# 金融業
# 紅隊演練服務案例

Red Team Assessment

## 背景

金融產業高度數位化，包含網銀、交易系統、客戶資訊等關鍵系統，成為駭客最具吸引力的攻擊目標之一。面對持續進化的資安威脅，企業必須確保自身不僅能阻擋攻擊，更能即時偵測與應對，以防止資安事件對財務與信譽造成嚴重影響。

## 挑戰

> **金融產業採取嚴格內外網隔離、系統審核嚴謹，仍面臨多重安全風險**

- 近 **90%** 的金融機構有機會被取得如 AD 或 LDAP 伺服器等核心系統的控制權。其中，近 **58%** 的金融機構可以透過外部系統被直接或間接控制 AD 伺服器。
- **82%** 以上的金融機構在紅隊演練過程中被發現外部可利用漏洞，平均在 **5天** 內被取得關鍵系統權限，可進而影響交易、客戶資料與營運安全。
- **70%** 的專案發現企業仍使用過時或弱加密機制、使用存在 CVE 弱點 Library，增加攻擊者可入侵的風險。

## 方案

DEVCORE 紅隊演練依照豐富的經驗，模擬內外部攻擊，測試駭客試圖入侵企業內部網路時，企業所具備的防禦能力。可針對 ATM、網路銀行、線上交易系統進行演練；或評估金融機構在事件回應計畫的有效性，確保金融機構能夠符合內部規範，於時限內針對攻擊事件進行判讀或處理。

### 建議採用紅隊演練第二階段：協調放行模式

演練過程中，將建立紅、藍隊溝通頻道，由紅、藍隊雙方共同針對演練過程的進展、回應狀況進行溝通，並透過特許方案或替代方案，兼顧識別高風險漏洞及強化偵測回應機制。

免責聲明：本手冊數據僅代表演練當下之情況，企業應根據自身情況，評估並採用合適的演練模式與安全防護措施。