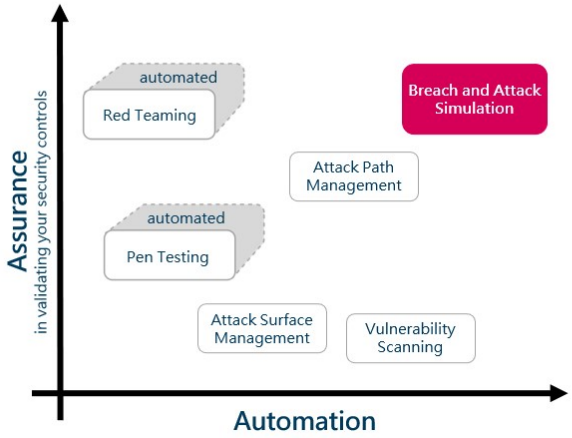
SafeCove 藍隊驗證模擬攻擊演練包-企業進階版(訂閱制)

產品簡介

頻繁的針對式資安攻擊事件，對於企業與機關的資安防護形成的巨大衝擊與影響，企業與機關用戶紛紛導入各項先進的資安防護機制，以抵禦先進攻擊的資安威脅。但進階威脅的攻擊手法，變化多端且變種快速，稍稍改變能輕易避開防毒軟體、入侵防禦設備的偵測，僅依靠特徵碼與制式偵測規則，並無法發覺此類未知的攻擊手法。因此，如何確保資安防護設備的防護有效性？如何進行驗證？是否對於時下最新的加密勒索攻擊手法與惡意軟體是否能有效偵測與防護？已經為全球各國政府與跨國大型企業資安長所關注的議題。

SafeCove 藍隊驗證模擬攻擊演練包，基於安碁資訊多年來的模擬攻防演練經驗，並搭配藍隊驗證模擬攻擊解決方案，提供自動化的藍隊驗證模擬攻擊演練包，讓政府機關用戶可對資安防護機制的防護有效性進行驗證，確保資安防護機制能充分發揮惡意行為偵測與攻擊防禦功能。除了驗證資安防護有效性外，對於資安監控機制的異常告警機制的有效性驗測與驗證，也可透過此產品來進行驗證。SafeCove 藍隊驗證模擬攻擊演練包提供五種攻擊演練模組，並系統定期更新最新模擬攻擊手法，可協助政府機關用戶即時驗測對新攻擊手法的偵測與防禦能力，確保資安防護無空窗。



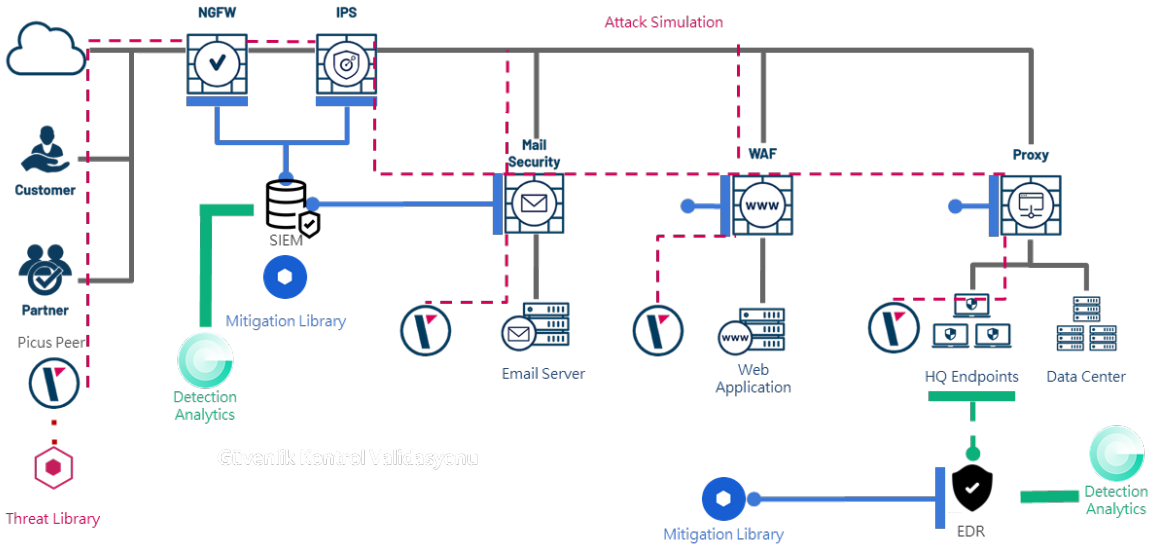


圖1　藍隊驗證模擬攻擊架構示意

產品功能說明

項目	內容說明
產品功能	
藍隊驗證模擬攻擊演練系統功能	●提供 BAS 檢測平台與模擬攻擊演練腳本，用以驗證資安防護設備（如防火牆、入侵防護系統、WAF、防毒軟體、Web Filer、EDR 等)之防護有效性，同時可驗證資安監控機制的監控有效性。BAS 系統內建 4000 多種模擬攻擊腳本，12000 多種攻擊行為，可於系統上依據 APT Factor、MITRE ATT&CK 攻擊階段、Kill Chain 等進行攻擊手法的選擇。 ●BAS 檢測系統提供五個檢測模組，包含 網路滲透攻擊模組、電子郵件社交工程攻擊模組、端點攻擊模組、WAF 攻擊模組、資料外洩演練攻擊模組。 ●提供系統提供檢測與模擬攻擊演練執行結果，系統提供漏洞修補與資安強化改善建議。 ●提供 3 個模擬演練端點代理程式，代理程式依據攻擊手法不同，可支援 Windows 作業系統或 Linux 作業系統或 MacOS 等。
技術支援	

產品授權

產品名稱	授權內容
SafeCove 藍隊驗證模擬攻擊演練包(每年訂閱)	● 提供 1 次藍隊驗證模擬攻擊演練授權 ● 3 個模擬演練端點代理程式 ● 提供 5 個模擬攻擊模組，包含網路滲透攻擊模組、電子郵件社交工程攻擊模組、端點攻擊模組、WAF 攻擊模組、資料外洩演練攻擊模組。 ●提供 SIEM 偵測分析模組及資安設備防禦分析模組

產品售價

- NT$70 萬(含稅)

交付項目

- SafeCove 藍隊驗證模擬攻擊演練包授權(訂閱制)

模擬演練端點代理程式硬體需求

- CPU ： Intel 4 核心 2.0 GHz 以上
- 記 憶 體： 8 GB
- 硬碟空間： 500 GB 以上
- 作業系統： Microsoft Windows 或 Linux 或 MacOS 等

預期效益

- 主動驗證資安防護機制有效性，發掘潛在防護漏洞與缺失。
- 驗證資安監控機制有效性，確保資安設備告警與資安監控規則能準確觸發事件通報。