DEVCORE
SECURITY
CONSULTING

攻擊一日，創業十年

翁浩正 (Allen Own)

戴夫寇爾股份有限公司

allenown@devco.re

2023.03.10
DEVCORE Conference

攻擊一日，創業十年

DEVCORE SECURITY CONSULTING

人類使用棍棒來作為武器
打擊敵人，保衛自己

人類利用金屬創造刀劍
透過斬擊，攻擊力更強

人類透過科技創造了戰鬥機，延伸作戰的空間


從現在到未來，人類的作戰已經跳脫了疆域

人類歷史上，科技一直在變

但只有攻擊與防禦不會變

DEVCORE SECURITY CONSULTING

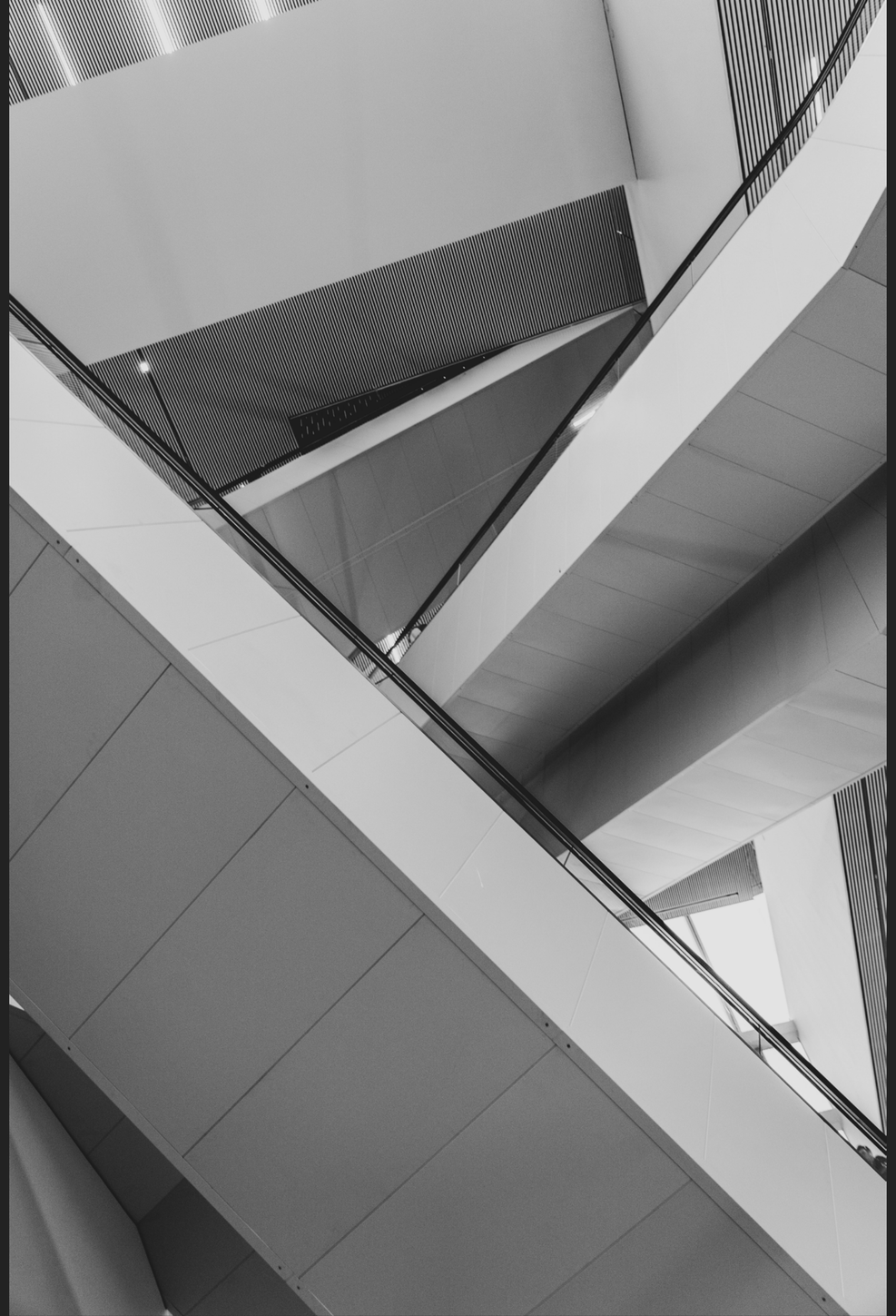
DEVCORE 在做什麼？

我們一直在做的是……

攻擊方

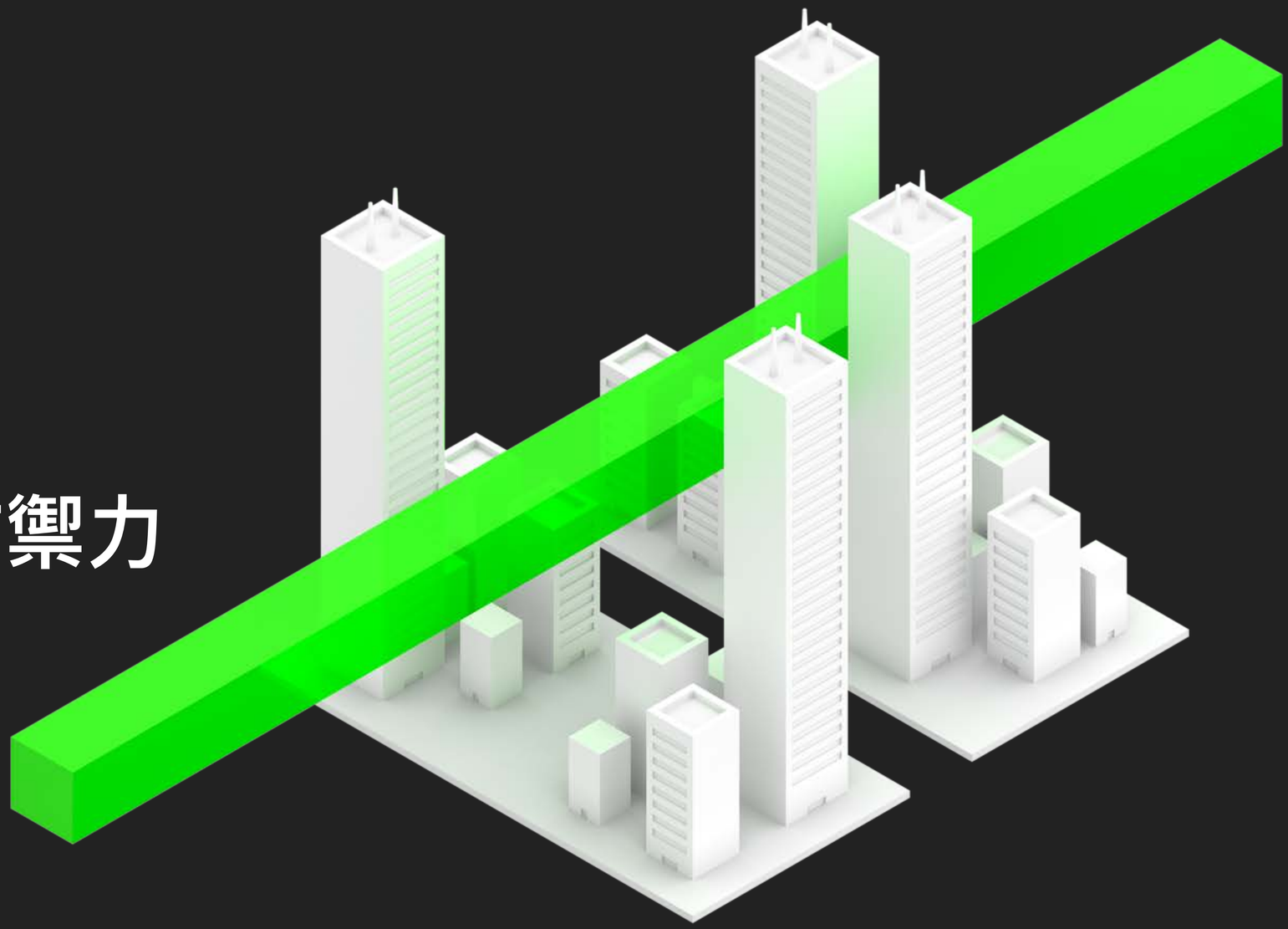

SECURITY MISCONFIGURATION
LOGON
HACKER MINDSET
PENETRATION
MAN IN THE MIDDLE

攻擊方與防禦方的思維落差極大



DEVCORE SECURITY CONSULTING

只有透過真實攻擊，
才能驗證企業真正的防禦力



DEVCORE SECURITY CONSULTING


資安的環境與困境

資安漏洞出在「人」身上

2005-10-12發表（18 年前）

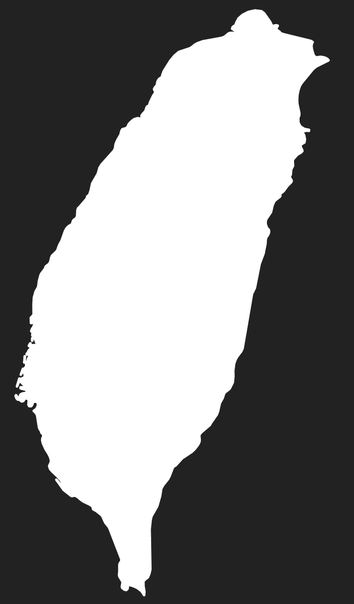
Steve Riley強調，並沒有什麼措施是萬無一失的，也不是安裝很多產品就能達到安全目的，因為問題或漏洞往往都在人的身上，以現在大肆風行的社會工程詐騙手法為例，技術本身並不高明，而是利用人性的弱點讓人上當，企業對內的安全教育訓練與分層管理都相當重要，很多工作必須從觀念宣導開始，再完善的設備防護也抵不上內部人員的疏失。

另外，企業資訊主管常苦於如何向經營者爭取資安預算，因為花的錢常常很難看到效益，往往得等到事件發生，老闆才會點頭，但Jesper M. Johansson認為，企業資訊主管必須有「不得不做」的覺悟，投資在資安上的效益的確很難評估，但是等到發生事情再做就來不及了，因為技術、系統、網路環境都持續改變當中，企業必須持續進行新的資安工作與建置。

Jesper M. Johansson還強調，預算高低與安全與否沒有絕對關係，產品並不能解決所有資安問題，儘管中小企業擁有的IT資源有限，只要預先評估企業本身能承擔的風險範圍，預算高低並不重要，掌握關鍵工作環節的安全更為重要，也就是所謂的投資價值、可承擔風險與防護措施間的平衡。文⊙高雅欣

DEVCORE 創立於 2012 年，
10 年前的台灣資安...

十年前



DEVCORE SECURITY CONSULTING

不重視資安　重視軟硬體大於服務

系統架構混亂　滿地都是Injection

最低價格標　APT事件

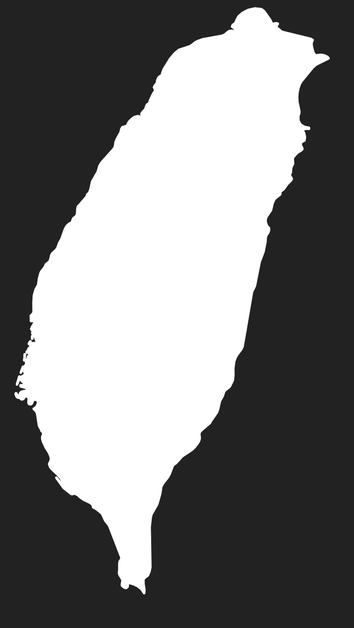
十年前

到處都是洞　只願求合規

買了產品不用　資安服務品質低落

沒有預算　出事問SI　資安產品複雜

十年後



資安意識提升

重視服務的價值

Security by Design

簡單漏洞減少

最有利標

十年後

資料外洩

漏洞複雜化

十年後其實變化很多

不單求合規

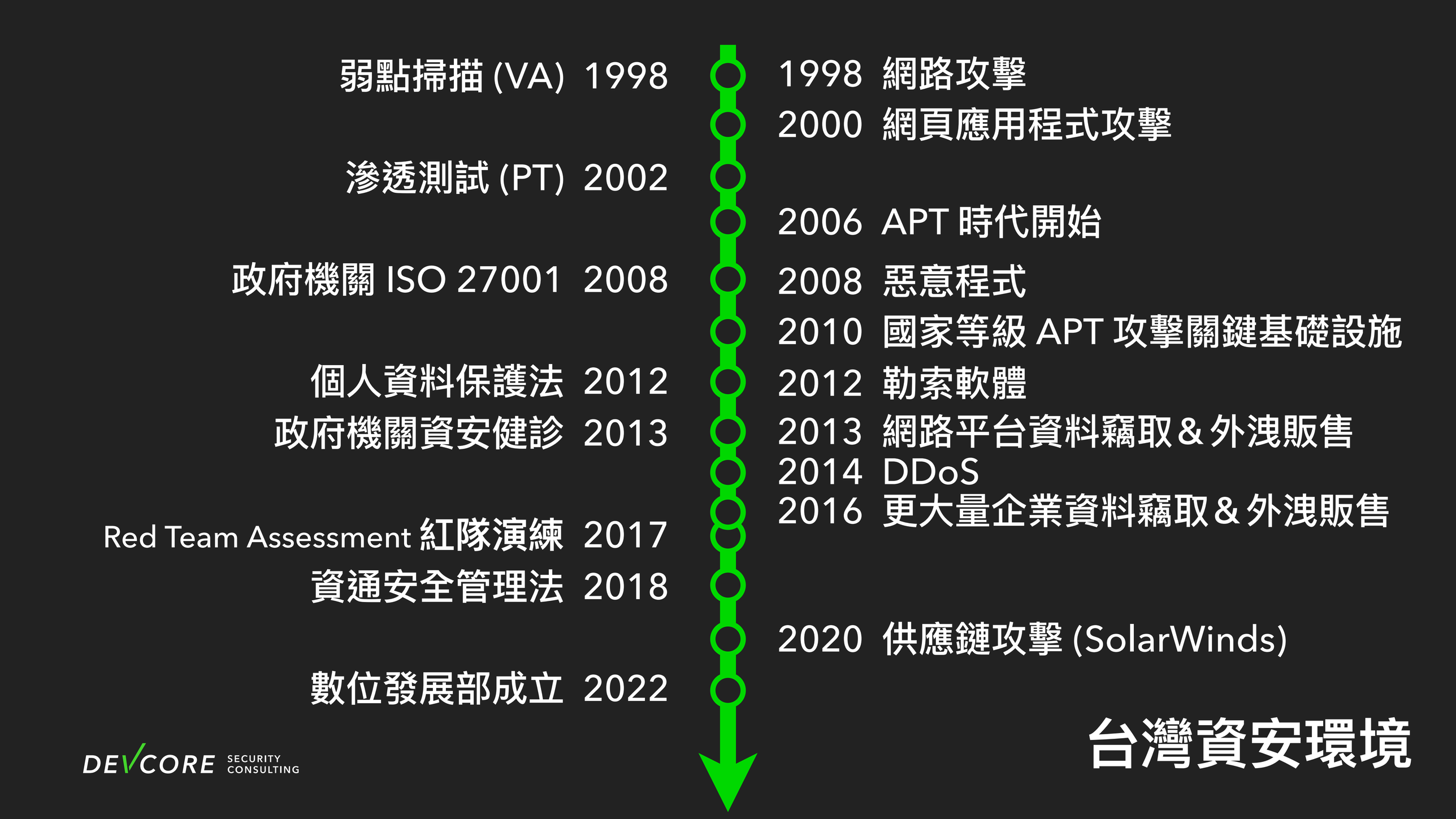
狂買產品及服務

服務品質提升

預算增加

攻擊型服務

產品有效性


弱點掃描 (VA) 1998
滲透測試 (PT) 2002
政府機關 ISO 27001 2008
個人資料保護法 2012
政府機關資安健診 2013
Red Team Assessment 紅隊演練 2017
資通安全管理法 2018
數位發展部成立 2022
1998 網路攻擊
2000 網頁應用程式攻擊
2006 APT 時代開始
2008 惡意程式
2010 國家等級 APT 攻擊關鍵基礎設施
2012 勒索軟體
2013 網路平台資料竊取＆外洩販售
2014 DDoS
2016 更大量企業資料竊取＆外洩販售
2020 供應鏈攻擊 (SolarWinds)
台灣資安環境
DEVCORE SECURITY CONSULTING

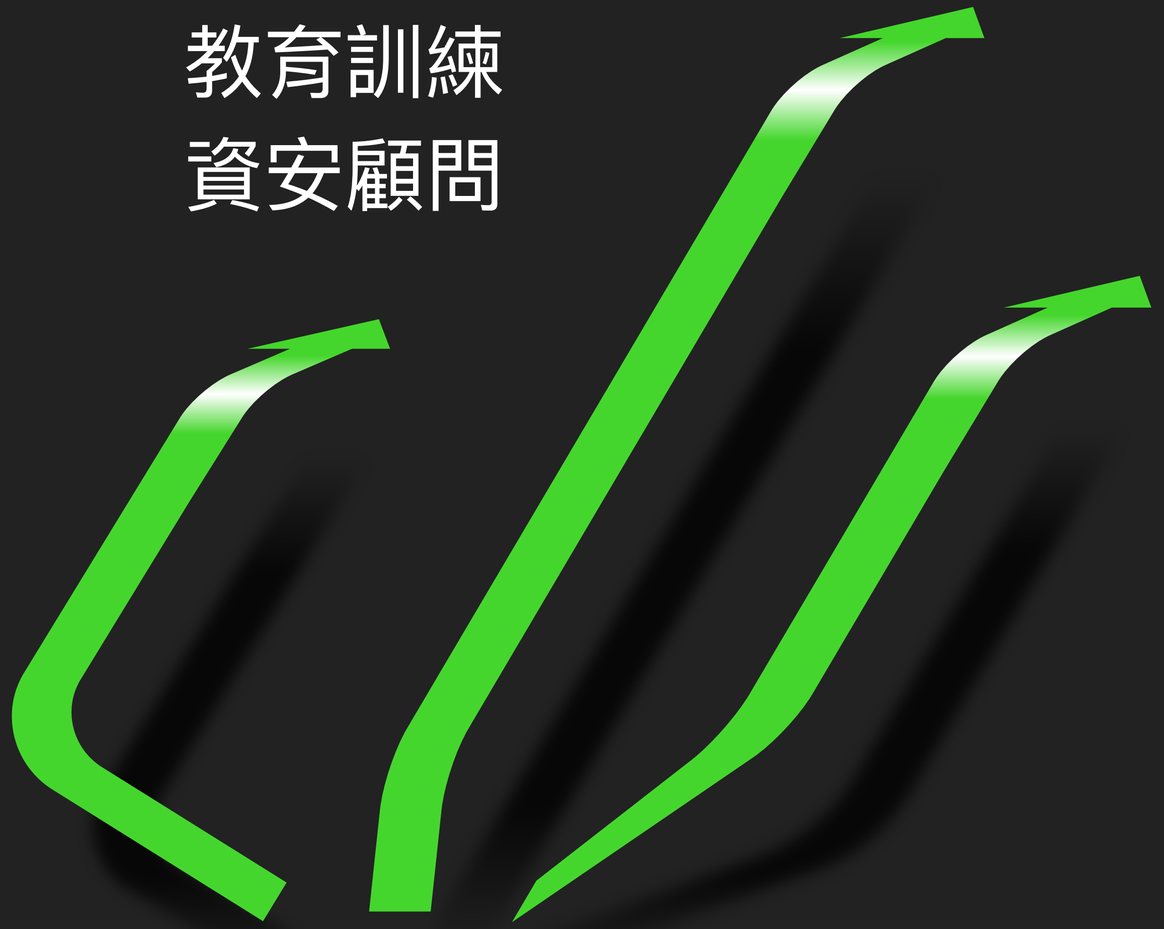
DEVCORE 的十年

駭客思維

教育訓練
資安顧問

前瞻研究

漏洞研究
研究發表



攻擊型服務

紅隊演練
滲透測試

DEVCORE

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

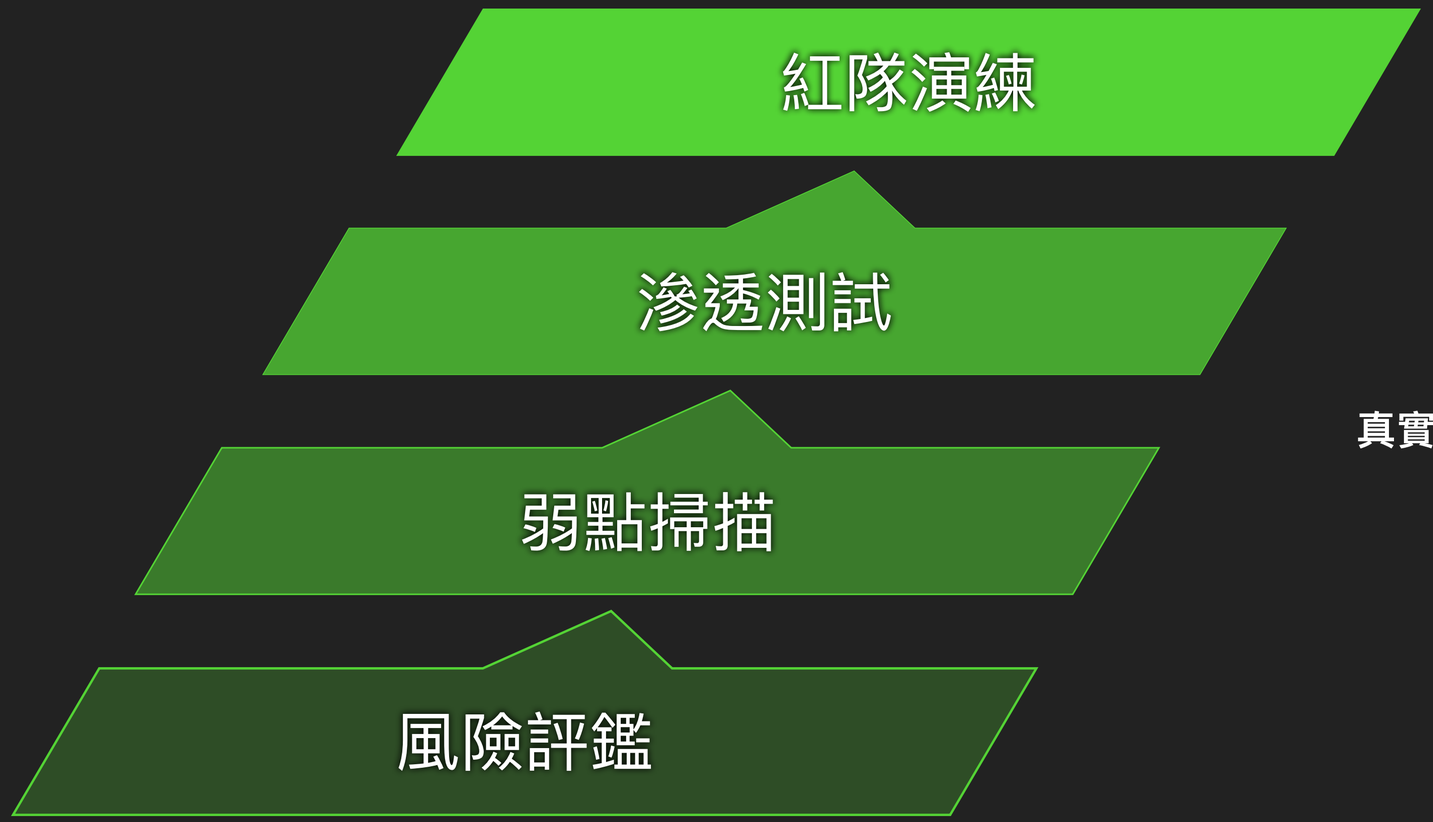
2022.01
DEVCORE 實習生計畫

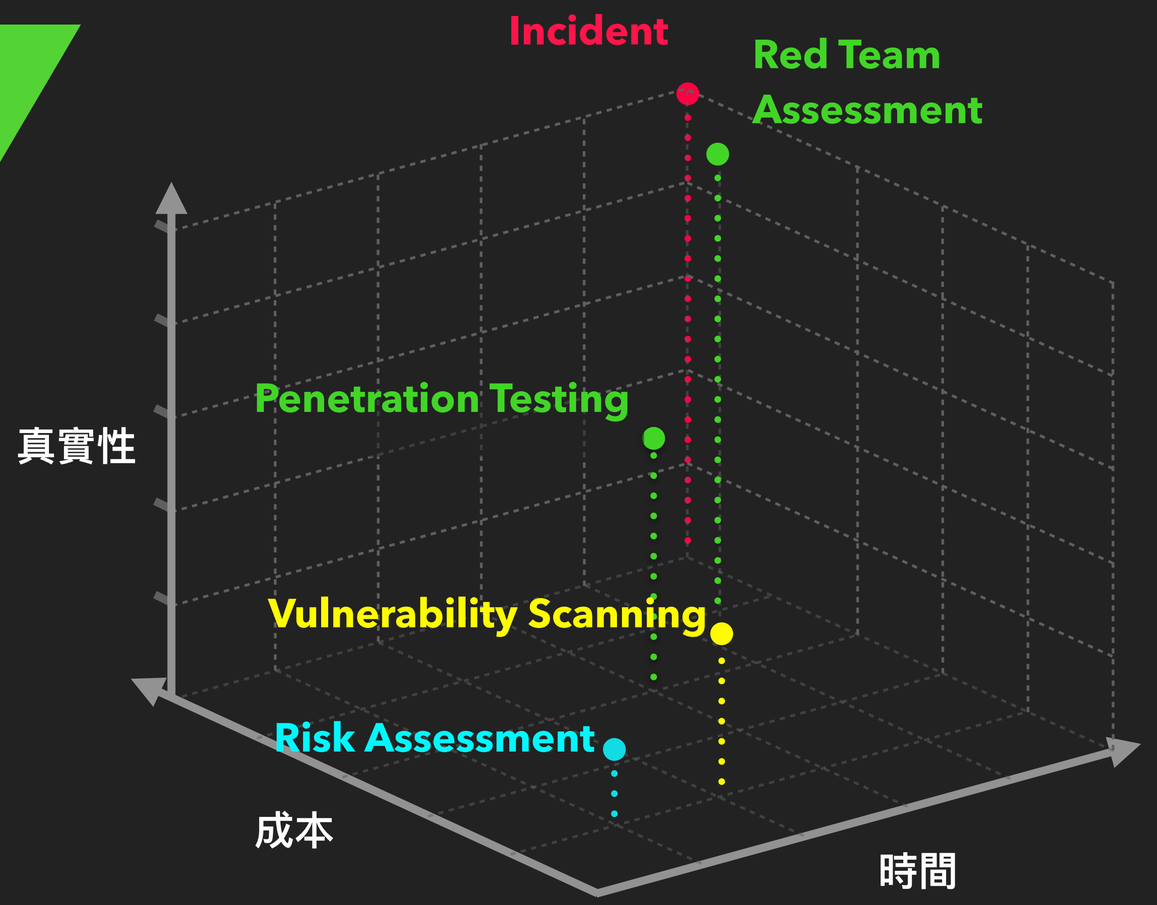
2022.12
獲得 Pwn2Own Toronto 冠軍

2023.03
DEVCORE Conference
2023

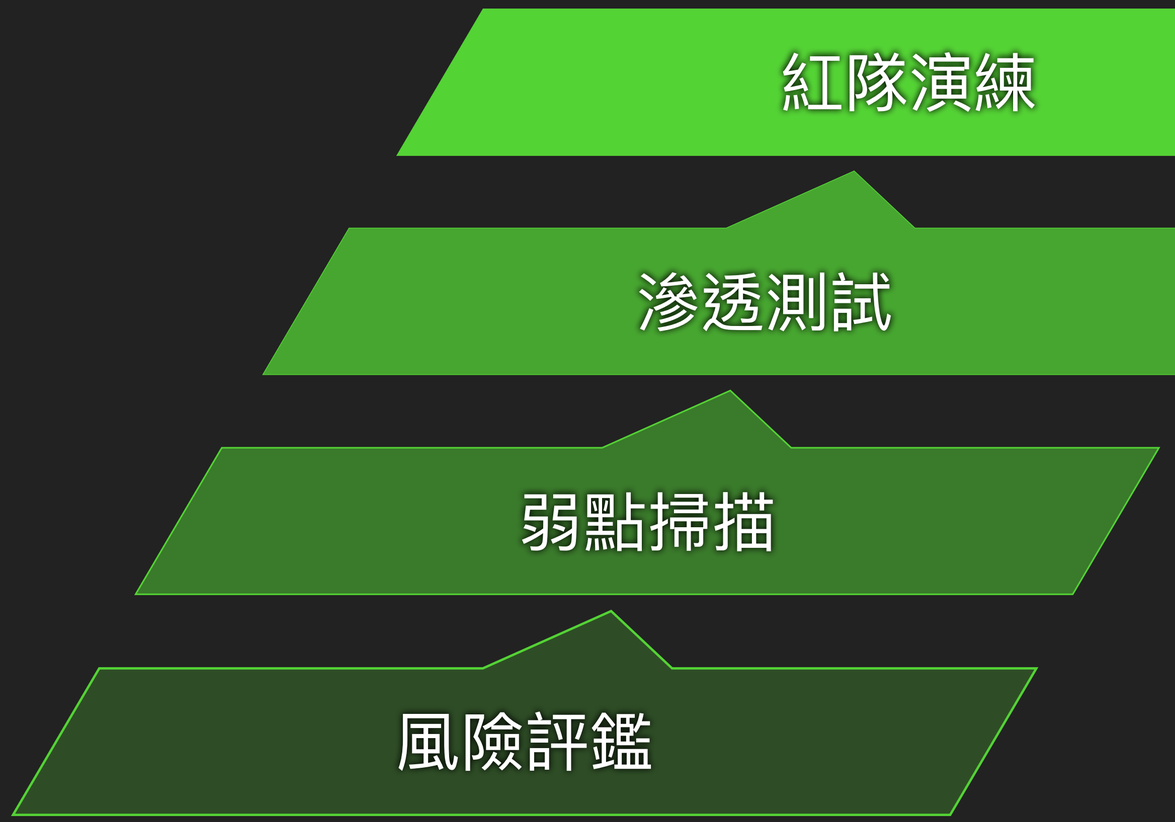
DEVCORE SECURITY CONSULTING

攻擊型服務的演化


紅隊演練
滲透測試
弱點掃描
風險評鑑


Incident
Red Team Assessment
Penetration Testing
Vulnerability Scanning
Risk Assessment
真實性
成本
時間

攻擊型服務的演化



企業對真實性的
需求持續增加

市場需求增加，亂象也會跟著變多...

甲方主管：「請問你們有提供紅隊演練嗎？」

不良廠商：

『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）

市場需求增加，亂象也會跟著變多...
但沒想到情況還可以更嚴峻...

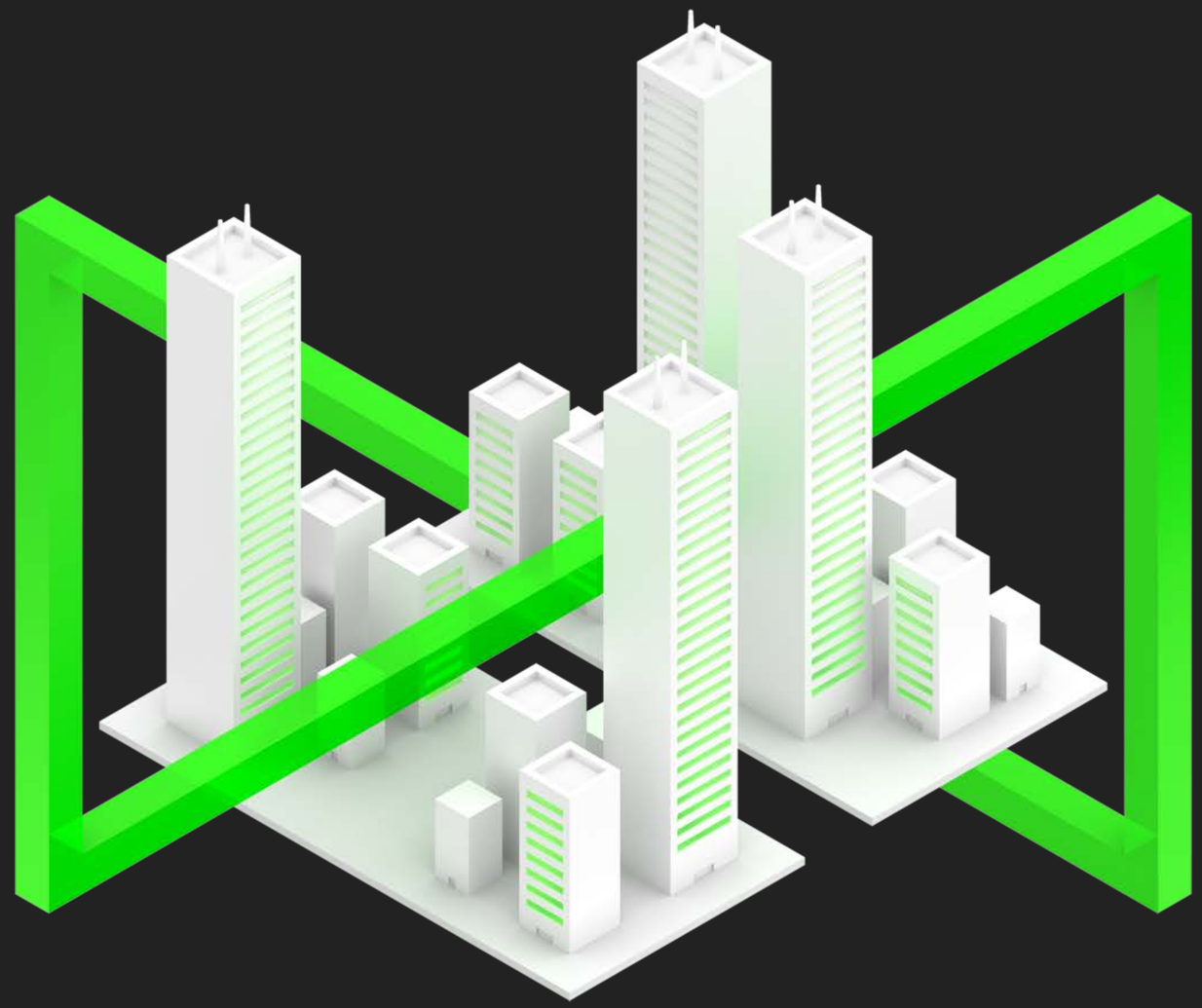
甲方主管：「我拿到的這份是紅隊演練報告？」

不良廠商：

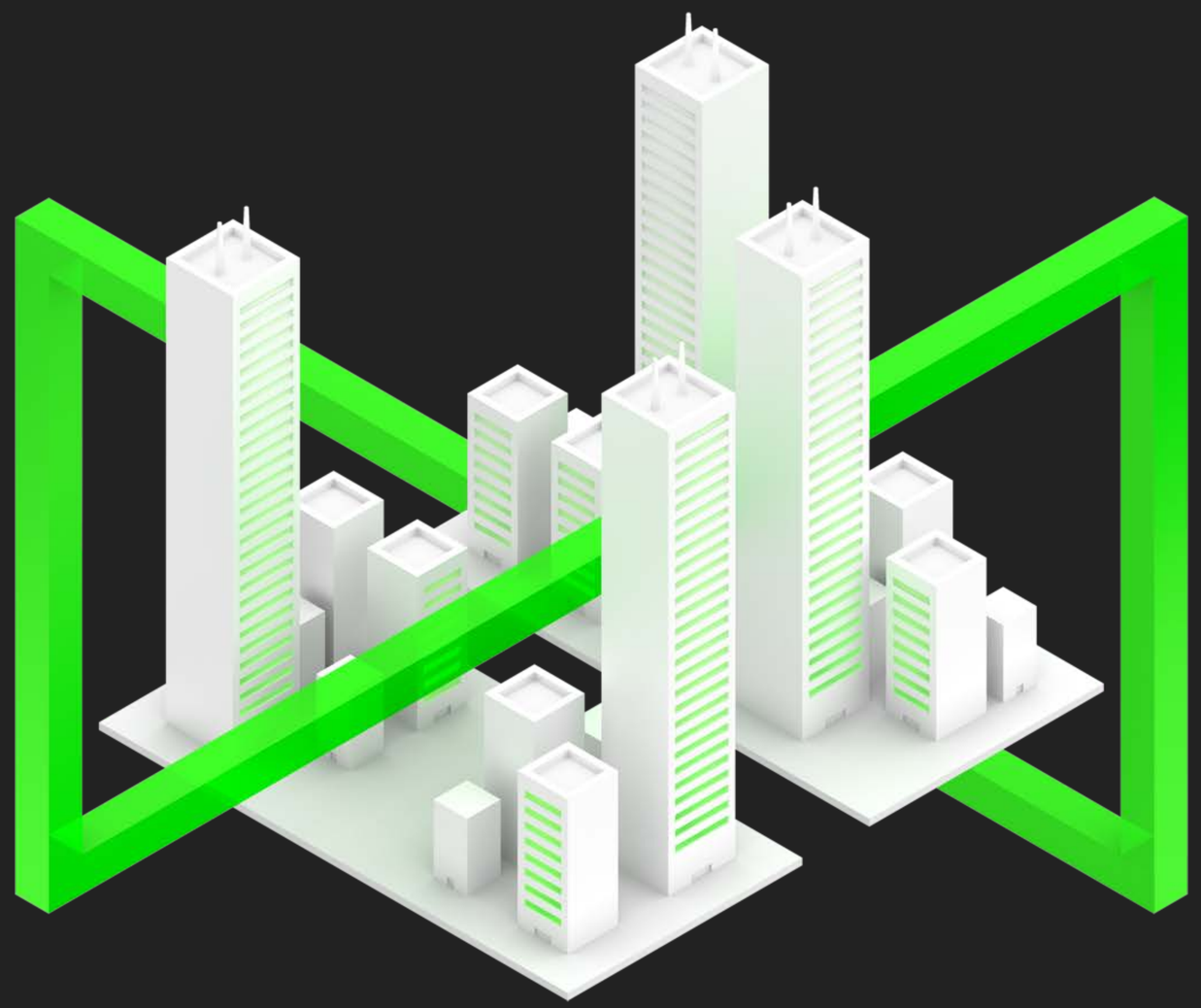
『當然！我們用紅隊演練工具 Ne##us 掃描出的報告喔！』

2023.02 來自甲方的悲歌

我們必須回到初衷
說明紅隊的精神

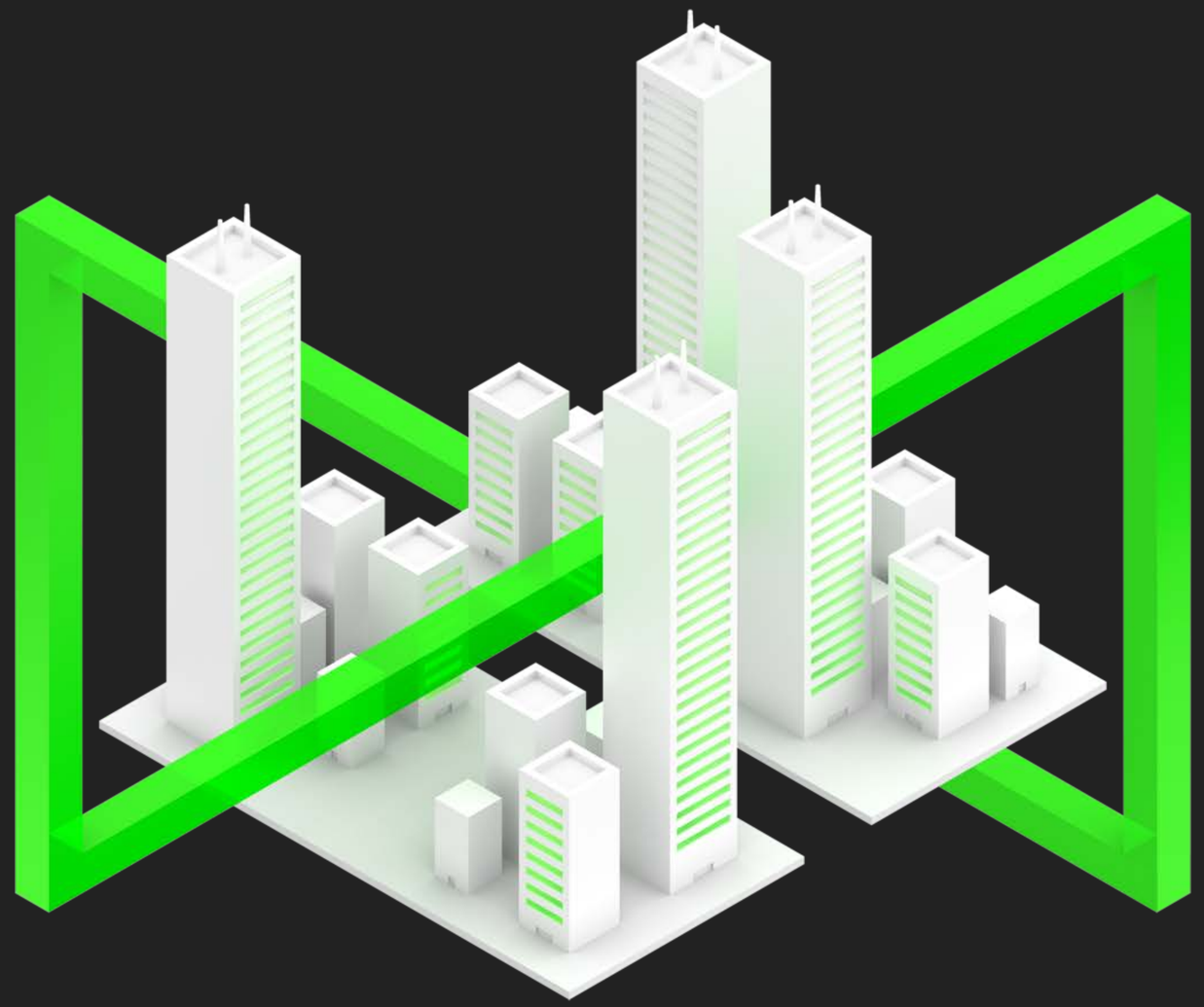


紅隊的精神是什麼？



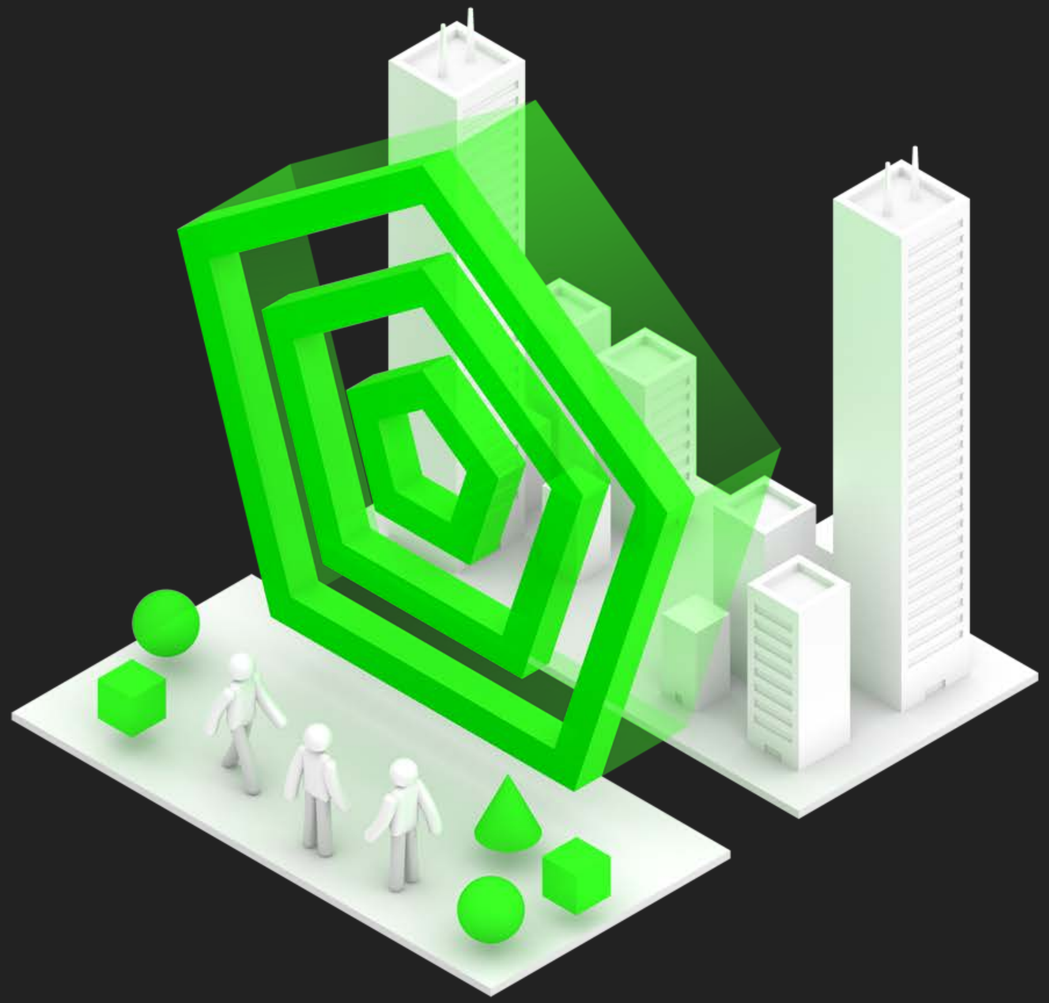
紅隊的精神是什麼？

運用駭客思維，
從有限的時間中，
研究無限種攻擊的可能



2019 - 2023：5 年紅隊經驗我們看到了什麼？

- **供應鏈**成為企業安全破口
- 資安產品**有效性**難以衡量
- 防禦方對資安投入**優先順序**感到無助
- 經過多次演練，
  企業的防禦及反應能力大幅增強
- 紅隊成功控制的系統中，
  發現已有惡意攻擊者在其中活動



DEVCORE SECURITY CONSULTING

DEVCORE
Research Team

DEVCORE SECURITY CONSULTING

DEVCORE Research Team 研究組

- 回報國際級產品重大漏洞增強安全性
- 發表研究至國際研討會促進技術交流
- 透過國際 Pwn2Own 等競賽證明台灣實力
- 發現網軍持續利用的 0-Day 漏洞，
  幫助原廠加速修補增強安全

DEVCORE SECURITY CONSULTING

ProxyLogon

2020.10 月 **開始研究 Exchange 漏洞**

https://proxylogon.com/

2020.10 月 **開始研究 Exchange 漏洞**

12 月 **漏洞研究完成**

https://proxylogon.com/

2020.10 月 **開始研究 Exchange 漏洞**

12 月 **漏洞研究完成**

2021.01 月 **回報漏洞至微軟**

Vulnerability Disclosure Timeline

October 01, 2020	DEVCORE started reviewing the security on Microsoft Exchange Server
December 10, 2020	DEVCORE discovered the first pre-auth proxy bug (**CVE-2021-26855**)
December 27, 2020	DEVCORE escalated the first bug to an authentication bypass to become admin
December 30, 2020	DEVCORE discovered the second post-auth arbitrary-file-write bug (**CVE-2021-27065**)
December 31, 2020	DEVCORE chained all bugs together to a workable pre-auth RCE exploit
January 05, 2021	DEVCORE sent (18:41 GMT+8) the advisory and exploit to Microsoft through the MSRC portal directly
January 06, 2021	MSRC acknowledged the pre-auth proxy bug (MSRC case 62899)
January 06, 2021	MSRC acknowledged the post-auth arbitrary-file-write bug (MSRC case 63835)
January 08, 2021	MSRC confirmed the reported behavior

https://proxylogon.com/

2020.10 月 開始研究 Exchange 漏洞

12 月 漏洞研究完成

2021.01 月 回報漏洞至微軟

03 月 外界發現駭客組織及網軍利用

https://proxylogon.com/

2020.10 月 開始研究 Exchange 漏洞

12 月 漏洞研究完成

2021.01 月 回報漏洞至微軟

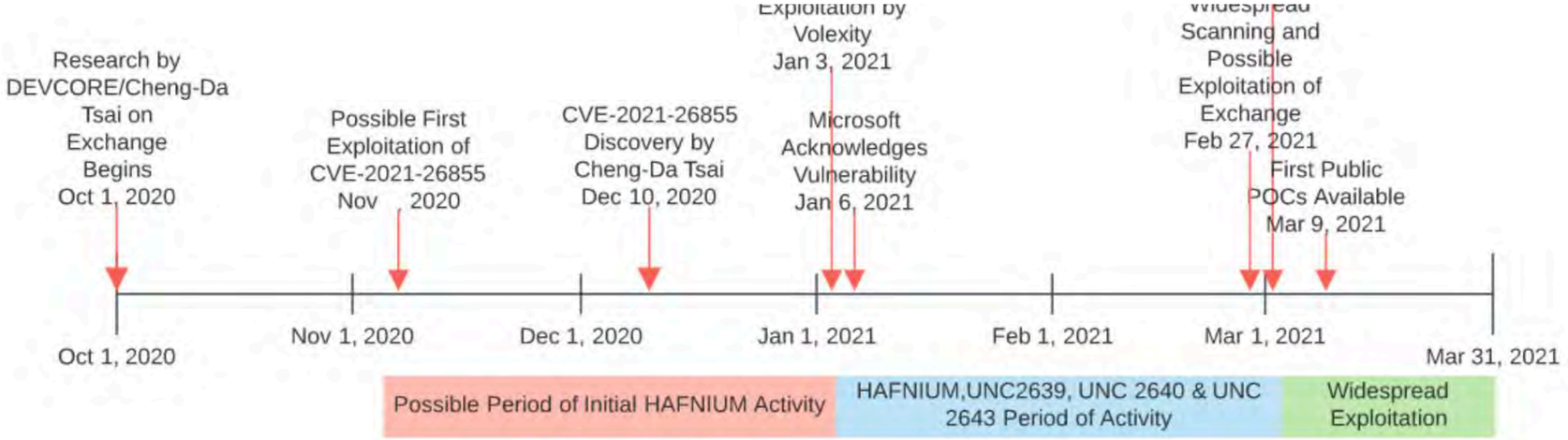
03 月 外界發現駭客組織及網軍利用

03 月 **內部調查排除外洩的可能性**

ProxyLogon

https://proxylogon.com/

根據 DomainTools 整理的 Exchange Server 漏洞事件時間表，知名的駭客團體 HAFNIUM 可能遠在 11 月初就開始用此漏洞攻擊。因此 DEVCORE 外洩之說，在邏輯上並不合理。



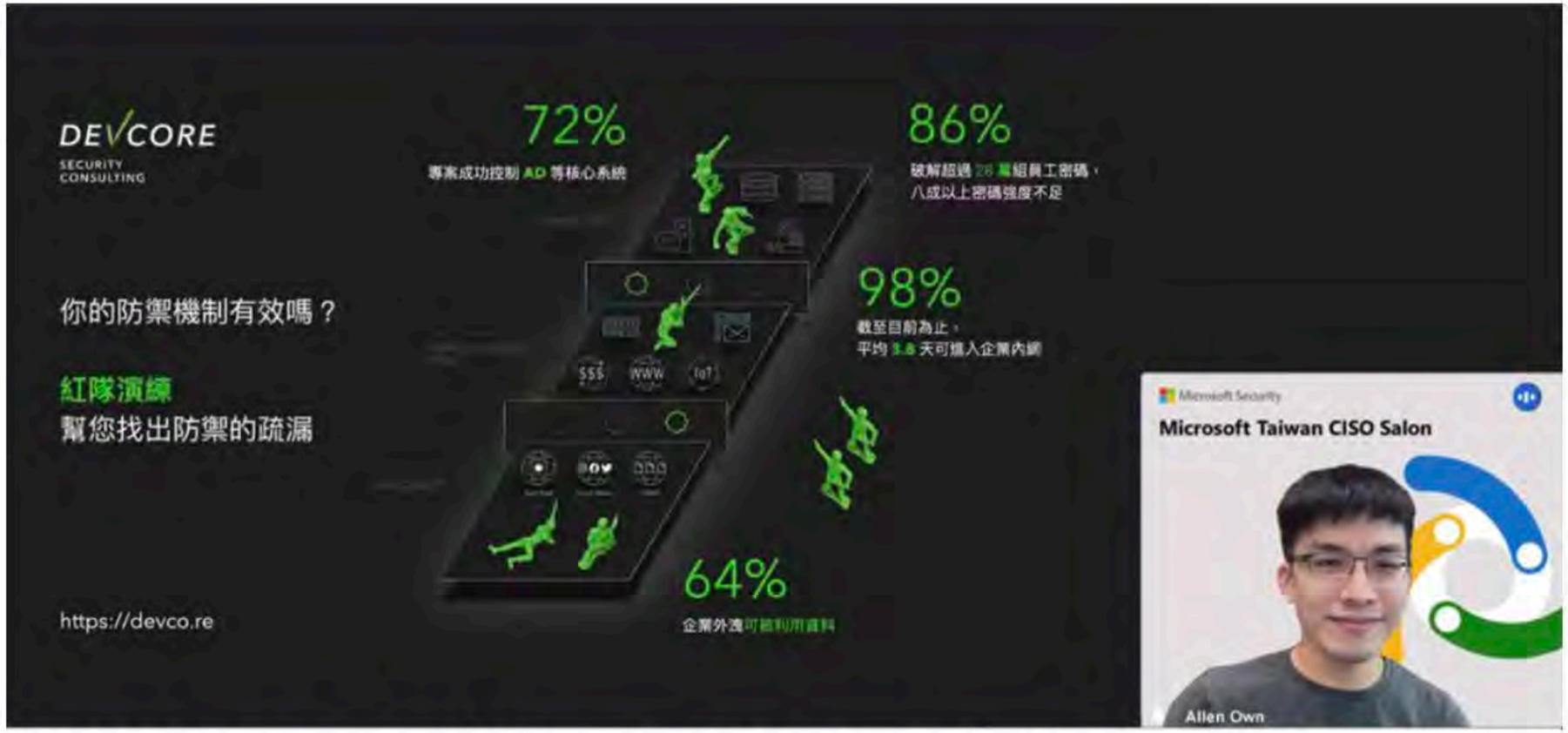
（圖片來源：DomainTools）

03 月 發現網軍利用漏洞早於我方研究

ProxyLogon

至今 **微軟致謝並持續與我們合作**

ProxyLogon



DEVCORE 受微軟邀請，於 Microsoft CISO Salon 以白帽駭客觀點分享企業資安風險及資源配置思維。 DEVCORE /提供

至今 **微軟致謝並持續與我們合作**

ProxyLogon

至今 **微軟致謝並持續與我們合作**

ProxyLogon

2020.10 月 開始研究 Exchange 漏洞

12 月 漏洞研究完成

2021.01 月 回報漏洞並獲取

03 月 外界發現駭客組織及網軍利用

03 月 內部調查排除外洩的可能性

03 月 發現網軍利用漏洞早於我方研究

至今 微軟致謝並持續與我們合作

為什麼要做研究？

因為我們想透過前瞻漏洞研究
幫助全世界變得更安全


故事總是充滿美好的，
但創業的故事並不是。

創業的死亡低谷

“創業一年內倒閉的機率高達 90%，剩下 10% 又有 90% 會在五年內倒閉

能撐過前五年只有 1%，前五年陣亡率高達 99%”

DEVCORE SECURITY CONSULTING


2014
第一個獨立辦公室

2014

第一個獨立辦公室


2015 - 2021
復興北路辦公室

2015 - 2021

復興北路辦公室


2015 - 2021
復興北路辦公室

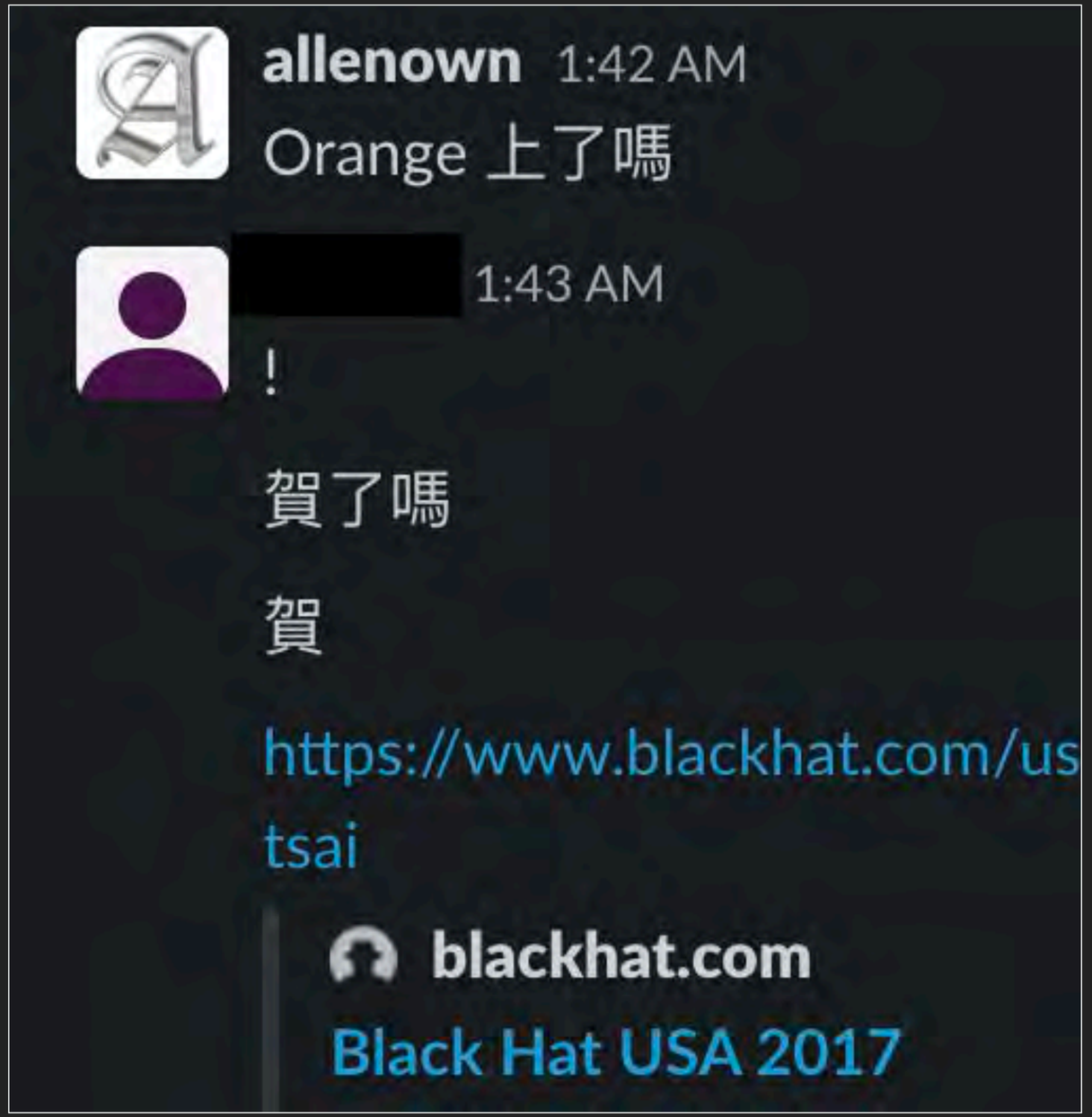
2015 - 2021
復興北路辦公室

2015 - 2021

復興北路辦公室


2015 - 2021
復興北路辦公室


無數個通宵被鎖住的夜晚



2017.05
研究組邁向世界的舞台

2017.07
Black Hat USA 2017

Taiwan No. 1 !

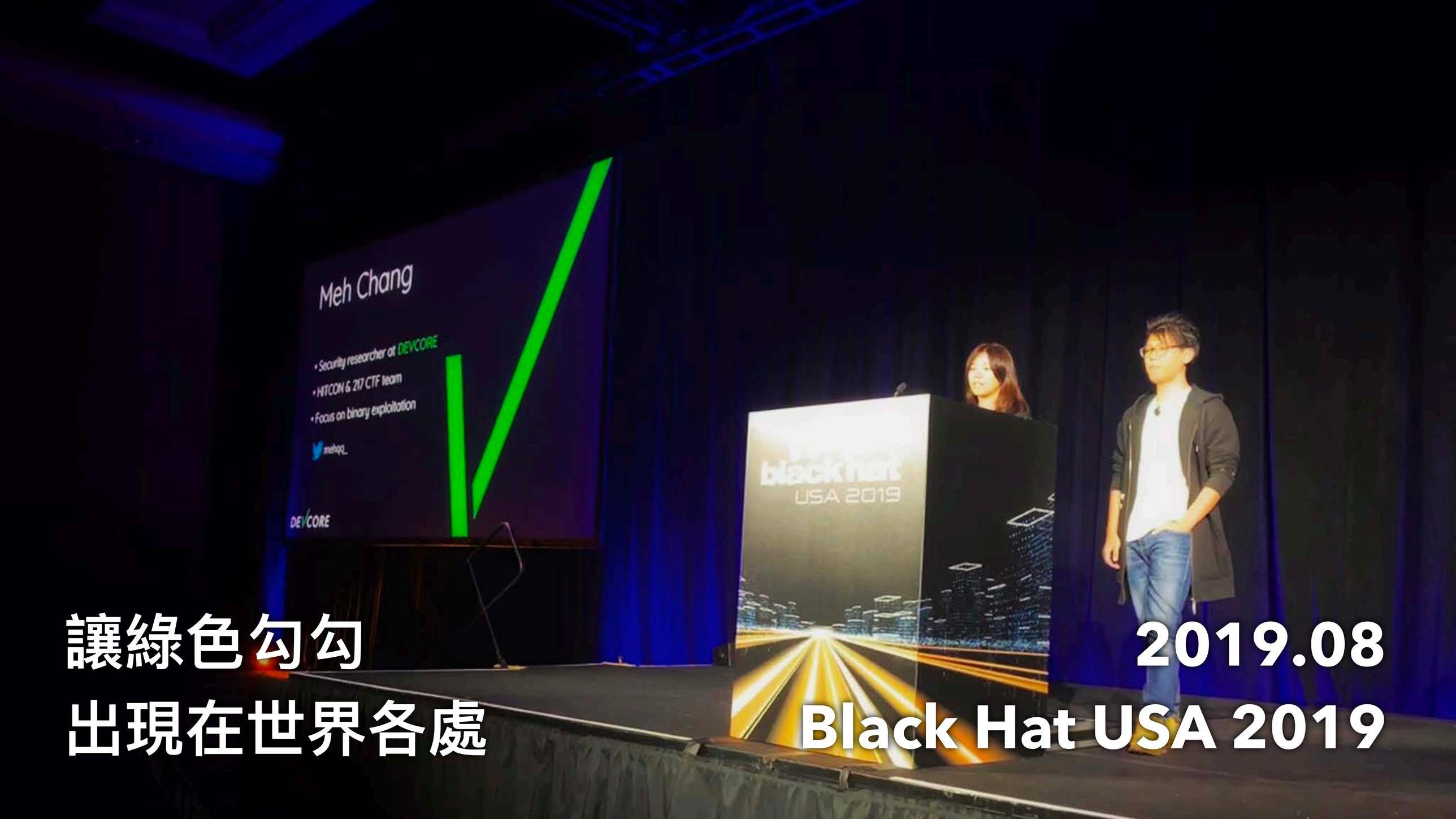
2017.07

DEF CON 2017

2017.07

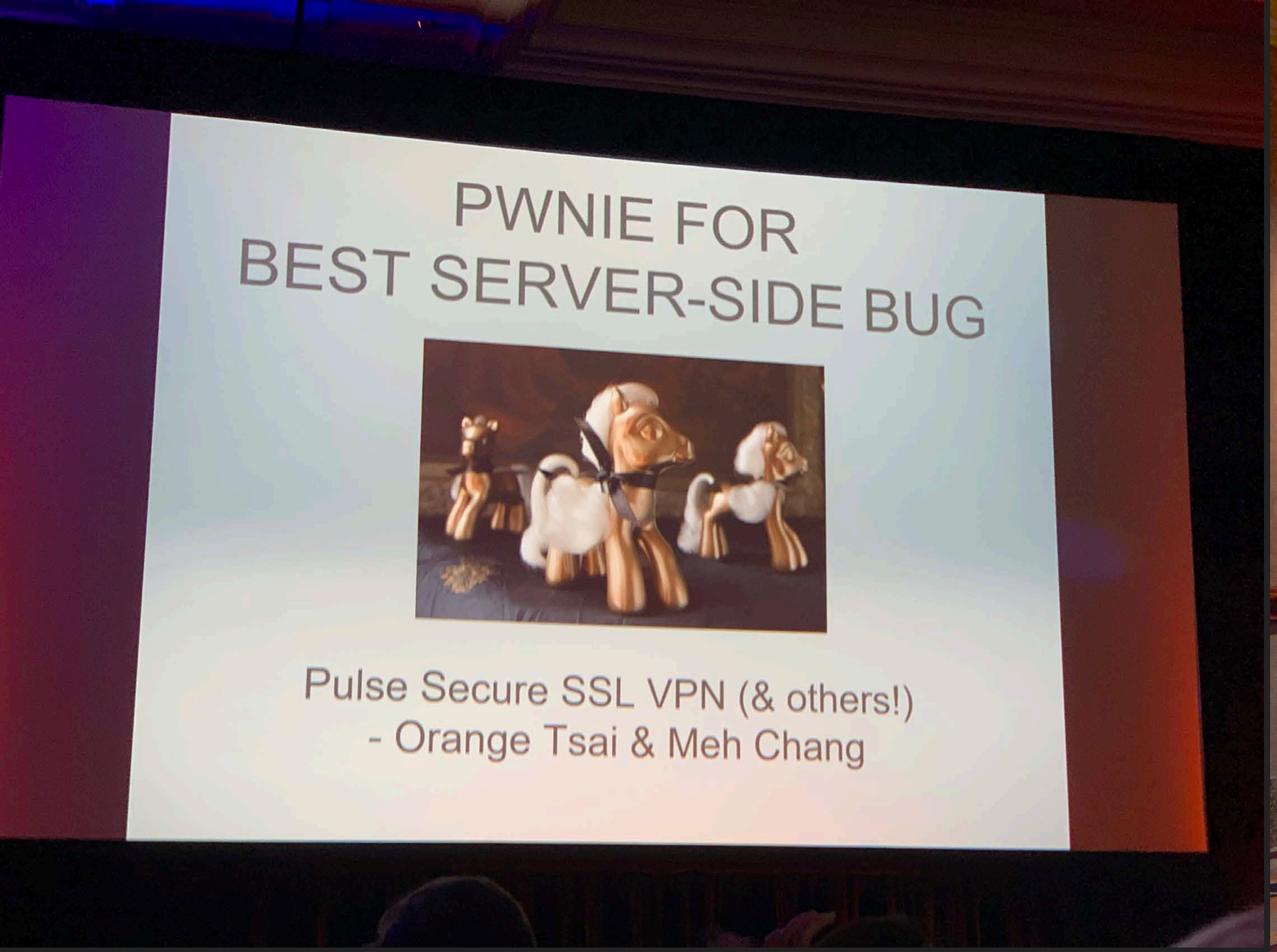
DEF CON 台下全滿

2019.03
Red Team Summit



讓綠色勾勾
出現在世界各處

2019.08
Black Hat USA 2019



2019.08

Pwnie Awards 最佳伺服器漏洞獎

2019.08
DEF CON 2019


2019.08
台下還是全滿


2019
DEVCORE
CONFERENCE 2019
ATTACK
DEVCORE
SECURITY CONSULTING
DEVCORE
CONFERENCE 2019
TAIPEI SEP 25,
ATTACK
DEVCORE
DEVCORE
CONFERENCE 2019
ATTACK
DEVCORE Conference


為了未來的發展
2021.11
八德辦公室

2023
八德辦公室

2023
八德辦公室

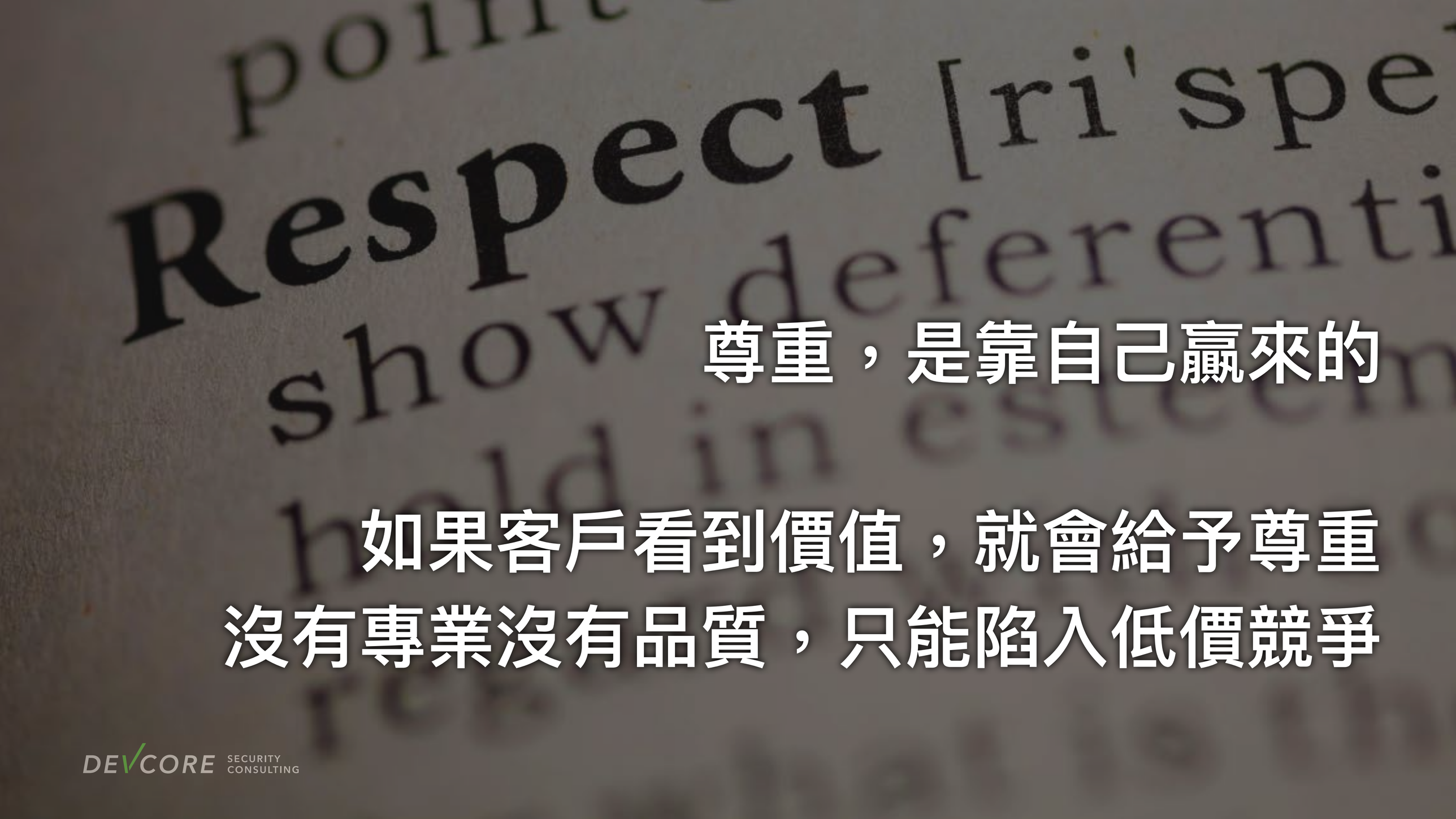
是什麼
讓我們努力奮鬥至今？

DEVCORE SECURITY CONSULTING

創業十年來我們深信，

將一件事情做到極致，
才是通往成功的道路。

DEVCORE SECURITY CONSULTING



尊重，是靠自己贏來的

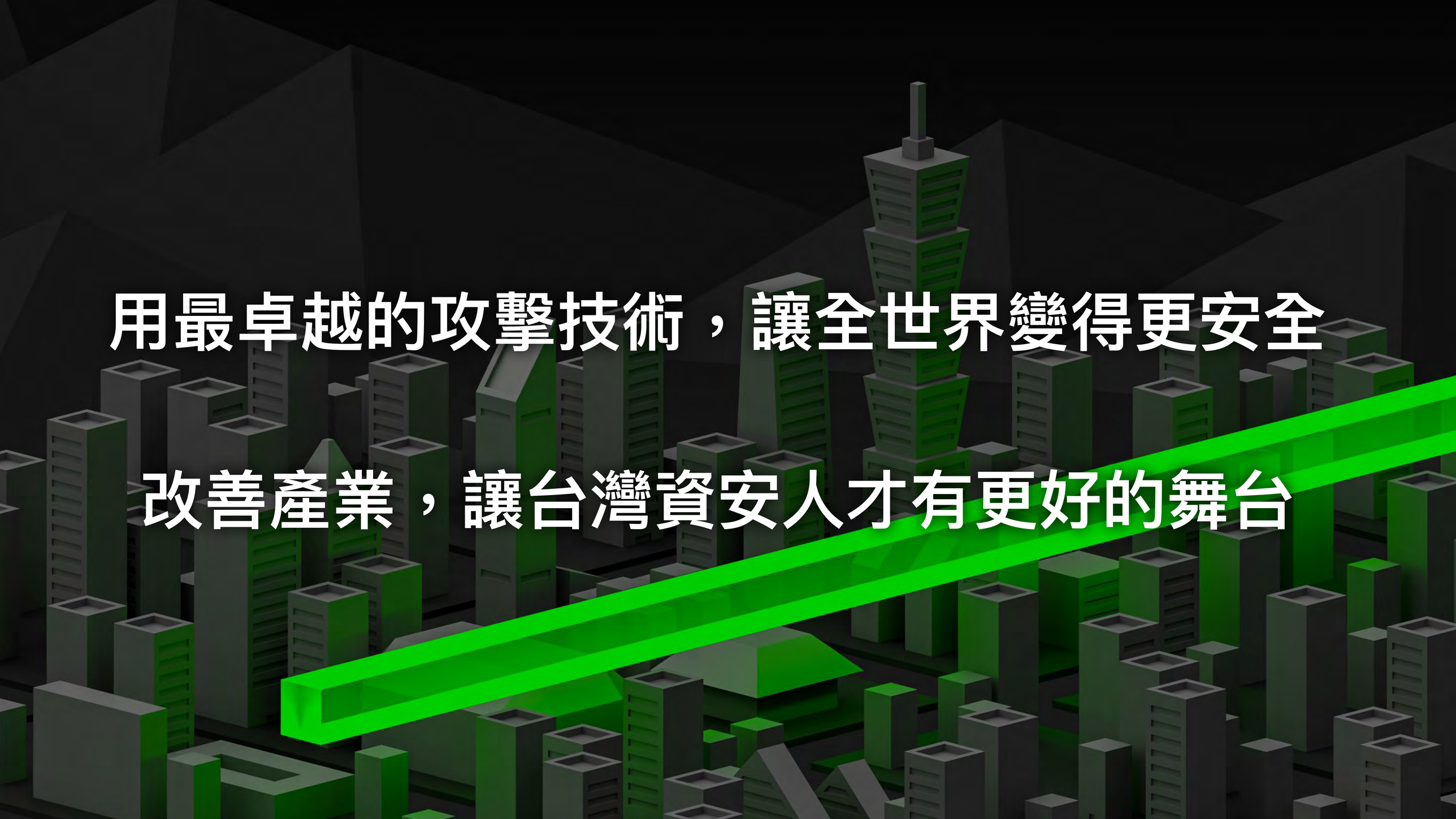
如果客戶看到價值，就會給予尊重
沒有專業沒有品質，只能陷入低價競爭

創業
絕對不是一個簡單的選擇

但台灣需要更多人做對的事情
期待有更多伙伴投入創業

持續培育更多人才

讓台灣資安人才
有更多發揮的舞台


用最卓越的攻擊技術，讓全世界變得更安全
改善產業，讓台灣資安人才有更好的舞台


The World Is Changed by Your Example,
Not by Your Opinion.
- Paulo Coelho

DEVCORE
SECURITY
CONSULTING

攻擊一日，創業十年

Q&A

戴夫寇爾股份有限公司

contact@devco.re