Task 1: Cyber Threat Intelligence analysis

- Goal:
  - To predict TTPs of a given CTI report and extract an IOC list for each TTP.
- Dataset:
  - CTI reports crawled from the references on various TTP webpages of MITRE ATT&CK.
- Method:
  1. Using a) technique ID matching and b) the TRAM tool[1] to annotate the TTPs label for each CTI reports.
  2. Referring to [2], design an NN model to predict the TTPs present in each CTI report.
     a. To identify whether each sentence in a CTI report belongs to a specific TTP.
- Extension work:
  - Extracting IOCs from each sentence labeled with TTP using regex.
- Contribution:
  - 幫助了解 TTP 多樣化的實作手法與相關 IOCs。

[1] THREAT REPORT ATT&CK MAPPER (TRAM) [ref]
[2] rcATT: Legoy et., Automated Retrieval of ATT&CK Tactics and Techniques for Cyber Threat Reports. [ref]

Task 2: Log-based Cyber Threat Analysis

- Goal:
  - To generate synthesize technique graph based on MITRE ATT&CK framework.
- Dataset:
  - TTP's procedure examples from MITRE ATT&CK framework.
  - Synthesize dataset/DARPA dataset
- Method1:
  1. Referring to [1], converting the procedure examples of each TTP into 1/n *Technique Knowledge Graphs (TKGs)*.
  2. Using the TTP IOC list obtained from Task 1, manually/algorithmically transforming the object's high-level descriptions in the TKG into low-level artifacts. E.g., malware set registry run key -> mssecsvc.exe RegSetValue HKCU\...\Run\mssecsvc.

[1]Li, Zhenyuan, et al. "AttacKG: Constructing technique knowledge graph from cyber threat intelligence reports." Computer Security–ESORICS 2022[ref]

Task 2: Log-based Cyber Threat Analysis(Cont.)

- Method2:
  1. Understanding MITRE ATT&CK TTP techniques, implementing custom TTP instructions based on MITRE CALDERA[1]
  2. utilizing procmon to record relevant audit logs to obtain the technique graph of a specific TTP.
- Extension work:
  - Storing the existing audit log dataset in a graph database (e.g., Neo4j) to enhance data search speed.
- Contribution:
  - 增加現有 technique graph 資料庫，增強基於 audit log 偵測多樣性 APT 威脅的能力。

[1] MITRE Caldera[ref]
[2] Process Monitor[ref]

Task 3: Malware Analysis(伻孜)

- Goal:
  - To predict TTPs of a given malware with static analysis features and explain the reasons for TTP detection.
- Dataset:
  - Malware PE files from Malshare/MITRE ATT&CK(MAMBA dataset)
- Method:
  1. Utilizing the radare2 tool[1] to extract static features (e.g., control flow graph, CFG) from each PE file.
  2. Referring to [2], designing an NN model based on the static analysis features extracted from each PE file to perform TTP detection for each malware.
- Extension work:
  - 利用 Function Call Graph(FCG) 驗證 CAPE dataset.
- Contribution:
  - 基於靜態分析偵測惡意程式使用的 TTP。
  - 可結合動態分析技術，加強偵測惡意程式使用哪些TTP的能力。

[1] radare2(R2pipe) [ref]
[2] Someya et., FCGAT Workshop on Binary Analysis Research(co-located with NDSS 2023)[ref]

Task 4 Malware anti-evasion technique implement

- Goal:
  - Enhancing the anti-evasion capabilities of Cuckoo/CAPE sandbox.
- Tool:
  - Cuckoo/CAPE sandbox
- Method:
  1. Referring to [1], given specific malware evasion techniques, modify the monitoring files of the Cuckoo/CAPE sandbox to enhance its anti-evasion capabilities.
- Contribution:
  - 增強沙盒抵禦惡意程式針對沙盒環境的規避能力，確保可錄製到惡意程式行為。

[1] Evasion techniques[ref]