政府機關
紅隊演練服務案例

Red Team Assessment

背景

政府機關負責管理大量個人資料 (PII)、國家機密文件與關鍵業務系統管理，長期為組織型駭客 (Nation-state Cyberattacks) 的重點針對目標。

挑戰

> **政府部門具備法規詳細指引安全方針，縱深綜效只差毫釐更能發揮效益**

- 委外開發系統成為攻擊標的、旁路攻擊同樣具備高度風險：近 **95%** 的政府機關於紅隊演練中被成功控制委外開發的系統或設備，比例居所有產業之冠。其中，近 **43%** 的政府機關可以透過外部系統直接或間接控制 AD 伺服器。
- 外部防禦能力不均：自演練開始，平均 **11.69天** 可以控制 AD 伺服器，然而最短案例僅需 **3天**、最長則需 **23天**。
- AD 密碼破解率將近 **90%**，特定排列組合、預設密碼，造成密碼破解風險增加。

方案

DEVCORE 紅隊演練建議優先模擬外部攻擊，優先降低資料遭到洩漏之風險，進而縮小攻擊表面並提升內部人員回應能力。亦可將定期社交工程演練結果，作為內部演練起始點，評估高風險同仁電腦遭入侵後，可能對機關的影響及回應機制之效益。

建議採用紅隊演練第一階段：合作模式

演練過程中，透過合作模式模擬已經掌握機關情資的組織型駭客，以灰箱方式由政府機關告知網路及系統架構，將演練情境著重於找出漏洞與入侵路徑。搭配特許方案，兼顧外部網路安全及內部偵測回應機制進行強化。