McAfee Investigator

讓分析人員搖身一變，成為專業調查人員

McAfee® Investigator 可協助分析人員判斷出根本原因，以更高的信心在更短時間內解決更多案例。分類警示能觸發由專家主導的探索，以收集支援資料、解讀證據；並提供所需的深入見解，以完整快速地驗證威脅並加以回應。

安全營運挑戰

大型事件容量和資料存留時間問題，會讓準確存取警示的重要資訊和範圍之難度增加。在缺乏背景知識，無法判斷警示是否應作為正常事件處理的情況下，分析人員經常會忽略警示內容。

任何特定事件的調查，都需要花費長時間並且具備與威脅媒介相關的實際專業知識，才得以深入挖掘問題核心。在此需求趨勢下，專業安全營運分析人員的需求便與日俱增；然而，目前的人才數量仍難以因應。

全新調查式分析

如要應付這個問題，安全營運團隊必須簡化並加快警示分類和調查，讓現有的員工和新進分析人員事半功倍。

McAfee Investigator 會啟用包含分類、全面資料收集和進階分析的引導式調查功能，供每個安全營運團隊使用。作為 SaaS 服務，專業系統和端點擷取工具會與現有的資料來源與安全性管理系統整合，以加快創造價值和提升工作效率。

此類互動式分析會提供持續更新的引導，使事件應變人員能在更短時間內，以更快的速度和更高的精準度完整調查惡意軟體、網路威脅及入侵指標 (IoC)。

以機器速度探索深入見解

McAfee Investigator 可允許安全性作業針對特定狀況自動排定優先順序，使狀況獲得立即關注，進而得以迅速分類。針對分析人員所需探索的此類警報和其他警示，McAfee Investigator 會收集、組織、彙總及視覺化從可疑攻擊上所取得的警示、活動、證據和情報。

主要優點

- **縮短暫留時間：**周密的案例資料探索可提升偵測根本原因的效率，並減少事後修補症狀的需求。
- **從提出警示轉變為處理案例：**減少花費在手動和低優先順序之調查的時間。
- **專注於未知：**鎖定於需要人工解譯和判斷的特殊產物和分析。
- **改善分類：**以更高品質提升處理更多案例的速度。
- **減少分析人員工作負載：**適當運用有限時間、體力及認知能力。
- **建立分析人員技能：**指導手冊和相關分析能教導分析人員如何於工作流程期間，瞭解真正的問題與提出適當的假設。
- **延伸目前系統價值：**增強現有資料來源和分析資訊，以增進系統精準度。

相關資料會在背景中收集，且其中僅包括會觸發決策之特定威脅調查的重要資料。安全性資訊與事件管理 (SIEM) 解決方案的資料，可透過端點資料擴充，無需在各節點使用端點偵測與回應 (EDR) 代理程式。此模型可讓您深入掌握各入侵指標、手法、技術、程序和關聯性的所有脈絡，藉此取代孤立的作業方式。

資料分析和機器學習引擎，會將證據資料與已知基準和威脅情報來源進行比對。此引擎將會處理所獲得之比對結果，並針對重要可疑項目提高分析等級。

透過自動收集與排定適當資料的優先順序，McAfee Investigator 可提升作業效率與工作速度，使分析人員能夠判斷事件的風險和緊急程度。分析人員可更快速精準判斷分類，進而專注處理最重要的威脅項目。

提升為組織等級，大幅增進效益。藉由將警示檢閱分類升級為情境案例，讓各個分析人員更有效率進行作業，使第 1 層分析人員能處理更多案例，並將分析時間花費在高價值活動上。

以專業知識引導調查進行

如果分析人員必須以詳細方式調查某事件，則可運用互動式指導手冊，使分析人員能在調查和評估期間專注於重要項目。互動式指導手冊並非以指令碼為基礎或靜態呈現。系統會仿效人類思維程序，以最大速度和精準度同時探索多個假設。

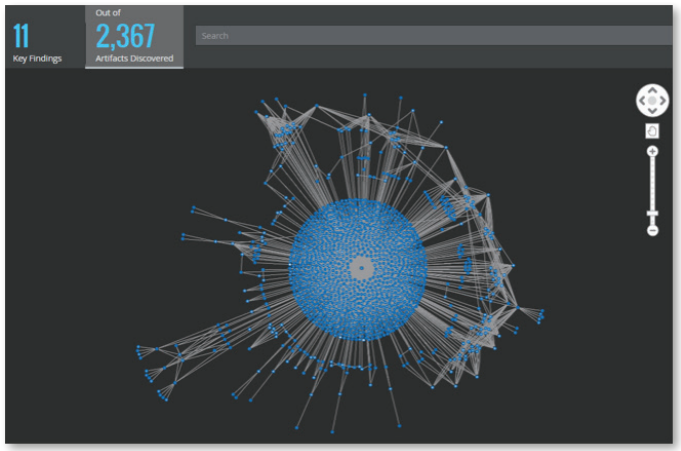

圖 1. McAfee Investigator 能收集上千筆證據資料。

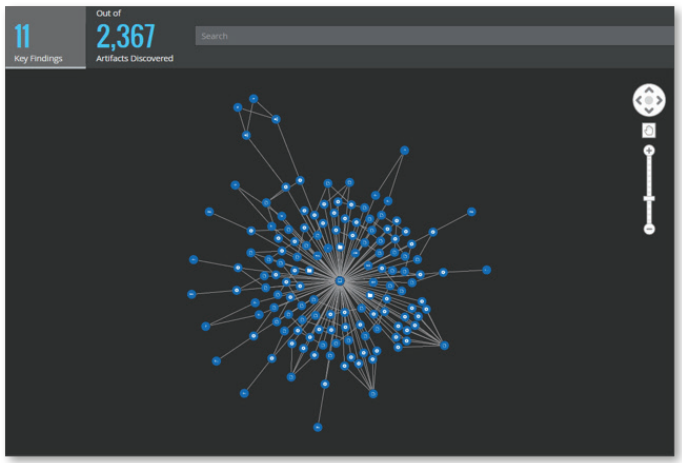

圖 2. McAfee Investigator 會接續套用專業分析與指示，以顯示重要調查結果。

主要功能

- 準確的按指定資料收集
- 暫時的端點收集代理程式
- 根據專業知識與人工智慧解讀所收集之資訊
- 互動式視覺呈現畫面
- 透過多媒介假設探索類似資料
- 機構情報的基準
- 案例管理可指示員工，並啟用調查期間的資訊共享功能

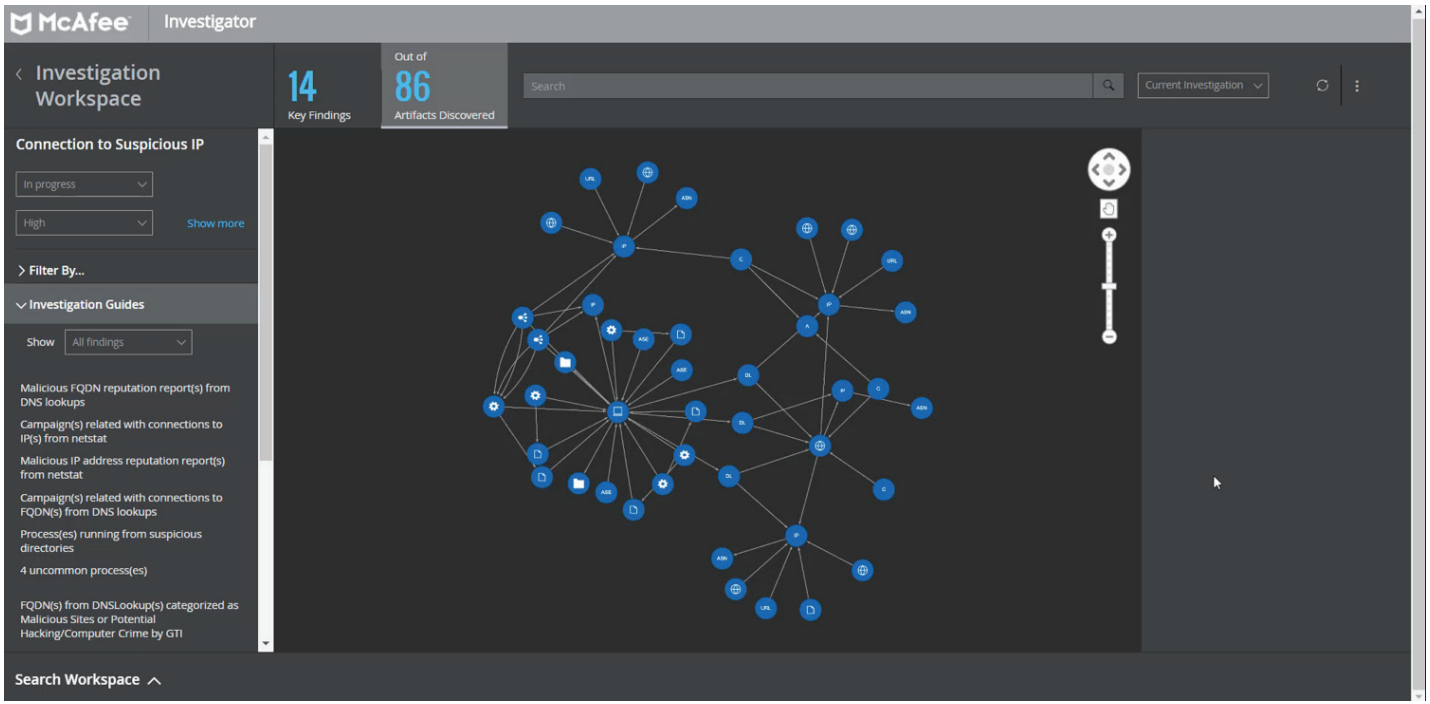

圖 3. 此工作區可明確顯示重要調查結果，並可輕鬆探索。

這本可供人類閱讀的指導手冊為結合 Foundstone® 研究人員的專業知識與人工智慧所建置而成。這是 McAfee Investigator 體現人機合作的其中一種方式。

其工作區可建立案例的結構分析與調查結果，藉此協助分析人員指出問題真正所在。這項集中式多媒介探索功能，可讓分析人員更有信心找出根本問題，以協助有效精準解決案例。

擴展專業知識和能力

McAfee Investigator 的互動式工作區會透過單一認知環境內的資料，來提示工作流程與導覽方式。此模型可提高效率、減少多種警示類型所產生的氾濫資訊，並免除檢閱多個畫面的需求。

此工作區可訓練新進和中階分析人員，使其以進階分析人員的思維流程來處理案例，進而建立技能，且無需進行個別培訓。

根據現有工具與資料建立分析

McAfee Investigator 可與 SIEM 和 McAfee® ePolicy Orchestrator® 軟體搭配運用，將進階分析新增至現有的資料來源、基準、關聯及警示。這款暫時的代理程式能收集更新的端點資料，特別有助於精準解讀細微證據。整合 McAfee Investigator 和 McAfee Active Response 可讓分析人員即時評估威脅在端點中的影響力。活動摘要會與第三方工具分享資料，以處理目前工作流程、簡化程序並提升協同合作能力。專家服務可加快入門速度，確保能順利啟用。

深入瞭解

一旦發生任何可疑事件，有了 McAfee Investigator 的協助，您無需再花費數小時收集資料，甚至更長時間解讀資料。McAfee Investigator 具備先進的分析引擎，可在情境化介面內針對威脅警示進行檢查與分類，以調整安全性作業。McAfee Investigator 可在安全營運中心調查期間自動運用專業知識，使您的分析能以更聰明、快速且精準的方式發揮作用。

這就是所謂人機合作的具體示現。

若要深入瞭解，請造訪 **www.mcafee.com/tw/products/investigator.aspx**。

台灣
台北市信義區忠孝東路五段 68 號 29 樓，11065
電話：+886 2 8729 9222
www.mcafee.com/tw