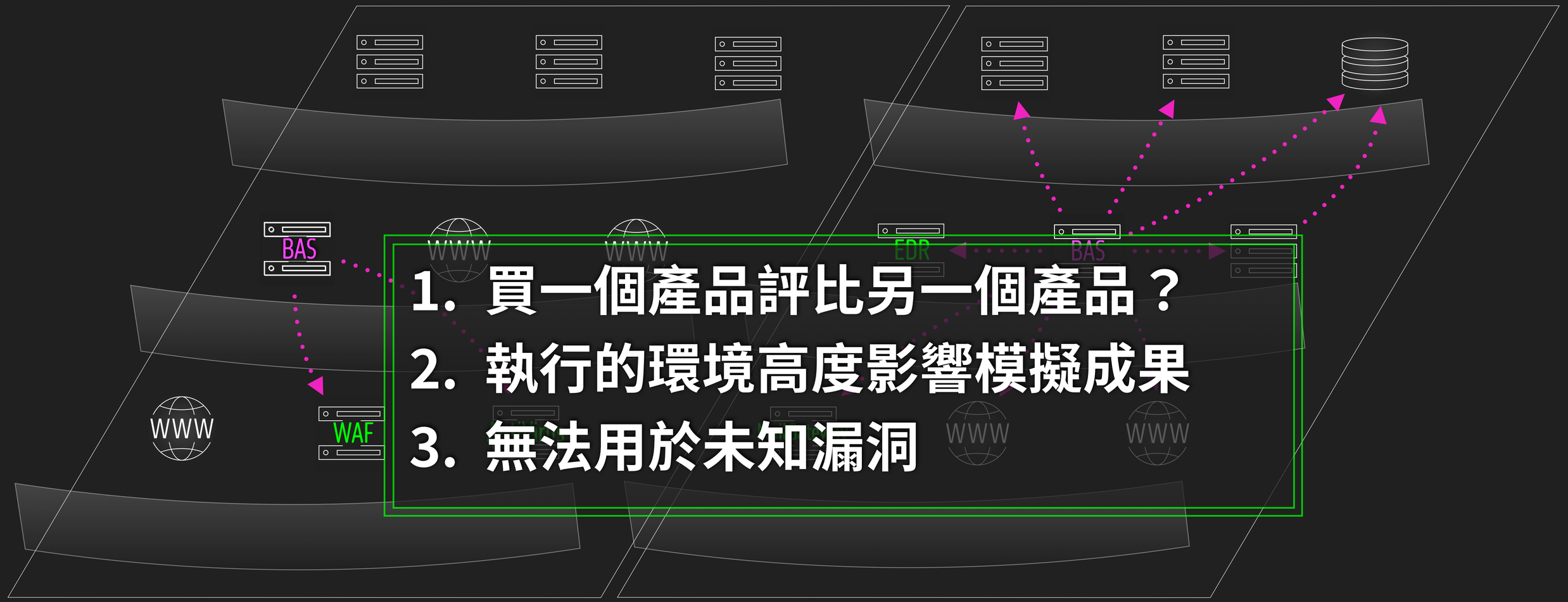
挑戰三、過度仰賴資安產品

謎之音：**沒有**要攻擊資安產品的意思

DEVCORE SECURITY CONSULTING

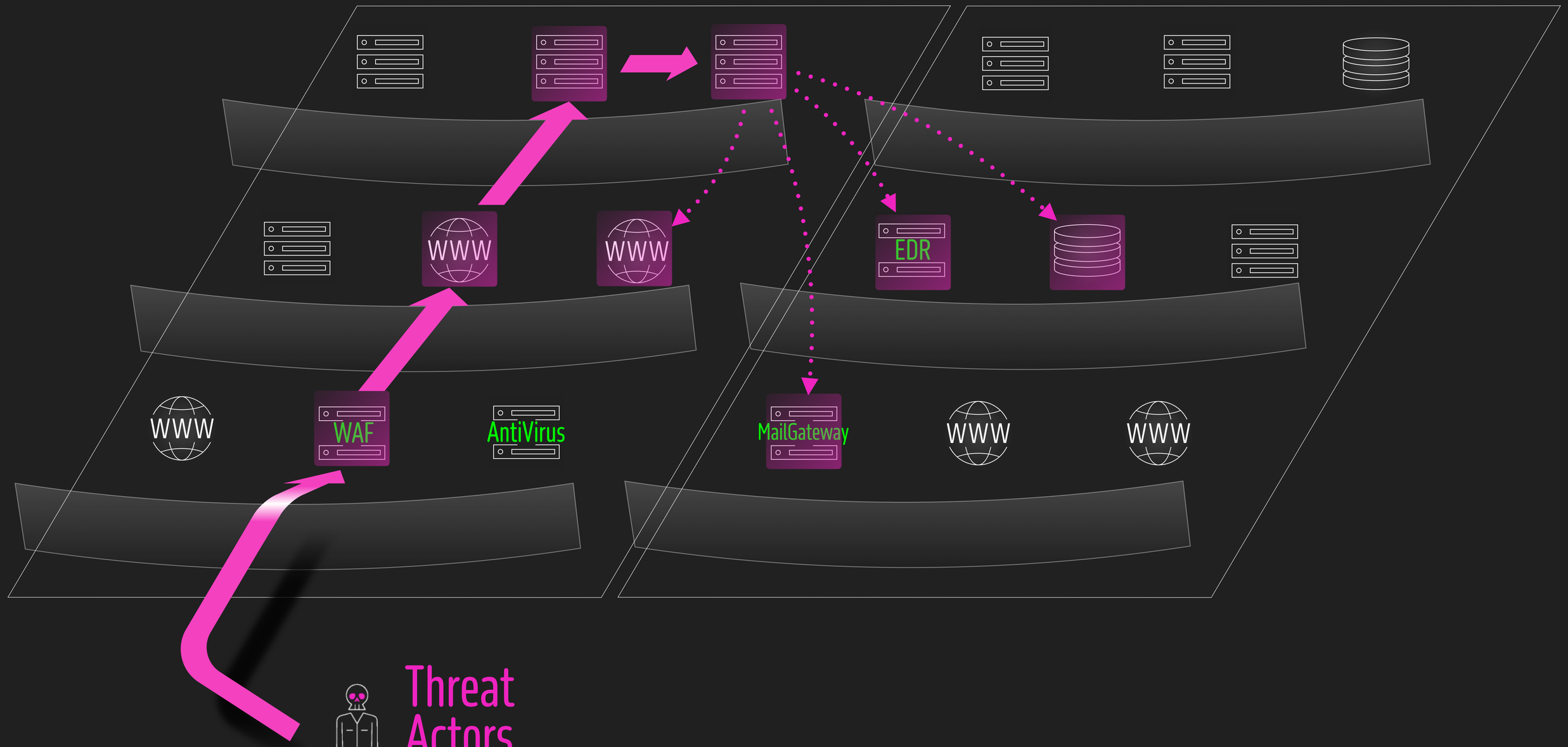


DEVCORE SECURITY CONSULTING



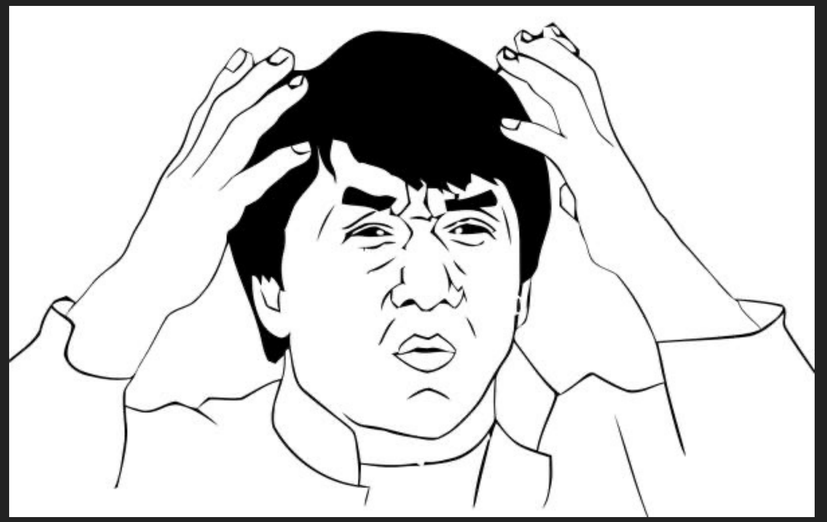
1. 買一個產品評比另一個產品？
2. 執行的環境高度影響模擬成果
3. 無法用於未知漏洞

DEVCORE SECURITY CONSULTING

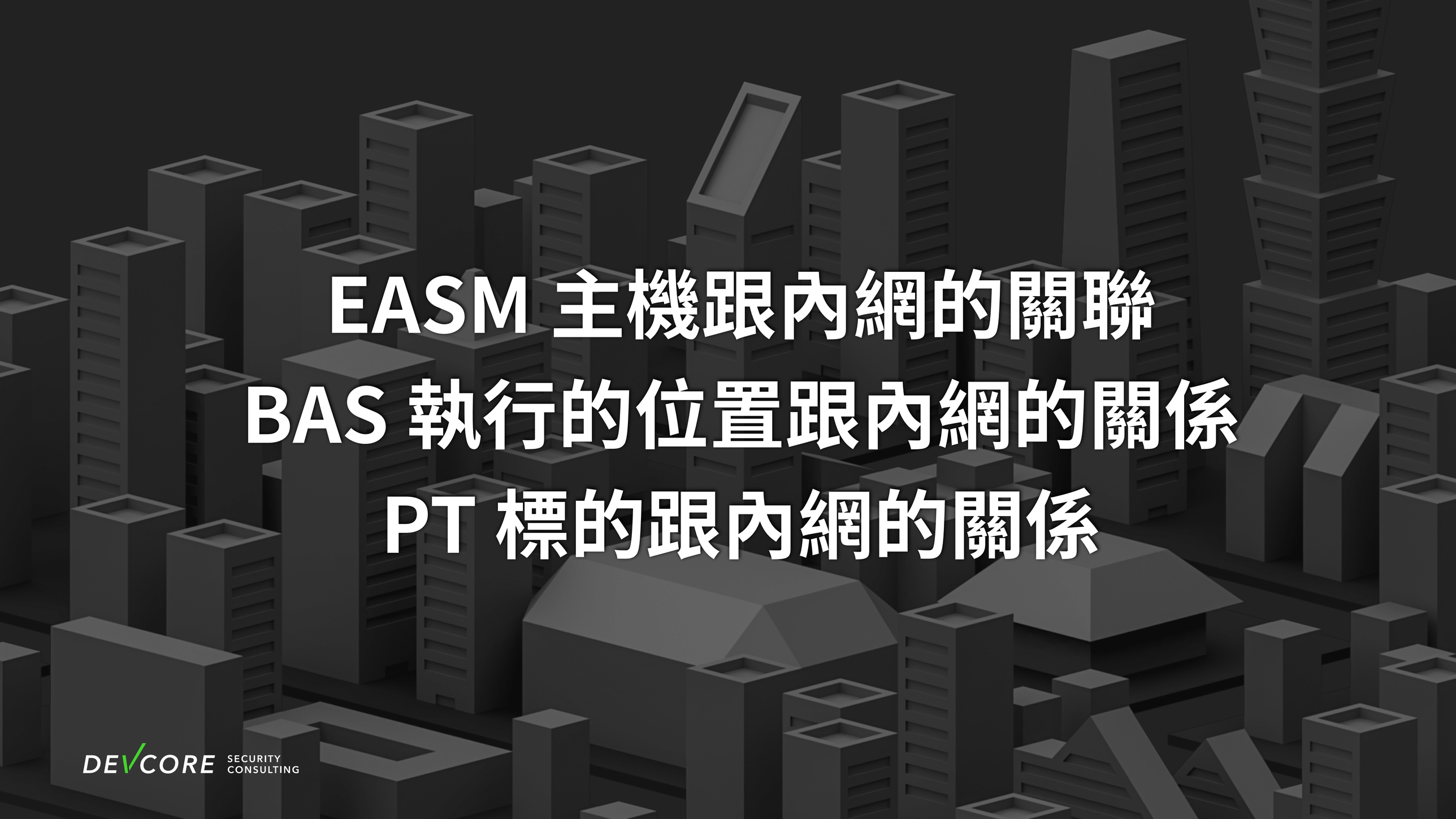


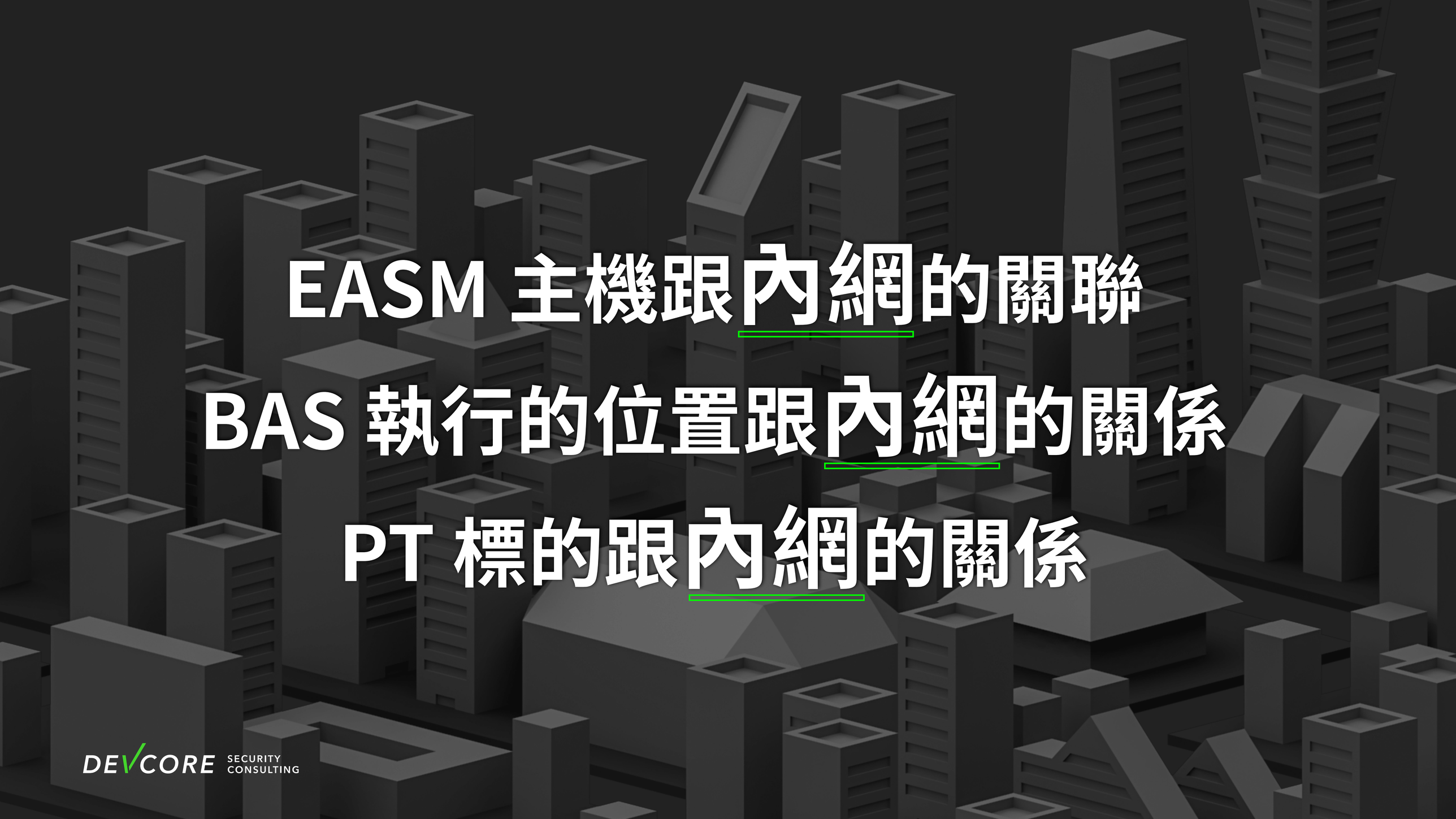
DEVCORE SECURITY CONSULTING

那我到底該怎麼辦？



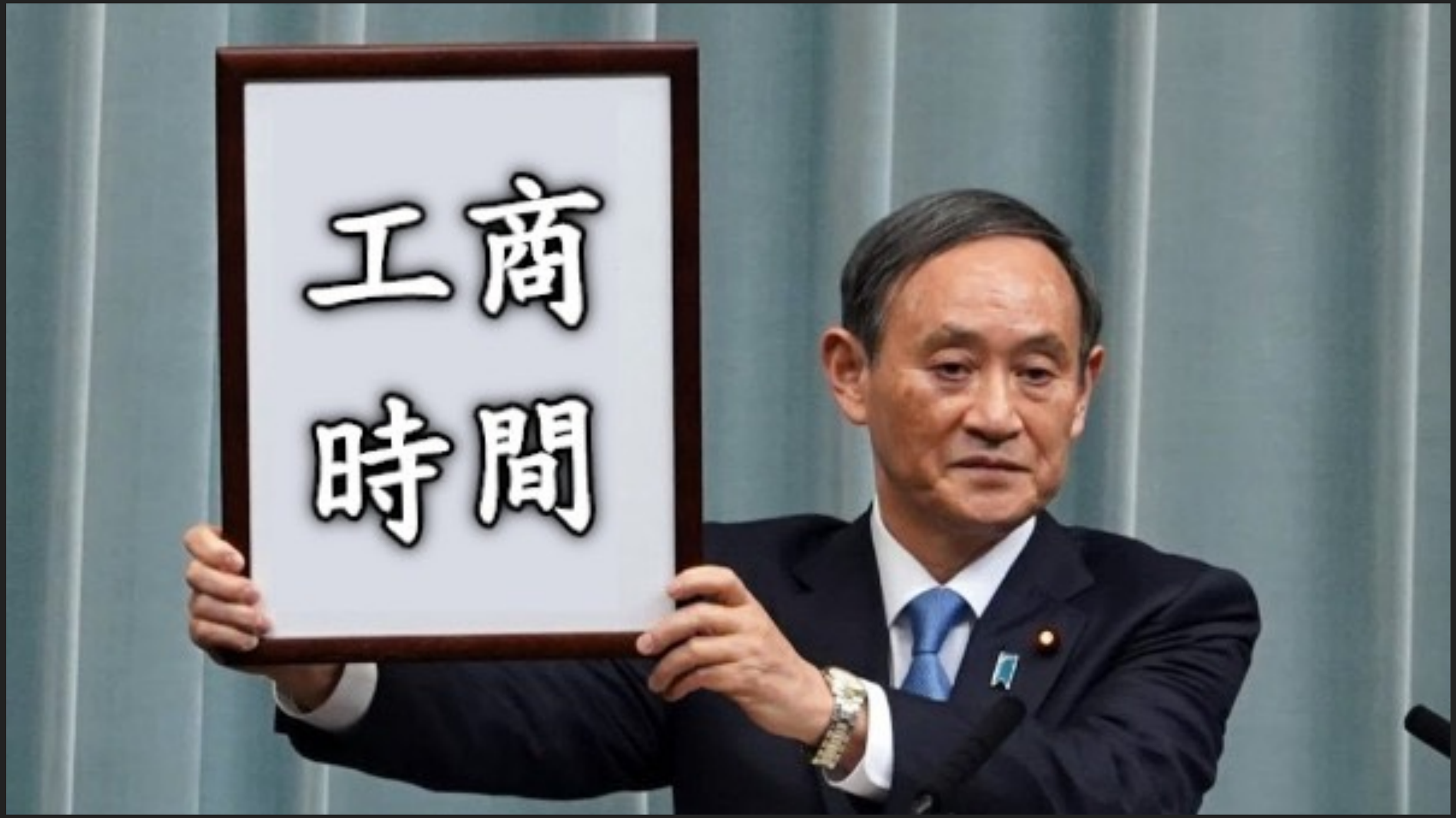
DEVCORE SECURITY CONSULTING


EASM 主機跟內網的關聯
BAS 執行的位置跟內網的關係
PT 標的跟內網的關係
DEVCORE SECURITY CONSULTING


EASM 主機跟內網的關聯
BAS 執行的位置跟內網的關係
PT 標的跟內網的關係
DEVCORE SECURITY CONSULTING

DEVCORE SECURITY CONSULTING


更要思考遺漏的風險跟回應機制
DEVCORE SECURITY CONSULTING


工商
時間

紅隊演練服務 (Red Team Assessment)

- 紅隊演練服務就像是**真實的攻擊演習**。
- 不限定標的、不限定手法，在有限的時間之內**針對目標進行攻擊演練**，讓企業透過瞭解攻擊者的思維、手法、工具，**協助企業評估資安防護投入的效益及控制措施之落實性**，並做真正有效的精準防禦。

DEVCORE Conference 2023
3/11 駭客場熱賣中

技術

09:40 — 10:10

以紅隊思維看藍隊防禦，紅藍攻防中的經典案例

Ding | DEVCORE 紅隊演練隊長

具備豐富指揮作戰經驗的 DEVCORE 紅隊演練隊長 Ding，將於本場議程中分享近 70 場橫跨金融、科技、電商、傳產等各產業經典案例，並以 MITRE ATT&CK 框架，逐一分析實戰經驗中使用的戰術與攻擊手法：初期存取除了OWASP TOP 10 中常見攻擊技巧外還有哪些方式？攻擊者如何持續潛伏，且同時達成防毒軟體未示警、亦無檔案落地？攻擊者如何在網路實體隔離時仍能橫向移動？攻擊者如何以出人意料的手段提升權限？

10:10 — 10:40

讓流量穿過你的巴巴 — 紅隊實戰 SSRF 經典案例

Vtim | DEVCORE 紅隊演練專家

紅隊演練專家 Vtim 將以過去於紅隊演練專案中遇到的 SSRF 真實案例，探討其究竟是報告上有名無實的高風險漏洞，或是企業仍不能忽視的重要安全問題。

15:10 — 16:10

From Zero to Hero — 從零開始的 Pwn2Own 奪冠之路

Orange & Angelboy | DEVCORE 首席資安研究員 & 資深資安研究員

此場議程將由駭客界頗負盛名、屢屢獲獎並受邀演講的 DEVCORE 首席資安研究員 Orange 及資深資安研究員 Angelboy 共同主講，與會眾分享如何挑選目標、建立團隊默契、試誤與學習、與廠商之間的攻防戰等參賽背後秘辛與趣事。

16:10 — 16:20

多樣化的演練模式

實體位置	虛擬位置	策略	執行方式	目標分類	目標項目	執行時間	防禦規避
遠端 Sec. 3, Bade Rd., Songshan Dist., TPE	**網際網路** Internet	**無所不用其極** Zero day	**黑箱測試** Black Box	**關鍵基礎設施** 路由器、Windows AD、ESXi、特權帳號	**網站** Web Application	**指定時間** 10:00 - 18:00	**動態 IP** Dynamic IP Address
指定現場 Reserved-site	**內部網路** VPN、OA、SF、DMZ	**Threat Intelligence** Threat Actor、Playbook	**灰箱測試** Gray Box	**核心資訊系統** SWIFT、ATM 、 Portal	**應用程式** Desktop Application	**排除日期** 排除峰日、特殊活動	**流量干擾** Traffic Log
現場 On-site	**混合模式** Hybrid	**第三方軟體** Third party Software	**白箱測試** White Box	**特殊權限** root、domain admin	**無線網路** WiFi	**不限定時間** 7x24	**日誌干擾** Event Log
		社交工程 Landing、Credential		**機敏資料** 演算法、合約 智慧財產、個人資料	**資安設備安全** Mail Gateway WAF		**防禦機制繞過** WAF、EDR、SOC
		WiFi Guest、OA		**IoT、OT** 製造機台、行控系統	**網段區隔** OA、NOC、OT		**比手速** RASAP
		供應鏈攻擊 Supply Chain Attack			**雲端安全** AWS、Azure		

DEVCORE SECURITY CONSULTING

紅隊演練的不同階段

Stage 1

初次進行

1

- 初步盤點資安體質
- 調整未來資安策略及優先順序

Stage 2

資安成熟度成長中

(需要 1~2 年)

2

- 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

資安成熟度高，真實攻防演練

(合作 2 次以上)

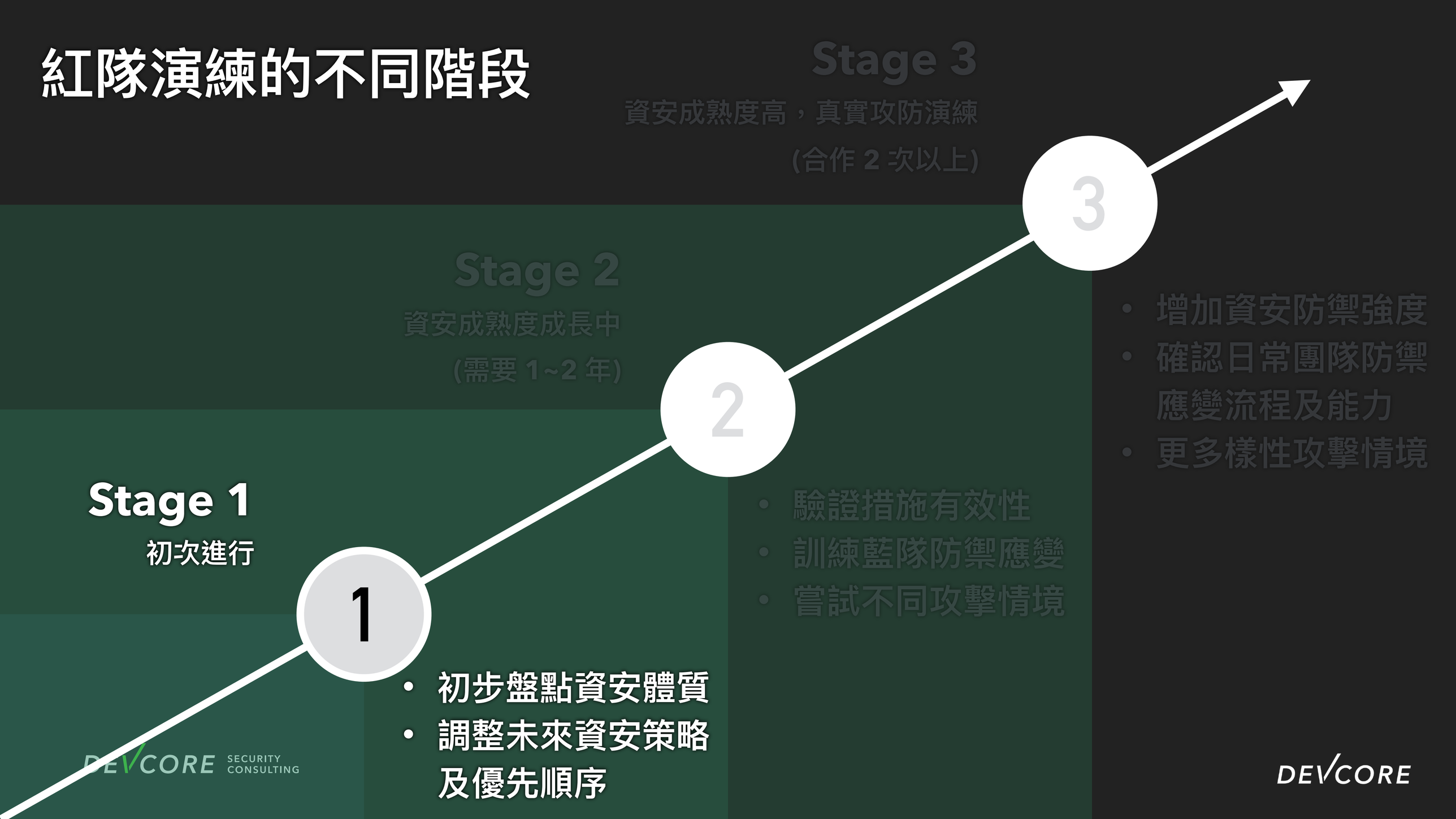
3

- 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 SECURITY CONSULTING

DEVCORE

紅隊演練的不同階段



DEVCORE SECURITY CONSULTING

DEVCORE

第一階段的紅隊演練模式

實體位置	虛擬位置	策略	執行方式	目標分類	目標項目	執行時間	防禦規避
遠端 Sec. 3, Bade Rd., Songshan Dist., TPE	**網際網路** Internet	**無所不用其極** Zero day	**黑箱測試** Black Box	**關鍵基礎設施** 路由器、Windows AD、ESXi、特權帳號	**網站** Web Application	**指定時間** 10:00 - 18:00	**動態 IP** Dynamic IP Address
指定現場 Reserved-site	**內部網路** VPN、OA、SF、DMZ	**Threat Intelligence** Threat Actor、Playbook	**灰箱測試** Gray Box	**核心資訊系統** SWIFT、ATM 、 Portal	**應用程式** Desktop Application	**排除日期** 排除峰日、特殊活動	**流量干擾** Traffic Log
現場 On-site	**混合模式** Hybrid	**第三方軟體** Third party Software	**白箱測試** White Box	**特殊權限** root、domain admin	**無線網路** WiFi	**不限定時間** 7x24	**日誌干擾** Event Log
		社交工程 Landing、Credential		**機敏資料** 演算法、合約 智慧財產、個人資料	**資安設備安全** Mail Gateway WAF		**防禦機制繞過** WAF、EDR、SOC
		WiFi Guest、OA		**IoT、OT** 製造機台、行控系統	**網段區隔** OA、NOC、OT		**比手速** RASAP
		供應鏈攻擊 Supply Chain Attack			**雲端安全** AWS、Azure		

DEVCORE SECURITY CONSULTING

紅隊演練的不同階段

Stage 1

初次進行

1

- 初步盤點資安體質
- 調整未來資安策略及優先順序

Stage 2

資安成熟度成長中

(需要 1~2 年)

2

- 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

資安成熟度高，真實攻防演練

(合作 2 次以上)

3

- 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 SECURITY CONSULTING

DEVCORE

第二階段的紅隊演練模式

實體位置	虛擬位置	策略	執行方式	目標分類	目標項目	執行時間	防禦規避
遠端 Sec. 3, Bade Rd., Songshan Dist., TPE	**網際網路** Internet	**無所不用其極** Zero day	**黑箱測試** Black Box	**關鍵基礎設施** 路由器、Windows AD、ESXi、特權帳號	**網站** Web Application	**指定時間** 10:00 - 18:00	**動態 IP** Dynamic IP Address
指定現場 Reserved-site	**內部網路** VPN、OA、SF、DMZ	**Threat Intelligence** Threat Actor、Playbook	**灰箱測試** Gray Box	**核心資訊系統** SWIFT、ATM 、 Portal	**應用程式** Desktop Application	**排除日期** 排除峰日、特殊活動	**流量干擾** Traffic Log
現場 On-site	**混合模式** Hybrid	**第三方軟體** Third party Software	**白箱測試** White Box	**特殊權限** root、domain admin	**無線網路** WiFi	**不限定時間** 7x24	**日誌干擾** Event Log
		社交工程 Landing、Credential		**機敏資料** 演算法、合約 智慧財產、個人資料	**資安設備安全** Mail Gateway WAF		**防禦機制繞過** WAF、EDR、SOC
		WiFi Guest、OA		**IoT、OT** 製造機台、行控系統	**網段區隔** OA、NOC、OT		**比手速** RASAP
		供應鏈攻擊 Supply Chain Attack			**雲端安全** AWS、Azure		

DEVCORE SECURITY CONSULTING

紅隊演練的不同階段

Stage 1
初次進行

1

- 初步盤點資安體質
- 調整未來資安策略及優先順序

Stage 2
資安成熟度成長中
(需要 1~2 年)

2

- 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
資安成熟度高，真實攻防演練
(合作 2 次以上)

3

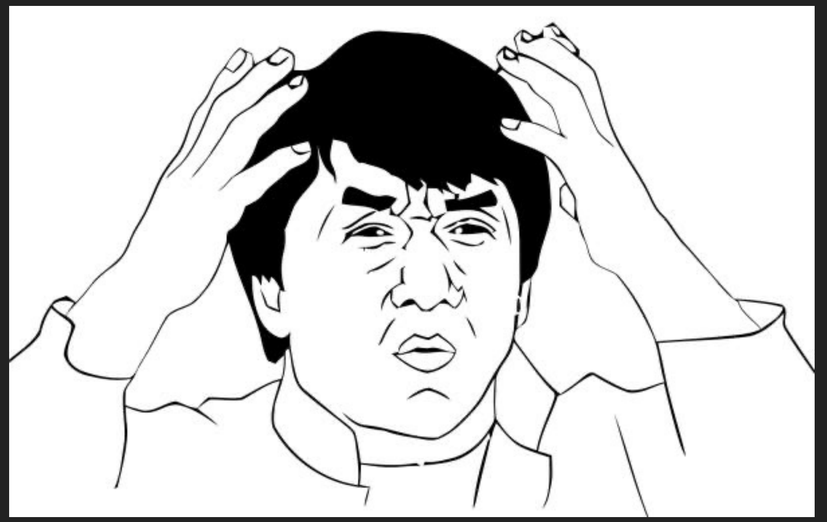
- 增加資安防禦強度
- 確認日常團隊防禦應變流程及能力
- 更多樣性攻擊情境

第三階段的紅隊演練模式

實體位置	虛擬位置	策略	執行方式	目標分類	目標項目	執行時間	防禦規避
遠端 Sec. 3, Bade Rd., Songshan Dist., TPE	**網際網路** Internet	**無所不用其極** Zero day	**黑箱測試** Black Box	**關鍵基礎設施** 路由器、Windows AD、ESXi、特權帳號	**網站** Web Application	**指定時間** 10:00 - 18:00	**動態 IP** Dynamic IP Address
指定現場 Reserved-site	**內部網路** VPN、OA、SF、DMZ	**Threat Intelligence** Threat Actor、Playbook	**灰箱測試** Gray Box	**核心資訊系統** SWIFT、ATM 、 Portal	**應用程式** Desktop Application	**排除日期** 排除峰日、特殊活動	**流量干擾** Traffic Log
現場 On-site	**混合模式** Hybrid	**第三方軟體** Third party Software	**白箱測試** White Box	**特殊權限** root、domain admin	**無線網路** WiFi	**不限定時間** 7x24	**日誌干擾** Event Log
		社交工程 Landing、Credential		**機敏資料** 演算法、合約 智慧財產、個人資料	**資安設備安全** Mail Gateway WAF		**防禦機制繞過** WAF、EDR、SOC
		WiFi Guest、OA		**IoT、OT** 製造機台、行控系統	**網段區隔** OA、NOC、OT		**比手速** RASAP
		供應鏈攻擊 Supply Chain Attack			**雲端安全** AWS、Azure		

DEVCORE SECURITY CONSULTING

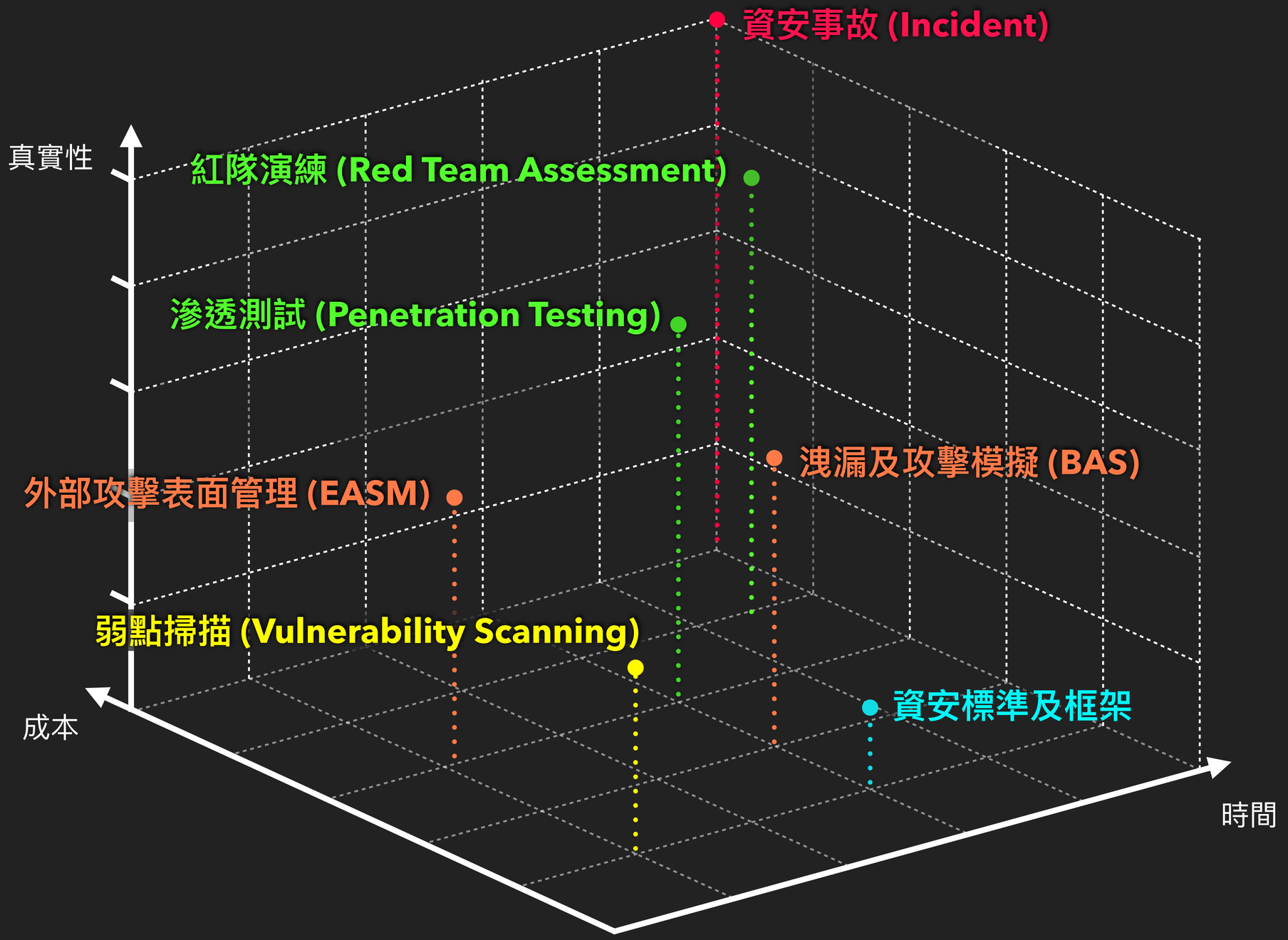
只能買紅隊嗎？



有其他建議嗎？

安全成熟度不同，應挑選合適的檢測方法

- 真實性
- 深度或廣度
- 持續性
- 時間
- 成本



DEVCORE SECURITY CONSULTING

Takeaways

- ✓ 善用攻擊型產品跟服務來減少被初始入侵的機率 (Initial Access)
- ✓ 防禦策略應該以核心系統為基礎，而非單點式的防護策略
- ✓ 資安作為都是用來縮小攻擊表面積，企業必須同時專注於回應事件的韌性

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