高科技業
紅隊演練服務案例

Red Team Assessment

背景

高科技業的 IT/OT 環境高度複雜，涵蓋自動化生產機台、專屬通訊協定與精密製造系統，對於安全性與可用性的要求極高。企業不僅需要能反應防禦姿態的演練，更須確保演練過程不影響營運。 DEVCORE 紅隊演練憑藉對產業的深度理解，透過精密規劃與真實攻擊模擬，協助企業檢視防禦機制，找出潛在風險。

挑戰

> **受限於可用性要求極高，老舊系統及漏洞管理成為重大議題，高科技產業仍存在諸多安全隱憂**

- **76%** 以上的企業在演練中被發現外部突破口，可在平均 **4天** 內控制外部系統，並在 **9天** 內取得 AD 伺服器等核心系統權限。
- **62%** 的企業存在半年以上未修補的 CVE，顯示漏洞管理的挑戰性與風險。
- **30%** 的專案發現供應鏈軟體的嚴重漏洞，顯示第三方工具仍是企業資安的破口。

建議採用紅隊演練第二階段：協調放行模式

在不影響生產環境的前提下，建議透過協調放行模式，讓企業能夠在安全、可控的情境下驗證資安機制：

- 模擬內外部攻擊，測試駭客如何滲透企業內部網路，找出最可能的入侵路徑。
- 針對特殊需求，對機敏資料、重要服務等提供針對性的測試及情境。
- 重點關注防禦機制與應變處理效益，訓練資安團隊快速發現並回應攻擊行為，避免資安事件擴大。

透過 DEVCORE 的深度紅隊演練，不僅強化企業安全防禦，更能即時應對攻擊、減少供應鏈風險，在確保生產運行的同時，打造更堅固的資安防線。