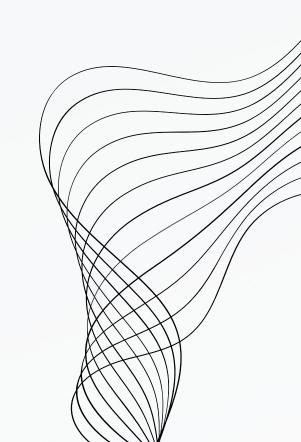


# PROJECT PROPOSAL

**Vincent Pai** 

2023/7/5



## CONTENT

01

TOPIC

02

CURRENT PROGRESS

03

FUTURE PLAN

## TOPIC

#### 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:
  - 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.
    - 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。

## CURRENT PROGRESS

#### Searching

Searching the terms and the documents and trying to understand

#### Reading the paper

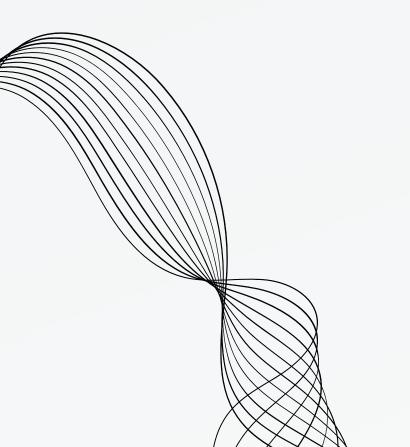
Reading the paper: Automated Retrieval of ATT&CK Tactics and Techniques for Cyber Threat Reports

#### Installing

Installing the Docker and trying to start the TRAM container

#### Crawling

Learning how to crawl



### FUTURE PLAN









#### 1ST WEEK

Getting familiar with the workflow and background knowledge.

Successfully installing the TRAM and run it

#### 2ND WEEK

Crawling the data and trying to use the TRAM to label them.

Write some program to automatically label the data and crawling them down to be our dataset.

Finishing the first paper.

#### **FUTURE**

Designing the NN model and training the classifier.

Trying some methods mentioned in the paper.

Helping Euni to train the classifier such that she can graduate.

#### **FUTURE**

Optimize and try to extract the IOC.

Helping Euni to train the classifier such that she can graduate.

## THANK'S FOR LISTENING

