DECEPT-CTI: A Framework for Enhancing Cyber Deception Strategies through NLP-based Extraction of CTI from Unstructured Reports

Amal Sayari, Slim Rekhis, Yacine Djemaiel, and Wiem Mahouachi

University of Carthage, Higher School of Communication of Tunis (SUP'COM), LR11TIC04, Communication Networks and Security Research Lab. & LR11TIC02, Green and Smart Communication Systems Research Lab

Ali Mabrouk

SAMA PARTNERS, Tunisia

The 22nd International Symposium on Network Computing and Applications (NCA 2024)

24-26 October 2024 // CEUB, Bertinoro (FC) - Italy

Outline

I. Context & Motivation

II. Research Problem

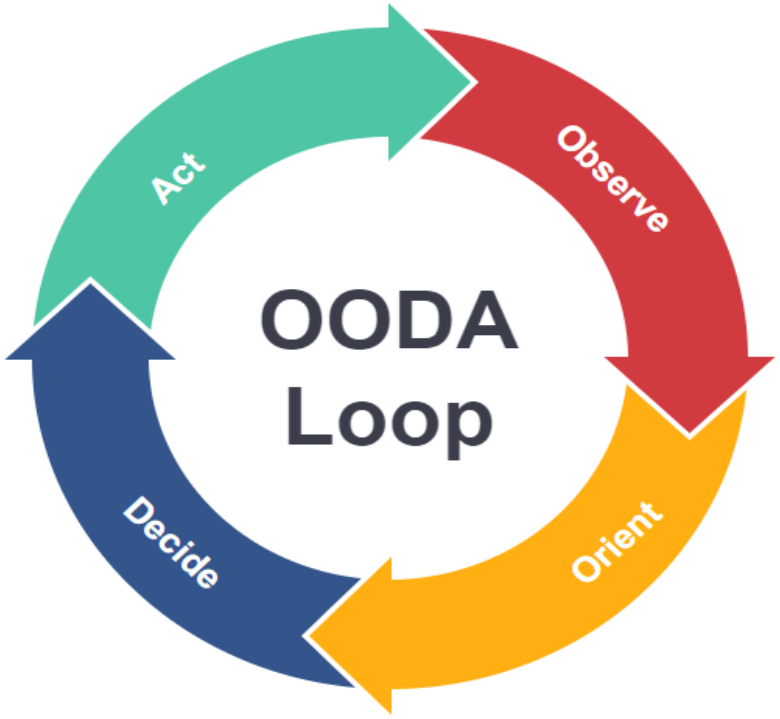
III. Proposed Solution Architecture

IV. Experiments and Analysis

V. Conclusion and Perspectives

Context & Motivation

- In the battle between the hacker and the cyber defender, the offense has the upper hand
- Cambridge(2018) , Twitter(2022), Facebook(2019) , Microsoft (2023), SolarWinds(2022), Norton(2022), etc. … All hacked
- The one that executes the OODA loop faster gains the battle



Context & Motivation

Need To be right once

Exact information about the Victim

Can chose the time and place of the attack

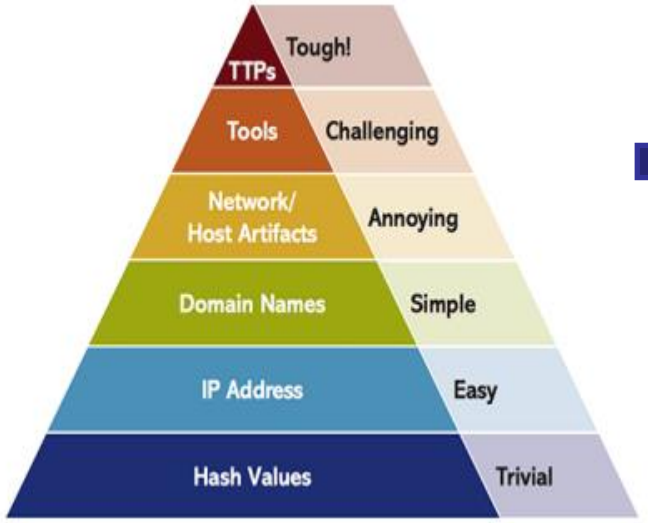
Should have everything well set

False positives

Be prepared all the time

Context & Motivation

Cyber Threat Intelligence



Reactive
Incident
Response

Security Solutions

Firewall
AntiVirus
AntiMalware

SIEM
UEBA
IDS
IPS
EDR
XDR

Proactive
Continuous
Response

Cyber Deception

Honeypots
Honeynets
Honeywords
Honeyaccounts
Honeyusers
Honeyfiles
Honeypatches
Honeyports
Honeymails
HoneyOS

Research Problem

- **Constatations**
  - Data dispersion & 78% unstructured
  - Manual analysis is time-consuming and resource-intensive
  - TTP extraction is complex
  - CTI data is often shared in the standardized STIX format

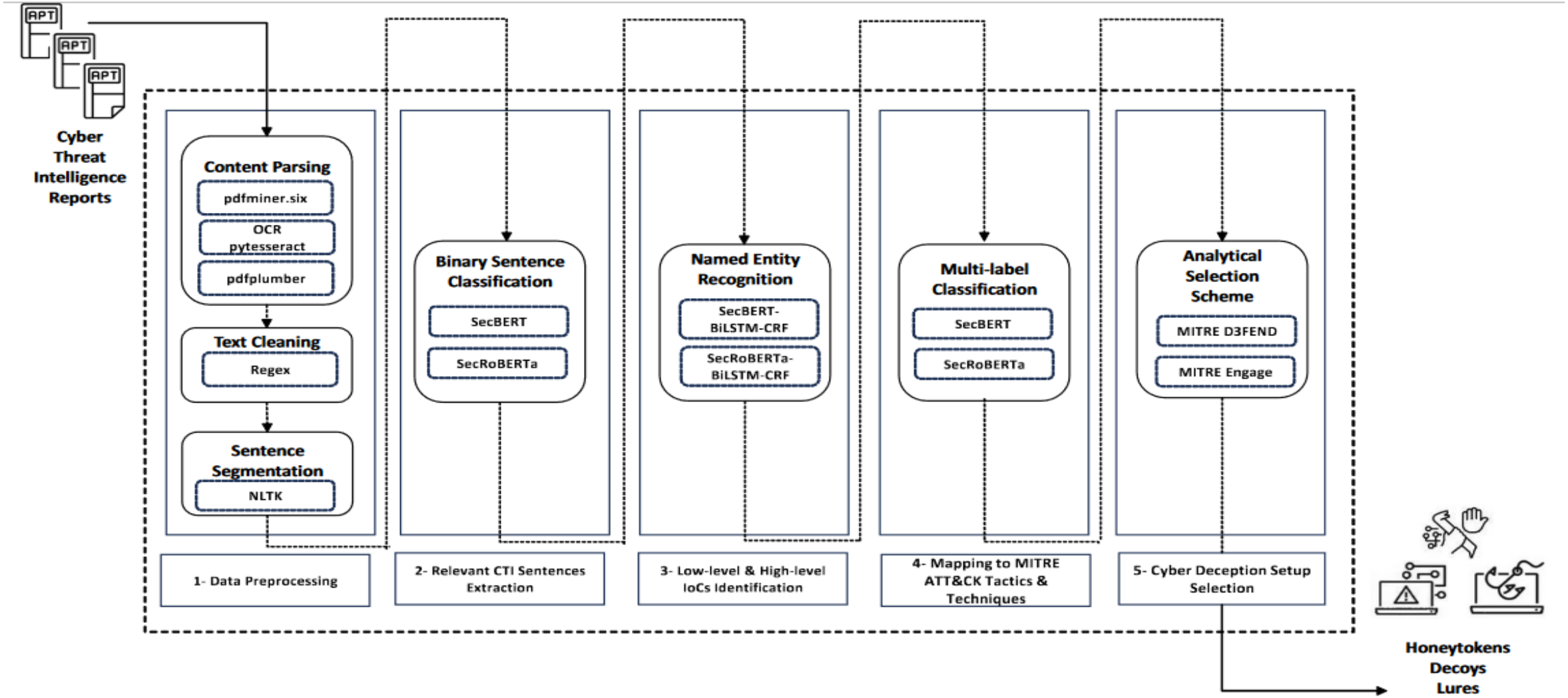
- **Research Question**
  - How to efficiently extract and structure CTI data to create tailored cyber deception strategies?

- **Challenges**
  - Processing large unstructured CTI data
  - Mapping extracted data to MITRE ATT&CK
  - Designing tailored deception strategies

Contributions

- DECEPT-CTI, a framework that pinpoints out the appropriate cyber deception strategies based on the extracted CTI knowledge from unstructured reports:
  - We propose and test SecBert and SecRoBERTa transformers for relevant CTI sentences extraction from unstructured reports, as a binary classification task.
  - We propose and test SecBert-BiLSTM-CRF and SecRoBerta-BiLSTM-CRF models for low-level and high-level IoCs identification, as an NER task.
  - We propose and test SecBert and SecRoBERTa transformers for the mapping of extracted CTI data to MITRE ATT&CK, as a multi-label classification task.
  - We propose an analytical scheme based on MITRE D3FEND and MITRE Engage for the mapping of extracted CTI data to appropriate cyber deception strategies.

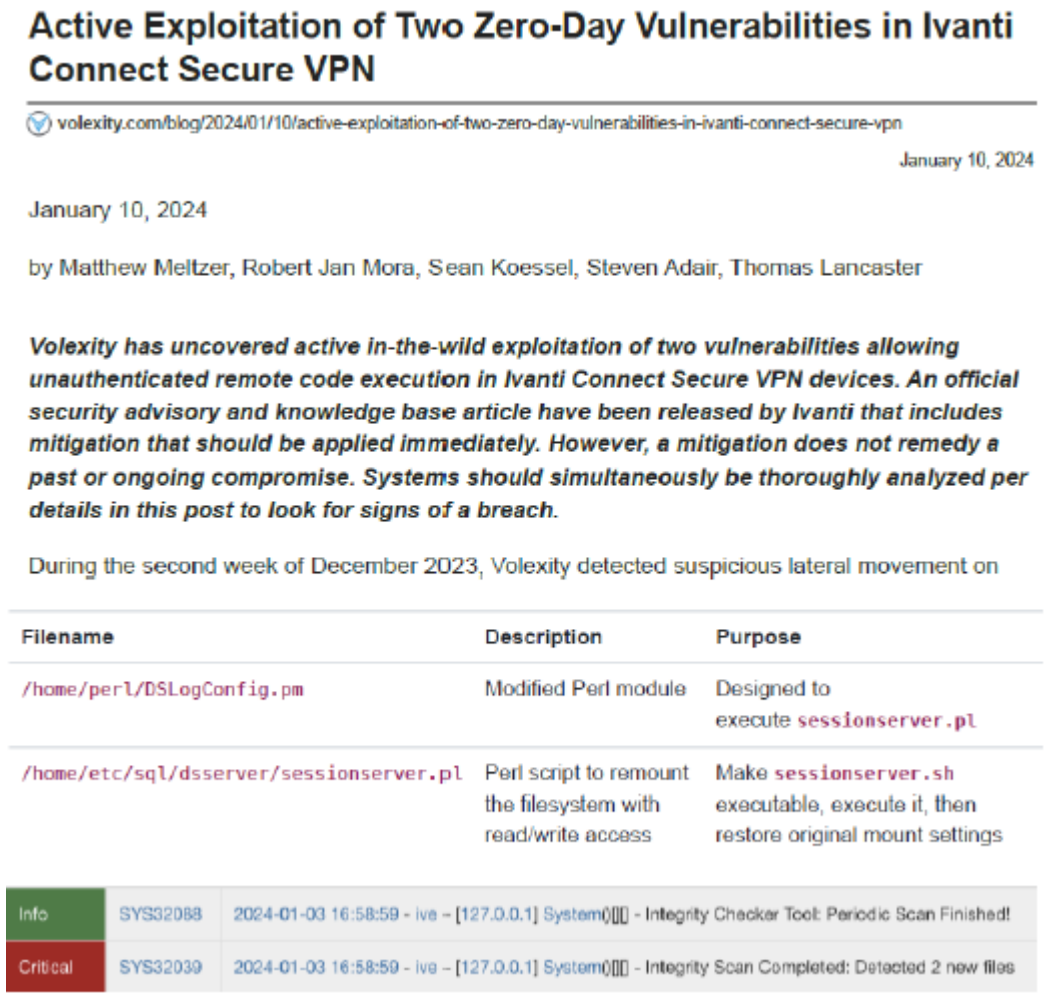
Proposed Solution Architecture



Experiments and Analysis

1- Data Preprocessing

- **Content Parsing**
  - **pdfminer.six** to extract content from textual descriptions
  - **OCR pytesseract** to extract content from images
  - **pdfplumber** to extract content from tables



Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN

volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn

January 10, 2024

January 10, 2024

by Matthew Meltzer, Robert Jan Mora, Sean Koessel, Steven Adair, Thomas Lancaster

Volexity has uncovered active in-the-wild exploitation of two vulnerabilities allowing unauthenticated remote code execution in Ivanti Connect Secure VPN devices. An official security advisory and knowledge base article have been released by Ivanti that includes mitigation that should be applied immediately. However, a mitigation does not remedy a past or ongoing compromise. Systems should simultaneously be thoroughly analyzed per details in this post to look for signs of a breach.

During the second week of December 2023, Volexity detected suspicious lateral movement on

Filename	Description	Purpose
/home/perl/DSLogConfig.pm	Modified Perl module	Designed to execute sessionserver.pl
/home/etc/sql/dsserver/sessionserver.pl	Perl script to remount the filesystem with read/write access	Make sessionserver.sh executable, execute it, then restore original mount settings

Info	SYS32088	2024-01-03 16:58:59 - ive – [127.0.0.1] System()[][] - Integrity Checker Tool: Periodic Scan Finished!
Critical	SYS32039	2024-01-03 16:58:59 - ive – [127.0.0.1] System()[][] - Integrity Scan Completed: Detected 2 new files

Experiments and Analysis

1- Data Preprocessing

- Text Cleaning with Regular Expressions (RegEx)

.	any characters
\w	alpha or numberic values or & or _
\d	digits
\s	space
[A-Z]	letter in uppercase from A to Z
\u	uppercase letters
[a-z]	letter in uppercase from a to z
\l	lowercase letters
[0-9]	number from 0 to 9
[abc]	a or b or c (any character in the set)
[^abc]	except a b c in the set
\W	NOT alpha or numberic values or & or _
\D	NOT digits
\S	NOT space
\special_characters	$ ^ {} () [] | * + \ ?

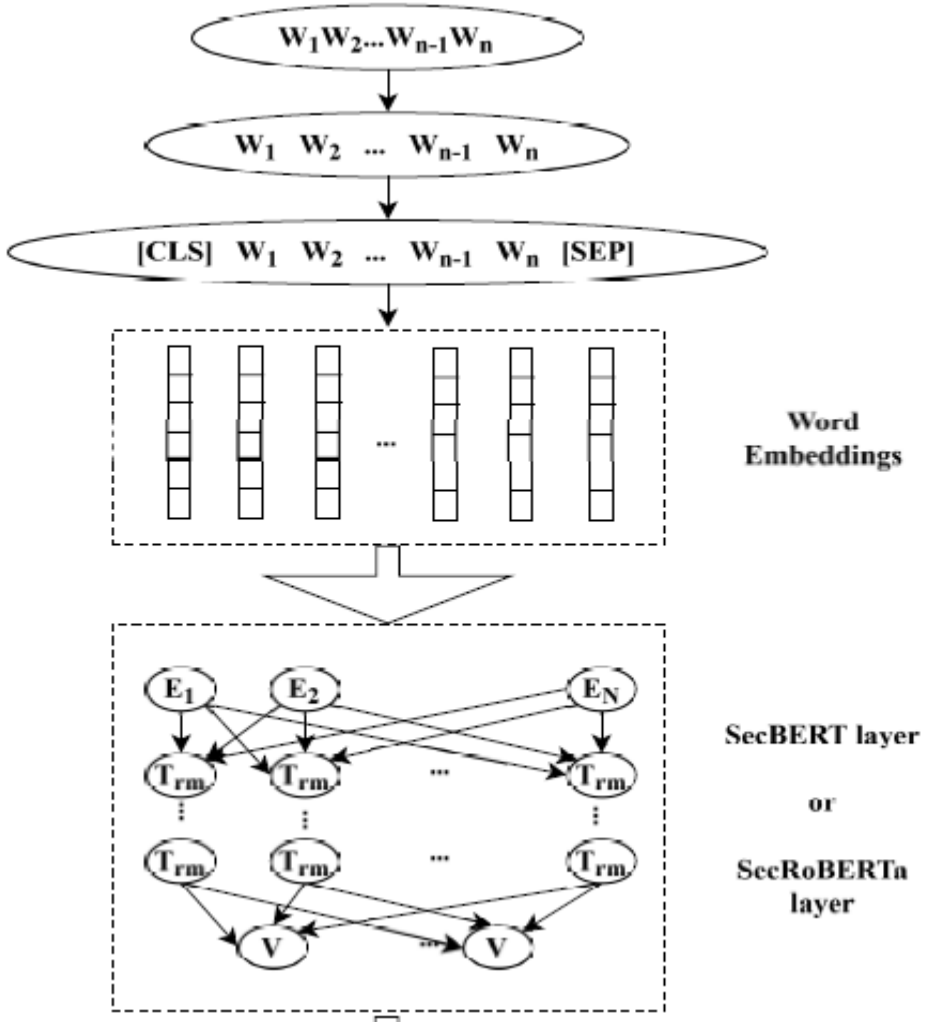
- Sentence Segmentation with Natural Language Toolkit (NLTK)

```
nltk.download('punkt')
sentences = nltk.sent_tokenize(paragraph)
```

Experiments and Analysis

2- Relevant CTI Sentences Extraction

- A publicly available dataset: contains a set of sentences and their corresponding labels (1 for a positive example, and 0 for a negative one)
- SecBERT: a variant of BERT (Bidirectional Encoder Representations from Transformers), designed for cybersecurity-related tasks -> we fine-tuned the pre-trained transformer model from Huggingface's transformers library
- SecRoBERTa: a variant of RoBERTa (A Robustly Optimized BERT Pretraining Approach), designed for cybersecurity-related tasks -> we fine-tuned the pre-trained transformer model from Huggingface's transformers library



Experiments and Analysis

2- Relevant CTI Sentences Extraction

- SecBERT tokenizer/ SecRoBERTa tokenizer: a maximum sequence length of 128 tokens
- AdamW optimizer, a learning rate of 1e-5, a batch size of 16, and 10 epochs

Results for the Binary Sentence Classification

Model	Accuracy	Precision	Recall	F1-score
SecRoBERTa	0.875661	0.874317	0.869565	0.871935
SecBERT	0.841270	0.829787	0.847826	0.838710

Volexity found that an attacker was placing webshells on multiple internal and external-facing web servers.

The attacker modified a legitimate ICS VPN component (compcheckresult.cgi) to support execution of remote command.

UTA0178 planted webshells on external-facing web servers in order to grant persistence to the customer environment.

In multiple instances, the attacker was able to use credentials they had compromised to log into various workstations and servers and dump the memory of the LSASS process to disk using Task Manager.

The attacker then exfiltrated this output to extract further credentials offline.

Lateral movement using compromised credentials to connect to internal systems via RDP, SMB, and SSH.

Examples of Extracted Relevant CTI Sentences

Experiments and Analysis

3- Low-level & High-level IoCs Identification

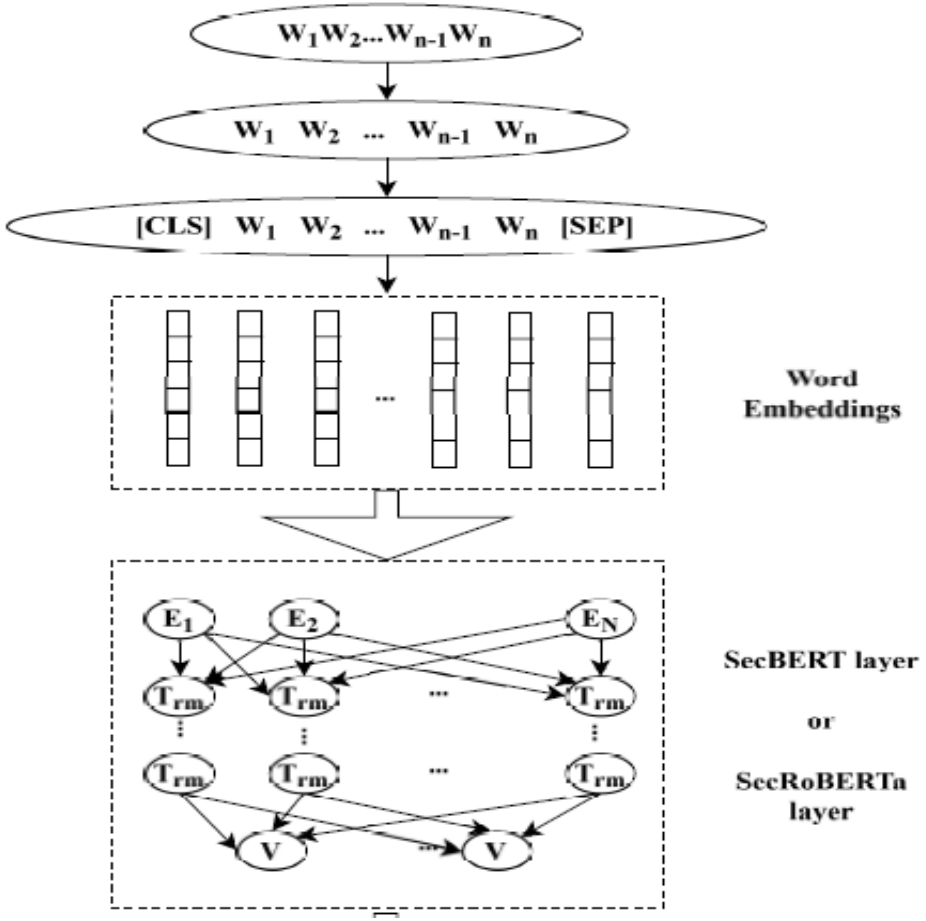
- A publicly available dataset called 2APTNER, and complies with the STIX 2.1 standard, includes a set of tokens labeled with 21 entities tagged with a BIOES (beginning, inside, outside, end, or single) tagging scheme

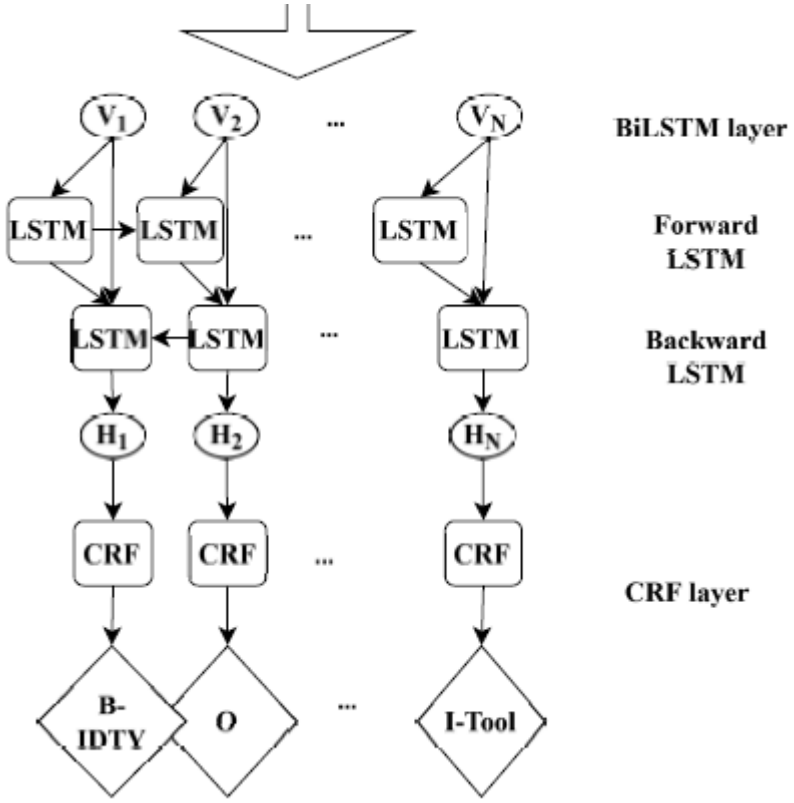
- SecBERT-BiLSTM-CRF / SecRoBERTa-BiLSTM-CRF
  - SecBERT or SecRoBERTa model for initial embedding generation
  - BiLSTM layer for processing word vectors
  - CRF layer for sequence tagging and classification

- SecBERT tokenizer/ SecRoBERTa tokenizer: a maximum sequence length was set to 256 tokens
- AdamW optimizer, a learning rate of 3e-5, a batch size of 16, and 10 epochs

Experiments and Analysis

3- Low-level & High-level IoCs Identification





Named Entity Recognition Models

Experiments and Analysis

3- Low-level & High-level IoCs Identification

206.189.208.156

75.145.243.85

50.243.177.161

98.160.48.170

gpoaccess[.]com

webb-institute[.]com

symantke[.]com

Examples of Identified IoCs

Comparison of NER Results for Different Entities

Entity	SecBERT-BiLSTM-CRF			SecRoBERTa-BiLSTM-CRF		
	Precision (%)	Recall (%)	F1-Score (%)	Precision (%)	Recall (%)	F1-Score (%)
ACT	55.12	67.34	61.28	62.47	70.21	66.19
APT	81.58	87.23	84.33	83.10	89.42	86.12
DOM	91.43	88.25	89.81	92.64	91.37	91.99
EMAIL	66.74	55.86	60.76	70.55	58.43	64.02
ENCR	84.32	90.48	87.29	86.18	92.61	89.28
FILE	71.50	74.13	73.10	73.27	76.35	74.80
IDTY	70.23	80.12	75.31	72.45	82.89	77.32
IP	93.67	93.45	93.56	95.21	95.34	95.27
LOC	87.45	89.13	88.28	89.74	91.08	90.40
MAL	70.58	71.32	71.00	72.19	73.41	72.79
MD5	68.23	62.67	65.33	70.43	66.81	68.57
OS	75.83	76.45	76.14	78.39	80.27	79.32
PROT	70.00	75.12	72.46	72.31	77.64	74.86
SECTEAM	85.74	87.63	86.68	87.93	89.75	88.83
SHA2	75.38	95.42	84.24	77.54	97.38	86.41
TIME	85.92	89.73	87.78	87.24	91.05	89.10
TOOL	52.34	56.87	54.52	55.47	58.29	56.84
URL	87.62	69.81	77.75	89.34	71.58	79.47
VULID	97.43	95.89	99.16	97.52	97.00	98.12
VULNAME	51.37	50.92	51.14	53.21	52.84	53.02

Overall Performance Results for the NER Models

Model	Accuracy	Precision	Recall	F1-score
SecRoBERTa-BiLSTM-CRF	0.897661	0.758916	0.784506	0.770063
SecBERT-BiLSTM-CRF	0.872470	0.731187	0.763015	0.745710

Experiments and Analysis

4- Mapping to MITRE ATT&CK Tactics & Techniques

- A publicly available dataset: includes a set of sentences labeled with the corresponding attack tactics and techniques.
- Multi-label classification task
- AutoTokenizer from the SecBERT/ SecRoBERTa models
- A batch size of 16, a learning rate of 3e-5, and 10 epochs

Overall Performance for Multi-Label Classification

Model	Techniques				Tactics			
	Accuracy	Precision	Recall	F1-score	Accuracy	Precision	Recall	F1-score
SecRoBERTa	0.784	0.795	0.782	0.788	0.810	0.825	0.813	0.819
SecBERT	0.772	0.782	0.771	0.775	0.798	0.812	0.801	0.807

- Lateral movement using compromised credentials to connect to internal systems via RDP, SMB, and SSH

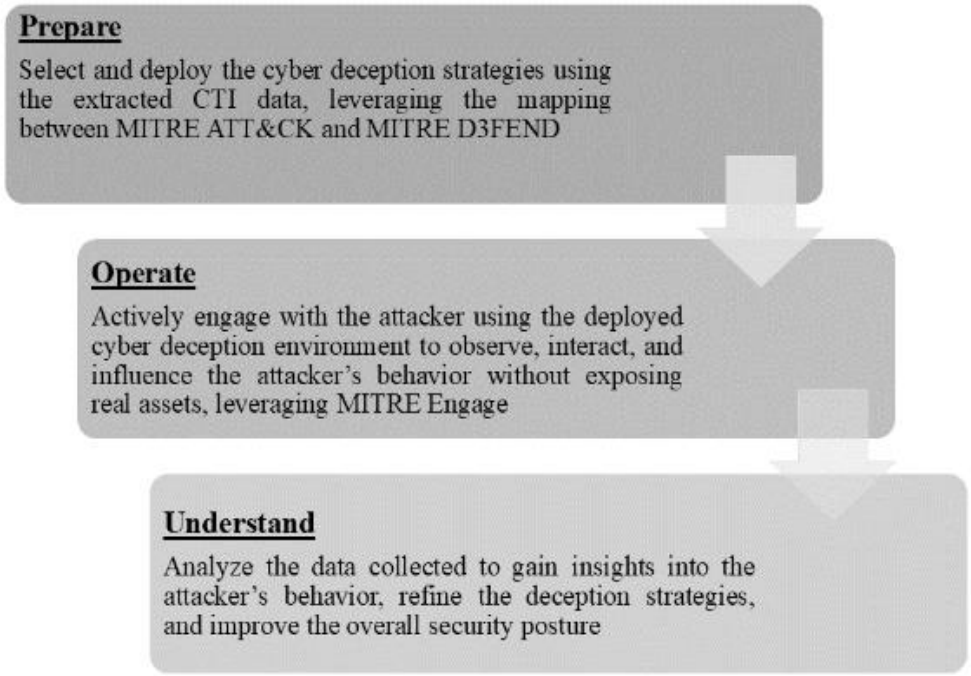
B-ACT **I-IDTY** **I-LOC** **I-TOOL**

→ **Lateral Movement via RDP -> T1021.001**

Experiments and Analysis

5- Cyber Deception Setup Selection

- Analytical scheme based on MITRE D3FEND and MITRE Engage



Cyber Deception Selection Scheme

Recommended Deception Techniques for Identified Attack Techniques and Tactics

Attack Technique	Attack Tactic	Recommended Deception Techniques
Webshell Injection (T1505.003)	Persistence	Deploy honey webshells mimicking vulnerable apps to attract attackers.
Credential Dumping via LSASS (T1003.001)	Credential Access	Use decoy credentials in memory to mislead attackers while monitoring them.
Lateral Movement via RDP (T1021.001)	Lateral Movement	Set up deceptive RDP sessions on decoy systems simulating critical infrastructure.

Conclusion and Perspectives

- **Conclusions**
  - DECEPT-CTI framework to proactively select the appropriate cyber deception strategies given an attacker's profile built based on the extracted CTI data
    - Relevant CTI sentences extraction from unstructured reports leveraging SecBert and SecRoBERTa transformers
    - Low-level and high-level IoCs identification using SecBERT-BiLSTM-CRF,and SecRoBERTa-BiLSTM-CRF models
    - Extracted CTI data mapping to MITRE ATT&CK tactics and techniques using SecBert and SecRoBERT
    - Analytical scheme based on MITRE D3FEND and MITRE Engage for appropriate cyber deception strategies selection

Conclusion and Perspectives

- **Perspectives**
  - A Reinforcement learning-based bidirectional approach
    - Leveraging CTI data to identify and deploy optimal deception strategies
    - Using the outcomes of these strategies to collect and generate new CTI data

THANK YOU FOR YOUR ATTENTION

E-mail: amal.sayari@supcom.tn