

產品型錄

事件回應服務

迅速、大規模且有效率地調查、遏制並修補重大資安事件



案例研究： MANDIANT IR 實務

某間在全球部署數萬台電腦的跨國專業服務公司聯絡 Mandiant，希望對可能外洩的重要客戶資料採取應變措施。

第 1 天 - Mandiant 的顧問在接到通知的 4 小時內，開始著手部署雲端威脅防護技術到 18,000 個端點。

- 調查亦於同一天開始。
- 調查開始 4 小時後，發現入侵的確切證據。

第 6 天 - 大部分調查工作皆已完成。分析的端點威脅超過 18,000 個，並對 80 個系統進行深入即時回應分析。

第 7 天 - 在不干擾業務的情況下進行遏制作業。Mandiant 的專家持續監控網路，以確保威脅發動者不再嘗試入侵。

第 11 天 - 客戶回復正常營業。

所有工作皆在遠端進行。

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。

我們具備豐富的調查和修補相關專業知識，靠的便是運用領先業界的 FireEye 威脅情報和尖端的 FireEye 網路與端點威脅防護技術來回應數以千計的事件。

Mandiant 處理很多則重大、具知名度的事件，因而具備獨一無二的專家優勢，能協助客戶因應事件，針對各個層面的回應工作，不論是技術應變乃至於危機管理，全面涵蓋。

我們可協助客戶更快更有效率地調查事件並加以修補，讓他們能繼續專注在最重要的事務上——也就是他們的業務。

概觀

使用雲端和內部部署解決方案，可在處理客戶資料隱私疑慮的同時，立即展開調查。只要幾個小時，Mandiant 事件回應人員就能從數千個端點開始分析網路流量和資訊。Mandiant 從攻擊研究的第一線和其他情報來源取得的威脅情報量相當龐大，讓 Mandiant 的事件回應團隊得以擁有最新的攻擊者策略、技術及程序 (TTP) 資訊。

Mandiant 的專家瞭解完善的事件和入侵回應機制，並不能只靠技術調查、遏制及復原工作達成。因此，我們在主管溝通和危機管理方面給予協助，這包括法務、監管及公關部門的考量。危機管理對控制聲譽損害和法律責任至關重要。

表 1. 我們通常處理的事件類型。

竊取智慧財產	竊取商業機密或其他機密資訊。
金融犯罪	竊取付款 / 信用卡資料、非法的 ACH/EFT 現金轉帳、勒索軟體。
個人識別資訊 (Personally identifiable information, PII)	用以識別個人的獨有資訊外洩。
受保護的醫療保健記錄 (Protected Health Information, PHI)	受保護的醫療保健資訊外洩。
內部威脅	員工、廠商或其他內部人士的不當或非法活動。
破壞性攻擊	單純使資訊或系統無法回復，意圖造成受害組織困擾的攻擊。

MANDIANT 的獨到之處

- **調查經驗：**Mandiant 進行過各種全球最大規模且最複雜的調查，並修復其造成的損害，旗下的調查人員因而練就一身出色的調查技巧。
- **威脅情報：**從事件回應、透過第三方數據資源進行廣泛的攻擊者交易工具的發現和研究、由 FireEye 技術人員與其他 FireEye Threat Intelligence 資源所收集的 FireEye Dynamic Threat Intelligence 的第一線所組成的領先業界的情報。
- **技術：**Mandiant 的專家使用最新的 FireEye 雲端和內部部署技術，能立即展開調查。我們的技術可在更大的範圍內快速回應—提供執行 Microsoft Windows、Linux 和 macOS X 系統的網路流量與端點的可見性。
- **危機管理：**事件回應人員擁有多年經驗，能就與事件相關的溝通事宜給予客戶建議—包括主管溝通、公關及揭露要求。
- **惡意軟體分析：**FireEye 反向工程師分析惡意軟體並編寫自訂解碼器和解析器，以深入瞭解攻擊者使用的功能和 TTP。
- **全天候無休的事件回應防護：**在 FireEye Managed Defense 提供調查和補救期間，會全天候提供攻擊者活動分析。

我們的作法

Mandiant 的調查包含了以主機、網路和事件為主分析，以便通盤評估整體環境。我們會為客戶量身制定應變行動，以協助客戶回應事件並從中復原，同時因應法規要求並處理聲譽受損事宜。在調查期間，Mandiant 的顧問通常會找出：

- 受影響的應用程式、網路、系統及使用者帳戶
- 惡意軟體和遭入侵的弱點
- 遭竊或被存取的資訊

事件分析

1. **技術部署 / 調查最初線索：**部署最適當的技術，以快速而全面地回應事件。我們也會同時調查客戶一開始提供的線索，以建立入侵指標 (Indicators of Compromise, IOCs)。IOCs 可在清理環境檢查所有惡意活動指標時，從中找出攻擊者的活動。
2. **危機管理規劃：**與高階主管、法務團隊、業務主管以及資深資安人員合作，擬定危機管理計劃。
3. **事件範圍評估：**即時監控攻擊者的活動，並搜尋過去攻擊者活動的鑑識證據，以判斷事件的範圍。
4. **深入分析：**分析攻擊者採取的行動以確定最初的攻擊媒介、建立活動時間軸，並辨別入侵程度。這可包含：
 - 即時回應分析
 - 鑑識分析
 - 網路流量分析
 - 記錄分析
 - 惡意軟體分析

5. **損害評估：**找出受影響的系統、設施、應用程式及外洩的資訊。

6. **修復：**依據攻擊者的行動以及業務需求，擬定遏制與修復策略，以消除攻擊者的存取權限，並改善環境的資安性狀態，以預防或限制日後攻擊造成的損害。

產出成果

經得起第三方檢驗的執行、調查及修復報告。

- **執行摘要：**說明時機和調查程序、重大發現及遏制 / 資安防護活動的概略摘要。
- **調查報告：**詳盡說明攻擊時間軸和關鍵路徑 (攻擊者在環境中的操作方式)。調查報告包含一份清單，其中列出受影響的電腦、位置、使用者帳戶，以及遭竊或有風險的資訊。
- **修復報告：**詳盡說明採取的遏制 / 資安防護措施，包括加強組織資安性狀態的策略建議。

懷疑可能發生事件？請傳送電子郵件至：investigations@mandiant.com 或造訪 <https://www.fireeye.com/company/incident-response.html>

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

© 2019 FireEye, Inc. 保留一切權利。FireEye 為 FireEye, Inc. 的註冊商標。所有其他品牌、產品或服務名稱均屬各擁有人之商標或服務標記。
M-EXT-DS-US-EN-000004-04

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。

