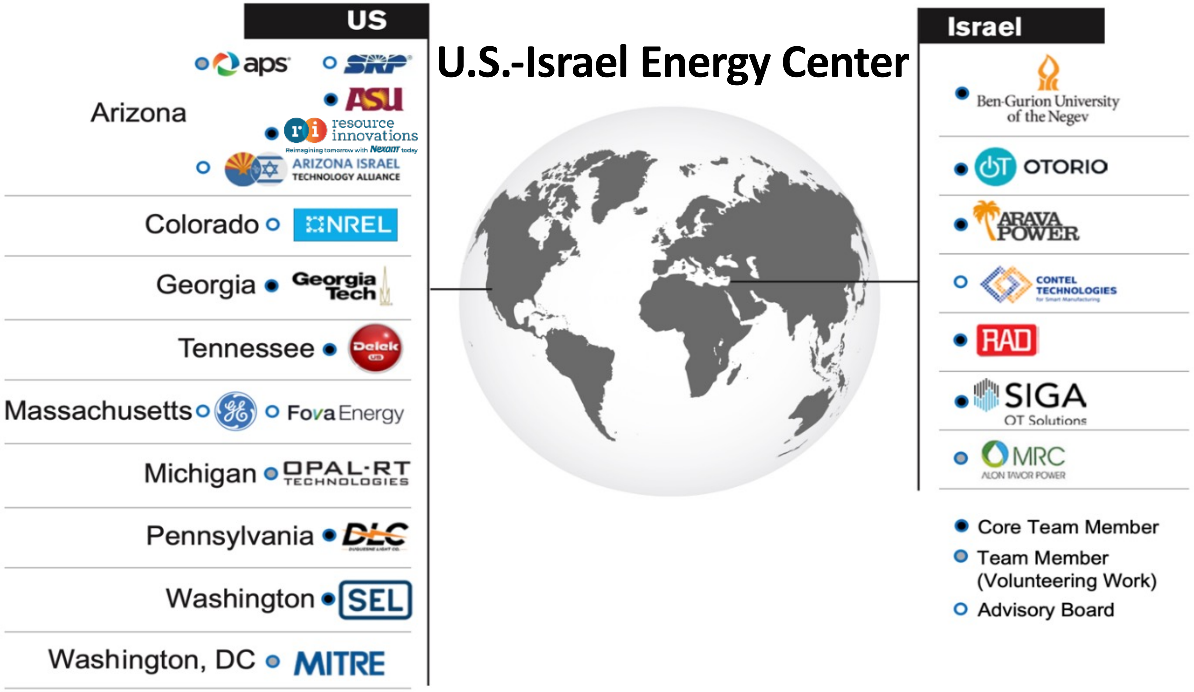
Task 4
Multi-Level Threat Intelligence Knowledge Base



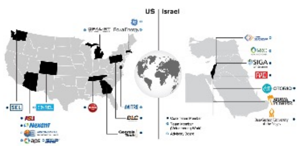
U.S.-Israel Energy Center ICRDE Workshop V

Nir Daniel

BGU

October 9th, 2023

Outline



Task 6 – Threat Hunting

“Labeling NIDS Rules with MITRE ATT&CK Techniques using ChatGPT”

Nir Daniel, Florian Klaus Kaiser, Anton Dzega, Aviad Elyashar, and Rami Puzis

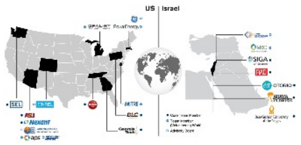
Accepted in The 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2023)

Task 4 – Multi-Level Threat Intelligence Knowledge Base

Extracting Observed Data from ICS Malware Reports (CybOX4ICS)

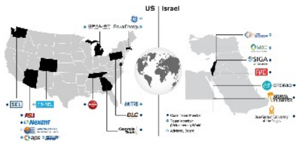
Rubin Krief

What is an Observable?



Any piece of information or data that can be used to detect or analyze a cyber threat or attack.

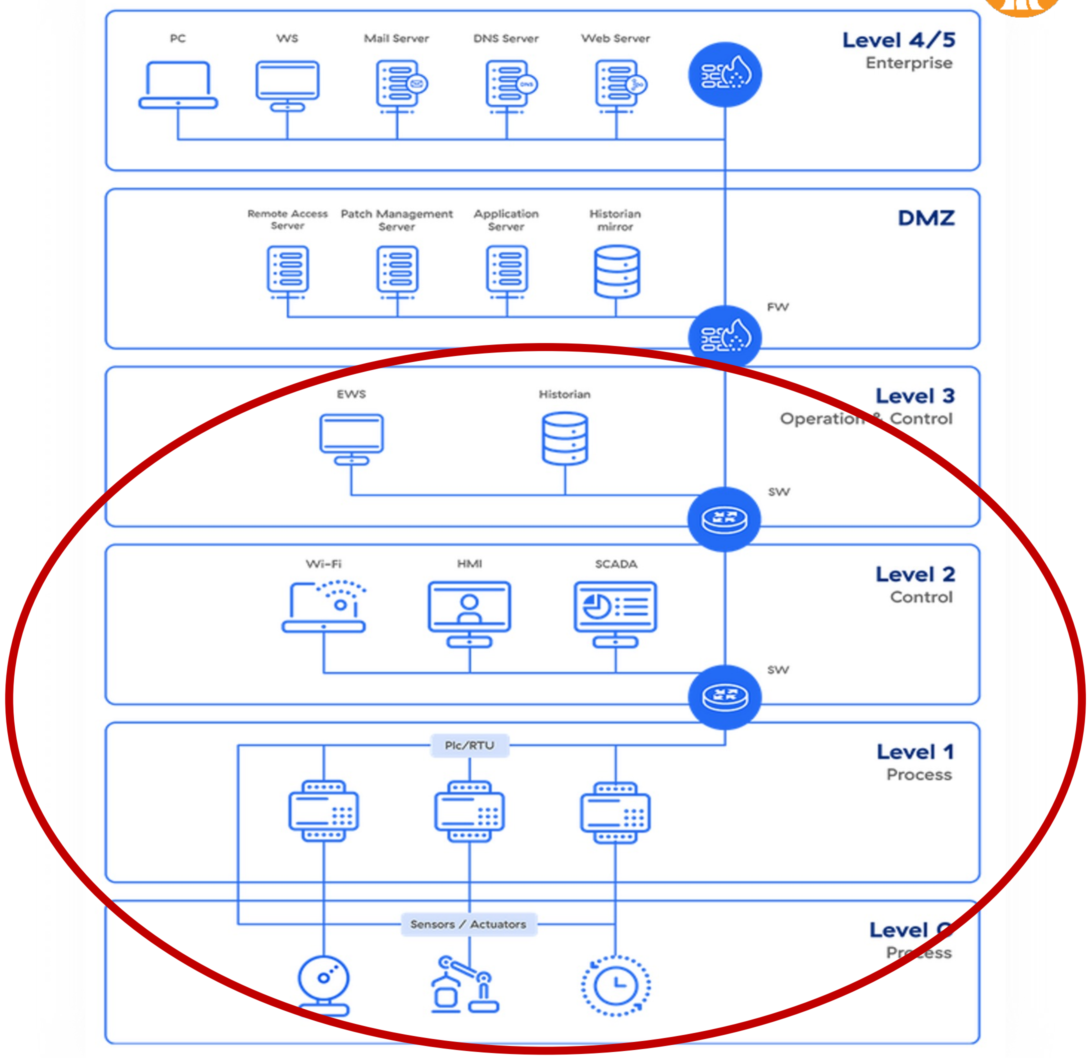
Goal



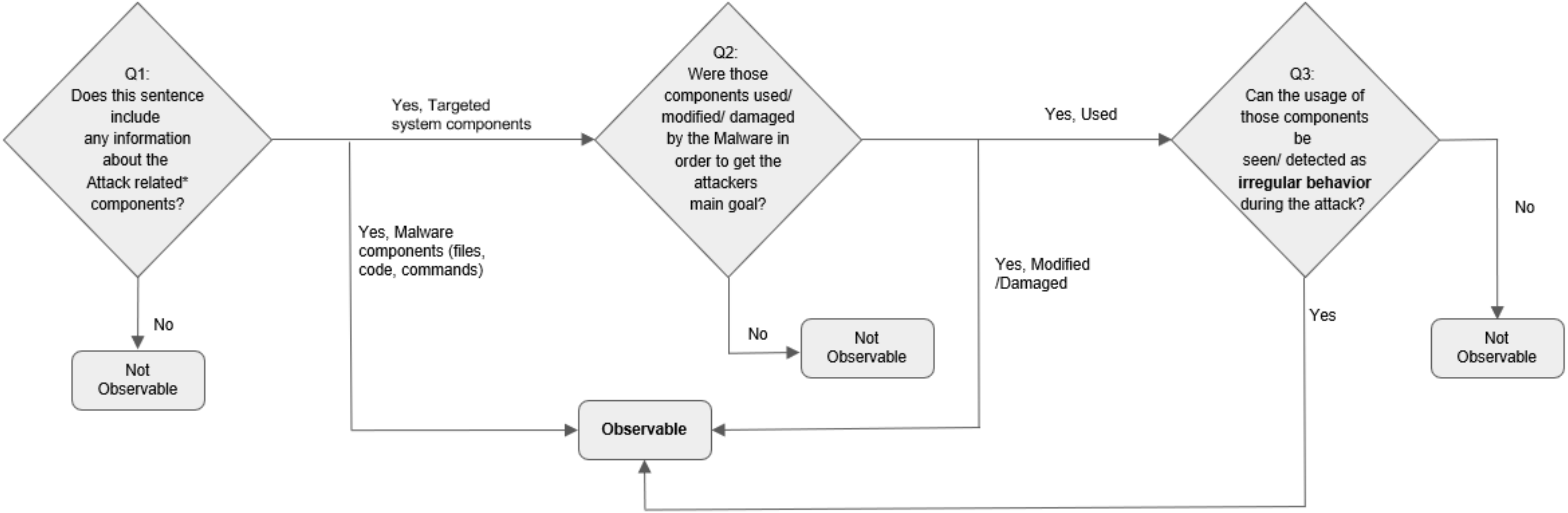
Extract ICS (OT level) observables from attack incident reports

↓

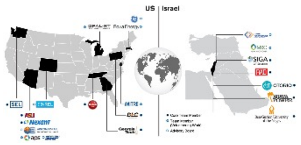
Q: Does this sentence contain an observable?



Rubric For Identifying Observables In a Sentence

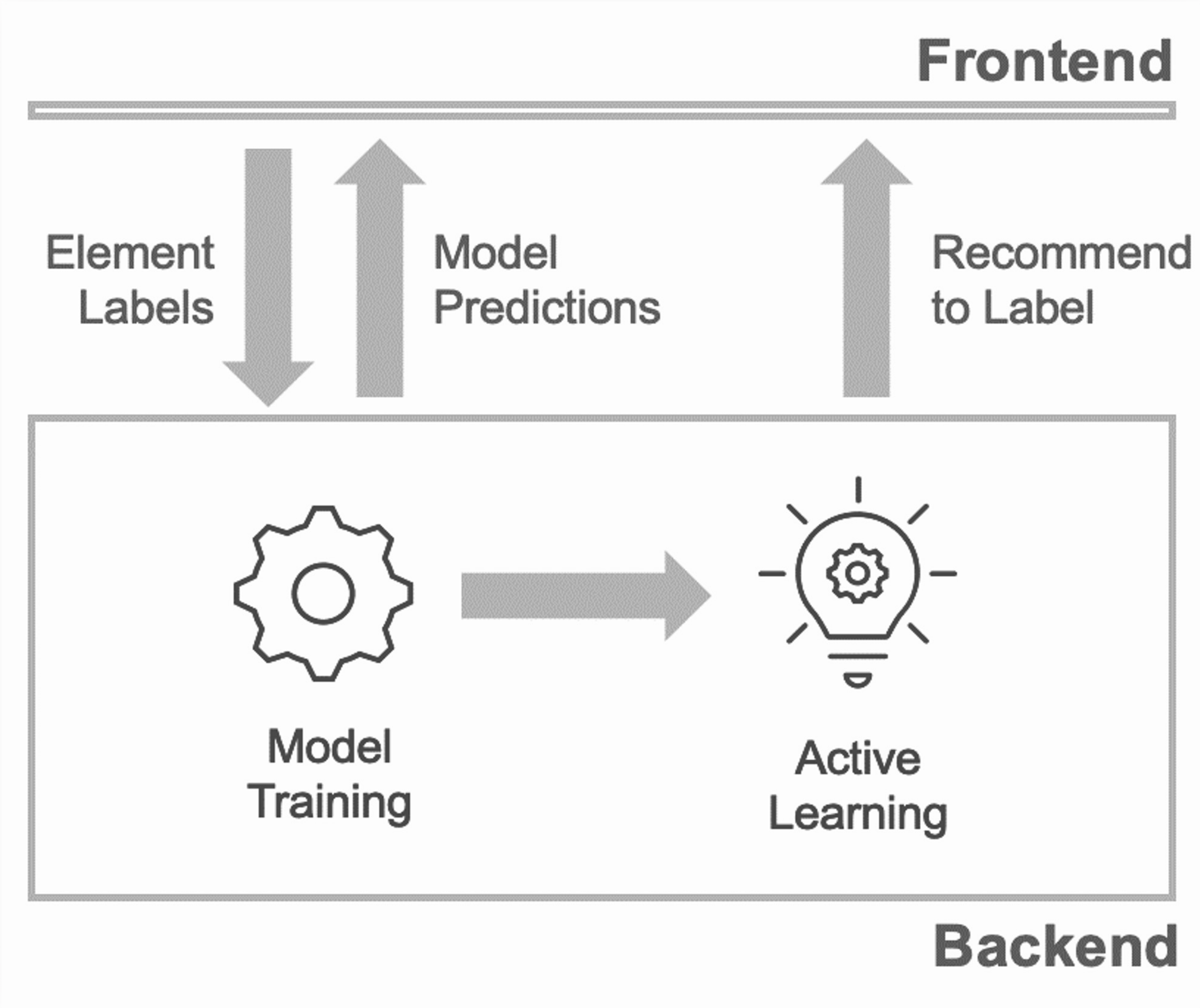

Q1:
Does this sentence include any information about the Attack related* components?
No
Not Observable
Yes, Targeted system components
Yes, Malware components (files, code, commands)
Q2:
Were those components used/ modified/ damaged by the Malware in order to get the attackers main goal?
No
Not Observable
Yes, Used
Yes, Modified /Damaged
Q3:
Can the usage of those components be seen/ detected as **irregular behavior** during the attack?
No
Not Observable
Yes
Observable

Label-Sleuth



An open-source, no-code framework designed for text labeling and the construction of text classifiers.

Label-Sleuth



Frontend

Element Labels

Model Predictions

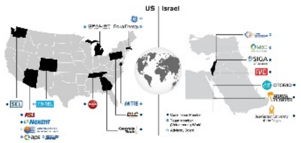
Recommend to Label

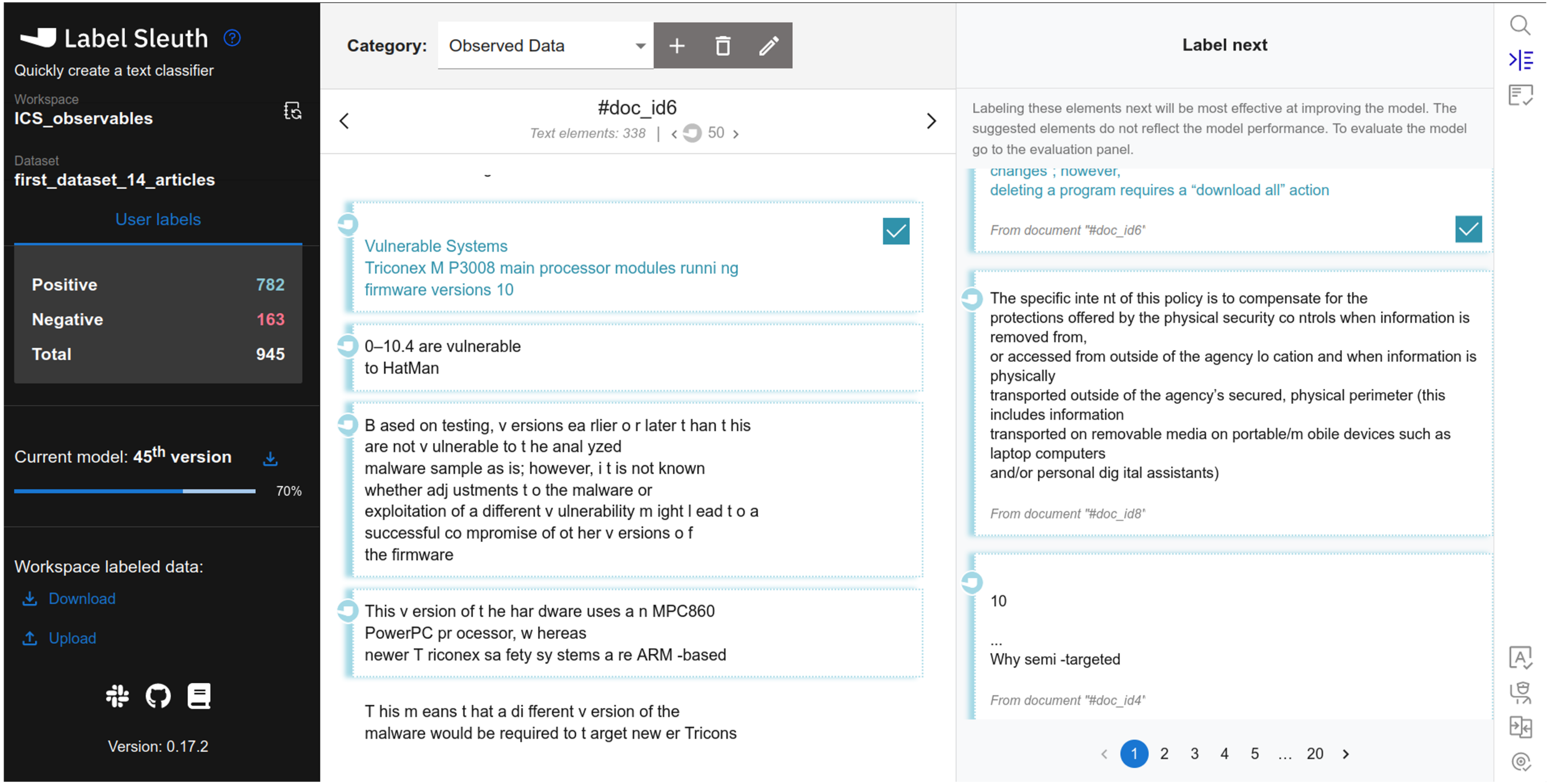
Model Training

Active Learning

Backend

Label-Sleuth – Interface





Label Sleuth

Quickly create a text classifier

Workspace
ICS_observables

Dataset
first_dataset_14_articles

User labels

Positive	782
Negative	163
Total	945

Current model: 45th version

70%

Workspace labeled data:

Download

Upload

Version: 0.17.2

Category: Observed Data

#doc_id6

Text elements: 338 | ‹ 50 ›

Vulnerable Systems
Triconex M P3008 main processor modules runni ng
firmware versions 10

0–10.4 are vulnerable
to HatMan

B ased on testing, v ersions ea rlier o r later t han t his
are not v ulnerable to t he anal yzed
malware sample as is; however, i t is not known
whether adj ustments t o the malware or
exploitation of a different v ulnerability m ight l ead t o a
successful co mpromise of ot her v ersions o f
the firmware

This v ersion of t he har dware uses a n MPC860
PowerPC pr ocessor, w hereas
newer T riconex sa fety sy stems a re ARM -based

T his m eans t hat a di fferent v ersion of the
malware would be required to t arget new er Tricons

Label next

Labeling these elements next will be most effective at improving the model. The suggested elements do not reflect the model performance. To evaluate the model go to the evaluation panel.

changes ; however,
deleting a program requires a “download all” action

From document "#doc_id6"

The specific inte nt of this policy is to compensate for the
protections offered by the physical security co ntrols when information is
removed from,
or accessed from outside of the agency lo cation and when information is
physically
transported outside of the agency’s secured, physical perimeter (this
includes information
transported on removable media on portable/m obile devices such as
laptop computers
and/or personal dig ital assistants)

From document "#doc_id8"

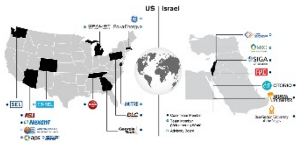
10

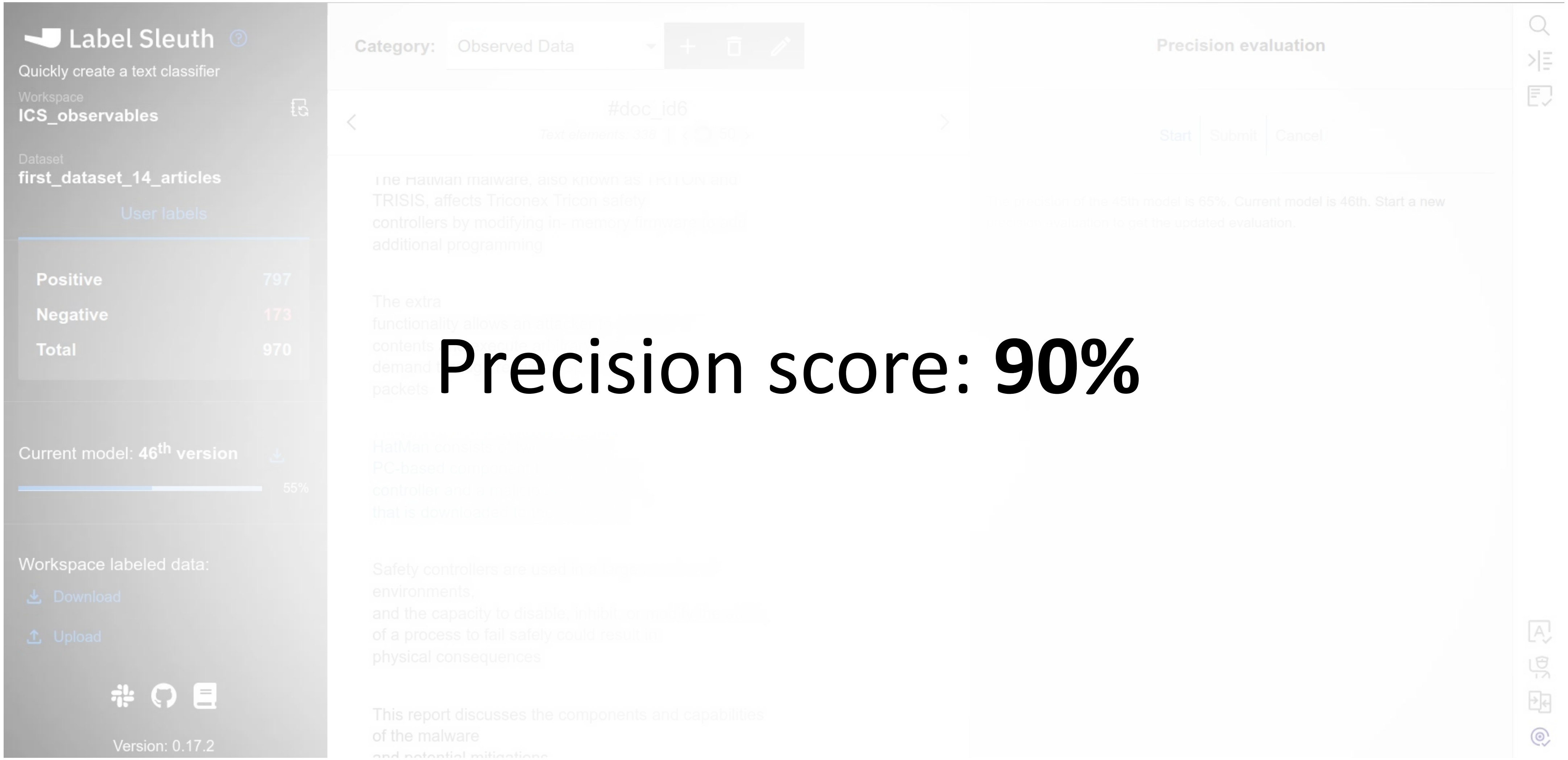
...
Why semi -targeted

From document "#doc_id4"

‹ 1 2 3 4 5 ... 20 ›

Label-Sleuth – Interface





Workspace
ICS_observables

Dataset
first_dataset_14_articles

Positive	797
Negative	173
Total	970

Current model: 46th version

55%

Workspace labeled data:

Version: 0.17.2

Category: Observed Data

#doc_id6

Text elements: 338 | 50

The HatMan malware, also known as TRITON and TRISIS, affects Triconex Tricon safety controllers by modifying in- memory firmware to add additional programming

The extra functionality allows an [illegible] contents [illegible] execute arbitrary [illegible] demand [illegible] packets

HatMan consists [illegible] PC-based comp[illegible] controller and a [illegible] that is downloaded [illegible]

Safety controllers are used in [illegible] environments, and the capacity to disable, inhibit, or [illegible] of a process to fail safely could result in physical consequences

This report discusses the components and capabilities of the malware and potential mitigations

Precision evaluation

The precision of the 45th model is 65%. Current model is 46th. Start a new precision evaluation to get the updated evaluation.

Precision score: **90%**

Thank You!

Any Questions?