經濟部 109 年度
智慧型資安與新興應用整合技術研發計畫(4/4)
合作研究計畫

《資安 AI 分析模組評測》

建議書徵求文件

財團法人資訊工業策進會

中華民國 109 年4月

109年度合作研究計畫建議書徵求文件

一、簡介

研析全球網路攻擊事件，從早期駭客以分散式阻斷服務攻擊癱瘓網路運作，逐漸聚焦至進階持續威脅攻擊竊取機密資料。而隨著資訊科技運用連網範圍擴及物聯網終端裝置及行動裝置，駭客成功駭進資安(訊)供應商，破壞整體供應鏈安全的事件頻傳，以及國內外持續發生的資料外洩事件，利用憑證填充攻擊(credential stuffing attacks)透過失竊帳號密碼登入不同社群媒體，造成的後續衝擊與後果，提升資安弱點威脅與風險。

美國MITRE公司提出的ATT&CK(攻擊者行為資料庫；Adversarial Tactics, Techniques and Common Knowledge)，是一種以剖析攻擊面為出發的資安框架，在說明網路攻擊鏈（Cyber Kill Chain）時，有統一的標準可依循，本案建立一套資安AI分析模組評測機制，運用樣本資料評估研發模組對應攻擊者行為資料庫分類準確性，強化威脅分析技術的實用性，協助主計畫完備端點系統威脅分析技術研發之目標。

二、計畫目標

本計畫的主要目標可分為四個部分：

- 建置虛擬開發環境，確立環境參數一致性

  使用Docker與Kubernetes等工具，提供虛擬容器並具自動部屬、擴充與管理之功能，以減輕資源消耗且排除環境差異之偏誤。

- 自動化資料生成腳本，簡化研究複雜性

  研擬自動化腳本蒐集系統日誌、封包流量與系統資源統計，且解決格式不一致和環境差異等問題，確保後續分析結果之可靠性。

- 發展資安AI分析模組評測技術，強化資訊系統(Information Technology)安全性

  能依資料來源萃取相對應之分析特徵，並以序列分析學習惡意威脅之樣態，精準預測異常行為。

- 設計技術評測機制，辨識機器學習之效率

  根據演算法之複雜性適當調整指標數值，再依資料來源、攻擊階段與攻擊類型探討合適之威脅偵測技術，提供最佳端點防護之模型。

三、 計畫範圍

本計畫範圍以研發資安AI分析模組評測技術，能依據攻擊階段與資料來源等條件篩選最佳模型，評估研發模組對應攻擊者行為資料庫(ATT&CK)分類準確性，主要研究範圍彙整說明如下：

- 研發威脅分析技術，強化端點防護能力

  將駭客威脅依攻擊性質分階探討，搭配多種資料來源解析攻擊樣態，萃取合適分析特徵資料。再以機器學習演算法建立威脅偵測模型，即時處理巨量資料且精準偵測惡意攻擊行為，並運用模擬資料與實際場域資料進行ATT&CK(攻擊者行為資料庫；Adversarial Tactics, Techniques and Common Knowledge)驗證。

- 建立模型成效評估機制，提升人工智慧技術應用效益

  以資料來源、攻擊階段和攻擊類型評比機器學習演算法之契合性，同時建立一套完善的測試流程，指標數值可因應模型結構、資料性質等差異調整；針對資安AI分析模組評測機制，提供合適之威脅分析技術，節省人工試驗之成本，運用樣本資料評估研發模組對應攻擊者行為資料庫(ATT&CK)分類準確性，強化威脅分析技術的實用性。

四、 預期成果

本計畫的預期成果應包含以下五項：

1. 威脅分析技術模組乙個，核心功能詳三、計畫範圍
2. 人工智慧技術模型評估機制乙套，核心功能詳三、計畫範圍
3. 研究報告書
   - 文獻蒐集與分析：文獻蒐集與分析、資料來源、攻擊階段與攻擊手法等相關文獻蒐集與分析技術整理
   - 演算法/機制設計：探討資料來源與機器學習演算法之特性，分析其適合之應用情境，並擬定一公正之評估機制，度量資料來源和分析模型成效
   - 實驗評量機制說明：設計實驗評量機制，用以評估威脅分析技術模組之效能，並能驗證模型成效評估機制之完整性
   - 成果展示：威脅分析技術模組之偵測率優於常見 benchmark，而模型評估機制可依條件（資料來源、攻擊階段與攻擊手法）自動判斷合適之人工智慧技術模型
4. 模組規格書
   - 規格說明：闡述演算法/機制設計架構，包含環境需求、設計方法、執行概念、元件設計（包含功能介紹、輸入與輸出描述）
   - 測試結果：依實驗機制說明測試結果，包含測試時程、測試過程、單元/整合測試結果、實驗結果
5. 本計畫預期撰寫國際或國內知名研討會或期刊論文一篇

※前述成果如有專利構想或專利申請產出時，需注意專利申請之新穎性(novelty)。因凡經公開發表之研發成果，如擬申請專利，須於公開發表後 6 個月內完成，前述成果如是以論文方式公開發表，將無法取得大陸與歐盟等國之專利。

五、 執行方式

本計畫預計將結合學界在理論面以及本會在資安滲透測試技術研發的實務面經驗，透過雙方相互合作討論的方式來進行，本計畫亦需提供教育訓練及經驗分享機制，藉此增進本會研究人員的專業能力，以提升本合作案成果之效益，相關執行方式步驟如下：

1. 完成相關文獻蒐集等先前技術整理
2. 完成演算法設計及機制流程規劃
3. 完成威脅分析技術模組與模型評估機制之雛形，並展示其功能完整性
4. 完成結案報告，評量技術效能

六、 計畫期程及預估計畫總經費

計畫執行區間：109 年 05 月 01 日 至 109 年 12 月 20 日

總經費：800,000元

七、 驗收標準(含教育訓練)

1. 期中報告：預計於 109 年 08 月 31 日完成
   - 研究報告書內容應包含文獻整理說明、演算法設計、機制流程說明、流程操作展示與效能評量結果說明
   - 模組規格書內容應包含規格說明、測試結果
2. 期末報告：預計於 109 年 11 月 30 日完成
   - 模組/機制雛形：期末完成威脅分析技術模組與模型評估機制，內容應包含執行檔、程式原始碼、單元測試及相關說明文件
3. 進度討論會議：每月召開一次進度研討會議
4. 國內外知名研討會或期刊論文一篇

八、 技術能力需求

1. 資訊安全相關背景：須瞭解作業系統核心底層運作原理、惡意程式偵防技術與資安滲透測試等各項技術，並熟悉相關資安分析工具與虛擬化平台的使用，方能掌控本計畫研發所需核心技術
2. 相關計畫參與經驗：曾執行滲透測試或熟悉機器學習演算法運作原理，並具相關研究論文發表及計畫執行參與經驗
3. 其他：如熟悉 Python、Docker 與 Kubernetes 等系統程式開發與操作

附件1：契約書格式
- 1-1：計畫書格式
- 1-2：經費動支報表
- 1-3：成果報告撰寫須知
- 1-4：報告格式
- 1-5：論文格式
- 1-6：保密聲明書
- 1-7：委託匯款同意書