FIREEYE™

產品型錄

紅隊演練 (Red Team Operations)

測試您對現實世界的目標性攻擊中保護您最關鍵資產的能力

優點

- 瞭解重要資料是否處於風險之中，以及惡意人士是否可輕易取得資料
- 評估您的環境是否具備足夠的安全性，可抵禦真實世界中「無所不用其極」的攻擊者
- 在嚴密控管的真實環境中，測試內部資安團隊對事件的防禦、偵測和應變能力
- 在攻擊者發動入侵之前，辨識複雜的安全性漏洞，降低安全風險
- 獲得以事實為主的分析，以及改善安全狀態的建議

為什麼選擇 Mandiant

Mandiant 為 FireEye 的一家公司，自 2004 年以來就站在資安與網路威脅情報的第一線。我們的資安事件處理團隊站在全球最複雜的入侵事件的最前線。我們對現有以及新興的威脅發動者以及他們快速變動的工具、攻擊手法、技術與程序，皆有深入的了解。

服務一覽

「紅隊演練」練習環境中包含真實的、無所不用其極的攻擊情境。Mandiant 紅隊演練會採取任何非破壞性的必要手段，模擬攻擊者的行為，完成一系列共同制定的工作目標。紅隊演練逼真地模仿實際攻擊者，使用近來實際事件回應接觸所見的 TTP，主動在暗中發動攻擊。此舉能評估您資安團隊偵測和回應主動攻擊者案例的能力。

目標範例		
竊取主管或開發人員的電子郵件	入侵含有業務關鍵資訊或機密資料的區段環境	取得自動化裝置的控制權，例如:物聯網裝置、醫療器材或生產設備

方法

「紅隊演練」先從共同決定紅隊是否應對您的環境有所了解而開始。Mandiant 應用產業經驗以識別代表您核心業務功能主要風險的目標。

「紅隊演練」遵照攻擊攻擊循環階段加以應對。

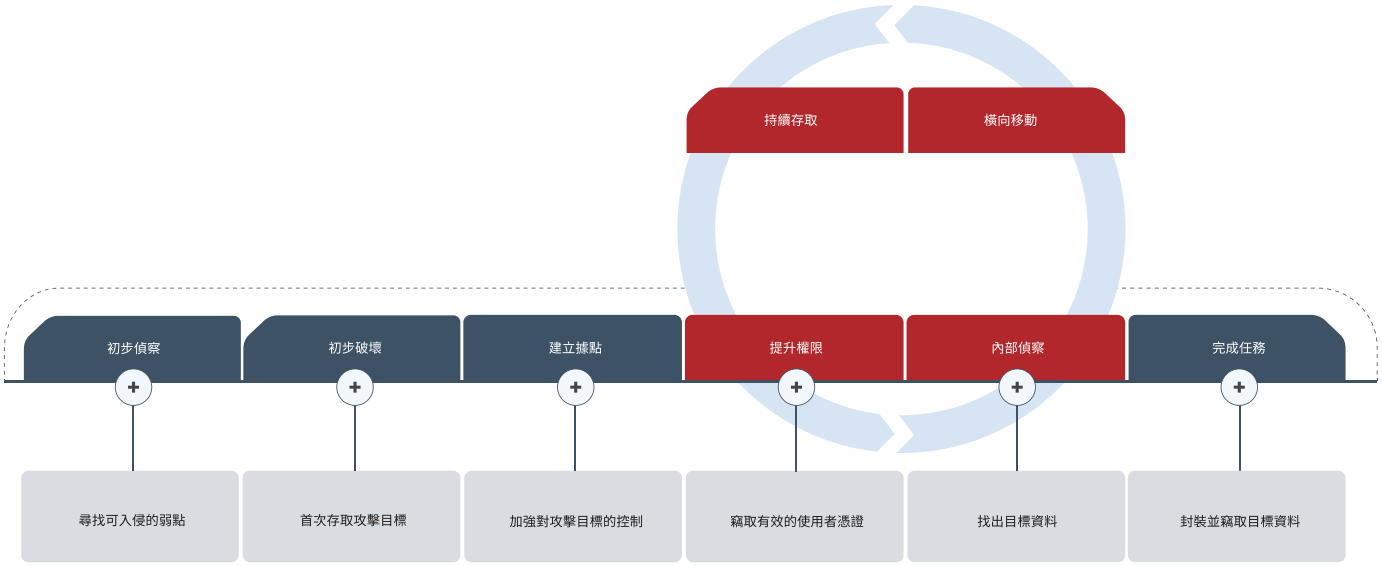

圖 1. 攻擊週期。

在設定目標後，紅隊演練開始進行初步勘查。Mandiant 採用獨家情報存放庫與開放源情報 (Open-Source Intelligence, OSINT) 工具與技術兩者結合，以執行目標環境的勘查。

Mandiant 會透過入侵弱點或進行社交工程攻擊，以獲得目標環境的初步存取權。Madiant 利用現實世界攻擊者所使用的技術，以獲得這些系統的特殊存取權限。

在獲得存取權後，紅隊演練會升級特權以透過部署命令和控制基礎設施，建立和維護環境內的持續性，就如同攻擊者會做的一樣。

在環境內建立持續性並命令和控制系統後，紅隊演練會試著透過任何必要的非干擾性方式來完成目標。

為何選擇「紅隊演練」

「紅隊演練」適合推薦給有以下需求的企業：

- *試驗偵測與回應功能*。為現實世界會發生的資安事件所預備的安全團隊，但您需要確認他們可以適當地對事件做出回應—而不會帶來真正的風險。
- *引起注意並展示影響*。Mandiant 紅隊演練會像現實世界的攻擊者一樣行動，努力透過僅可在網隊網路上使用的資料，從網際網路上入侵您的作業環境。成功的紅隊演練應對可以幫助調整漸增的資安預算，並找出需要進一步投資的缺口。

您可獲得的好處

- 給執行團隊和高層管理團隊的摘要
- 包含詳細逐步說明的技術詳細資料，讓您可重現我們的發現結果
- 根據事實所做出的風險分析，讓您瞭解重要發現與您的環境息息相關
- 可立即看到成效的策略建議
- 可帶來長期成效的策略建議
- 處理過實際事件的寶貴經驗，讓您不再有因入侵事件成為頭條焦點的壓力

要知道更多關於 FireEye，請前往：**www.FireEye.com**

FireEye Taiwan | 台灣火眼有限公司
| 10683 臺北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE /
taiwan@FireEye.com

關於 FireEye, Inc.

FireEye 是一間情報主導的資安公司。FireEye 以流暢、可擴充的客戶資安作業延伸，提供了混合創新資安技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平臺。藉由此方法，FireEye 得以讓對於準備、預防及回應網路攻擊感到苦惱的組織，消除資安機制的複雜性和重擔。