

## SafeCove 資安弱點管理 - 分散式阻斷服務攻擊演練包

(每年訂閱)

### 產品簡介

隨著駭客攻擊手法的演進，分散式阻斷服務攻擊不再單純以發動海量封包流量的手法，來阻塞網路達到癱瘓政府或企業網站服務，進而能以近似正常流量的網路交易行為來進行攻擊，讓分散式阻斷服務攻擊的發生更加容易，攻擊手法也更容易穿透現今政府與企業所已經部屬的資安防護設備與方案。

歷次的國際重大攻擊事件也證明，一般防火牆與網路層的入侵防護設備已無法抵擋與分辨分散式阻斷服務攻擊行為，這讓分散式阻斷服務攻擊對於政府與企業的網站服務安全威脅等級也快速提升。因此，政府機關與金融單位已紛紛開始著手評估分散式阻斷服務攻擊（簡稱 DDoS 攻擊）對於網站服務與整體資安防護所可能帶來的威脅與相關的防護措施。

為協助政府機關與企業瞭解現有的資安防護架構、應用系統安全強度、網路與主機硬體資源對於分散式阻斷服務攻擊的抵擋與耐受程度。本產品透過自動化模擬攻擊平台，採分散式阻斷服務攻擊手法，網站進行模擬攻擊，並對網站系統進行可用性監測，藉此取得實際攻擊與防禦性能數據，綜合攻擊流量與模擬攻擊標的之網站系統監測，取得演練結果數據，作為網站防禦的參考建議。演練結果數據可納入 SafeCove 資安弱點管理系統進行追蹤管理，作為資訊安全的管理依據。

### 產品內容

SafeCove 資安弱點管理 - 分散式阻斷服務攻擊演練包，採用自動化演練系統，從雲端模擬數種 DDoS 攻擊手法，產生真實的網路攻擊流量，對受測標的網站系統進行模擬攻擊演練。攻擊流量將對 OSI 網路模型的第 3/4 層（網路層/傳輸層）和第 7 層（應用層）發起可控制、可度量的攻擊。

用戶可利用演練的擬真攻擊手法，同步自行啟動相關應變程序進行情境演練，驗證應變程序之落實程度與妥適性，提高用戶對分散式阻斷服務攻擊的應變能力。

攻擊演練完成後，提供系統演練紀錄供客戶存查(如下圖之演練結果樣態示意圖)。



#### 演練方式

1. 以對外服務網站為演練攻擊標的
2. 系統提供三種演練模式擇一進行：
  - 1). 應用層攻擊 (3種攻擊手法)，攻擊演練約1小時
  - 2). 滿頻攻擊 (最多產生500M攻擊流量)，攻擊演練約1小時
  - 3). 應用層+滿頻攻擊，攻擊演練約2小時

#### 交付項目

- SafeCove 資安弱點管理系統-分散式阻斷服務攻擊演練包授權書  
(一次檢測，每年訂閱)

## 產品定價

- 應用層+滿頻攻擊 NT\$400,000
- 應用層攻擊 NT\$250,000
- 滿頻攻擊 NT\$200,000

## 方案效益

- 驗證網站應用系統與資訊基礎架構對 DDoS 攻擊手法耐受程度
- 驗證現有資安防護、網路與資安監控機制的表現與有效性
- 驗證相關應變程序落實程度與妥適性
- 掌握弱點現狀，作為制訂安全政策的管理依據



演練結果樣態示意圖