MANDIANT®

產品型錄

Microsoft 365 資安評估

重點

- **減少**常用錯誤設定
- **減少** Microsoft 365 攻擊面
- **深入**瞭解與現有設定相關的最緊迫資安風險
- **增強**監控、可見性和偵測
- **優先**考慮增強安全性

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。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。

概觀

隨著資料向雲端遷移，涉及雲端平台和服務的資安事件明顯上升。Microsoft 365 因其受歡迎程度和其代管的珍貴資料而成為高度針對的目標。存在漏洞的 Microsoft 365 租用戶使攻擊者可以遠端存取雲端的敏感性資料，而無需滲透企業內部。威脅實施者可透過利用或攻擊以下方面存取 Microsoft 365 租用戶：

- 脆弱或舊的認證機制
- 未經過優化設定的資安管控
- 具有存取權限等級的帳戶
- 密碼較弱的帳戶或不需要多因素身分認證的帳戶

識別和降低 Microsoft 365 中的風險

Mandiant Security Assessment 的 Microsoft 365 資安評估是根據應對威脅實施者攻擊和存取 Microsoft 365 租用戶的事件的豐富經驗而開發的。透過主動檢閱和減少常見錯誤設定、程序漏洞和攻擊方式，組織可以降低總體風險，並確保針對 Microsoft 365 租用戶發生的事件提供最佳的保護和可見性。

評估的基礎包括短期遏制和長期補救資安管控以及消除租用戶攻擊者所需的設定。

我們的作法

Mandiant 資安評估將評估六個核心重點領域中的常見的 Microsoft 365 身分認證平台和存取控制：

- 資安架構和強化
- 身分和存取管理
- 可視性
- 資料防護
- 災害復原
- 威脅偵測與回應

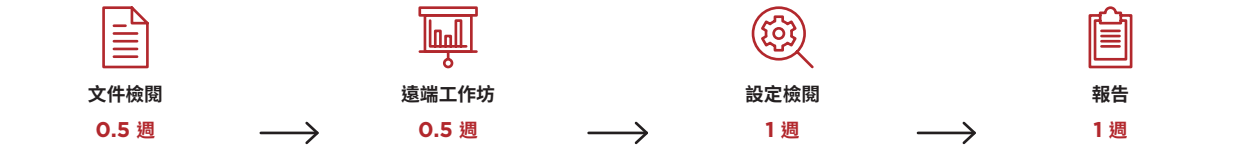
常見的認證平台

常見的存取控制

核心重點領域

評估持續時間

Microsoft 365 資安評估一般會花費三週時間，包含 4 個步驟。Mandiant 顧問執行以下活動：



包括對與存取 Microsoft 365 租用戶相關的遷移策略、電子郵件設計和體系結構文件、強化文件、日誌記錄標準以及行動裝置管理 (MDM) 設定的異地檢閱。

與客戶的主要利益相關者合作，針對每個核心重點領域舉行一系列遠端工作坊。

對 Microsoft 365 租用戶進行徹底的設定檢閱，以確保根據強化、安全性和保護性指導對資安設定進行優化。

詳細列出實用技術建議的報告，以強化 Microsoft 365 租用戶，增強可見性和偵測能力，並改進程序以降低雲端租用戶和相關基礎架構受到漏洞攻擊的風險。

產出成果

互動結束後，Mandiant 專家將提供一份詳細的報告，其中包括：

- 現有 Microsoft 365 租用戶資安設定的快照。
- 特定的 Microsoft 365 最佳安全實踐，與目前設定和運維程序保持一致。
- 增強可見性和偵測能力的實用建議。
- 進一步強化 Microsoft 365 租用戶資安態勢的優先和詳細建議。

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-000208-02