Forensics 鑒真數位
專業數位資訊鑑識公司

eDetector

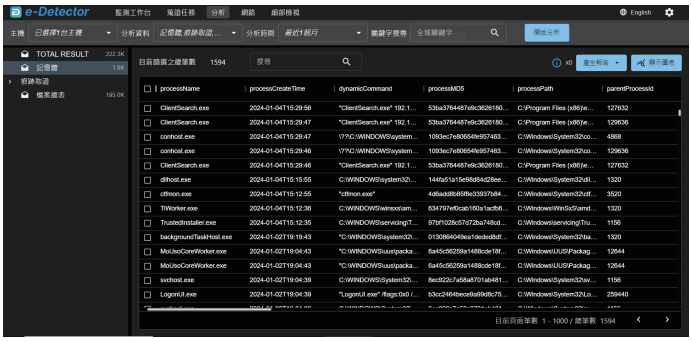
次世代資安事件應變-調查蒐證工具

即時　高效　自動

全新雲端版本可跨機追蹤蒐證分析結果，
結合 AI 技術自動生成分析報告，資安蒐證與調查輕鬆上手!

- 大規模部署、自動化蒐證、高效搜尋
- AI 自動化報告生成
- 端點支援各類型 Windows、Linux 作業系統採集關鍵數位跡證

eDetector 主要功能



eDetector 為全新端點蒐證鑑識系統，具備雙服務模式：雲端版與本機版。在對蒐證目標主機運作影響最小化的情況下，進行數位跡證與程式分析。資安事件發生初期，資安人員可透過強效蒐證功能與高效搜尋分析，找出事件可能根因。eDetector 同時結合多項先鋒技術，支援 Yara 掃描技術、支援大型惡意程式資料交叉比對，及通用型人工智慧分析技術，產出自動化生成報告，協助資安人員迅速掌握調查方向。

功能說明

自動化蒐證分析
- 惡意程式偵測
- 動態行為分析

人工智慧報告生成
- 結合多樣AI技術
- 支援大型惡意數據庫

YARA 掃描技術
- 導入Yara 技術支援
- 迅速辨識惡意程式

雲端擴充架構
- 高可用擴充性
- 多端點蒐證與關聯監控

雙模式服務

具雲端版與本機版，支援 Windows 及 Linux 等多樣/多版本作業系統。雲端版可透過網頁界面監控，跨機管理蒐證分析作業；本機版可安裝64位元平台。

簡易部署

agent 部署輕鬆簡單，一步驟即可進行安裝啟用服務，並可支援高達500台 agent 部署。

強效蒐證及搜尋能力

未知型惡意程式偵測及動態行為分析，自動追蹤潛在威脅。蒐集多樣系統資訊，包含瀏覽網頁、文件開啟、USB 使用、程式執行...等等。高效搜尋功能支援數秒間千萬數據搜尋。

人工智慧報告生成

結合多項 AI 技術，快速生成分析報告。結合 VirusTotal 大型惡意數據庫惡意程式情報分析，捕捉惡意行為痕跡與來源 IP。

Yara 掃描技術

導入 Yara 掃描支援，迅速過濾各項惡意程式特徵，快速辨認惡意程式並鎖定潛在風險。

雲端擴充架構

提供高度穩定服務與儲存擴充彈性，並確保資料機密性、完整性、可用性。資安人員可透過網頁管理介面輕鬆執行跨機蒐證工作監控。