MANDIANT

MANDIANT ADVANTAGE
資料工作表

攻擊面管理

競爭優勢

攻擊面管理提供完整的資產探索與風險緩解，讓您能安全地採用能加速創新的新技術與流程。貴組織可以透過以下優勢更具競爭力：

- 支援遠距混合工作
- 保護周邊設備
- 擴充至大型環境
- 管理雲端與影子 IT
- 將管理內嵌至工作流程中
- 建立供應鍊恢復能力
- 將安全性原則擴展到企業之外

以攻擊者的視角觀察自己

IT 環境的設計天生就是動態的。透過雲端運算、不安全的網路、SaaS 部署、容器、微服務、IoT 設備、應用程式、基礎設施與資料等有機地發展，且通常在不遵守組織安全政策的情況下加入。遺留的擴展、孤立的基礎設施與日益分散的勞動力是永遠存在的複雜問題。

即便使用自訂工具，安全團隊也無法輕易看到其快速擴大的攻擊面全貌，並解決其挑戰。Mandiant Advantage 攻擊面管理是 Mandiant Advantage 平台的一個模組，結合了擴充的企業可見性與持續監控功能，以及最新的 Mandiant Advantage 威脅情報，可以幫助組織發現暴露並分析在現今動態、分散式與共享環境中的網際網路資產。

完整的擴充式企業可見度

攻擊面管理讓網路安全團隊透過攻擊者的視角，以完整真實的方式檢視自己的環境。這個模組能操作攻擊者情報，以將安全程式從被動模式轉變為主動模式。

攻擊面管理能在現今動態、分散式且共享的環境中，發掘並分析網際網路資產。此模組透過啟用圖形的映射生成全面的擴充式企業可見度，而該映射能闡釋資產、發出風險警報，並使安全團隊能夠以難以置信的速度與敏捷性操作情報。攻擊面管理能辨識基礎設施整體中的業務關係，並透過對已知與未知資產的全面可見度來移除擴展。因此能讓網路安全團隊盤點其資產，並調查任何已發掘的暴露。

在雲端時代之前設計的工具僅能支援靜態工作位置以及在網絡防火牆後運行的有限設備與應用程式集。攻擊面管理建置的目的是為了支援最苛刻的安全團隊的動態分散式 IT。

持續暴露監控

讓網路安全團隊能夠監控並評估資產與基礎設施，包括軟體堆疊與配置。攻擊面管理能即時偵測變更與暴露，在建立安全的雲端採用與數位轉型的同時，辨識出可被入侵的弱點。此模組能幫助網路安全團隊快速理解已發掘的資產威脅與其他風險，以便對其進行分類。

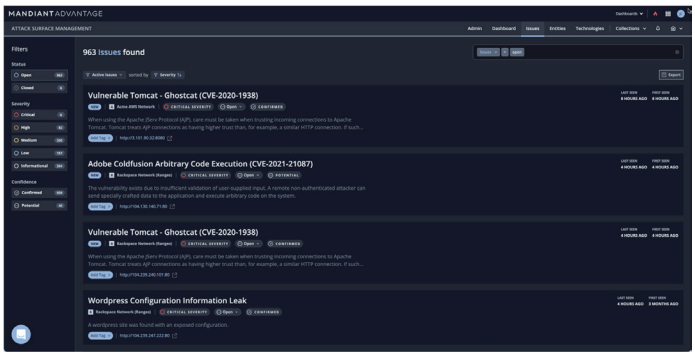

圖 1. 分析資產以偵測漏洞、評估暴露並減輕風險。

操作專業知識與情報

賦能安全操作，減輕真實世界威脅。Mandiant 專家的專業知識與威脅情報會自動套用至攻擊面，用以確定已暴露的部分並持續監控風險。此模組整合了目前的工作流，並在環境中加入了新資產時通知網路安全團隊，並在出現任何暴露時發出警告。

圖 2. 在全球最重要的威脅情報與專業知識的支持下，隨著時間的推移管理攻擊面的變化。

統計資料

攻擊面管理包括：

- 超過 250 種可用整合：與資料來源和發掘技術整合
- 超過 30 種分類資產類型：整個生態系統中廣泛的資產可見度
- 超過 6 萬種已辨識的技術：深入分析技術與配置
- 包含超過 1 萬種漏洞：從主動威脅與錯誤配置中探索漏洞

結果

使用了攻擊面管理的組織可以從多種高價值結果中獲益：

- **透過基於圖形的映射實現完整可見度：**使用多種整合與技術發掘資產與雲端資源，並辨識合作夥伴與第三方關係。檢視暴露在外的資產組成、技術與配置。
- **持續資產監控，以預防威脅：**即時監控基礎設施以偵測變更與暴露，同時打造雲端採用與數位轉型的安全網路。
- **賦能安全操作，減輕真實世界威脅:**自動套用 Mandiant 專業知識與情報，以便檢視攻擊面的已暴露區域。

請在 www.mandiant.com 上瞭解更多

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703)935-1700
taiwan@mandiant.com

關於 Mandiant
自 2004 年起，Mandiant® 就一直是具有資安意識之組織值得信賴的合作夥伴。如今，產業領先的 Mandiant 威脅情報與專業知識所推動的動態解決方案能幫助組織制定更有效的計畫，並增強其對網路準備度的信心。

MANDIANT®
YOUR CYBERSECURITY ADVANTAGE

S-EXT-DS-TW-ZH-000415-02