FIREEYE™

產品型錄

沙盤推演

透過模擬情境遊戲評估您的網路事件回應計畫

優點

- 與實際發生的狀況作比較，找出訂定和預期回應之間的差異。
- 根據現實世界的事件回應的最佳作法提供建議。
- 快速、有效、非入侵式的評估。

「能夠對資安事件作出有效率且有效的回應，對我們企業來說十分重要。桌上演練是十分珍貴的機會，這為團隊提供了驗證決策和參與討論的方法。」

-Global Technology Distribution 公司，資訊安全長

為何選擇 FireEye Mandiant

FireEye Mandiant 自 2004 年以來就站在網路資安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。我們對現有和新興的威脅發動者以及他們快速變動的戰略、技術與程式，皆有深入的瞭解。

沙盤推演會利用這項專長，提供以現實世界經驗為藍本的自訂案例片段，其目的是要解決您在關鍵業務及技術領域的風險。

概觀

桌上演練會從管理策略及技術事件回應的角度，評估您組織在應對網路攻擊方面的網路危機程序、工具及熟練程度。在每次演練過程中，Mandiant 顧問們會在圓桌上，引入以現實世界經驗為藍本的多個案例片段，以觀察組織回應的模擬行動與決策。

方法

在開始沙盤推演之前，Madiant 專家們首先會對組織的威脅檔案、作業環境以及特別的關注事項進行瞭解。我們會與關鍵人員進行現場研討會，並根據我們在事件回應工作期間所觀察到的攻擊者的行為、技術和手法建立演變性的案例片段。

我們會在推演時觀察遊戲玩法，以決定模擬行動和決策與組織訂定的計畫和程序與由 Mandiant 專家們所識別的事件回應最佳作法是相同還是相異。

您可獲得的好處

執行概要 [PPT]

- 針對遊戲玩法的面對面概觀說明，內容特別針對：
  - 參與者與事件回應計畫 (Incident Response Plan, IRP)、通訊計畫和呈報程序的互動
  - 汲取的經驗教訓
  - 策略建議

桌上演練後續行動報告 [PDF]

- 事件時間軸
  - 所有片段
  - 利害關係人/參與者回應
- 策略網路事件回應分析，以及遊戲玩法的相關改善建議，會以下列幾項來分類：
  - 偵測
  - 回應
  - 遏制
  - 修復

追踪

我們提供兩種沙盤推演追踪：**技術事件回應**和**執行危機管理**。最佳實踐要求每年要執行一次，追踪一單獨或作為協調演練的一部份。

技術事件回應追踪非常適合資安團隊管理和希望測試回應過程功能的人員。

對於想要測試其危機策略有效性的高層管理人員來說，執行行政危機管理 (Executive Crisis Management) 追踪是理想的選擇。

在研討會後，我們親自向組織進行了簡要介紹，並提供一份書面的「演練行動後續報告 (After-Action Report)」，其中包含案例片段和回應的逐步說明摘要。

服務追踪比較

服務追踪	技術	執行
目標	評估並分析組織技術回應能力，以偵測、回應並遏止進階威脅。	透過管理團隊的視角評估並分析在進階威脅事件發生時，組織的危機管理能力。
參與時間	• 規劃：1 星期 (異地) • 模擬情境遊戲：1 至 2 天 (現場) • 最後回報：1 星期	• 規劃：1 星期 (異地) • 模擬情境遊戲：1 至 2 天 (現場) • 最後回報：1 星期
目標參與者	• 網路資安事件回應團隊 (CSIRT) • 資安主管 • 技術人員 (如：使用網路、伺服器和電子郵件使用者)	• 資訊安全長 (CISO) • 一般高級主管 • 公共關係與企業傳播 • 總法律顧問
重點領域	• 何時要隔離網路上的主機 • 何時要重灌系統映像檔 • 分析人員應如何遵循已定義的 IRP、傳播方案和升級矩陣 • 何時以及如何接觸第三方廠商	• 何時應支付敲詐勒索或勒索威脅 • 有關遏制影響的策略決策 • 監察機關與重要利害關係人的入侵披露需求 • 客戶通知最佳實踐 • 媒體通訊最佳實踐
傳遞方法	現場模擬情境角色扮演	現場模擬情境角色扮演

要知道更多關於 FireEye，請參閱：**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

關於 FireEye, Inc.

FireEye 是一間情報主導的資安公司。它作為客戶資安監控的無縫、可擴展的延伸，提供單一平台，FireEye 將創新的資安技術、國家級別的威脅情報和世界知名的Mandiant® 諮詢融合在一起。藉由此方法，FireEye 為努力準備、預防和應對網路攻擊的組織，消除資安機制的複雜性和重擔。

FIREEYE™