DEVCORE
SECURITY
CONSULTING

如何正確使用紅隊演練

翁浩正 (Allen Own)

戴夫寇爾股份有限公司

allenown@devco.re

2022.09.22 iThome CYBERSEC

講者簡介

翁浩正 (Allen Own)

戴夫寇爾 DEVCORE 執行長

台灣駭客協會 HITCON 理事長

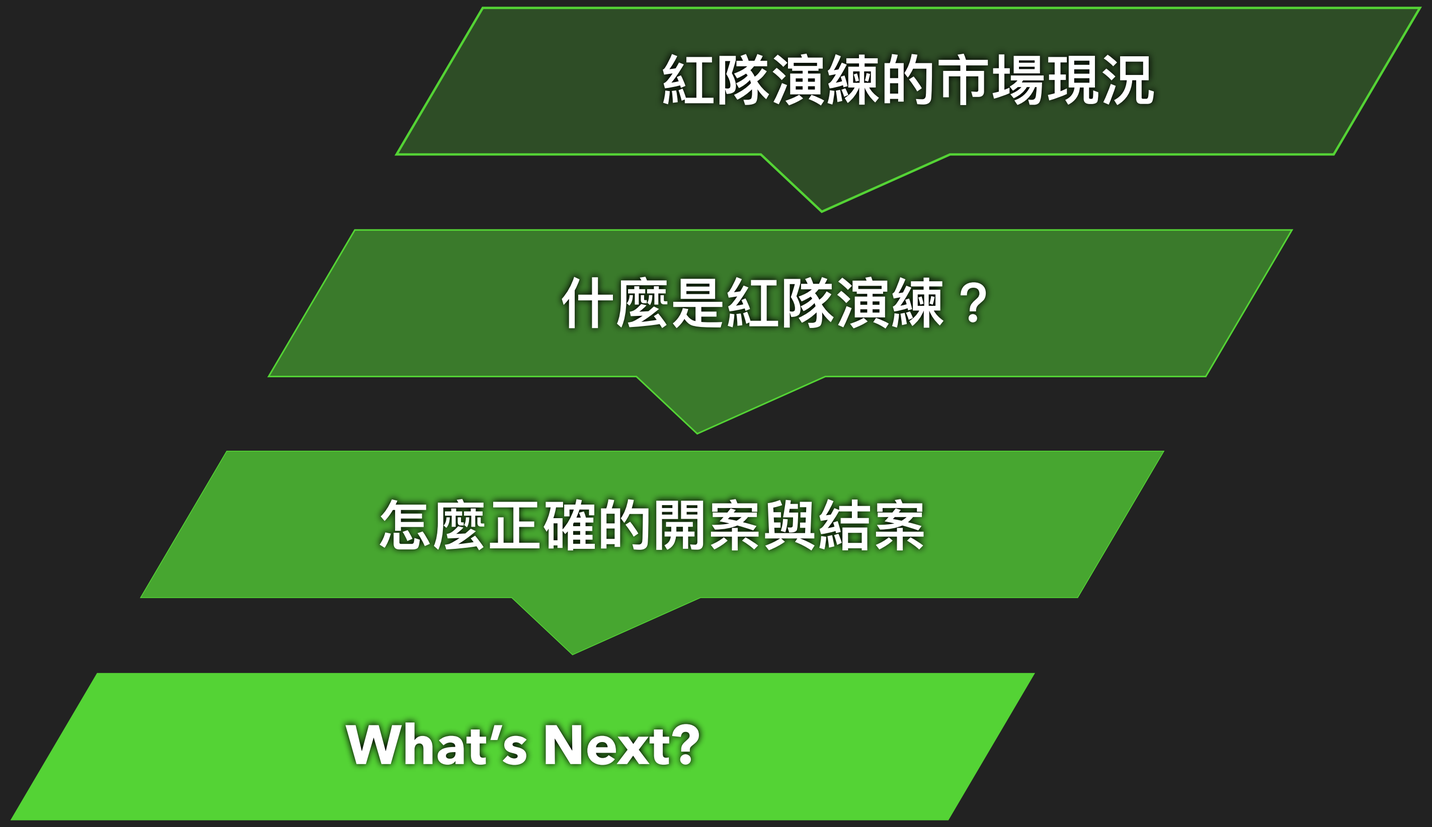
TiEA 協會理事及資安小組負責人

allenown@devco.re

專長：駭客攻擊手法分析、紅隊演練

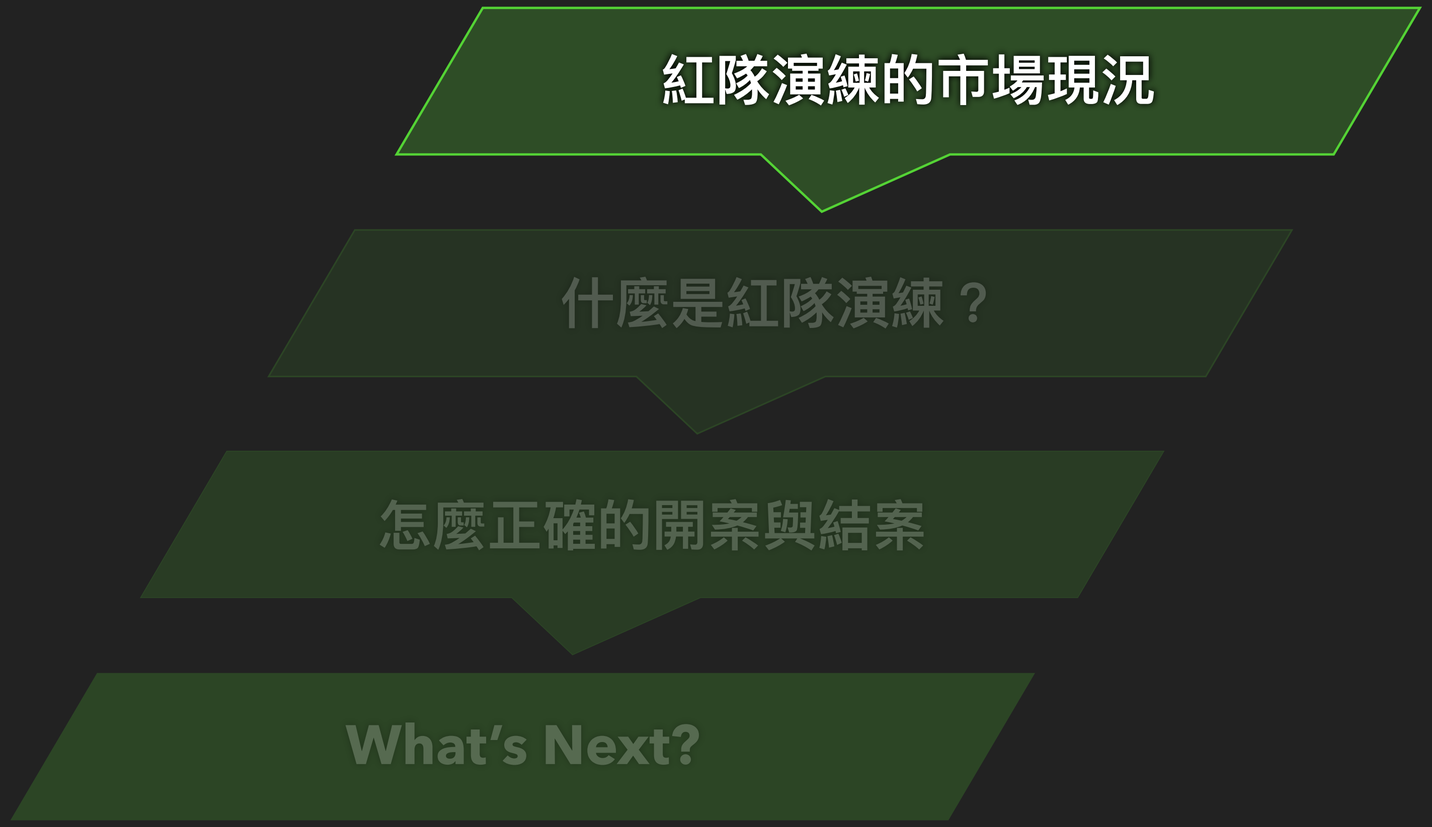
DEVCORE SECURITY CONSULTING

如何正確使用紅隊演練



如何正確使用紅隊演練

- 市場的現況與亂象
- 大量需求與不足的供給

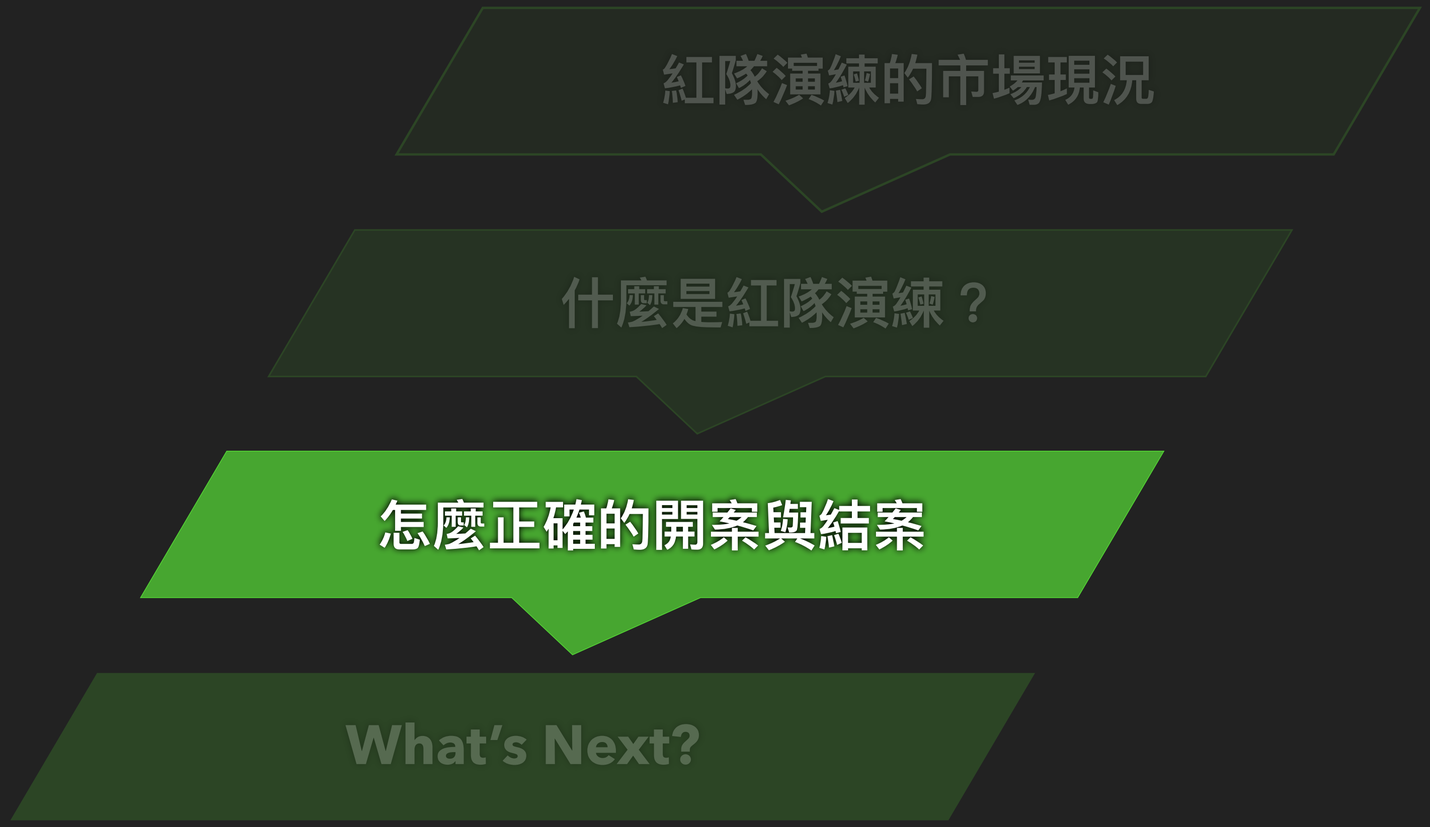


如何正確使用紅隊演練

- 什麼是紅隊演練
- 紅隊演練的起源是什麼
- 紅隊的正確與錯誤觀念
- 紅隊解決了什麼問題

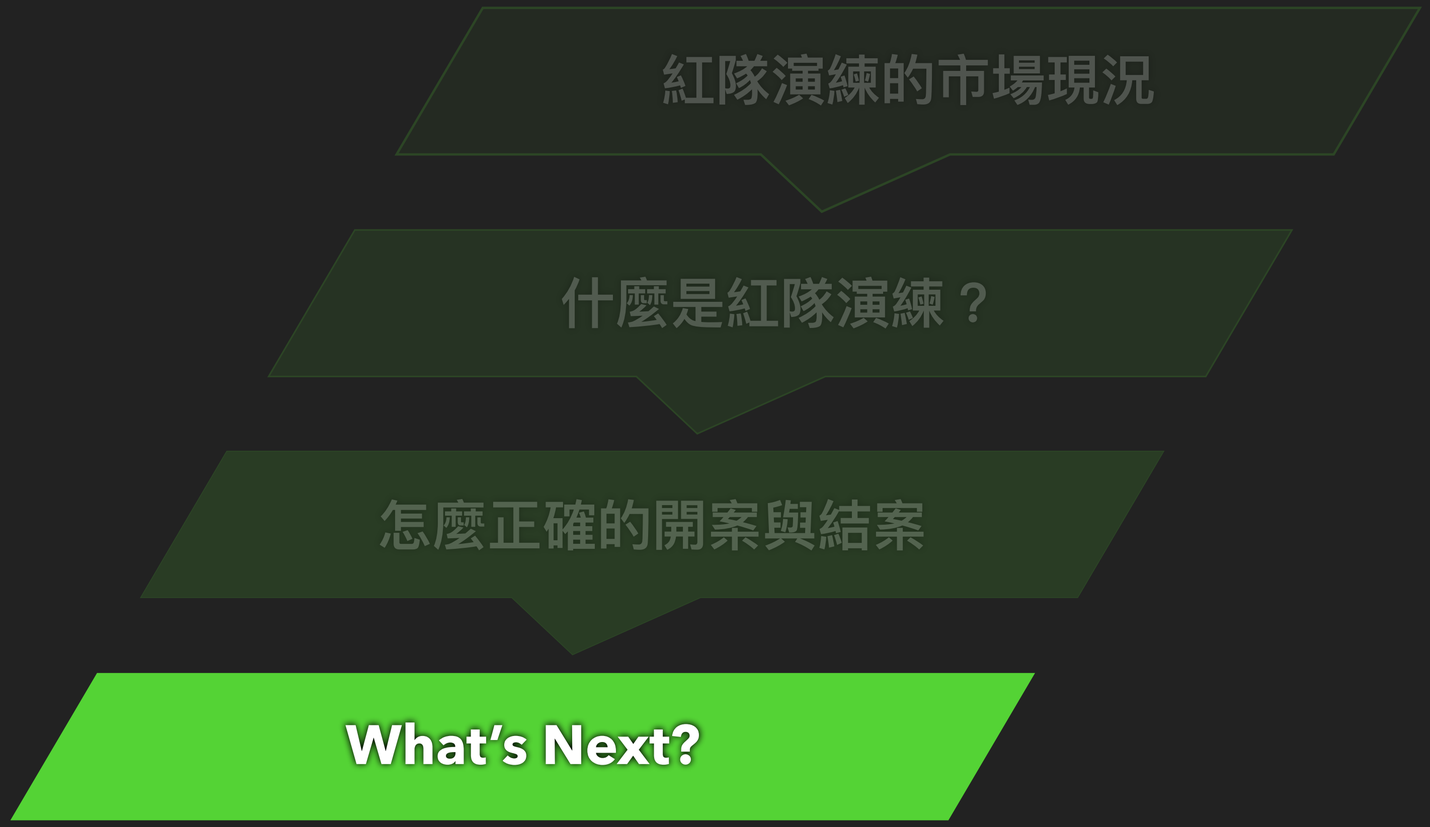
如何正確使用紅隊演練

- 開案前有什麼準備事項
- 怎麼選商
- 怎麼正確的開案與結案
- 執行專案中該怎麼合作



如何正確使用紅隊演練

- 下一步我們該怎麼做？




DEVCORE


你面對的是駭客，我們也是
主動出擊、知己知彼
聚焦威脅、防範未然
RED TEAM
ASSESSMENT
BROKEN ACCESS CONTROL
SECURITY MISCONFIGURATION
DETERMINATION
PROXY
LOGON
HACKER MINDSET
PENETRATION
TEST
MAN IN THE MIDDLE
LATERAL MOVEMENT
STACK SMASHING
INJECTION
USE AFTER FREE
BUG BOUNTY
META-PROGRAMMING
CROSS-SITE SCRIPTING
PASS THE TICKET
PRIVILEGE ESCALATION
XXE
CREDENTIAL STUFFING
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

獎項與研究成果

10 項
國際肯定

2021 Pwn2Own Austin 亞軍
2021 Pwnie Award (Best Server-side Bug)
2021 Pwn2Own Vancouver 冠軍
2021 Top 10 Web Hacking Techniques #3
2020 Pwn2Own Tokyo 亞軍
2020 Top 10 Web Hacking Techniques #7
2019 Pwnie Awards (Best Server-side Bug)
2019 Top 10 Web Hacking Techniques #4 & #8
2018 Top 10 Web Hacking Techniques #1
2017 Top 10 Web Hacking Techniques #1

130+ 個
漏洞揭露

超過 30 種產品類型，
包含最企業常使用的
Microsoft Exchange、
Pulse Secure、Fortinet、
Palo Alto、Jenkins、
Mail2000、Synology、
HiNet GPON 數據機

30+ 場
國際研討會

Black Hat USA
DEF CON
Black Hat Asia
Red Team Summit
CODE BLUE
HITB
HITCON

25+ 次
漏洞獎金計畫

Amazon
Facebook
Microsoft
GitHub
Google
LINE
Twitter
Uber

DEVCORE SECURITY CONSULTING

2021 年最常被利用的15 個漏洞

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

https://www.securityweek.com/national-cybersecurity-agencies-list-most-exploited-vulnerabilities-2021

2021 年最常被利用的15 個漏洞








CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	**ProxyShell**	**Microsoft Exchange Server**	**Elevation of privilege**
CVE-2021-34473	**ProxyShell**	**Microsoft Exchange Server**	**RCE**
CVE-2021-31207	**ProxyShell**	**Microsoft Exchange Server**	**Security feature bypass**
CVE-2021-27065	**ProxyLogon**	**Microsoft Exchange Server**	**RCE**
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	**ProxyLogon**	**Microsoft Exchange Server**	**RCE**
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		**Pulse Secure Pulse Connect Secure**	**Arbitrary file reading**
CVE-2018-13379		**Fortinet FortiOS and FortiProxy**	**Path traversal**

https://www.securityweek.com/national-cybersecurity-agencies-list-most-exploited-vulnerabilities-2021

客戶實績

高科技製造業

全球前五大半導體製造廠
全球前五大半導體設計廠
全球前五大半導體封測廠
電腦及週邊設備業

政府機關

總統府
衛生福利部
交通部
中央健康保險署
台北市政府

金融服務業

兆豐國際商業銀行
臺灣證券交易所
國泰世華商業銀行
國泰人壽保險
臺灣證券交易所

重要產業

交通運輸
電子商務
醫療衛生
新創產業

聽眾：為什麼你們有資格講「如何正確使用紅隊」？


私密瀏覽
紅隊演練
Google
紅隊演練
登入
全部
新聞
圖片
影片
地圖
更多
工具
約有 1,220,000 項結果 (搜尋時間：0.34 秒)
https://devco.re › services › red-team
紅隊演練服務Red Team Assessment | DEVCORE 戴夫寇爾
紅隊演練(Red Team Assessment) 是在不影響企業營運的前提下，對企業進行模擬入侵攻擊，在有限的時間內以無所不用其極的方式，從各種進入點執行攻擊，嘗試達成企業指定 ...
https://www.chtsecurity.com › service
紅隊演練服務 - 中華資安
紅隊演練(Red Teaming) 係用以補足傳統滲透測試容易忽略之邊界防禦，以及基於人為疏失之佈署盲點，利用公開資訊、社交網路、暗網等搜集目標情資、結合資訊安全專家之 ...
https://www.fisc.com.tw › Upload PDF
淺談紅隊評估
2. 行政院國土安全辦公室(2008)，國家關鍵基礎設施防護—演習參考手冊。 3. The New York Times，Banks Adopt Military-Style Tactics to Fight Cybercrime(2018/05/20)。 4.
5 頁
https://www.informationsecurity.com.tw › article_detail
「不知攻、焉知防」，目標導向的紅隊演練提升台灣資安能量
2022年1月13日 — 而紅隊演練（Red Team Assessment）就是提供在不影響企業營運的前提下，進行模擬入侵攻擊，在有限的時間內以無所不用其極的方式，從各種進入點執行 ...
其他人也搜尋了以下項目
紅隊演練滲透測試差異
DEVCORE 薪水
紅隊演練流程
紅 隊 工具
資安攻防演練
紅 藍隊


私密瀏覽
紅隊演練
Google
紅隊演練
登入
全部
新聞
圖片
影片
地圖
更多
工具
約有 1,220,000 項結果 (搜尋時間：0.34 秒)
https://devco.re › services › red-team
紅隊演練服務Red Team Assessment | DEVCORE 戴夫寇爾
https://devco.re › services › red-team
紅隊演練服務Red Team Assessment | DEVCORE 戴夫寇爾
紅隊演練(Red Team Assessment) 是在不影響企業營運的前提下，對企業進行模擬入侵攻擊，在有限的時間內以無所不用其極的方式，從各種進入點執行攻擊，嘗試達成企業指定 ...
5 頁
https://www.informationsecurity.com.tw › article_detail
「不知攻、焉知防」，目標導向的紅隊演練提升台灣資安能量
2022年1月13日 — 而紅隊演練（Red Team Assessment）就是提供在不影響企業營運的前提下，進行模擬入侵攻擊，在有限的時間內以無所不用其極的方式，從各種進入點執行 ...
其他人也搜尋了以下項目
紅隊演練滲透測試差異
DEVCORE 薪水
紅隊演練流程
紅 隊 工具
資安攻防演練
紅 藍隊

Google red team assessment Sign in

All Images Videos News Maps More Tools

About 3,420,000,000 results (0.35 seconds)

https://www.synopsys.com › glossary › what-is-red-tea...

What Is Red Teaming and How Does It Work? | Synopsys

A **red team assessment** is a goal-based adversarial activity that requires a big-picture, holistic view of the organization from the perspective of an ...

https://devco.re › services › red-team

Red Team Assessment | DEVCORE

Red Team Assessment is a simulated intrusion attack on an organization without affecting their regular operation. In a limited time period, attacks will be made ...

https://www.redteamsecure.com › blog › penetration-testi...

Penetration Testing Vs. Red Teaming: What's the Difference?

Red team assessments begin with reconnaissance to collect as much information as possible about the target to learn about the people, technology and environment ...

https://www.mandiant.com › technical-assurance › red-t...

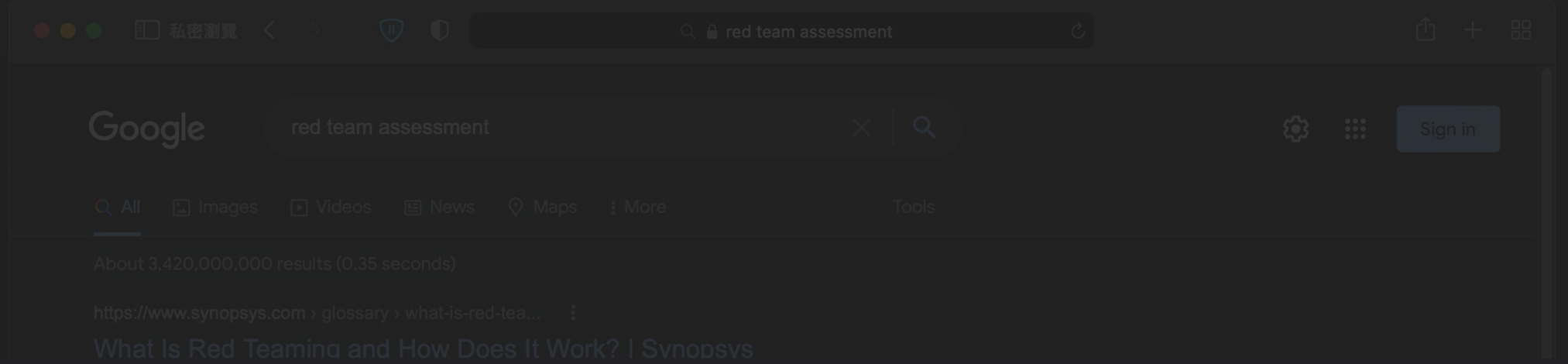
Cyber Attack Simulation & Assessment | Red Team ... - Mandiant

Red Team Assessment · Test your security program against real-world attacks. Experience attack objectives that expose your organization to worst-case business ...

https://www.sisainfosec.com › ... › Network Security

Red Teaming Exercise And Assessment Testing Services | SISA

Red Team Exercise follows a structural approach and it is conducted based on the strategy that has been followed by intruders traditionally. The core ...



https://devco.re › services › red-team

Red Team Assessment | DEVCORE

Red Team Assessment is a simulated intrusion attack on an organization without affecting their regular operation. In a limited time period, attacks will be made ...

Penetration Testing vs. Red Teaming: What's the Difference?

Red team assessments begin with reconnaissance to collect as much information as possible about the target to learn about the people, technology and environment ...

https://www.mandiant.com › technical-assurance › red-t...

Cyber Attack Simulation & Assessment | Red Team ... - Mandiant

Red Team Assessment · Test your security program against real-world attacks. Experience attack objectives that expose your organization to worst-case business ...

https://www.sisainfosec.com › ... › Network Security

Red Teaming Exercise And Assessment Testing Services | SISA

Red Team Exercise follows a structural approach and it is conducted based on the strategy that has been followed by intruders traditionally. The core ...

回顧過去的連載主題

您可能已經成為企業資安的加害者

企業的安全堡壘聽起來無堅不摧，只要盲目的把城牆蓋得越高彷彿就越安全，但對於駭客來說並不是這麼一回事。本場議程將跟以往一樣以駭客思維出發，用攻擊者角度看待企業的安全防護，並且以滲透測試案例說明企業的資安缺口往往是人，別讓我們成為企業資安的加害者。

- 滲透測試如何無堅不摧
- 台灣企業資安現況
- 員工如何成為企業資安缺口
- 滲透測試案例

議程時間 2017-03-14 16:50:00 教室 101AB

2017

DEVCORE SECURITY CONSULTING

你還在用紙牆抵禦步槍嗎？Try Red Team.

Red Teaming 紅隊測試的概念，一直以來都是驗證防禦的最佳方式，也是客觀推測敵人攻擊手法的途徑。企業資安最大的困境在於無法瞭解防禦是否有成效，更對於敵暗我明的現況感到恐慌。盲目的採購資安設備？…

3月13日 16:10 101A

Red Team Pentest Hackers & Threats

Speaker

戴夫寇爾 DEVCORE 執行長 / 翁浩正 (Allen Own)

2018

DEVCORE SECURITY CONSULTING

金融安全論壇

用紅隊演練最佳化資安投資 (15:40-16:00)

3月21日　15:40　TICC 201 BC

大型企業面對專業縝密的攻擊時，擬定防禦策略是最難的議題。當資安事件不斷發生之後，企業不得不重新思考：我們真的知道我們要保護的是什麼嗎？我們的防禦戰略方向是正確的嗎？

紅隊演練是最擬真的攻擊測試，模擬企業在面對網軍等級的攻擊時將如何應對。在每次演練之後，我們幫助企業最大的不是找到漏洞，而是重新盤點資安現況，其中最重要的就是最佳化資安的資源、預算等投資。

你還在投入重兵防禦駭客不感興趣的網站嗎？你的防禦戰略契合真正的攻擊思維嗎？我們將在這場演講分享紅隊演練的實際案例，紅隊的必備戰技及戰術編制、以及紅隊如何在戰略思維上幫助企業最佳化資安投資及防禦策略。

2019

Red Team | Penetration Testing | Risk Management

你的資安策略夠明確嗎？透過框架優先緩解真實威脅

8月12日　15:50　7F_701 B

任何企業要達到適切的安全都須仰賴正確的資安策略。但資安策略的困境往往不夠明確、難以實踐、脫離真實，除了難以幫助企業減緩資安威脅、也無法達成有限預算的投放。

資安策略的制訂很困難，但參考框架的話就可以事半功倍，像是 NIST Cybersecurity Framework (CSF)、MITRE ATT&CK、CIS 等等。而這麼多框架到底是什麼？彼此間的關係為何？怎麼選用才能避免淪為紙上談兵？而面對真實威脅時，如何以更完整的角度去緩解一連串的脆弱的環節？

我們期待透過這場議程，幫助企業理解資安策略的訂定方式。選擇適合自己的框架項目，更可明確制訂每個階段的目標，讓企業推動資安實踐的過程更為具體並且正確對應真實威脅。

2020

Security Strategy　NIST Cybersecurity Framework　Red Team

Cyber Leadership Forum

發光吧！臺灣資安研究員

5月 4日 星期二　15:30 - 16:00　7F 701D

他山之石，未必可以攻錯！你認知的威脅真的解決了問題嗎？

供應鏈攻擊、第三方軟體漏洞、產品出廠預設密碼、雲端服務資料外洩，面對變幻莫測的攻擊型態，企業該如何確保防禦措施符合預期？企業往往以強化木桶理論中的「短板」來降低風險，卻苦於如何挑出短板或難以評估短板對企業造成的威脅程度，也就難以衡量緩解機制的成效，只能將資源投注在防範普遍或近期最流行的攻擊型態。然而，這些常見的攻擊，真的是企業亟需解決的問題嗎？

DEVCORE 將從 2020 年企業的資安需求調查出發，並分享執行 3 年紅隊演練的企業從發現的問題，以及攻擊者如何繞過企業防禦體系。議程中將點出企業對於自身資安需求與實際情形的落差，盼能讓企業以更宏觀的視野重新思考其資安風險評估機制，以提高資安資源投入的效益。

2021

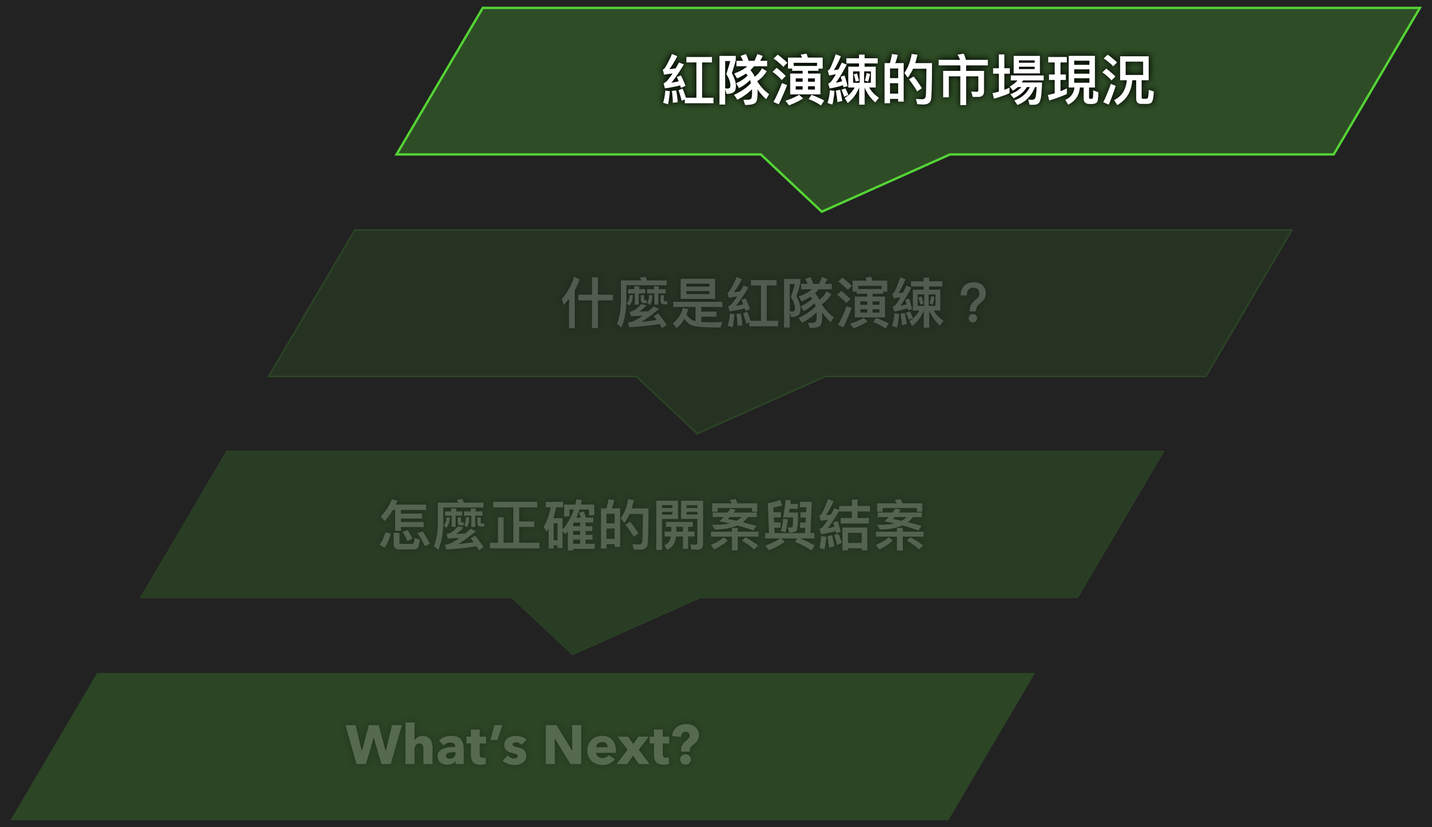
2022

如何正確使用紅隊演練

DEVCORE SECURITY CONSULTING

如何正確使用紅隊演練

- 市場的現況與亂象
- 大量需求與不足的供給



目前的市場現況

目前的市場亂象現況

我們業務人員的日常

某天一早，電話響起...

客戶：「你好... 我想買紅隊演練。」
我們：『您好，我們想先瞭解為什麼想要紅隊演練呢？』
客戶：「因為我們前陣子被入侵，想找人抓駭客。」
我們：『...好的，我們得先從定義好好聊聊。』

客戶的日常

某日，老闆的指示...

老闆 A：「主管你去評估一下採購紅隊演練。」

主管 B：『老闆，請問預算多少？』

老闆 A：「有做就好，**看哪家便宜選哪家**啊！這樣其他資安服務預算也都省了。」

客戶的日常

主管 B：「請問你們有提供紅隊演練嗎？」

廠商 C：『當然有！原本滲透測試加點錢就行了！

（把原本滲透測試報告名字換一下就可以啦）』

劣質廠商的日常

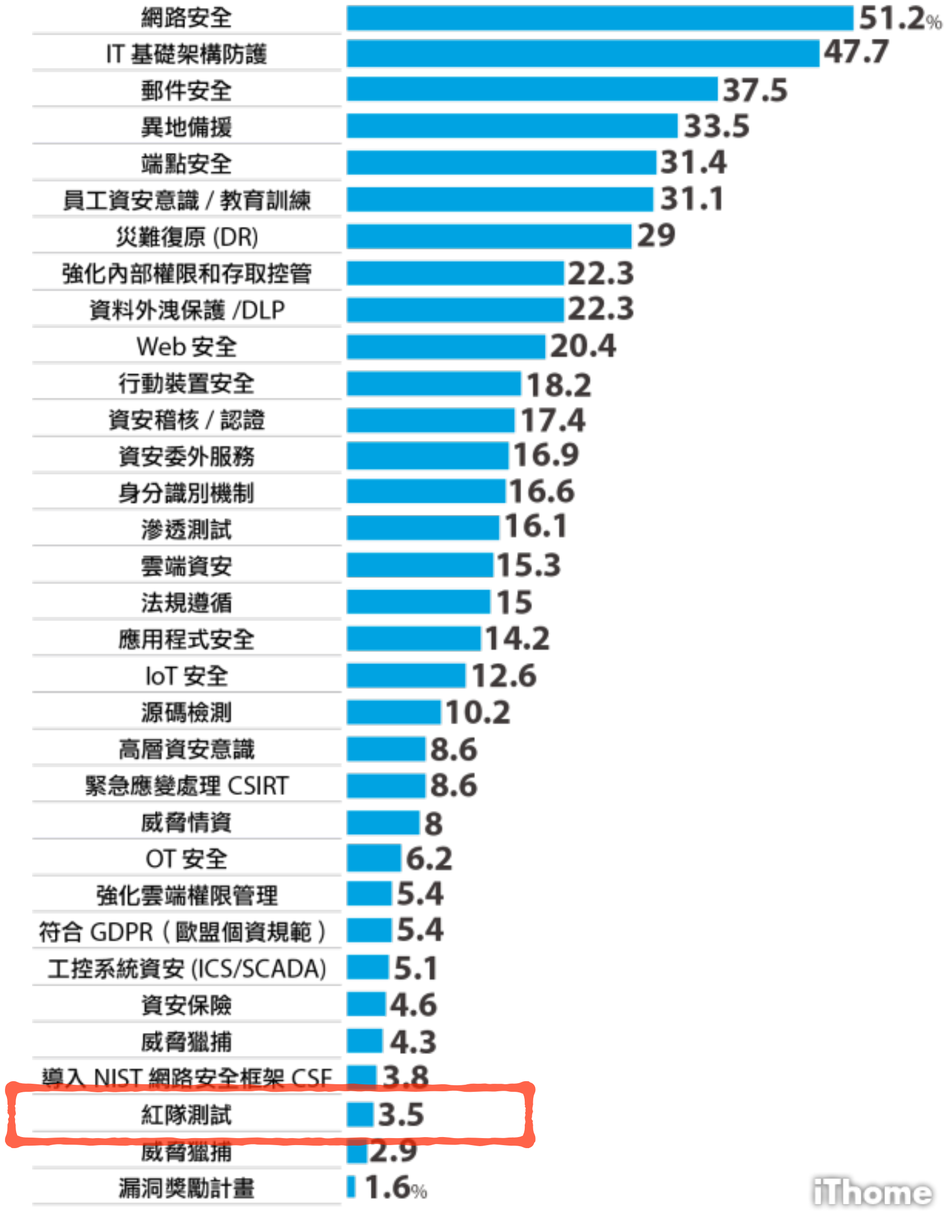
某日，客戶有了紅隊演練的需求...

廠商老闆 C：「那個 D，你去做紅隊演練專案。」
廠商員工 D：『老闆，我沒做過耶？紅隊是什麼？』
廠商老闆 C：「你就裝 Kali 掃一掃客戶主機就好啦！報告標題有出現紅隊演練四個字就可以了。」

我們只能認為，
亂象多，代表大家重視，市場變大了。
這是好事（？）

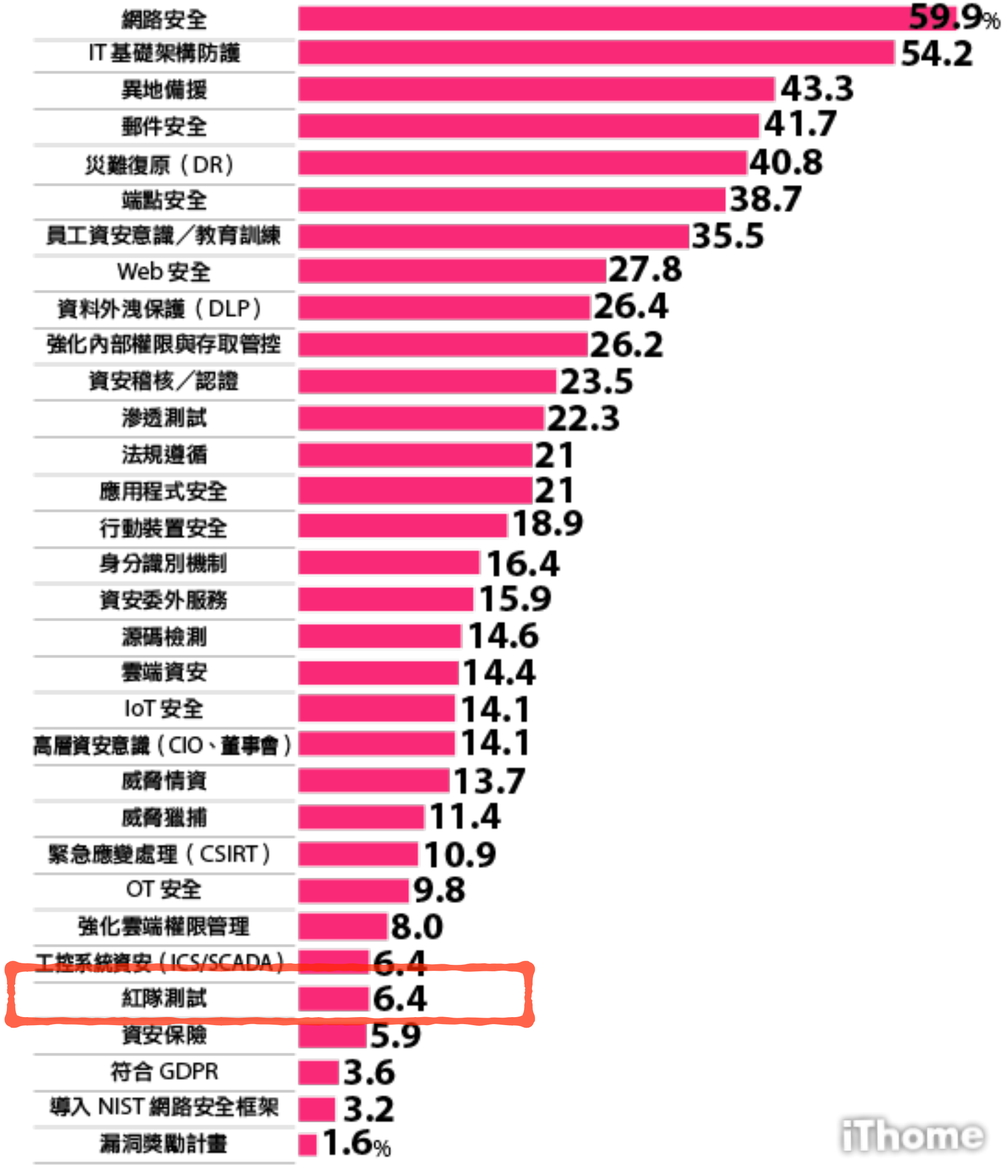
2020 企業資安投資重點

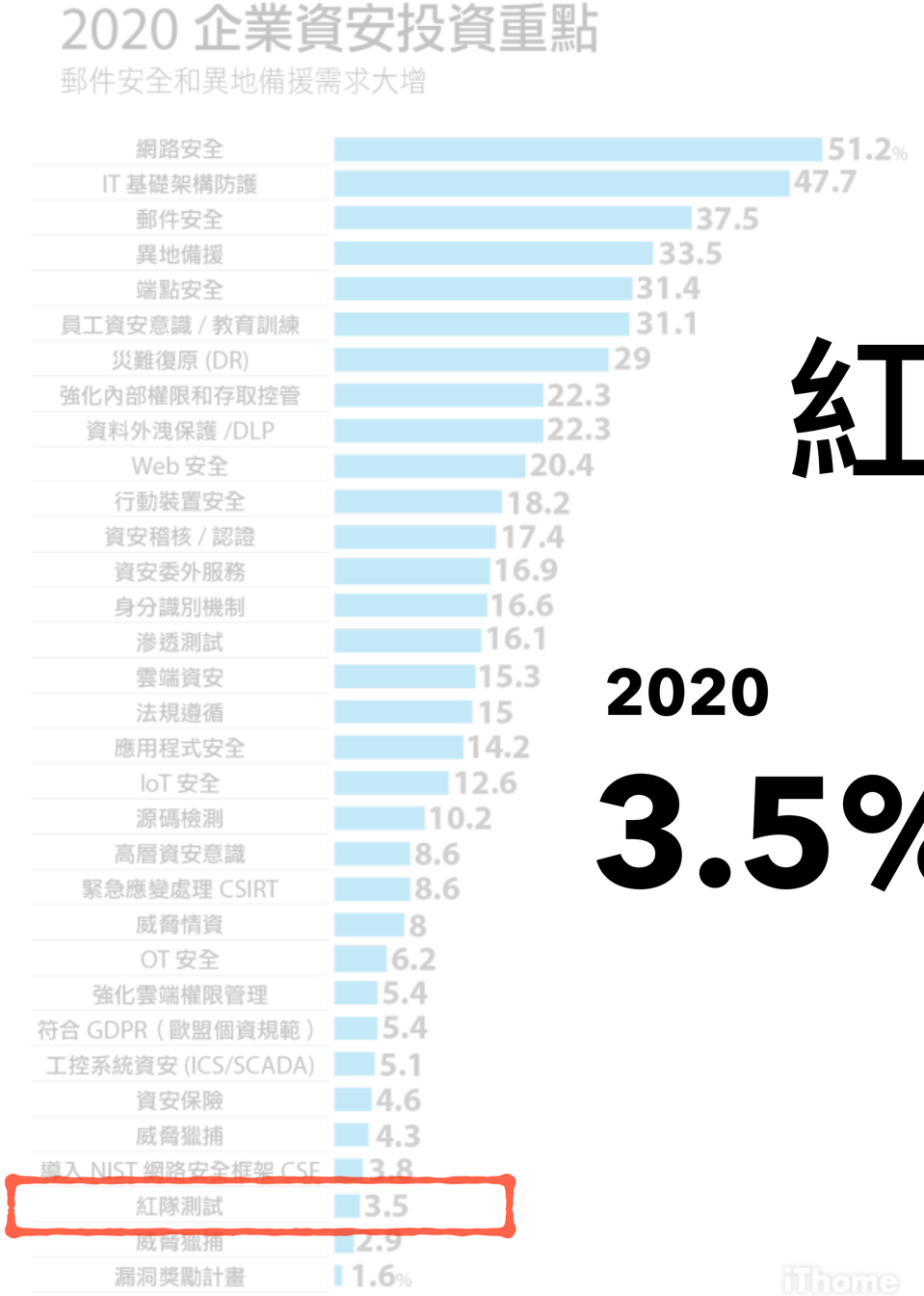
郵件安全和異地備援需求大增



今年企業資安投資重點

對於網路安全與 IT 基礎架構投資，今年比例明顯更高，而異地備援與災難復原需求大增，目標提升資安復原速度並增加資安韌性



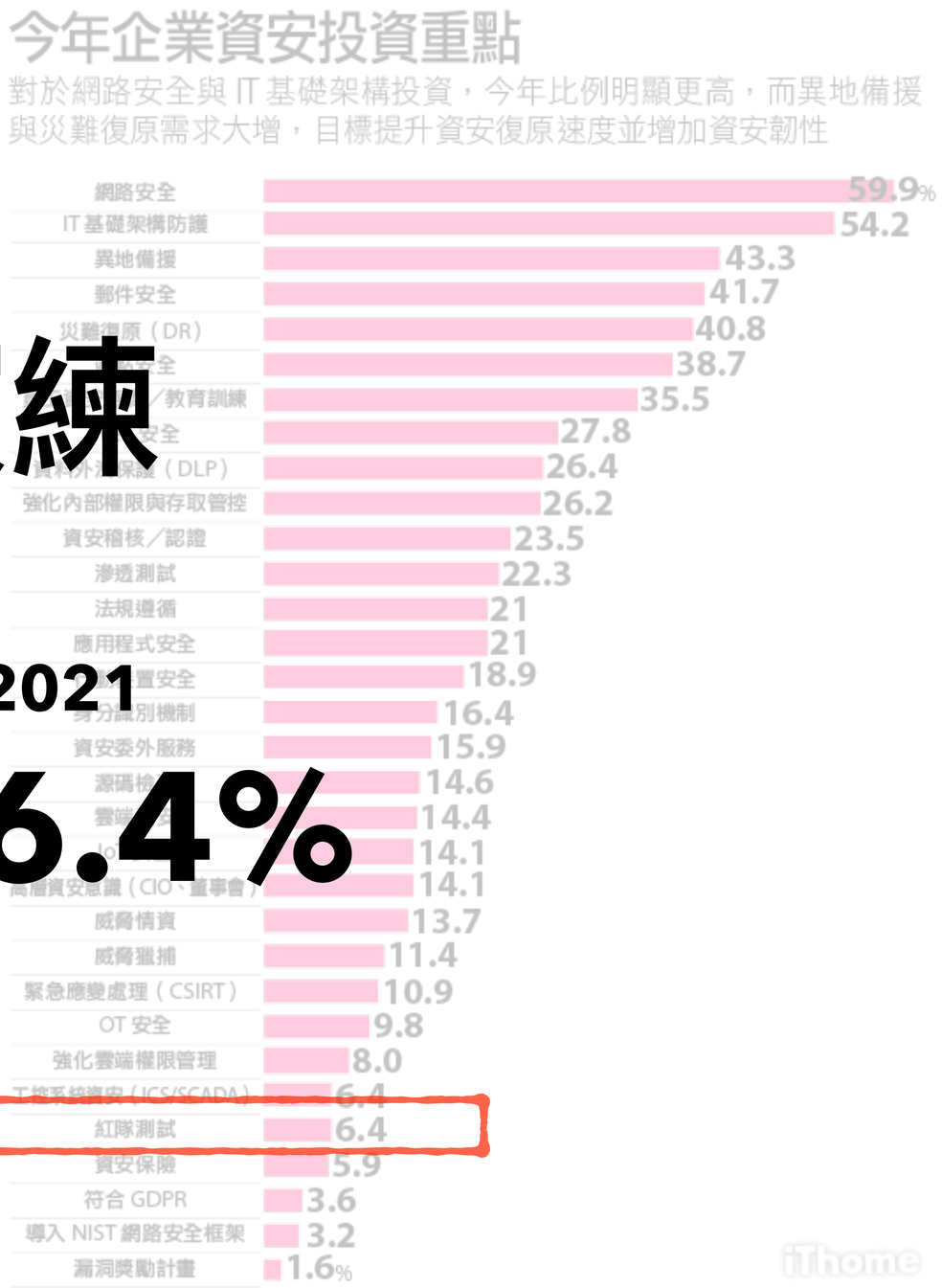


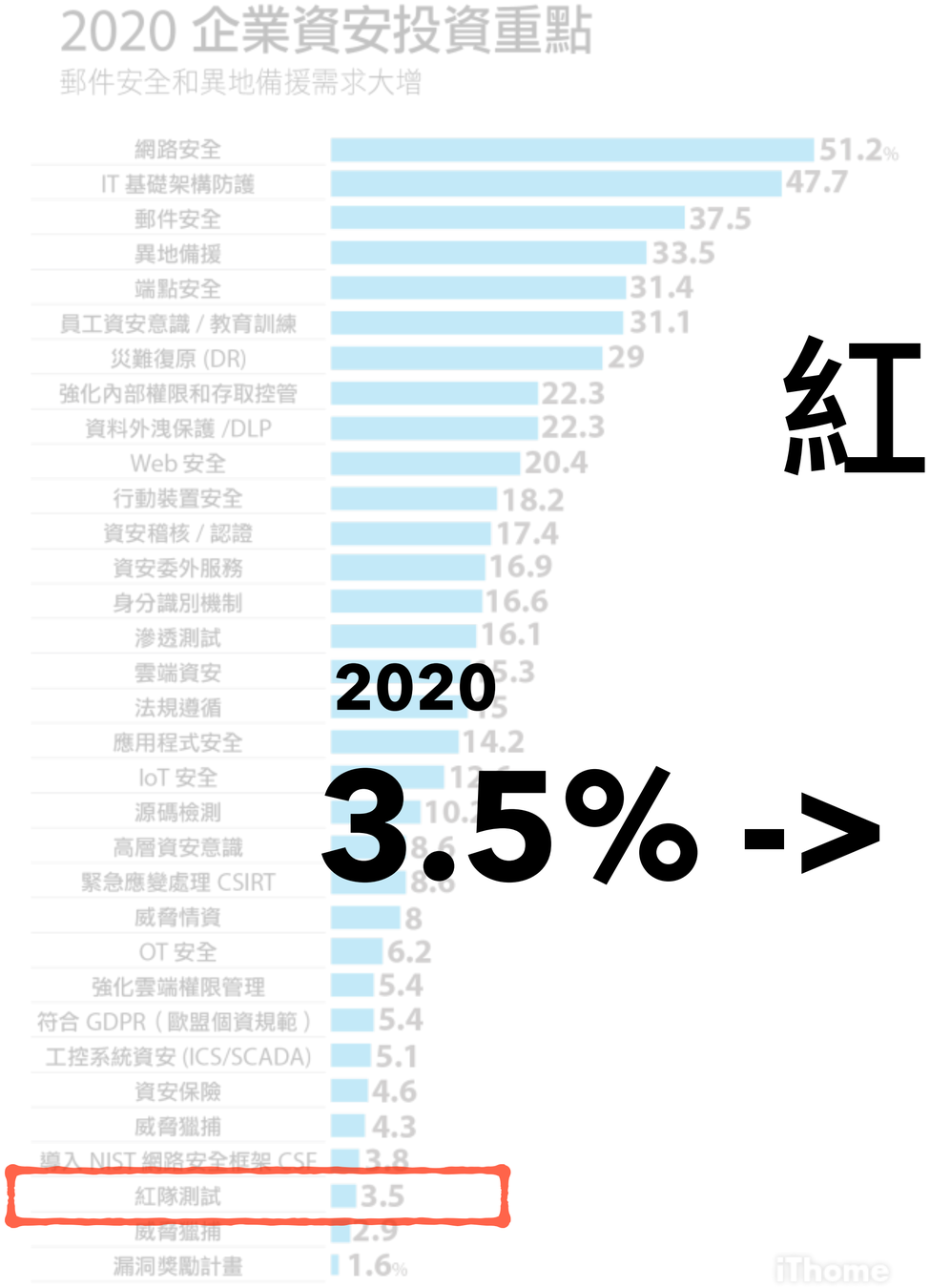
紅隊演練

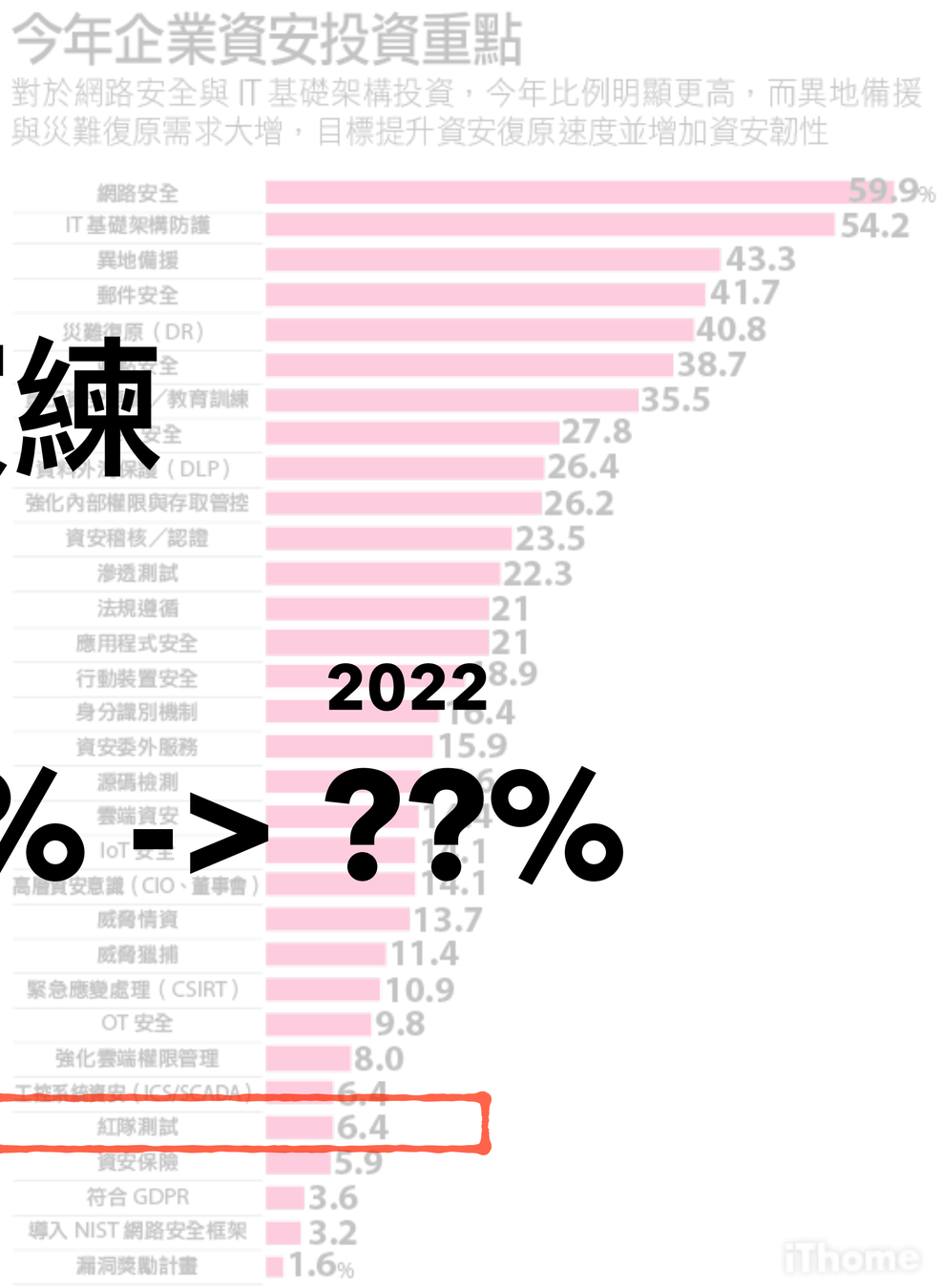
2020

3.5% -> 6.4%

2021







紅隊演練

2020 2021 2022

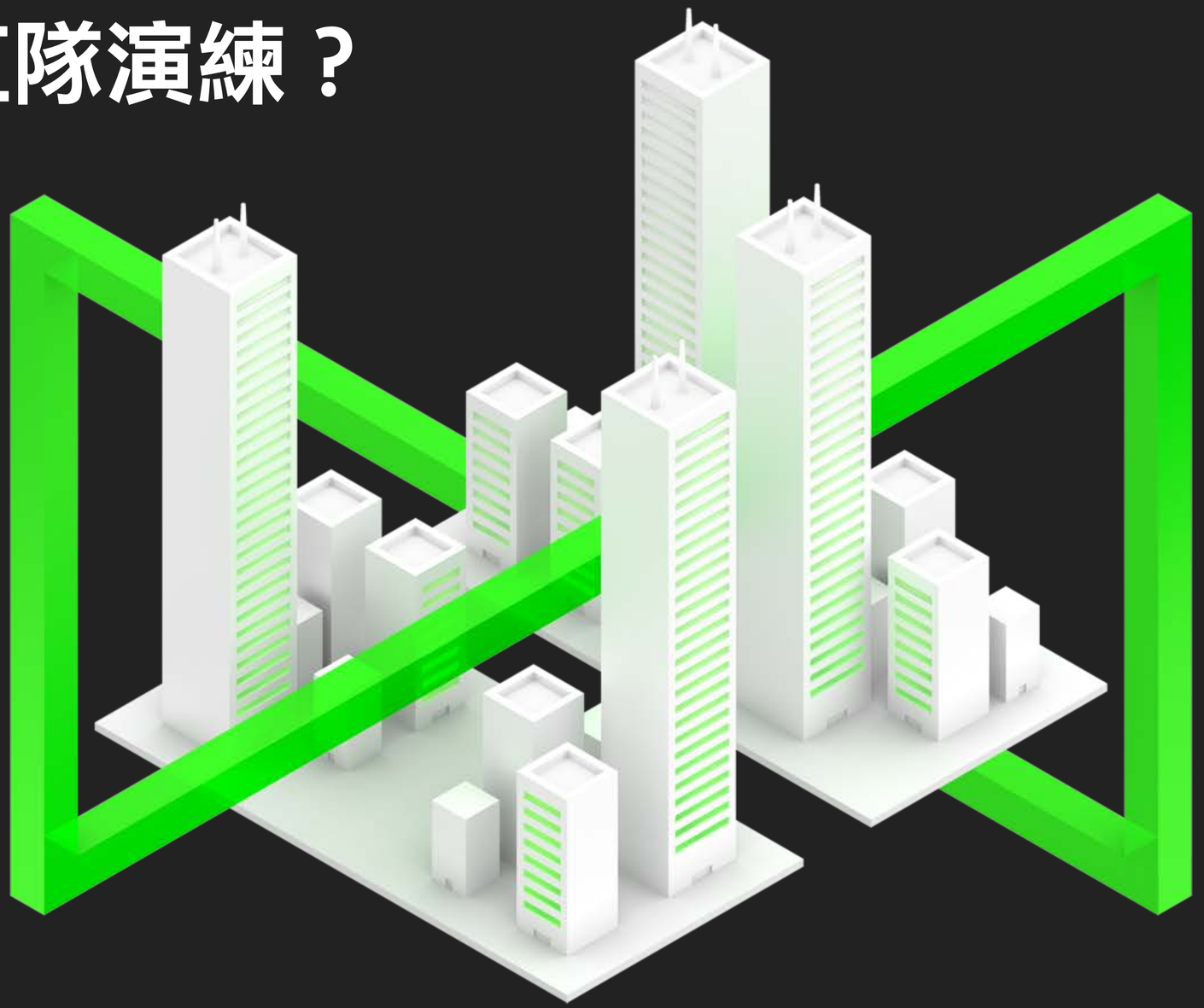
3.5% -> 6.4% -> ??%

想一想，
你真的需要紅隊演練嗎？為什麼？

如何正確使用紅隊演練

- 什麼是紅隊演練
- 紅隊演練的起源是什麼
- 紅隊的正確與錯誤觀念
- 紅隊解決了什麼問題

什麼是紅隊演練？



DEVCORE SECURITY CONSULTING

DEVCORE 的 10 年

2012.11 創立
提供 Penetration Testing
滲透測試及資安顧問服務

2014.08
PT 逐漸無法解決企業問題
協助企業做更廣更真實的檢測

2016
累積大量企業滲透攻擊經驗
分析並研究企業整體安全議題

2017.11
在台灣推出 Red Team Assessment
並將其正式命名為「紅隊演練」

2018.09
台北市政府紅隊演練發現衛生局
系統市民個資於地下網站兜售

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

2019.08
以 SSL VPN 獲得 Black Hat USA 頒發
Pwnie Awards Best Server-Side Bug 大獎

2019.09
舉辦 DEVCORE CONF 2019
純攻擊導向的專業技術研討會

2021.03
研究並回報
Microsoft Exchange Server 漏洞

2021.04
奪得白帽駭客最高殊榮
Pwn2Own 冠軍

2022
現在

DEVCORE SECURITY CONSULTING

DEVCORE 的 10 年

2012.11 創立
提供 Penetration Testing
滲透測試及資安顧問服務

2014.08
PT 逐漸無法解決企業問題
協助企業做更廣更真實的檢測

2016
累積大量企業滲透攻擊經驗
分析並研究企業整體安全議題

2017.11
在台灣推出 Red Team Assessment
並將其正式命名為「紅隊演練」

2018.09
台北市政府紅隊演練發現衛生局
系統市民個資於地下網站兜售

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

2019.08
以 SSL VPN 獲得 Black Hat USA 頒發
Pwnie Awards Best Server-Side Bug 大獎

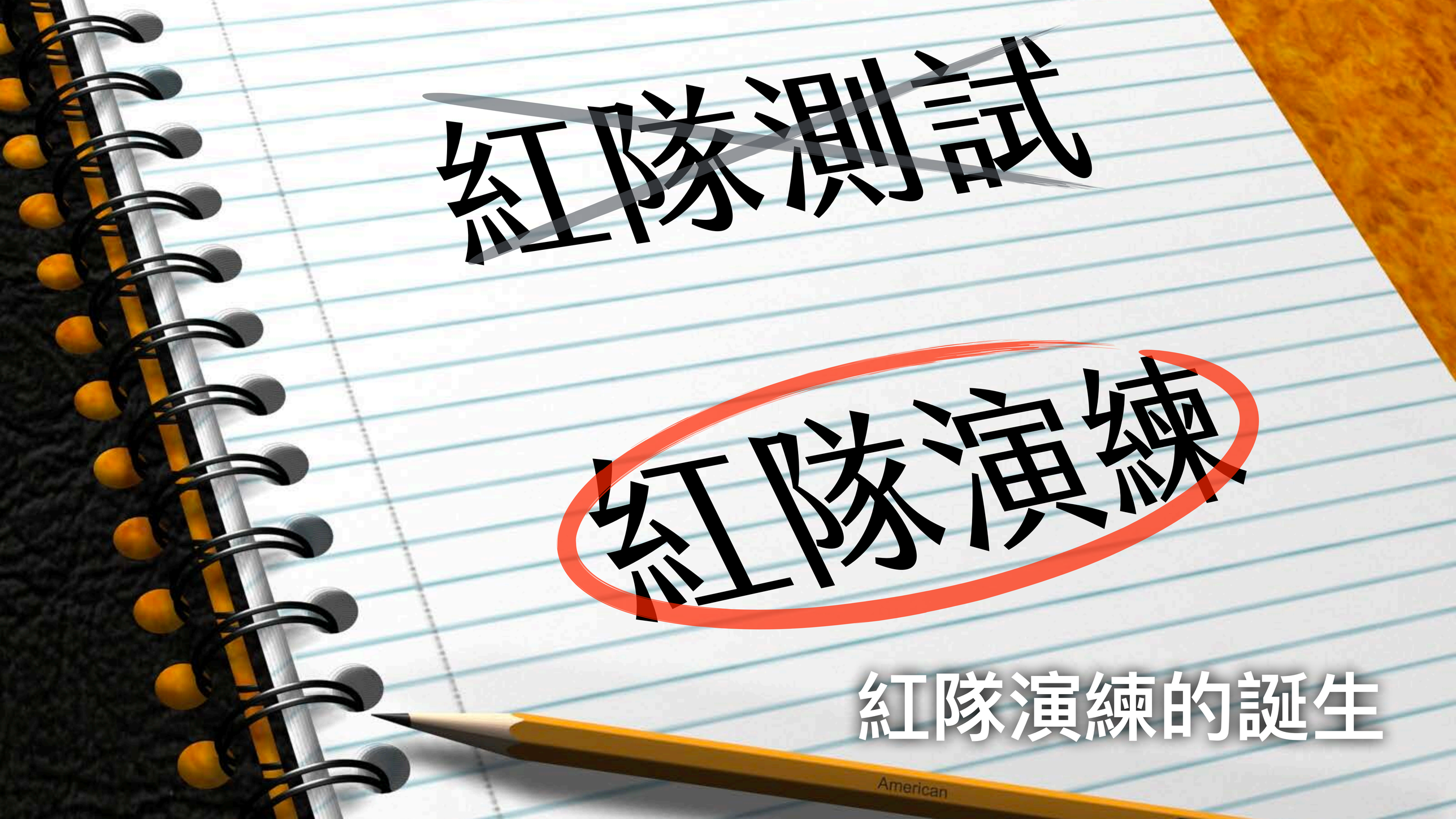
2019.09
舉辦 DEVCORE CONF 2019
純攻擊導向的專業技術研討會

2021.03
研究並回報
Microsoft Exchange Server 漏洞

2021.04
奪得白帽駭客最高殊榮
Pwn2Own 冠軍

2022
現在

DEVCORE SECURITY CONSULTING


紅隊測試
紅隊演練
紅隊演練的誕生
American

回到剛剛的問題：

你真的需要紅隊演練嗎？為什麼？

TAIWAN CYBER SECURITY LANDSCAPE VERSION BETA41 2022 JUL

iThome

Endpoint Prevention

Endpoint Detection & Response

Network Firewall

DDoS Protection

Network Analysis & Forensics

Advanced Threat Protection

Web Security

Risk Assessment & Visibility

WAF & Application Security

Application Security Testing

iThome 臺灣資安市場地圖

TAIWAN CYBER SECURITY LANDSCAPE
VERSION BETA41

Managed Security Service

Security Awareness & Training

Encryption

Data Leak Prevention

Mobile Security

Penetration Testing

Container Security

Cloud Security

GCB

Security Incident Response

NAC

Firewall Management

Secure File Sharing

Authentication

Privileged Access Management

Identity Governance

SOAR

Messaging Security

Security Information and Event Management

Security Analytics

Threat Intelligence

DNS Security

OT Security

《臺灣資安市場地圖》BETA41版，囊括目前熱門的33種資安產品與服務，以及314家廠商，日後將持續更新資訊，以呈現臺灣資安市場完整面貌，歡迎與我們交流討論。

《臺灣資安市場地圖》BETA41版，囊括目前熱門的33種資安產品與服務，以及314家廠商，日後將持續更新資訊，以呈現臺灣資安市場完整面貌，歡迎與我們交流討論。

正確的心態是什麼

There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese.

- James Comey (美國聯邦調查局局長)

BUSINESS INSIDER

Subscribe

DOW +0.36% | S&P 500 +0.45% | NASDAQ 100 +0.52%

FBI Director: China Has Hacked Every Big US Company

James Cook Oct 6, 2014, 6:24 PM

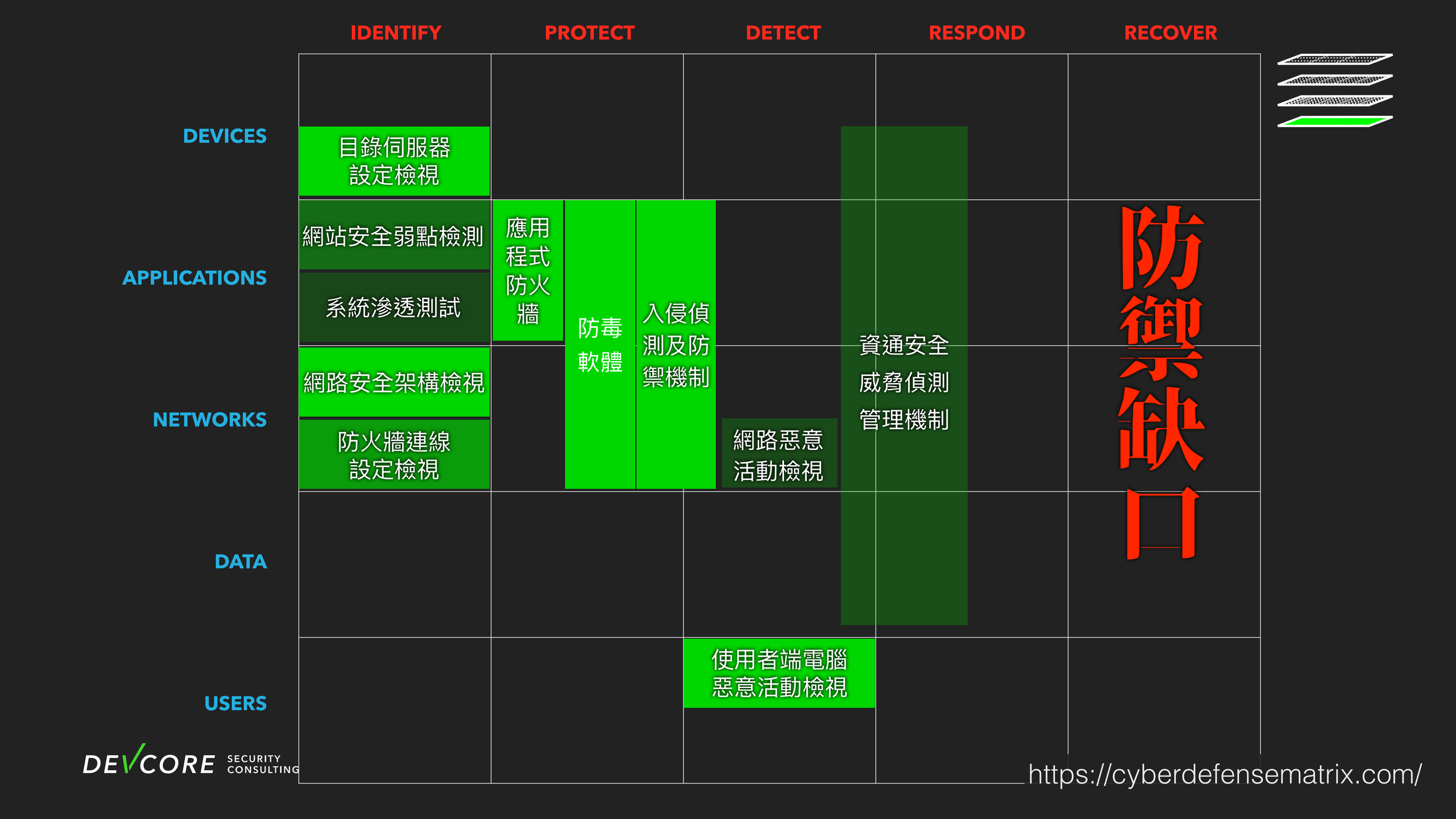
In his first major television interview, the director of the FBI has warned that Chinese hackers have embarked on a widespread campaign of cyberwarfare against the US.

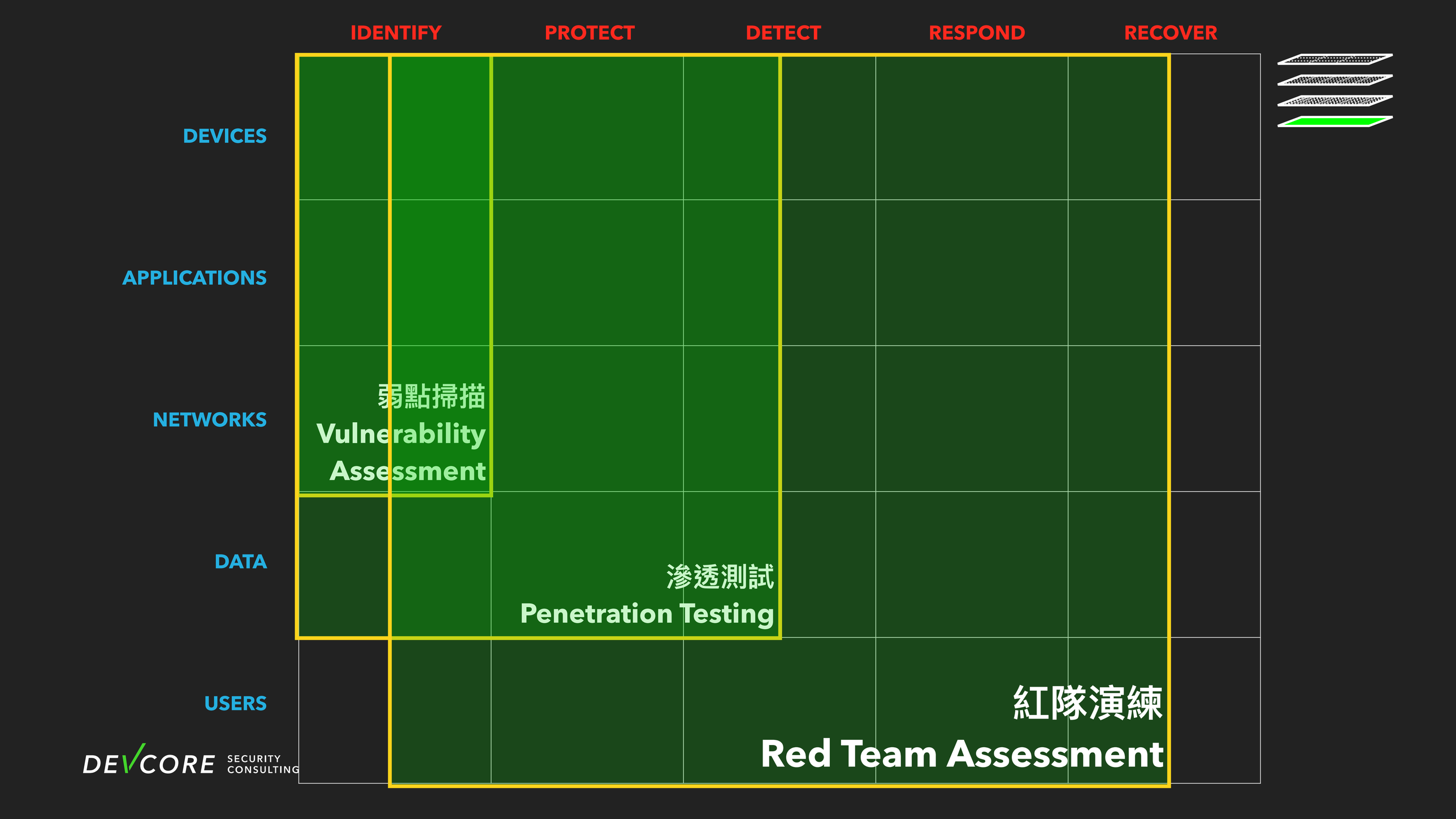
FBI Director James Comey. Reuters

Speaking to CBS' "60 Minutes," James Comey had the following to say on Chinese hackers:

> There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.

https://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10


IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
DEVICES
APPLICATIONS
NETWORKS
DATA
USERS
目錄伺服器
設定檢視
網站安全弱點檢測
系統滲透測試
網路安全架構檢視
防火牆連線
設定檢視
應用
程式
防火
牆
防毒
軟體
入侵偵
測及防
禦機制
網路惡意
活動檢視
資通安全
威脅偵測
管理機制
使用者端電腦
惡意活動檢視
防禦缺口
DEVCORE SECURITY CONSULTING
https://cyberdefensematrix.com/


IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
DEVICES
APPLICATIONS
NETWORKS
DATA
USERS
弱點掃描
Vulnerability Assessment
滲透測試
Penetration Testing
紅隊演練
Red Team Assessment
DEVCORE SECURITY CONSULTING

安全檢測方法

依企業安全的成熟度給予不同權重，選擇合適的檢測方法

- 真實性
- 範圍
- 時間
- 成本

DEVCORE SECURITY CONSULTING

錯誤的使用會有錯誤的成效

錯誤的使用會有錯誤的成效

病患：「醫生，我付了錢，
你保證我不會生病對吧？」


醫生


目標就在這，我們衝！

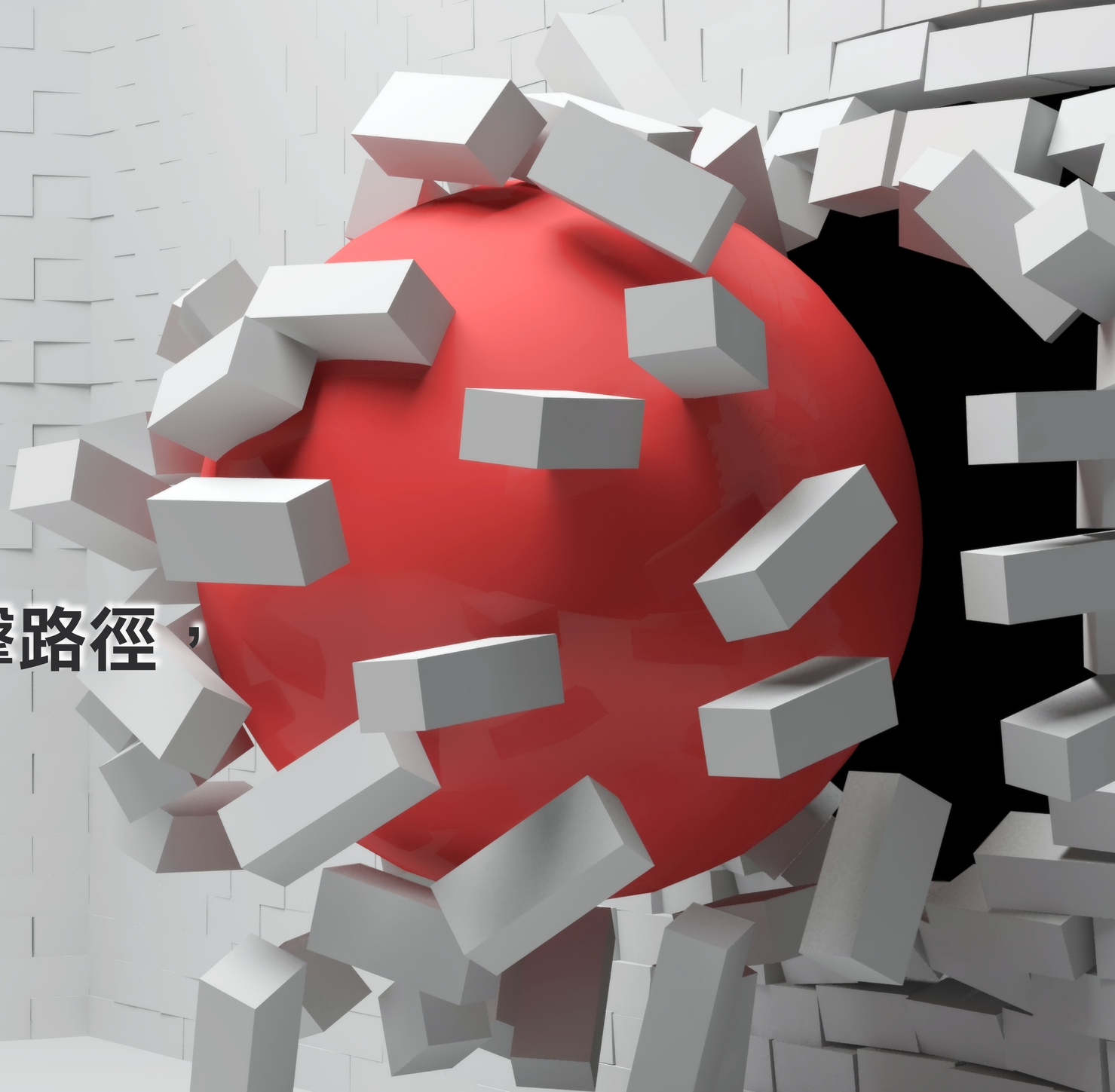
什麼都沒有是要演練什麼...

>~<

信任紅隊，並接受結果！

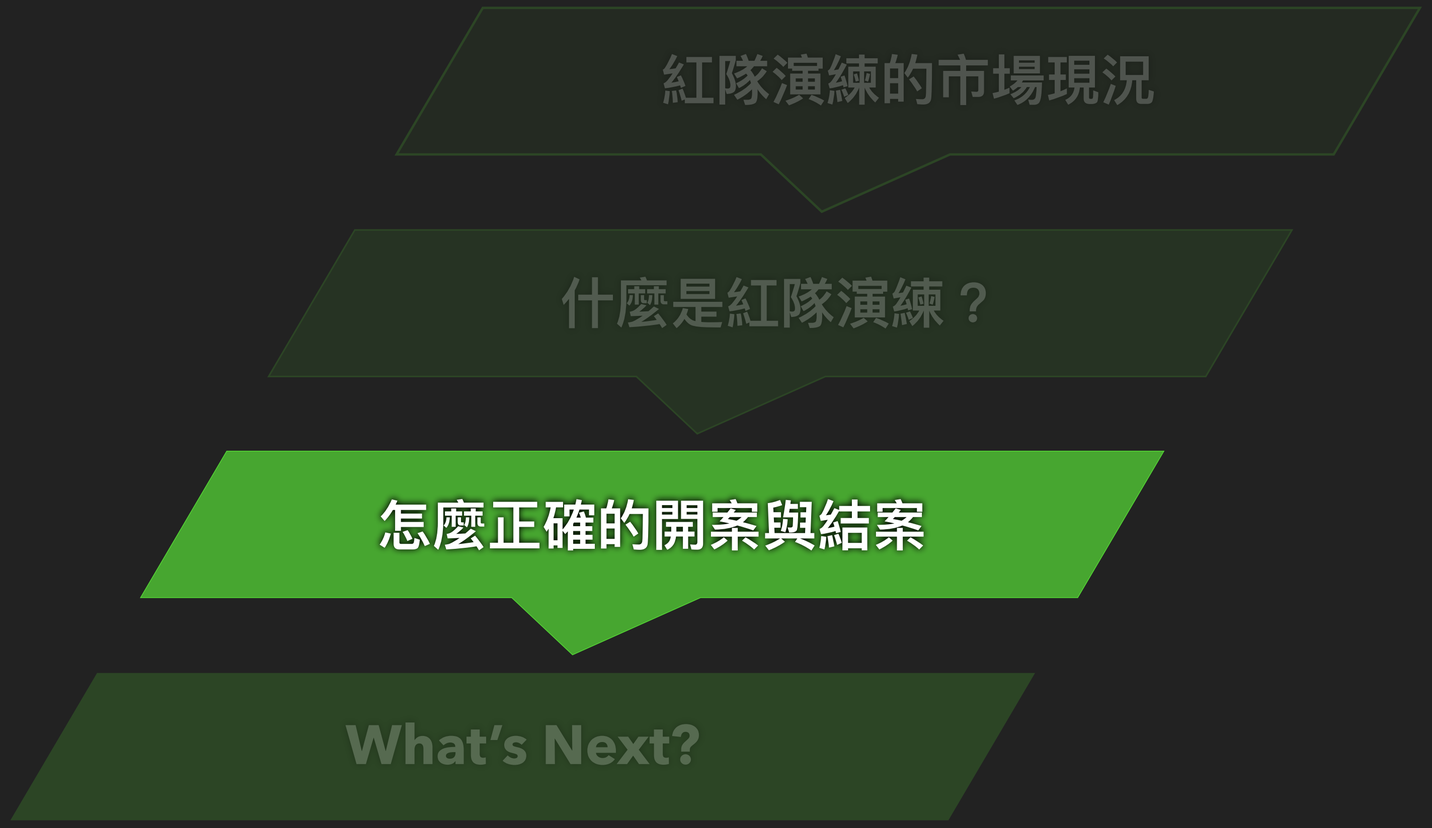
紅隊的任務：

與企業站在同一側，
以攻擊者的觀點盤點攻擊路徑，
協助企業減緩威脅。



如何正確使用紅隊演練

- 紅隊演練的不同階段
- 開案前有什麼準備事項
- 如何選商
- 怎麼正確的開案與結案
- 執行專案中該怎麼合作



紅隊與企業並不是對立方
而是協助盤點企業的不足

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

1 Stage 1
初次合作

- 時間：揭露演練日期、時間
- 網路：固定 IP 位址
- 範圍：以企業最常使用的網域、IP 位址、雲端服務為主
- 溝通：若藍隊有任何疑問，可由紅隊提出說明
- 情境：以外網入侵為主
- 藍隊：監控但不阻擋

2 Stage 2
資安成熟度成長中

- 時間：揭露演練時間、拉長日期
- 網路：可用動態 IP 位址
- 範圍：除常見範圍，也考慮納入設備、供應鏈、子公司、跨國辦公室
- 溝通：若藍隊提出疑問紅隊視情況說明
- 情境：先以外網為主，後變換其他情境
- 藍隊：發現攻擊行為可阻擋，多次阻擋成功後，再採取監控但不阻擋的放行機制

3 Stage 3
資安成熟度高

- 時間：不限演練日期與時間
- 網路：全程使用動態 IP 位址以及雲端服務作為跳板
- 範圍：所有數位資產納入範圍
- 溝通：紅隊僅通知重大資安漏洞，其餘資訊不提供
- 情境：視情境可從內網開始演練，並納入實體入侵、社交工程等方式
- 藍隊：發現攻擊行為可立即阻擋，不必放行

DEVCORE

1 **Stage 1**
初次合作

2 **Stage 2**
資安成熟度成長中

3 **Stage 3**
資安成熟度高

- 時間：揭露演練日期、時間
- 網路：固定 IP 位址
- 範圍：以企業最常使用的網域、IP 位址、雲端服務為主
- 溝通：若藍隊有任何疑問，可由紅隊提出說明
- 情境：以外網入侵為主
- 藍隊：監控但不阻擋

DEVCORE

1 Stage 1
初次合作

2 Stage 2
資安成熟度成長中

3 Stage 3
資安成熟度高

- 時間：揭露演練時間、拉長日期
- 網路：可用動態 IP 位址
- 範圍：除常見範圍，也考慮納入設備、供應鏈、子公司、跨國辦公室
- 溝通：若藍隊提出疑問紅隊視情況說明
- 情境：先以外網為主，後變換其他情境
- 藍隊：發現攻擊行為可阻擋，多次阻擋成功後，再採取監控但不阻擋的放行機制

DEVCORE

1 Stage 1
初次合作

2 Stage 2
資安成熟度成長中

3 Stage 3
資安成熟度高

- 時間：不限演練日期與時間
- 網路：全程使用動態 IP 位址以及雲端服務作為跳板
- 範圍：所有數位資產納入範圍
- 溝通：紅隊僅通知重大資安漏洞，其餘資訊不提供
- 情境：視情境可從內網開始演練，並納入實體入侵、社交工程等方式
- 藍隊：發現攻擊行為可立即阻擋，不必放行

DEVCORE

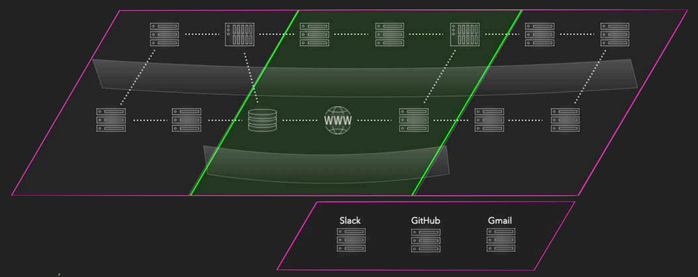
如何選商

- 紅隊是團隊作戰，且具備駭客思維
- 具備多次大型紅隊演練經驗
- 專注提供安全服務，且為公司主要產品
- 發表研究文章或於國際研討會發表

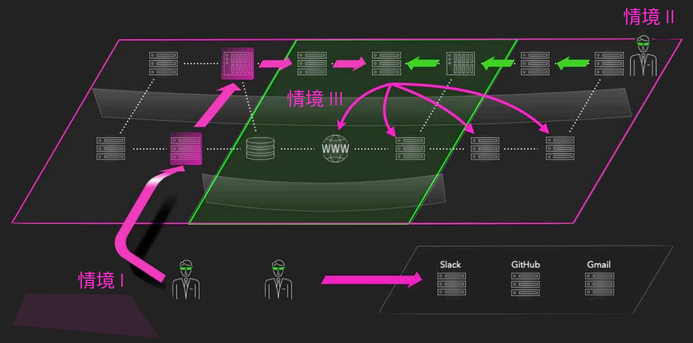
Penetration Testing Provider Selection
https://partner-security.withgoogle.com/docs/annex/provider_selection.html

紅隊演練開案前準備

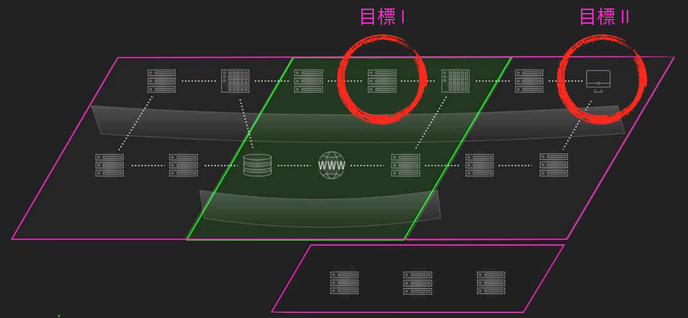
步驟 1 確認演練範圍



步驟 2 確認演練情境

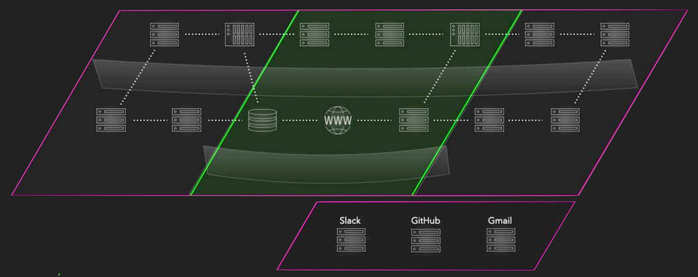


步驟 3 確認演練目標



紅隊演練開案前準備

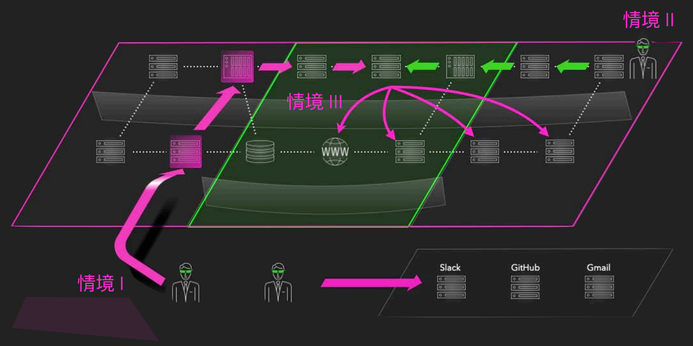
步驟 1 確認演練範圍



- 公司授權演練範圍，如網域、主機、子公司
- 盤點高機敏資料主機
- 須避開的範圍、時段或手法

紅隊演練開案前準備

步驟 2 確認演練情境

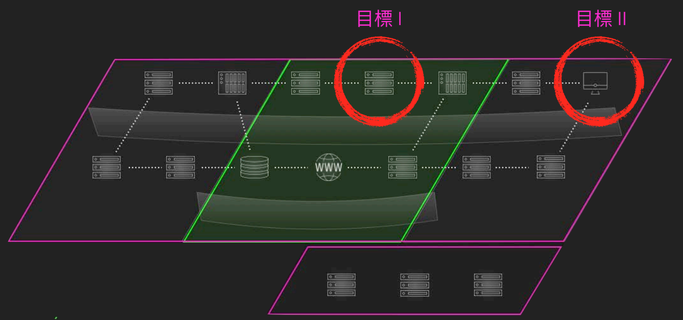


- 從外部網路出發（外部系統）
- 從內部網路出發（內部資安事件）
- 演練之前遇到資安事件的情境類型
- 特定攻擊手法，如 WIFI 入侵、實體入侵

紅隊演練開案前準備

- 盤點公司最在意的主機、資料是什麼
- 與核心目標有相依性的主機是哪些
- 曾經發生過事件的高危險主機
- 盤點重要基礎設施、核心系統、機敏資料、特權帳號權限

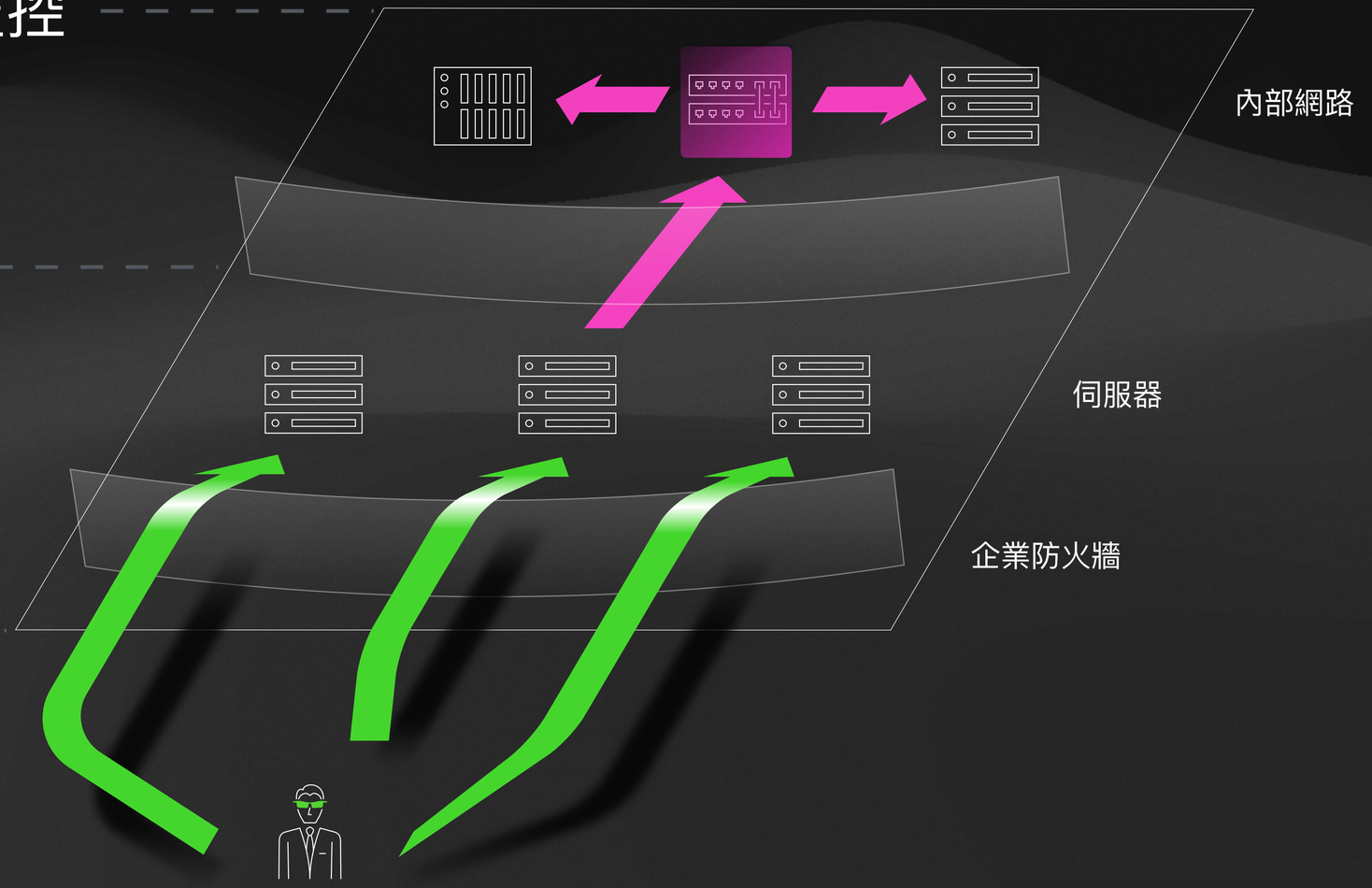
步驟 3 確認演練目標



專案中怎麼合作

企業整體資安強度

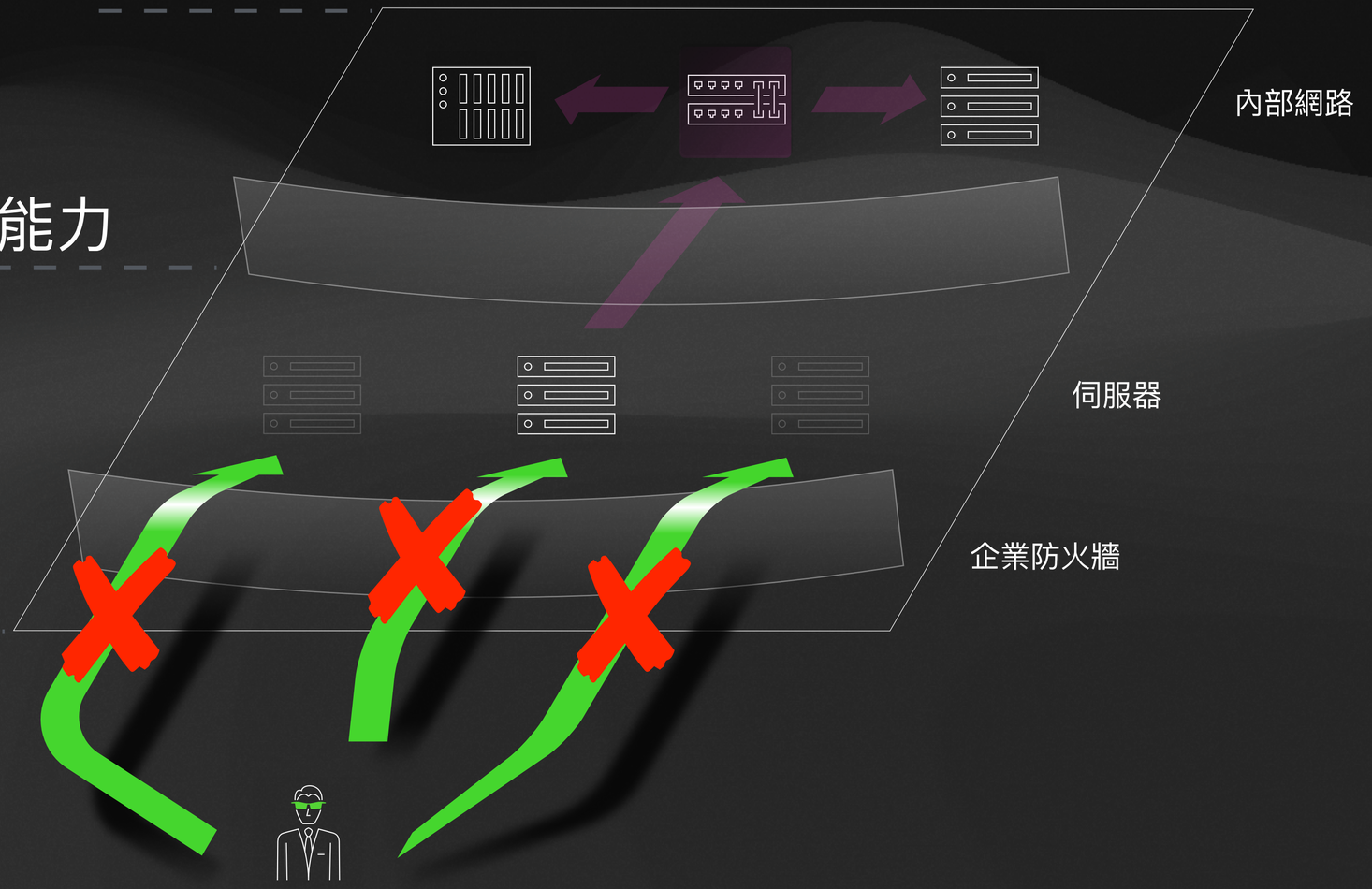
- 核心系統（目標）監控
- 防禦系統告警
- 資安團隊應變處理
- 伺服器行為監控
- 網路監控
- 網路邊界盤點



DEVCORE SECURITY CONSULTING

專案中怎麼合作

- 透過演練結果檢討如何修正強化
- 測試資安服務團隊（藍隊）防禦能力
- 驗證資安防禦措施及流程有效性
- 重新最佳化防禦策略
- 調整未來資安資源的投放位置



DEVCORE SECURITY CONSULTING


戰後 - 怎麼結案驗收

戰後 - 怎麼結案驗收

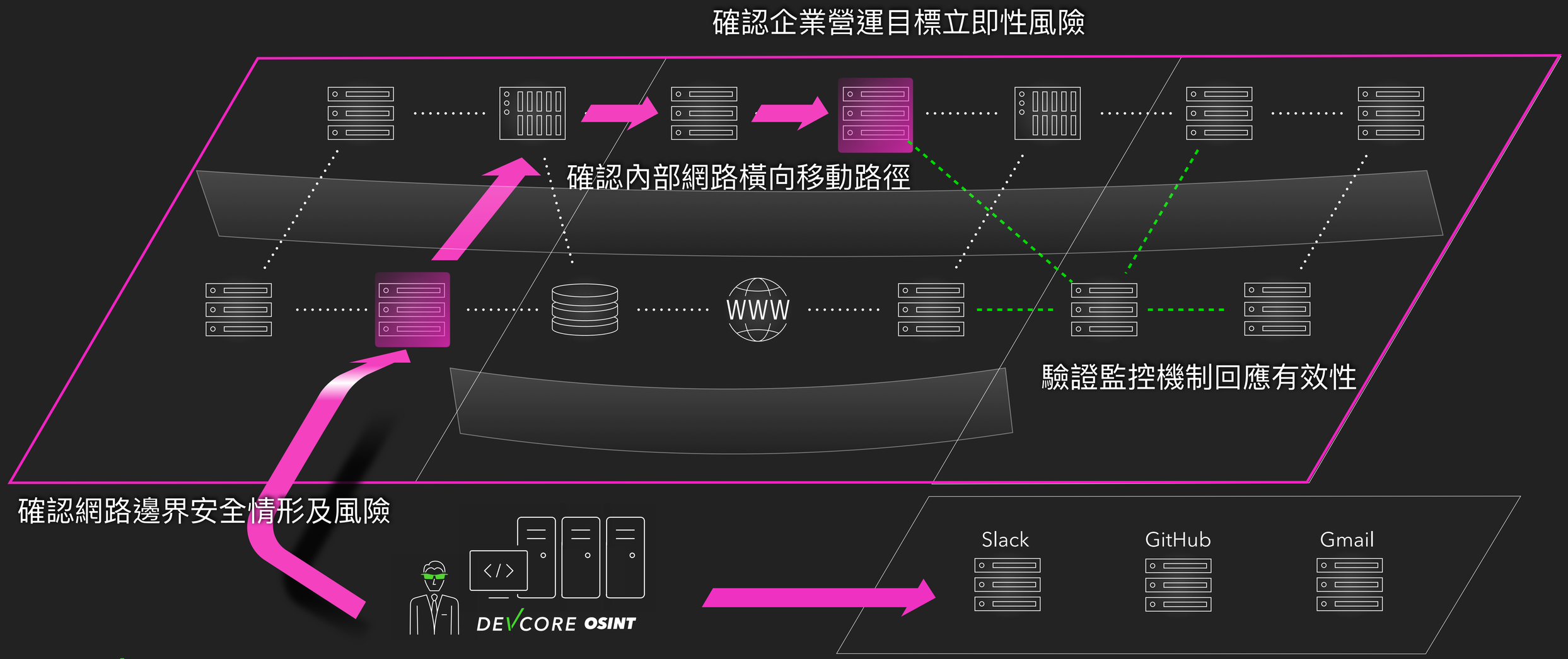
資安廠商：

- 攻擊的方法論、策略，攻擊觀點的安全建議
- 詳細的攻擊路徑、漏洞說明
- 簡報交流雙方攻防的想法

企業內部：

- 回顧演練流程
- 重新調整資安策略
- 擬定長期演練計畫

紅隊演練效益

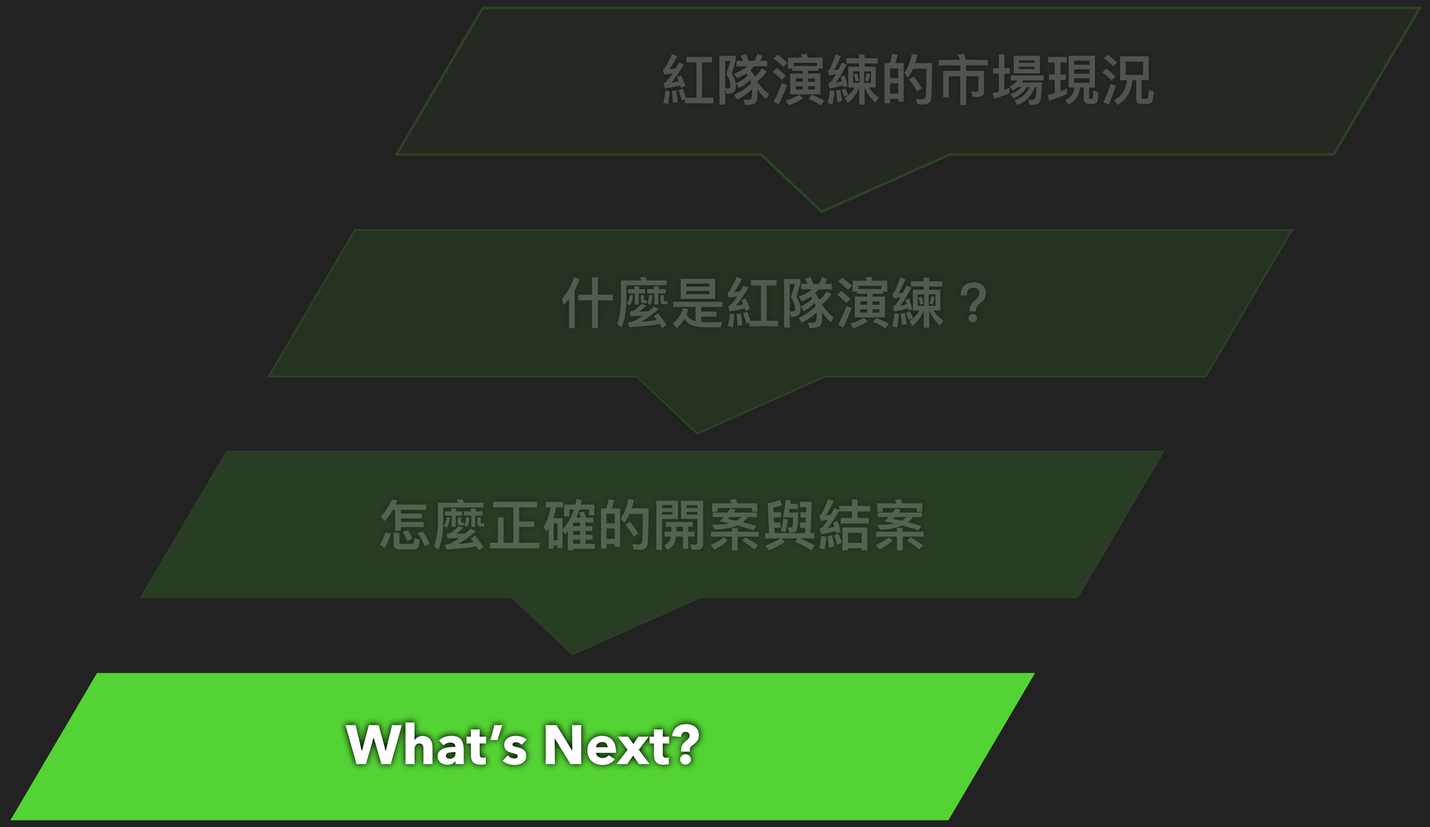


DEVCORE SECURITY CONSULTING

廠商說打不出來怎麼辦？
如何要求及監督紅隊廠商？

如何正確使用紅隊演練

- 下一步我們該怎麼做？



我接下來該怎麼辦 (Takeaways)

- 從需求出發，思考**為什麼**我需要這個服務，我想要**解決什麼問題**
- **紅隊就是盟友**，藉由演練盤點人員、設備、流程的問題
- 做好開案、成案、結案的**準備**，將資源發揮最大效益

別讓紅隊演練只是一個勾勾

DEVCORE

DEVCORE
SECURITY
CONSULTING

別讓紅隊演練只是一個勾勾！

Q&A

戴夫寇爾股份有限公司

contact@devco.re