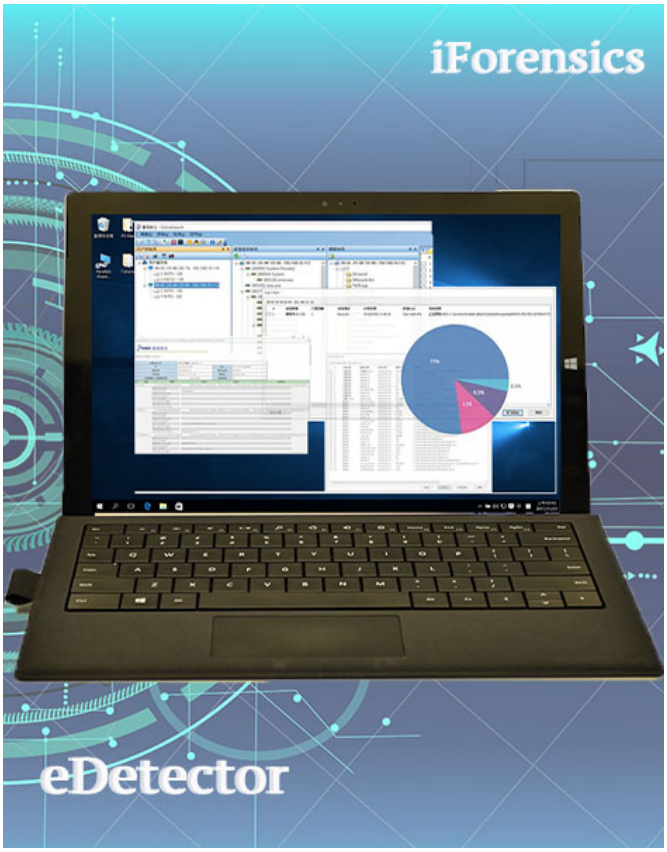
內網安全威脅獵殺系統



eDetector 主要功能

▸惡意程式分析鑑識

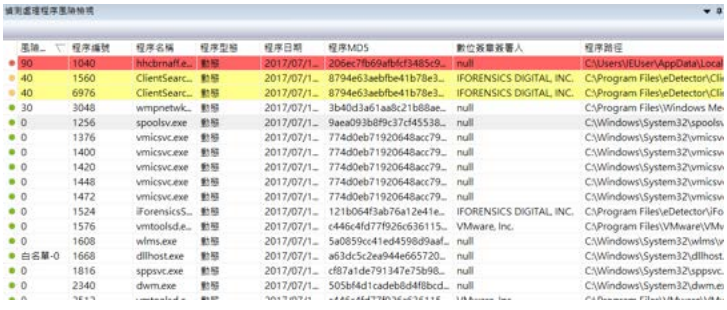
eDetector 具備偵測未知型惡意程式功能，讓您面對 APT 的攻擊不再束手無策，更能協助您建構內網安全預警系統，及早發現內網潛伏之殭屍電腦，以便能在最短時間採取必要措施因應，避免資安事件災情擴大。

▸資安事件蒐證分析

eDetector 除具有惡意程式分析鑑識功能，亦提供快速蒐證功能，一但發生惡意程式滲透植入資安事件初期時，得以透過蒐證功能深入分析，有助找出這些資安事件發生之源頭，作為未來強化資安架構與政策擬定之參考資訊。

eDetector 惡意程式分析功能

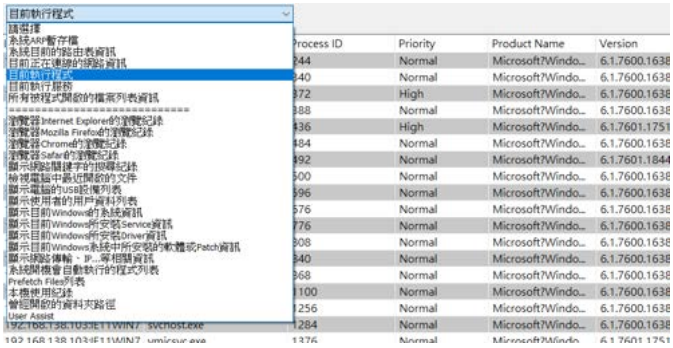
採記憶體動態行為分析，偵測惡意程式植入系統時在記憶體中行為痕跡，包含惡意程式碼注入、程序隱藏/檔案隱藏、核心攔截、連網行為、非正常啟動之服務、偵測互斥...，透過這些行為分析，無論該惡意程式如何隱密躲藏，仍無法避開 eDetector 的偵蒐。



eDetector 除針對記憶體採動態行為分析模式，同時也可選購整合 Metadefender 多合一防毒大數據知識庫，對已部署之電腦/伺服器進行全硬碟檔案完整掃描，協助資安管理員能及早發現儲存於硬碟未被觸發之惡意程式，以避免電腦遭駭淪陷。

eDetector 蒐證分析功能

eDetector 可搜集電腦執行狀態下 20 多種系統狀態資訊，包含上網瀏覽網頁行為、最近開啟之文件、USB裝置使用紀錄、程式執行痕跡、開機自動執行之程式、檔案系統索引表($MFT)，透過這些資訊的蒐證與分析，可以協助資安管理員針對惡意程式植入初期，資安事件發生之原因，此資安管理員藉由分析所獲資訊找到之源頭，便能作為未來強化資安或加強教育訓練之依據。



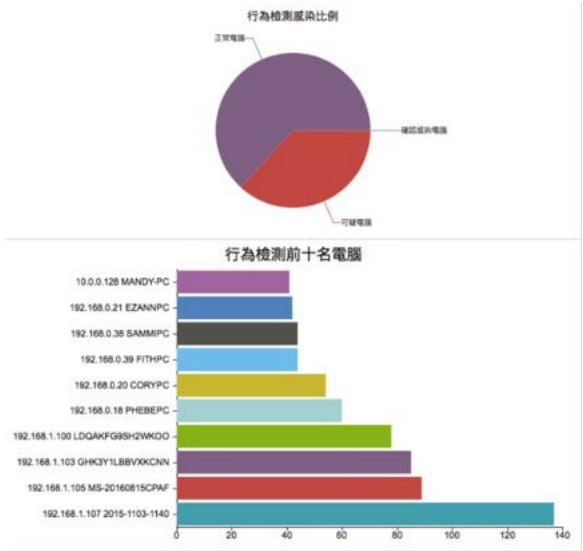
報表功能

當經過分析、確認惡意程式與過濾後，可產出企業/機關之分析報告，報告內容分成三部分

- 摘要報告：顯示惡意程式感染電腦/疑似感染電腦/正常電腦分佈之圓餅圖，及顯示用戶端電腦惡意程式累計數量排名之橫條圖
- 惡意程式動靜態分析指標：顯示判定遭植入惡意程式之各類危險指標
- 惡意程式檔案路徑：顯示該惡意程式檔案實體路徑

eDetector 產品特色

- 支援中央控管，將程式派送至用戶端之Windows作業系統執行後，即可進行用戶端之硬碟檔案搜尋、蒐證及記憶體程序偵測分析
- 採行為分析，可偵測分析所有執行中程序及其所載入之模組，並定時email通知異常情況
- 針對發現問題之執行程序，可以繪製關聯圖協助人員尋找惡意程式根源
- 針對執行中之惡意程序可暫停或終止其程序並繪製相關連線IP位置地圖
- 可分析已被刪除之檔案(例如惡意程式下載器)
- 可檢視開機啟動服務、自我啟動程序及排程任務，供使用者檢視不正常的啟動程序
- 內建白名單，自動排除微軟發行之應用程式，並可自訂/匯入黑白名單
- 可搜集用戶端的檔案總管資訊，並對其進行搜尋、篩選及取回檔案
- 具鑑識級別的蒐證特性，自動將蒐證資訊進行MD5/SHA計算以保留原始證據能力



研發原廠
鑒真數位有限公司
iForensics Digital Inc.
台北市中山區松江路 309 號 11 樓之 5
http://www.iforensics.com.tw