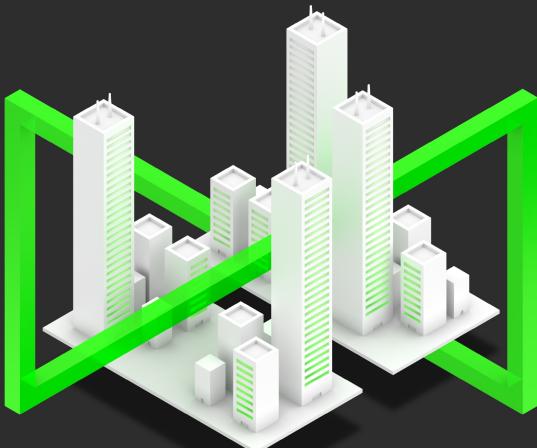


# Red Team Assessment

## 紅隊演練服務 保護企業高戰略價值資產



### 關於 DEVCore

DEVCORE 致力於提供客戶最頂尖的紅隊演練服務，透過模擬真實駭客攻擊，協助客戶找出潛在的安全漏洞，並強化整體防禦能力。本手冊旨在分享 DEVCORE 在不同產業的攻擊經驗、專業能力，以及獨到見解，協助企業更了解如何應對網路威脅。

LEARN MORE



### 資安防護的挑戰：為何紅隊演練如此重要？

隨著組織型駭客、勒索軟體及供應鏈滲透的攻擊快速演進，企業面臨嚴峻的挑戰。將攻擊阻絕於企業之外，已非可行的防禦思維。企業需要的，是全盤瞭解當面臨攻擊時，設備及人員該如何及時因應，這正是紅隊演練成為企業提升資訊安全韌性的關鍵所在。

### 紅隊演練：模擬真實世界的潛在威脅者

紅隊演練（Red Team Assessment）在不影響企業營運的前提下，模擬攻擊者入侵企業系統，在有限時間內無所不用其極，找到進入點並模擬攻擊，達成企業指定的演練目標。

DEVCORE 紅隊演練專注模擬真實世界攻擊情境，具備精湛攻擊技術，從不同攻擊面進行測試，找出系統漏洞與防護盲點，讓企業瞭解攻擊者的思維、手法、工具（TTPs），透過「以戰代訓」，協助企業在面對真正攻擊前能獨當一面。

### 依企業演練目的，挑選演練模式

第一階段 — 合作模式：以找到重大弱點（突破點）為主要目的，針對演練範圍及目標的入侵途徑，尋找漏洞，降低漏洞被利用的風險。

第二階段 — 協調放行模式：尋找系統強化後仍存在的重大弱點、關鍵入侵途徑，同時驗證防禦措施有效性與藍隊應變機制。

第三階段 — 實真演練模式：最真實的方式，不提供演練軌跡，著重驗證藍隊防偽能力與應變機制，找出企業疏忽的攻擊面與未知攻擊途徑。



### 用最細緻的演練規劃，最大化演練效益

紅隊與藍隊唯有密切協作、相互配合，才能確保演練成效最大化，達成預期目標。我們提供多樣且細緻的演練規劃，包含：演練時段限制、靜/動態 IP 的調整、動態專案代號、攻擊進度揭露、限制演練範圍、執行特定操作或不同的久攻不克方案等。透過最佳實務的經驗，來與客戶一同最大化紅隊演練效益。

### DEVCORE 紅隊演練模型

實體位置	虛擬位置	策略	執行方式	範圍	目標分類	目標項目	執行時間	防禦規避
遠端	網際網路	零時差攻擊	黑箱測試	全範圍	基礎設施	網站	指定時間	動態 IP
指定現場	內部網路	情資收集	灰箱測試	部分範圍	應用程式	排除日期	流量干擾	
現場	混合模式	第三方軟體	白箱測試	指定範圍	特殊權限	不限定時間	日誌干擾	
		社交工程			無線網路			
		Wi-Fi			資安設備			
		供應鏈攻擊			IoT- OT			
		外網攻擊			雲端安全			

### 實績與規範

60+  
間企業合作

110+  
場紅隊演練經驗

81%  
專案成功控制  
AD 等核心系統

82%  
員工密碼強度不足，  
破解超過 71 萬  
員工密碼

77%  
專案可進入企業  
內網，平均 4.43 天

53%  
企業外洩  
可被利用資料

### 高科技產業

半導體設計、製造、封裝，  
電腦零組件、通訊網路等

### 金融業

6 家系統性重要銀行  
(D-SIBs) 中，已有 5 家選擇  
DEVCORE 作為資安合作夥伴

### 關鍵基礎設施

國家 8 大關鍵基礎設施  
執行包含 7 大領域，  
如：交通、能源、醫療等

### 政府機關

中央及地方資通安全  
責任等級 A、B 級機關

### 研究與貢獻

我們長期精研資安領域最前衛、最新研究及攻擊趨勢，並將之轉化為紅隊演練與滲透測試服務的技術及手法，協助企業掌握新型攻擊趨勢。

13+ 國際肯定

'24 Top 10 Web Hacking Techniques #1 & #4  
'23 Pwn2Own Toronto 季軍  
'22 Pwn2Own Toronto 冠軍  
'21 Pwn2Own Austin 亞軍  
'21 Pwnie Awards (Best Server-side Bug)  
'21 Pwn2Own Vancouver 冠軍  
'20 Pwn2Own Tokyo 亞軍

290+ 漏洞揭露

超過 30 種產品類型，  
包含企業最常使用的 Microsoft Windows / Exchange / Office / IIS Linux Kernel、Apache HTTP Server、Exim、PHP Fortinet、Pulse Secure

60+ 國際研討會

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

50+ 漏洞獎金計畫

Amazon, Meta (Facebook), GitHub, Google, LINE, X (Twitter), Uber



### 基本觀念與實施

紅隊演練的基本觀念、適用情境及執行方式，幫助企業了解紅隊演練的價值與準備需求。

Q1

#### 紅隊演練與滲透測試的差異？

滲透測試僅針對單一系統或產品確認其安全性。紅隊演練則是在有限時間內，於企業授權的範圍內，針對最擔心的資訊資產進行模擬攻擊，找出駭客可能的攻擊路徑、手法，同時驗證防禦機制的有效性。

Q2

#### 資安成熟度到什麼層級才適合執行紅隊演練？

針對不同成熟度的企業，我們提供不同的演練模式。我們建議，當企業已經建構基礎的防禦機制（例如：防火牆、防毒軟體、網段區隔、端點監控機制等），即可藉由紅隊演練來驗證現有防禦機制的假設，並作為後續強化資安措施的策略工具。

Q3

#### 組織已經有內部紅隊是否仍需委託外部紅隊？

外部紅隊著重於黑箱測試、漏洞研究、偵測規避，是以更貼近真正的外部攻擊者的角色進行演練，協助企業評估防禦機制的有效性。

內部紅隊更了解企業的系統、網路架構、業務流程、員工行為及潛在弱點等，因此可以在外部紅隊演練後，針對關鍵路徑及節點進行細緻的檢測，相輔相成。

Q4

#### 紅隊演練的收費方式？

DEVCORE 紅隊演練是依產業類型、企業規模、內外部資產數量、演練目標、企業的防禦能量及合作模式，提供客製化報價。若提早達成演練目標，則會持續尋找其他入侵途徑與弱點。

Q5

#### 紅隊演練建議的執行頻率？

依企業規模、防禦體質及演練目標而定，建議 1 至 2 年至少執行一次紅隊演練服務，以確保企業資安防禦有效性。



### 執行方式與影響

紅隊演練的實施細節，包括執行時間、與 IT 團隊的合作模式，探討如何確保企業正常運作不受影響。

Q1

#### 紅隊演練服務需要多久時間？

所有紅隊演練皆為客製化專案。平均而言，完整專案流程約需時 4 至 6 個月，包含情報蒐集、紅隊演練初測、檢測結果分析及報告、弱點修補與系統安全強化、弱點修復驗證等流程。

Q2

#### 第一次執行紅隊演練，需要準備哪些資料給 DEVCORE？

為了真實模擬並呈現攻擊情境，首次演練僅須提供授權檢測範圍及任務目標即可。若已執行多次紅隊演練，則可依演練目標提供部分資訊，提升演練成效。

Q3

#### 演練期間是否需事先通知 IT 團隊？紅隊與企業內部藍隊應如何合作？

根據客戶不同的資安體質及目標，DEVCORE 將建議不同的演練模式，從第一階段合作模式、第二階段協調放行模式、到第三階段真實演練模式，客戶可依照演練的擬真程度，決定通知的藍隊成員或主管層級。

Q4

#### 紅隊如何模擬內部威脅(Insider Threat)？是否可以模擬社交工程攻擊？

紅隊演練可於客戶指定主機作為演練起點，模擬該主機若遭入侵後，可能對企業資訊資產造成的威脅。

Q5

#### 如何確保紅隊演練不會影響企業正常營運？

專案執行過程中不會刪除客戶的任何內部資料。對客戶環境具有潛在影響的檢測僅會在有必要、且客戶同意的情況下執行。此外，也不會執行任何具插旗性質的動作，例如：更換網站首頁等。



### 資安效益與長期價值

紅隊演練對企業資安的長期影響，包括資料保護、資安 KPI、資安預算。

Q1

#### 紅隊演練過程有機會接觸到企業內部資訊，DEVCORE 如何保護這些資料？

DEVCORE 已通過 ISO 27001 驗證，客戶機敏資料與其他相關資料的管理、程序及流程均在驗證範圍之內。客戶資料皆保存在 DEVCORE 機房內部的主機，僅負責執行該專案、已簽署 NDA 的專案成員可以存取，並會保留存取紀錄。測試用的專案資料將於專案結束後刪除，只留下相關報告。專案維護期後，若客戶要求刪除資料，將配合要求並能出具文件證明。

Q2

#### 紅隊演練的結果如何轉化為可行的資安改進計畫？如何爭取更多資安預算？

企業應於設定紅隊演練目標時，將關鍵系統作為演練目標。因此，若演練結果顯示關鍵系統遭到攻擊，企業可評估從發現攻擊事件到處理完成的時間，即是企業可能造成的營業損失。

Q3

#### 紅隊演練如何幫助企業建立資安 KPI？

我們建議至少可使用以下幾個方式來衡量藍隊的 KPI：

- 初始偵測時間 (MTTD, Mean Time to Detect) 從紅隊發動攻擊到藍隊偵測到威脅所需的平均時間
- 事件回應時間 (MTTR, Mean Time to Respond) 從偵測到攻擊到啟動應對措施所需的平均時間
- 事件遏制時間 (MTTC, Mean Time to Contain) 從發現威脅到完全遏制攻擊的時間