

rcATT: retrieving ATT&CK tactics and techniques in cyber threat reports

Marco Caselli, Siemens AG

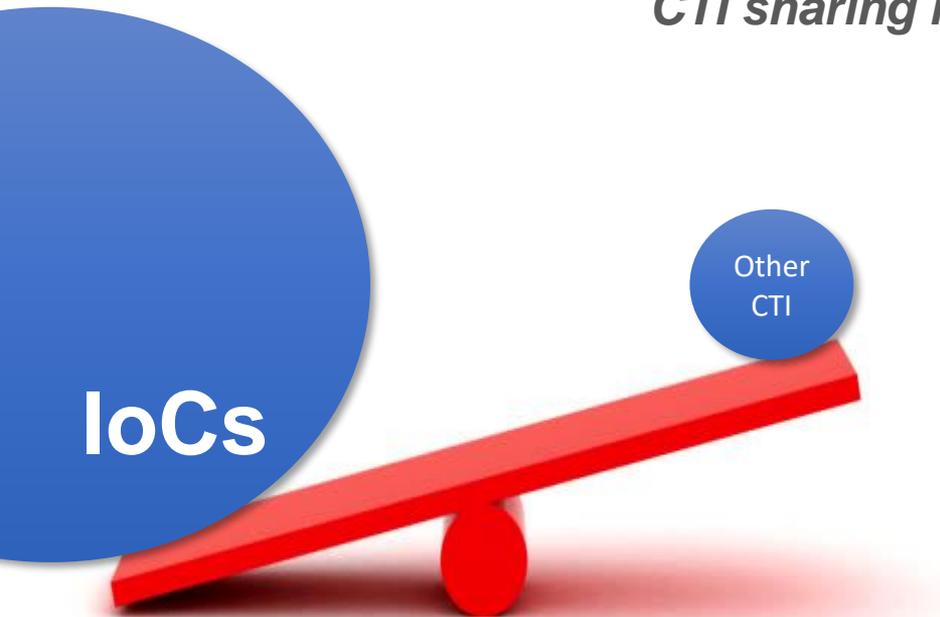
Valentine Legoy, University of Twente

Andreas Peter, University of Twente, Services and Cybersecurity group

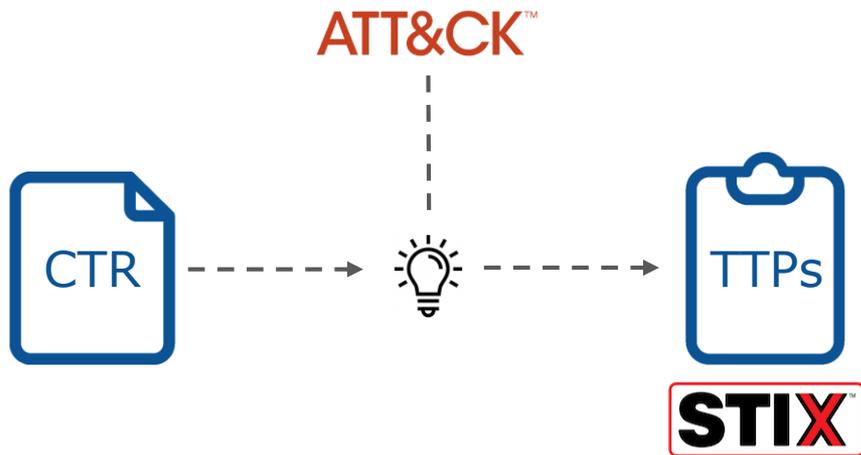
Christin Seifert, University of Twente, Data Science Group

Problems and motivation

CTI sharing is growing but...



Proposed Solution

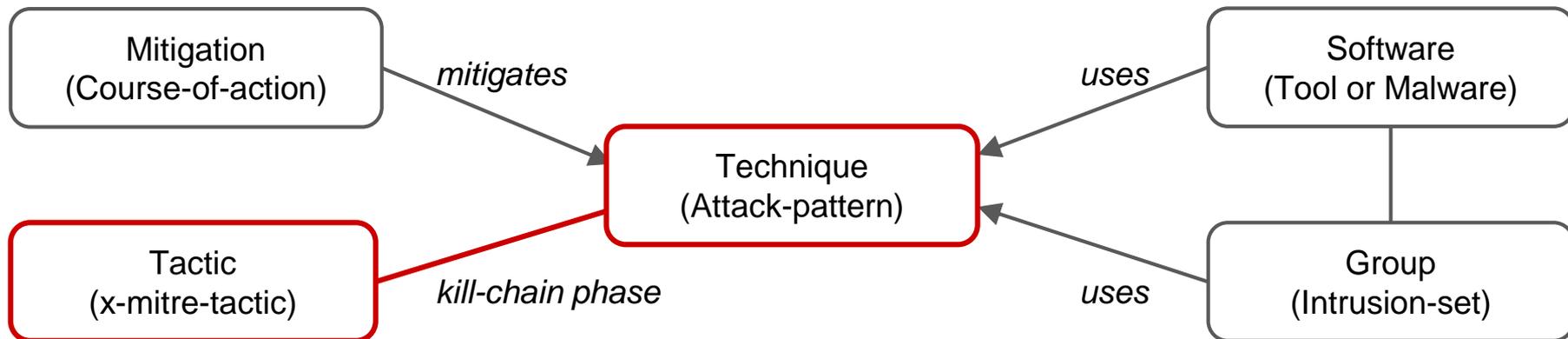


- Automating the extraction of **Tactics, Techniques and Procedures (TTPs)**
- Taking advantage of known TTPs such as the **MITRE ATT&CK framework** for the classification
- Organizing the obtained results in a **structured format**, namely STIX 2.0

Analysis & Implementation

Available Data Sources

- “ATT&CK - Adversarial Tactics, Techniques, and Common Knowledge”
- MITRE’s Github¹ offers the entire ATT&CK framework represented in STIX 2.0
- Techniques include references to ~1500 different CTRs



¹<https://github.com/mitre/cti>

Challenges & Countermeasures

- Multiple techniques and tactics in each report



- *Multi-label text classification*

- Limited amount of data
- Imbalanced dataset



- *Rebalancing and increasing the dataset by getting more data*

- Tactics and techniques are not independent



- *Use tactics and techniques relationship in post-processing*

Evaluation Measures

$$\textit{precision} = \frac{tp}{tp+fp}$$

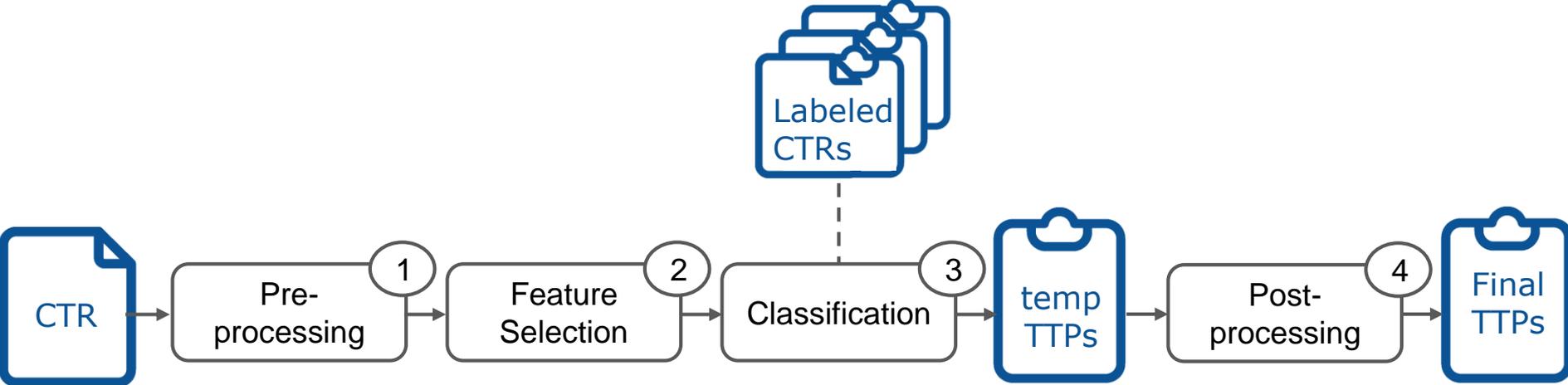
$$\textit{recall} = \frac{tp}{tp+fn}$$

$$F_{\beta} = \frac{(1 + \beta^2) \cdot (\textit{precision} \cdot \textit{recall})}{(\beta^2 \cdot \textit{precision} + \textit{recall})}$$

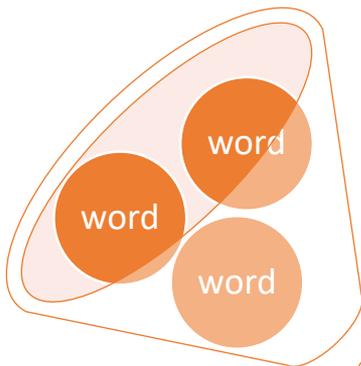
$$\beta = 0.5$$

tp = true positives; *fp* = false positives; *fn* = false negatives

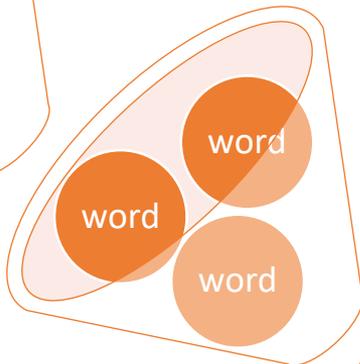
Classification Process Schema



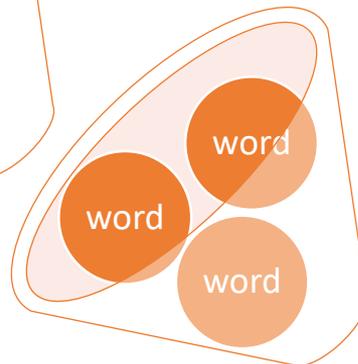
Pre-processing



Removing noise (e.g., with regular expressions)



Removing stop-words (e.g., "a", "and", "but")



*Stemming
(e.g., **attacking** → **attack**)*



Feature Selection

1
Pre-processing

2
Feature Selection



Word frequency based

- Term frequency (TF)
- Term frequency-inverse document frequency (TF-IDF)



TF-IDF



Word embedding

- Word2Vec

TF-IDF "Tuning"

- Bags-of-words representation
- Filtering lowest scores

Classification



Classification algorithms:

- Naive Bayes, Nearest Neighbors, Support Vector Machine, Decision Trees, Linear Models, etc.

Solving overfit and unbalance

- Re-sampling, fine-tuning on parameters, etc.



Linear SVM to identify both Tactics and Techniques

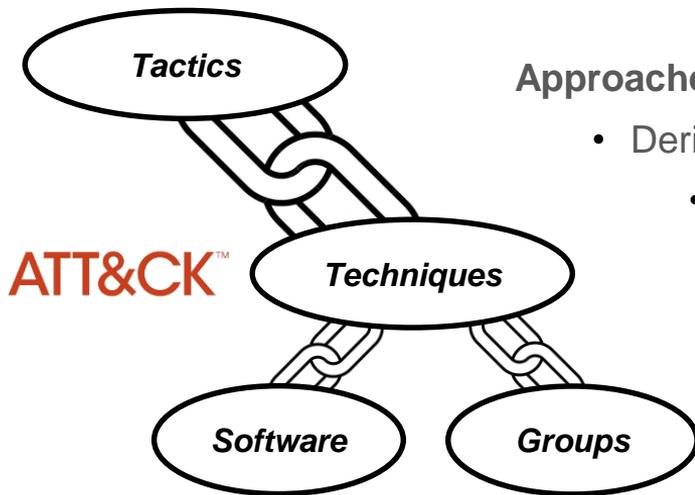
1
Pre-processing

2
Feature Selection

3
Classification

Post-processing

Goal: making use of the ATT&CK structure



Approaches:

- Deriving tactics from techniques classification
- Confidence propagations
- Association among techniques

Confidence propagation

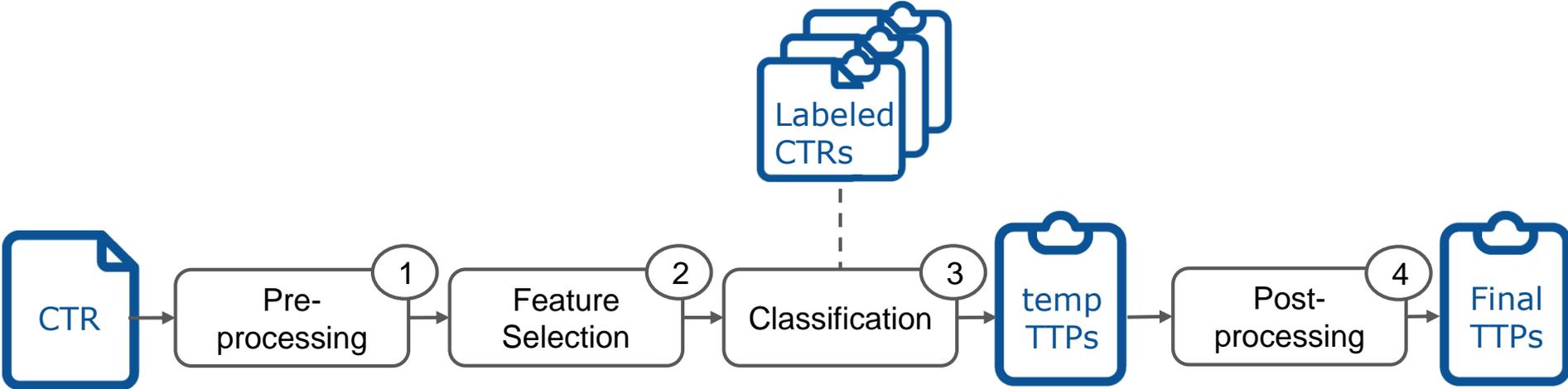
1
Pre-processing

2
Feature Selection

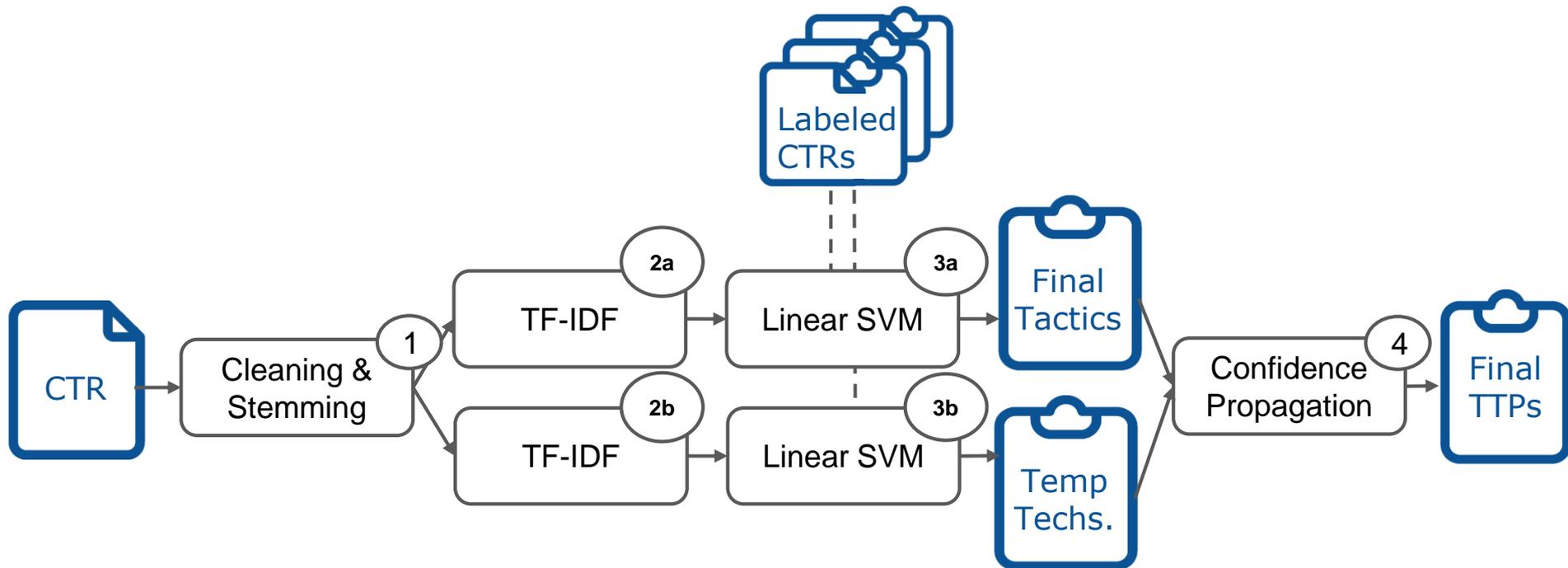
3
Classification

4
Post-processing

Classification Process Schema



Final Classification Process



rcATT Report Classifier based on
ATT&CK tactics and techniques

rcATT - Report classification by ATT&CK tactics and techniques

- Coming with graphical and command-line interfaces
- Returning the confidence values of all predictions
- Possibility of modifying and feedbacking results to improve tool's classifier
- Exporting results as STIX 2.0 (referencing the actual ATT&CK STIX objects)

rcATT



rcATT is a python tool to predict ATT&CK tactics and techniques from cyber threat reports. Paste your report in the text area so it can be predicted. Tactics and techniques displayed in a darker colored background are predicted as included in the report. The percentage displayed next to the name of the tactic/technique is the likelihood of this tactic/technique of being in the report. If the tactic/technique is indicated as not being in the report, despite the displayed likelihood, it is due to the post-processing in our model. If you disagree with the prediction, you can correct these results and save them to the training set to improve it.

```
Predict
```

Overview

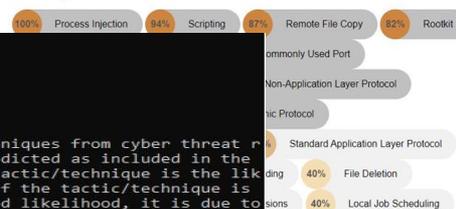
- Intelzer has discovered a new, sophisticated malware that we have named "Hiddenasp", targeting Linux systems.
- The malware is still active and has a zero-detection rate in all major anti-virus systems.
- Unlike common Linux malware, Hiddenasp is not focused on crypto-mining or DDoS activity. It is a trojan purely used for targeted remote control.
- Evidence shows in high probability that the malware is used in targeted attacks for victims who are already under the attacker's control, or have gone through a heavy reconnaissance.
- Hiddenasp authors have adopted a large amount of code from various publicly available open-source malware, such as Mirai and the Azezel rootkit. In addition, there are some similarities between this malware and other Chinese malware families, however the attribution is made with low confidence.
- We have detailed our recommendations for preventing and responding to this threat.

Correct the results Save the results for training Export the results

Tactics



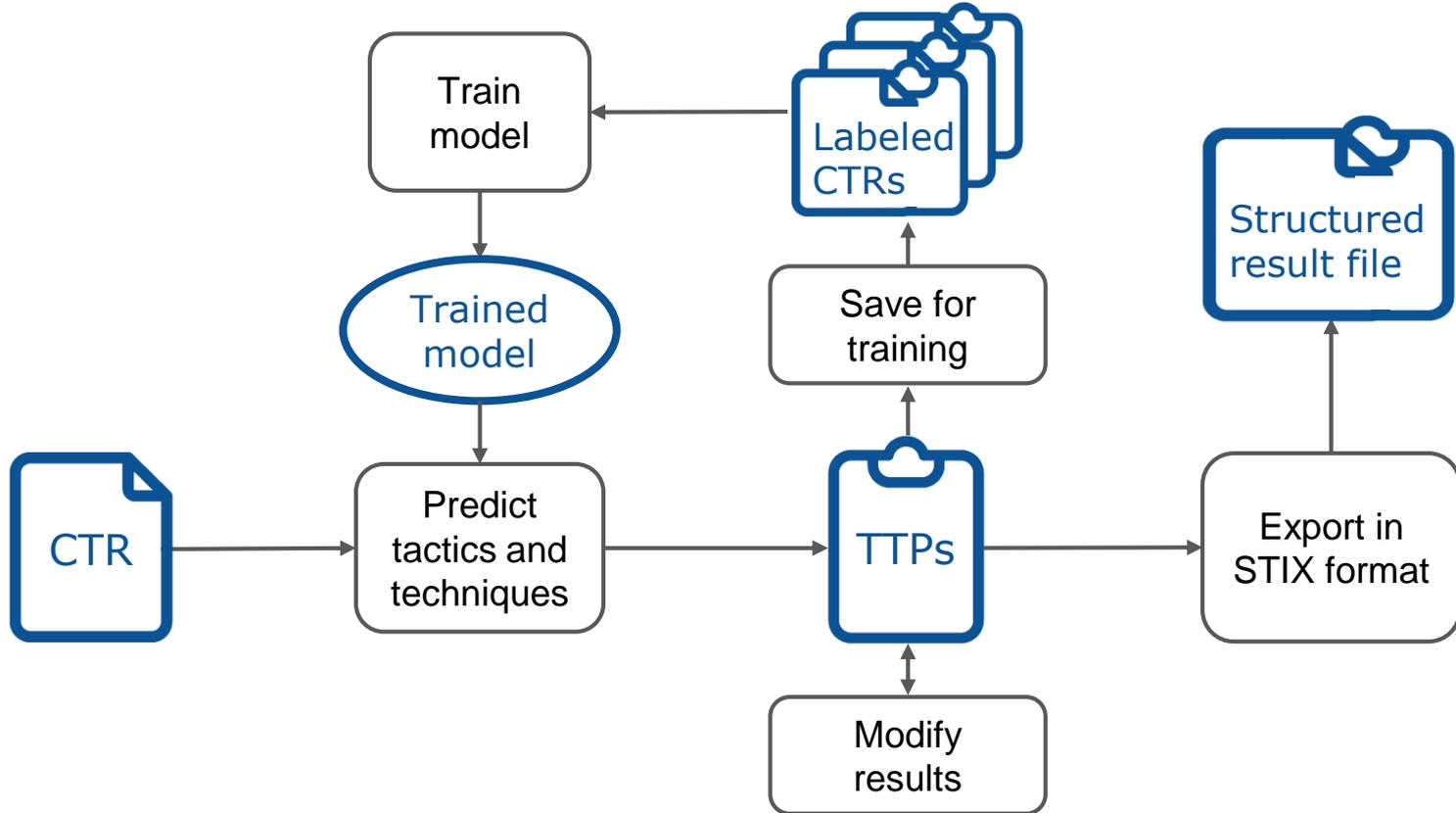
Techniques



```
rcATT is a python tool to predict ATT&CK tactics and techniques from cyber threat reports. Tactics and techniques displayed in yellow are predicted as included in the report. The percentage displayed next to the name of the tactic/technique is the likelihood of this tactic/technique of being in the report. If the tactic/technique is indicated as not being in the report, despite the displayed likelihood, it is due to the post-processing in our model. If you disagree with the prediction, you can correct these results and save them to the training set to improve it.
```

```
Commands :
-t --train      : petrain the tool with the newly added reports
-p --predict   : predict TTIPS for report in the input file
-f --feedback  : change the results given by the tool in a previously output json file by a list of given TTIPS
-a --add-to-training : add a json file output by the tool to the training set
-i --input-file : input file: .txt for --predict, .json for --feedback and --add-to-training (required)
-o --output-file : output file: json for --predict (if not given no results will be saved) and --feedback (if not given, changes will be saved in the input file)
-n --report-title : title of the report to add to the json file
-d --publishing-date : publishing date of the report to add to the json file (use the YYYY-MM-DD format)
```

rcATT – Tool structure



rcATT – Output File

“name” and “published” are defined by the user

“Description” contains the report

All references to tactics and techniques defined by MITRE are included in the “object_refs” field

```
    "type": "report",
    "id": "report--4932ef6d-3e08-4e3b-9862-1d72477a32f7",
    "created": "2019-11-17T16:43:59.045Z",
    "modified": "2019-11-17T16:43:59.045Z",
    "name": "HiddenWasp",
    "description": "Overview Intezer has discovered a new, sophi
    "published": "2019-05-25T00:00:00Z",
    "object_refs": [
      "x-mitre-tactic--78b23412-0651-46d7-a540-170a1ce8bd5a",
      "x-mitre-tactic--5bc1d813-693e-4823-9961-abf9af4b0e92",
      "x-mitre-tactic--5e29b093-294e-49e9-a803-dab3d73b77dd",
      "x-mitre-tactic--7141578b-e50b-4dcc-bfa4-08a8dd689e9e",
      "x-mitre-tactic--f72804c5-f15a-449e-a5da-2eecd181f813",
      "x-mitre-tactic--4ca45d45-df4d-4613-8980-bac22d278fa5",
      "attack-pattern--43e7dc91-05b2-474c-b9ac-2ed4fe101f4d",
      "attack-pattern--7fd87010-3a00-4da3-b905-410525e8ec44",
      "attack-pattern--e6919abc-99f9-4c6c-95a5-14761e7b2add",
      "attack-pattern--0f20e3cb-245b-4a61-8a91-2d93f7cb0e9b",
      "attack-pattern--b3d682b6-98f2-4fb0-aa3b-b4df007ca70a",
      "attack-pattern--c848fcf7-6b62-4bde-8216-b6c157d48da0",
      "attack-pattern--01df3350-ce05-4bdf-bdf8-0a919a66d4a8",
      "attack-pattern--c21d5a77-d422-4a69-acd7-2c53c1faa34b",
      "attack-pattern--e01be9c5-e763-4caf-aeb7-000b416aef67",
      "attack-pattern--3b3cbbe0-6ed3-4334-b543-3ddfd8c5642d",
      "attack-pattern--3ccef7ae-cb5e-48f6-8302-897105fbf55c"
    ],
    "labels": [
      "threat-report"
    ]
  }
```

Demo

```
C:\Users\z003ruzz>cd Desktop
```

```
C:\Users\z003ruzz\Desktop>
```

Conclusion

Comparison with existing solutions

	rcATT	TTPDrill	Ayoade et al.	Unfetter Insight	TRAM
Classification method	Multilabel text classification (Linear SVM)	Ontology	Text classification (SVM+KNN)	Multilabel text classification (Multinomial NB)	Multilabel sentences classification (Logistic regression)
Features	Word frequency	Threat actions	Word frequency	Word frequency	Word frequency
Evaluation metrics	F0.5 score	Precision and recall	Accuracy	/	/
Post-processing	Make use of tactics to retrieve techniques	Use techniques to retrieve tactics	Make use of tactics to retrieve techniques	None	/

Final remarks

Lesson learned

- Lack of labeled data
- False positives vs. false negatives
- Plain machine learning vs classification enhancements (e.g., ATT&CK structure)

Key aspects

- Incident response automation
- Open source software
 - rcATT is currently available at: github.com/vlegoy/rcATT
 - Description available at: <http://arxiv.org/abs/2004.14322>

Dr. Marco Caselli
Senior Key Expert
Siemens AG

Otto-Hahn-Ring 6
81739 Munich

E-mail: marco.caselli@siemens.com

SIEMENS
UNIVERSITY
OF TWENTE.

Thanks

rcATT is available at:
github.com/vlegoy/rcATT