FIREEYE™

產品型錄

勒索軟體防禦評估

優點

- 識別受勒索軟體影響風險較大的資產
- 識別勒索軟體針對的資安漏洞
- 識別對檔案共用的寬鬆存取權限監控
- 認識勒索軟體任務管理中的操作缺陷
- 接受高度可行的建議和指導，以緩解勒索軟體攻擊

為何選擇 FireEye Mandiant

FireEye Mandiant 自 2004 年以來就站在網路安全與網路威脅情報的最前線。我們的資安事件回應團隊站在全球最複雜入侵事件的最前線。透過利用對手、機器和受害者的綜合情報資源，我們對威脅實施者及其快速變化的戰略、技術和程序 (tactics, techniques and procedures, TTPs) 有著深刻的理解。

勒索軟體防禦評估是根據對勒索軟體事件的回應和補救，以及收集有關新興和不斷發展的勒索軟體威脅情報的豐富經驗而開發的。

概觀

FireEye Mandiant 勒索軟體防禦評估主要評估組織在預防、偵測、阻止和補救勒索軟體攻擊方面的能力之有效性。Mandiant 專家將評估您的資安計畫中的技術和非技術元素，來確定您的團隊如何回應勒索軟體攻擊。

Mandiant 專家將評估勒索軟體攻擊可能對您的內部網路造成的技術影響，發現哪些資料可能受損或遺失，並測試您的資安監控措施在偵測和回應勒索軟體攻擊方面的能力的優點和缺點。

方法

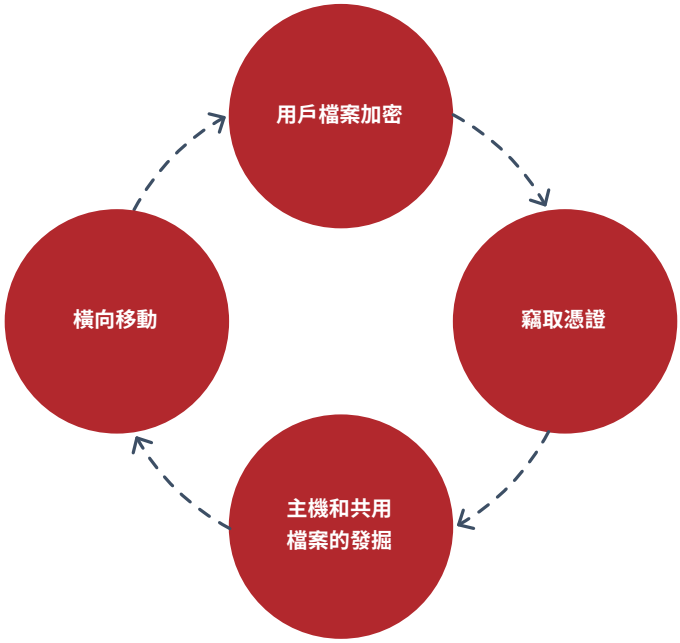
勒索軟體防禦評估包括文件審查、日誌記錄設定分析、深入式研討會以及模擬真實場景的勒索軟體攻擊行為。

勒索軟體防禦評估專注於勒索軟體的四大核心能力：

- **資安架構。**防禦勒索軟體攻擊，並保持業務營運連續性所需的資安技術、監控和網路。
- **回應。**組織快速回應，並阻止勒索軟體攻擊的能力。
- **溝通。**向主要利益相關者傳達公司資訊的內部和外部溝通流程。包括與網路保險和法律顧問的協調。
- **恢復。**補救或從勒索軟體攻擊中復原的過程和方法。

我們將模擬真實場景的勒索軟體攻擊行為：

- 掃描可能被勒索軟體攻擊的 Windows 漏洞。
- 掃描可能被勒索軟體存取的可存取之共用文件。
- 嘗試探討發掘的漏洞或重複利用竊取的憑證，來模擬勒索軟體的橫向移動。
- 測試網路間的分割，來確定勒索軟體是否可以傳播到其他環境，例如：
  - 製造和工廠網路
  - 備份基礎設施網路
  - 零售網路
  - 其他資安網路
- 利用自訂的非破壞性勒索軟體模擬工具來模擬大量加密檔案，從而模擬勒索軟體的加密行為。
- 執行威脅實施者用來部署勒索軟體的技術。



持續時間和可交付之成果

勒索軟體防禦評估通常需要一週時間。可在內部部署或遠端進行。

評估之後，Mandiant 將會列出一份報告，其中包括：

- 執行摘要，包括優點和需要改進的地方。
- 關於測試過程的技術資訊。
- 詳細的發現結果（按嚴重性分類）。
- 執行簡報。

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

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

M-EXT-DS-US-EN-000285-01

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，消除其資安機制的複雜性和重擔。