

eDetector

端點資安鑑識蒐證工具

即時、高效、自動化

eDetector 是一款專為資安事件調查設計的端點資安鑑識蒐證系統，屢獲殊榮，包括經濟部創新研究獎。



自動化蒐證分析

1. 惡意程式偵測
2. 動態行為分析

人工智慧報告生成

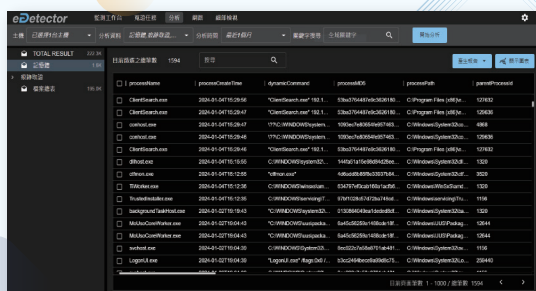
1. 結合多樣 AI 技術
2. 支援大型惡意資料庫

YARA 掃描技術

1. 導入 YARA 技術支援
2. 迅速辨識惡意程式

雲端擴充架構

1. 高可用性與高擴充性
2. 多端點蒐證與關聯監控



“結合記憶體偵測與行為痕跡分析，eDetector 可快速發現惡意行為，如程式注入、隱藏程式、核心攔截與連線歷史，找出可疑活動並提供攻擊根因分析。系統能生成程序關聯圖，並標註來源 IP，協助用戶掌握事件全貌！”

eDetector

更全面的數位蒐證解決方案



多模式與輕鬆部署

雲端版支援跨機管理與蒐證分析，本機版則適用於本地安全需求；Agent 部署快速且支援大規模同步安裝，最多可達 500 台。

高效蒐證與威脅分析

支援多達 40 種以上之數位證據蒐集與未知型威脅偵測，透過動態行為追蹤快速發現潛在風險並生成分析報告。



蒐證與分析

- 支援超過 40 種數位證據類型的蒐集，包括瀏覽器記錄、USB 資訊、網路流量、DNS 資訊、Windows 活動等。
- 高效搜尋功能可於數秒內完成對數千萬筆資料的檢索，並提供即時檔案列表與動態資料檢索。
- 整合 AI 技術與 VirusTotal 資料庫，快速生成分析報告，捕捉惡意程式特徵與來源資訊。



威脅偵測與防護

- 支援未知型惡意程式的動態偵測，透過記憶體分析與行為追蹤發現潛在威脅。
- 提供程序樹狀圖、載入模組與 DLL 清單，標註程式連結與來源 IP，快速辨認惡意行為。
- 導入 Yara 掃描技術，迅速過濾惡意程式特徵，鎖定潛在風險。



雲端擴充與管理

- 提供穩定的雲端服務與彈性儲存擴充，確保資料的機密性、完整性與可用性。
- 資安人員可透過網頁介面進行跨機監控與任務進度管理，提升操作便利性。
- 提供視覺化時間軸，可供快速檢視與分析資料概況。分派特定金庫管理職務。
- 多重身份驗證。



關於區塊鏈科技

成立於 2018 年，由擁有超過 17 年數位鑑識、證據保全和資訊安全經驗的行業專家所創辦。深感區塊鏈發展帶來新轉機和挑戰，我們結合區塊鏈及資訊安全這兩大核心技術，開始我們打造安全數位未來的任務。