OPSWAT.

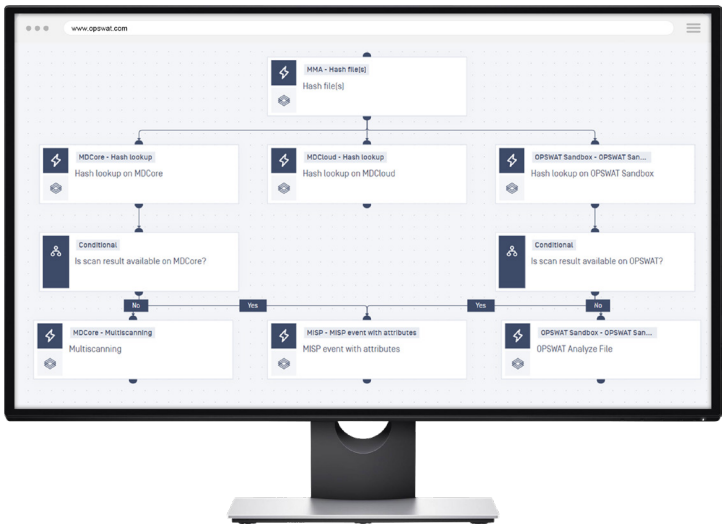
DATASHEET

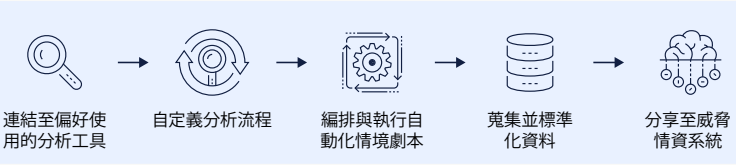
MetaDefender Malware Analyzer

針對關鍵性基礎架構提供惡意軟體的分析

現今的資安團隊由於大量的警告、缺乏熟練的網路安全人員、太多的工具和中斷的流程而不知所措，因為這些因素使其無法有效地偵測進階和目標性的攻擊，並對其做出回應。資安團隊需要一個更好的解決方案，以避免警告疲勞 (Alert Fatigue)、了解攻擊者的行為、對攻擊做出回應，並建立更主動且防禦性更強的態勢。

MetaDefender Malware Analyzer 能協調惡意軟體分析的流程、將其自動化，並迅速將可採取行動的威脅情資用於分類和事件回應的活動。





主要特色

情境劇本 (Playbook) 管理和視覺化的工作流程
支援環境視覺化 (Visual Canvas)，以建立惡意軟體分析工作流程或情境劇本，用來定義在您工具集中複雜的分析序列 (Sequence)。

高效力的多重掃描
應用 OPSWAT MetaDefender 多重掃描技術。該技術同步運用 30 多個防毒引擎的簽名、啟發法 (Heuristics) 和機器學習，以提供最高的惡意軟體偵測率。

超迅速的動態分析
利用 OPSWAT Sandbox 迅速地對以 IT 和運營技術 (Operational Technology, OT) 為基礎的惡意軟體做出判斷，從一開始的感染到進階階段以安全的方式監控攻擊。

自動化分析
提供統一的整合、協調、自動化和報告架構，其中納入一組偵測功能，包括廣泛的靜態和動態分析技術，以及威脅情資服務。

本地的威脅情資
使整個安全生態系統的所有入侵分析指標 (Indicators of Compromise, IOC) 更加豐富，並運用與惡意軟體資訊共享平台 (Malware Information Sharing Platform, MISP) 相容的本地或私有雲端指標儲存庫。

OPSWAT.

效益

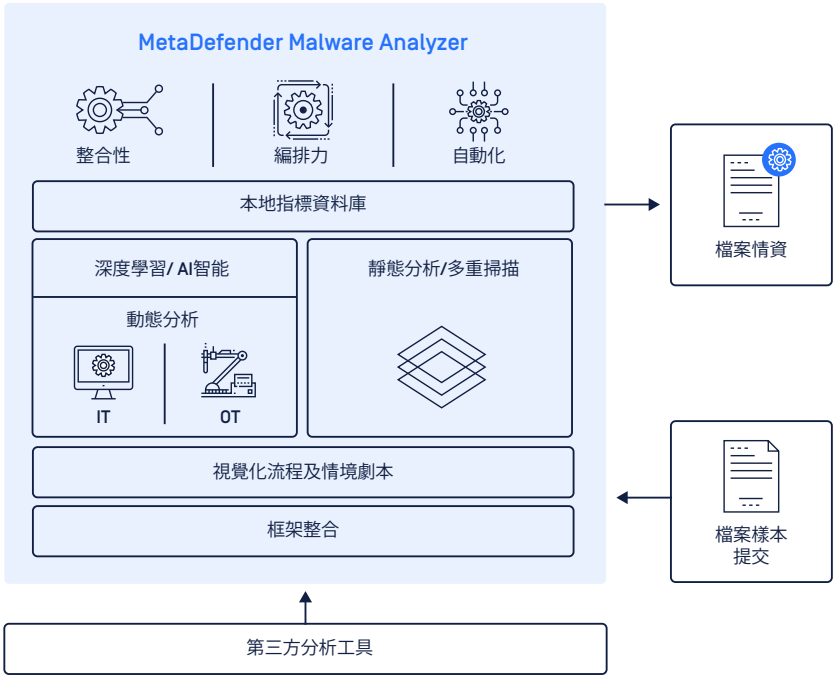
降低複雜性
提供容易使用的視覺化環境，以建立並迅速運用預先定義的配置文件和分類的資源，藉以確保執行的一致性更高，並減少網路技能短缺的影響。

簡化協調
定義特定的工作流程，並針對正確的威脅和環境類型執行恰當的分析，藉此方式以可採取行動的威脅情資得出更準確的結果。

加強分析
對 IT 和 OT 環境提供準確的惡意軟體偵測和分析，將數個工具的協調自動化，以提供更完整且更準確的威脅洞見。

充分運用工具
將最佳的互補性分析技術統一，並就惡意軟體的行為建立最全面性的資料集，藉以延展 OPSWAT 的原生性惡意軟體分析技術。

提升能見度
從單一虛擬管理平台 (Single Pane of Glass) 確保在整個分析工具集中提供完整的能見度。



功能

將惡意軟體分析自動化
協調來自單一解決方案多個工具集的分析，並將其自動化，藉以簡化安全性工程、作業和分析。

提升對事件的回應
減少與手動分析有關的開銷、消除對專業技能的需求，並在不同的工具和無關聯的工作流量當中讓資訊自由流通。

加速整合和分析
消弭手動整合分析工具的需求，並在工具當中建立更高的相互操作性和一致性。

達到最佳的分析結果
確保在統一的報告中，可以輕鬆地迅速取用所有分析引擎中全部最佳的檔案資料。

支援關鍵性的基礎架構防護
偵測針對 IT 和工業控制系統 (Industrial Control System, ICS) 的惡意軟體，以管理整個關鍵性基礎架構的威脅。

摘要

MetaDefender Malware Analyzer 能將惡意軟體分析自動化、強化其他安全系統的效力，並為事件回應者提供可採取行動的情資，藉此讓企業組織能夠使其安全實務達到最理想的境界。藉由將安全性工程、作業和分析簡化為單一的解決方案，OPSWAT 因此能為關鍵性基礎架構防護提供一個更有智能化的方法。

OPSWAT.
Trust no file. Trust no device.

For further information
https://www.opswat.com/products/metadefender/malware-analyzer