MANDIANT®

產品型錄

資安入侵評估

在您的環境中辨識現今或過去的攻擊者活動

為什麼選擇 MANDIANT 解決方案

Mandiant 解決方案自 2004 年以來就站在網路資安與網路威脅情報的第一線。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。

優點

- 對您特定環境的全面分析，將焦點放在尋找現在或過去入侵的證據
- 提供對系統性風險與風險暴露的見解
- 辨識資安意識問題
- 對於增進您組織的能力，為有效回應未來事件提供建議
- 可有彈性地在地部署或以雲端託管技術部署

在我們現有的資安狀態中，資安入侵是無法避免的。

— Kevin Mandia
FireEye 執行長

Mandiant 入侵評估結合了我們應對進階威脅行為者入侵行動所做回應的豐富經驗、領先業界的威脅情報以及 FireEye 的技術，以提供一種符合下列條件的評估：

- 辨識在您組織中現在或過去的入侵事件
- 透過找出在資安架構、漏洞、不適當使用或違反政策和系統不當設定的弱點，來評估風險
- 增加您組織對未來入侵事件有效回應的能力

入侵評估的需要

在新聞報導中知名的入侵事件僅呈現出全球入侵活動的一小部分而已。了解您的組織是否已經被入侵，並確定降低風險的方法，對於防止您的組織成為下一個重大數據洩露的頭條新聞至關重要。

我們的作法

我們結合了回應入侵的豐富經驗與領先業界的威脅情報以及 FireEye 的模組化堆疊，以提供符合您速度、規模和效率的企業目標之評估。除了辨識過去或持續攻擊活動的證據外，本評估還提供：

從威脅情報擷取出背景資料
提供攻擊者屬性與動機的深入見解，以便讓組織了解他們是否為其目標。

辨識風險
辨識資安性架構與配置的弱點，包含遺失的修補程式或資安軟體。

未來投資的協助
可以讓您組織的資安團隊對入侵回應做出更好的預備策略選項之建議。

Mandiant 顧問使用 FireEye 技術搜尋端點威脅、監視網路流量、偵測電子郵件，並從其他資安裝置分析日誌，以找尋攻擊者活動的證據。顧問也使用無特徵碼資料分析技術，找尋之前不為人知的攻擊者活動。客戶選擇針對他們環境使用的最合理、正確的技術組合。

- 端點威脅偵測：FireEye 端點威脅防禦程式對於攻擊者活動提供實時偵測，包含惡意軟體及其他攻擊手法、技術和程序，並偵察 Windows、macOS 和 Linux 端點威脅。Mandiant 專家提供現場和雲端部署的靈活調度。
- 網路偵測：FireEye Network Security 網路資安偵測器部署在您的企業中以進行戰略性監控，偵測如惡意軟體命令與控制通訊、未授權遠端存取和資料竊取這類入侵活動。
- 電子郵件偵測：FireEye Email Security 在現場或雲端進行監控，並可設定偵測輸入與輸出的電子郵件。附檔的動態偵測允許 Mandiant 專家在其他特徵碼產品前辨識到入侵活動。
- 日誌偵測：Mandiant 顧問利用多項技術以檢視來自應用程式和基礎架構的日誌，來辨識惡意活動。

端點威脅偵測

- 對正在進行的惡意或可疑的活動發出即時警報
- 使用 FireEye 代理程式內建的防毒引擎偵測商業惡意軟體
- 跨平台作業系統支援
  - Windows
  - macOS
  - Linux
- 辨識可以指明進階惡意軟體出現的異常現象

網路偵測

- 完整封包擷取結合自訂偵測特徵碼
- 自動偵測並解碼攻擊者的命令並控制流量

電子郵件偵測

- 偵測在修復事件後，攻擊者用來重新獲得環境存取權的目標性網路釣魚攻擊事件
- 利用無特徵碼的 Multi-Vector Virtual Execution™ (MVX) 引擎，針對作業系統、應用程式及網站瀏覽器等全面的交叉矩陣上分析電子郵件附件及 URL
- 支援分析—用來針對 Microsoft Windows 及 macOS 作業系統圖示
- 分析隱藏在檔案中的威脅，包括有密碼保護及加密的附件

若要深入瞭解 Mandiant 解決方案，請參訪：**www.FireEye.com/mandiant**

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 Mandiant 解決方案
Mandiant 解決方案聚集了世界上領先的威脅情報和一線專業知識，並用持續的資安驗證來為組織提高資安效益和提供減少業務風險所需的工具。

MANDIANT®

M-EXT-DS-US-EN-000010-03