自定義惡意程式辨識與分析

你的網路攻擊情資

是公開新聞稿

還是真實攻擊樣本

訂閱最真實的

攻擊規則樣本

自定義惡意程式辨識與分析軟體

此產品是一種用於可自定義辨識惡意程式樣本(malware samples)的工具。
核心軟體：核心是以YARA的主要引擎，負責執行規則並進行樣本分析。

支援多種作業系統：
Linux：支援許多 Linux 發行版上運行，包括Ubuntu、Debian、Fedora、CentOS。
Windows：支援 Windows 版本，可在 Windows 7、8、10、11 和 Server 等作業系統上運行。
macOS：支援macOS上運行。
FreeBSD： 支援FreeBSD 等類 Unix 作業系統上運行。

建議安裝規格
處理器：2核心以上
記憶體：4GB以上
硬碟：1GB以上
網路連接：不限制

集成到安全設施中：可將是安全信息和事件管理(SIEM)系統、入侵檢測系統(IDS)、防火牆等安全設施，您可以將 YARA rules 的更新集成到這些平台中。

自定義惡意程式辨識與分析樣本更新半年訂閱

軟體核心安裝完成之後，提供訂閱最新的惡意軟體辨識規則，這些規則通過YARA引擎進行加載和解析，或者是您可以創建或使用現有的規則。

辨識與分析樣本檔更新方式：
一、線上惡意程式辨識與分析樣本訂閱服務：提供惡意程式辨識與分析樣本訂閱服務，每月定期更新，其中包括即時更新的 YARA rules。通過訂閱這些服務，您可以獲取最新的惡意程式辨識與分析樣本和rules。

二、離線手動更新：離線獲取最新的rules，然後將其應用到您的系統中。

三、線上自動化腳本：應用自動化腳本進行 YARA rules的下載和應用過程。

四、自定義規則創建：除了使用外部提供的rules，您還可以根據您組織的需求創建自己的 custom rules。

無論選擇哪種方式，都應該確保您的 YARA rules 定期更新，以應對不斷變化的威脅環境。定期更新 rules 可以提高惡意活動的檢測能力，確保您的安全機制保持有效。