SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

Introduction, Highlights and Results

Mischa Obrecht

Dreamlab Technologies AG

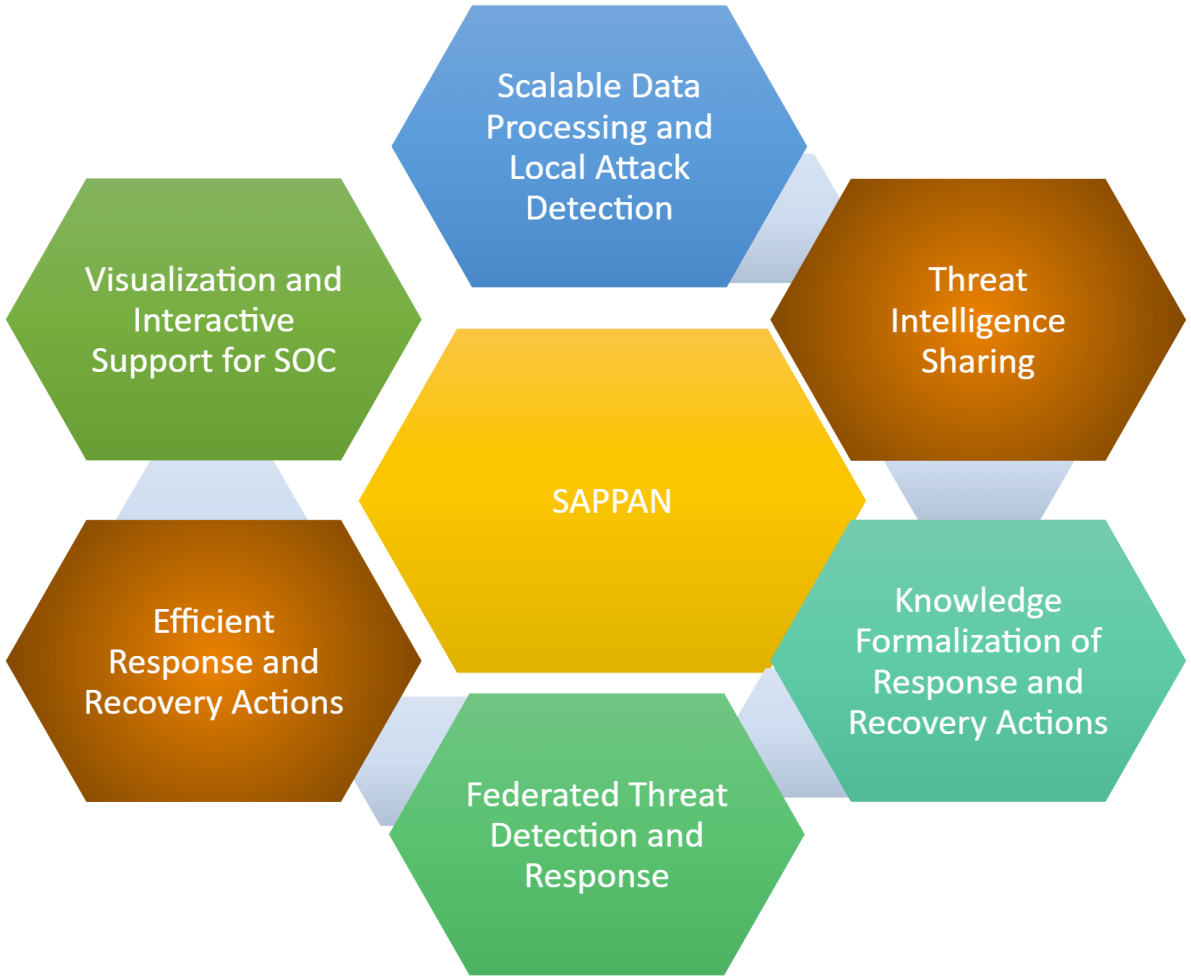
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Outline

- Project overview
- Research areas
- Spotlights:
  - Neural Nets for Domain Generation Algorithm Detection
  - Response automation
  - Sharing of playbooks
- Conclusion

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

SAPPAN project



Fraunhofer FIT

Hewlett Packard Enterprise

cesnet

F-Secure

DREAMLAB TECHNOLOGIES

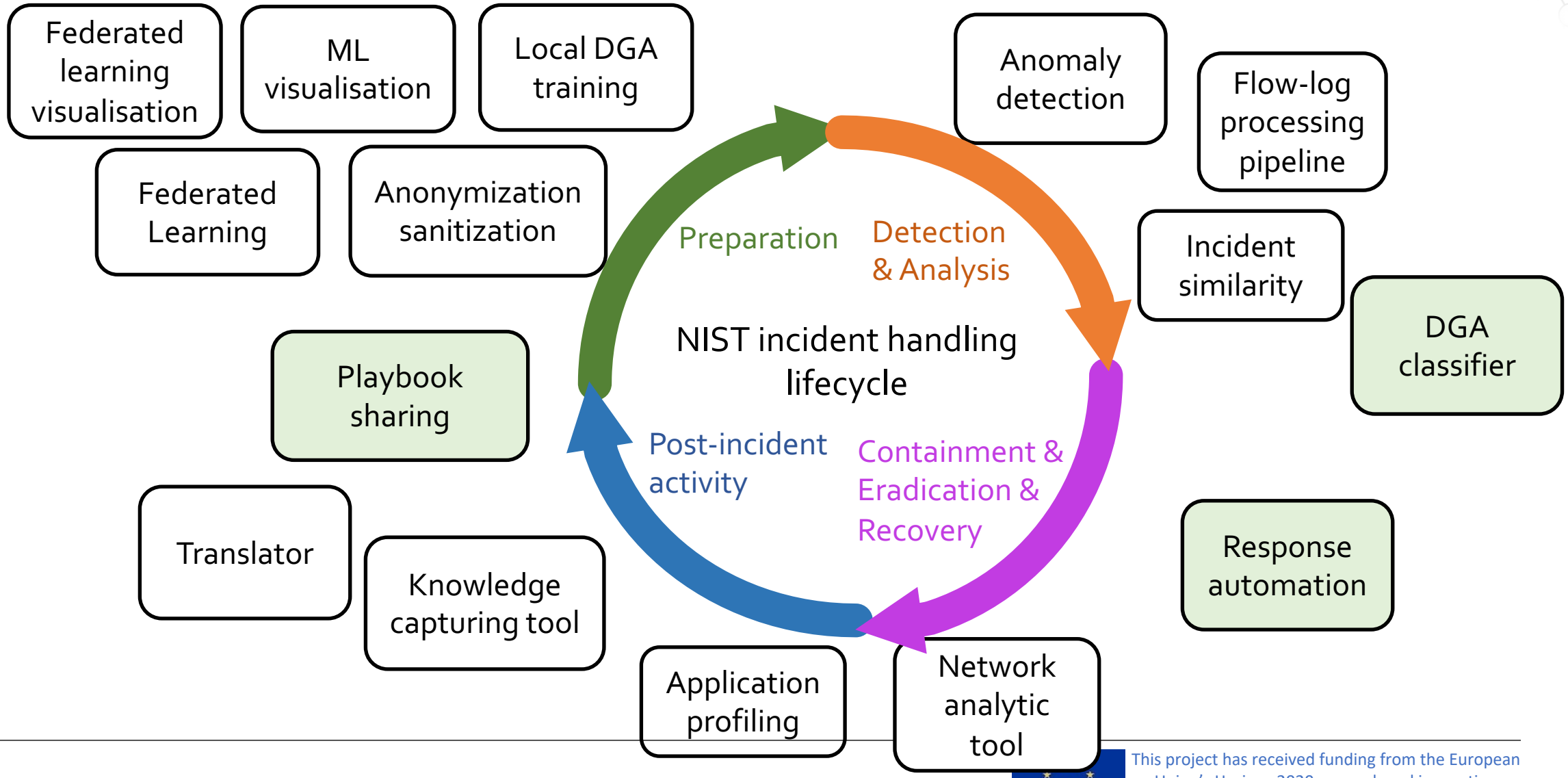
Universität Stuttgart

MUNI

RWTH AACHEN UNIVERSITY

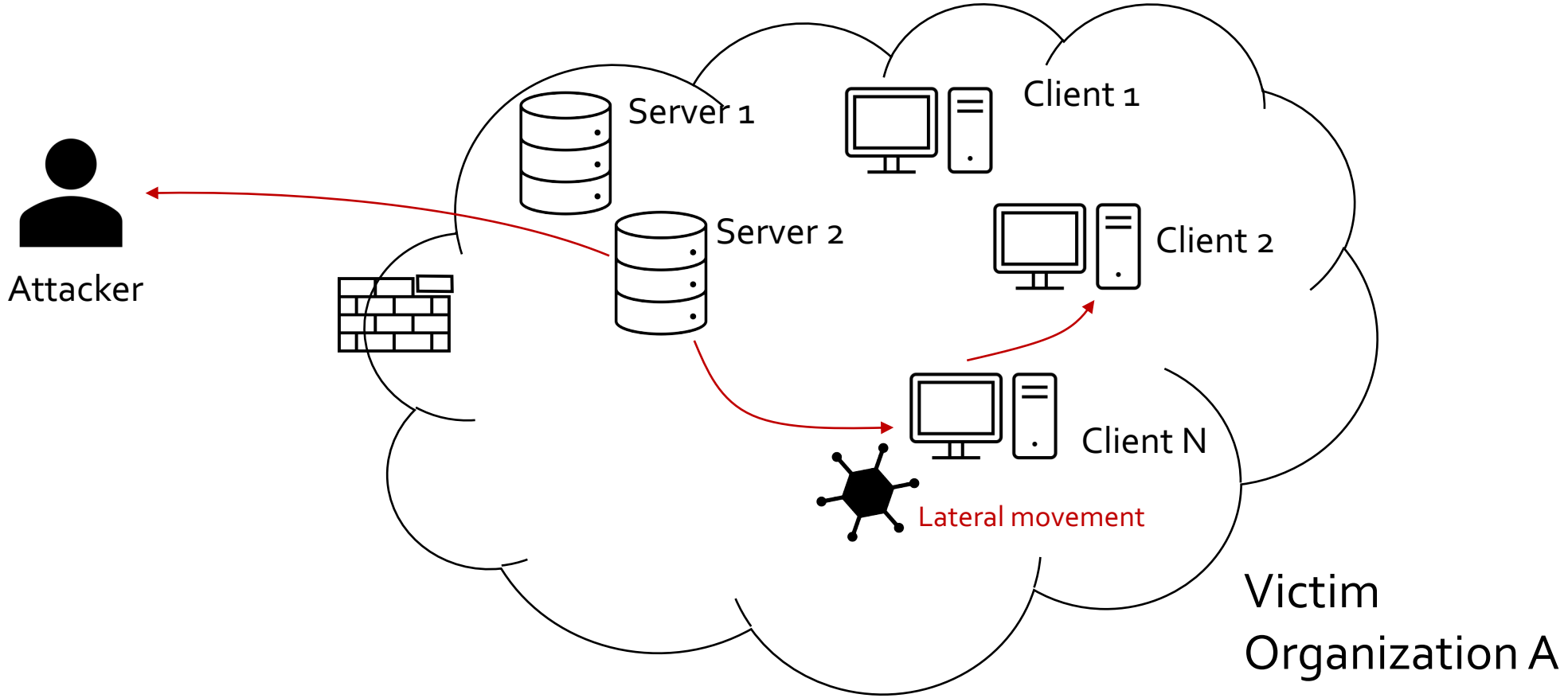
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Areas of research



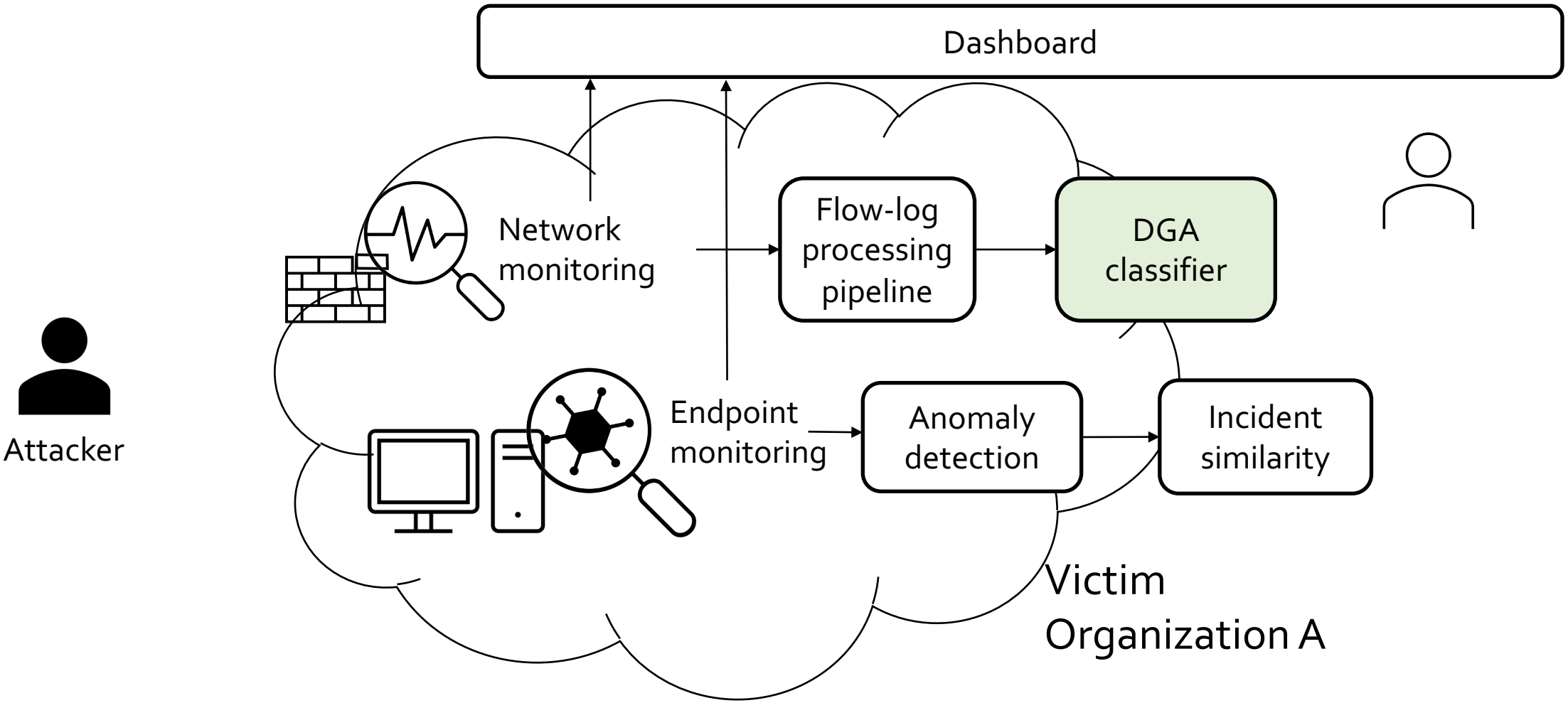
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

A day in the live of Victim Organization A



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

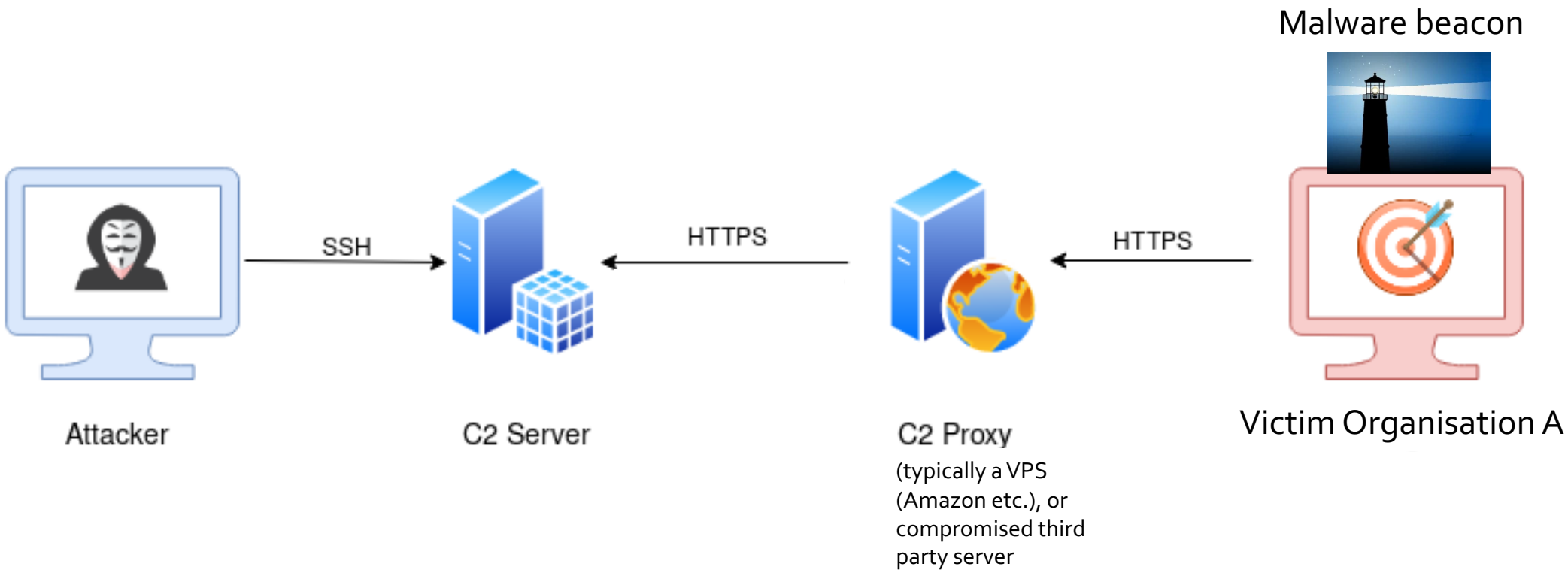
SAPPAN Detection and analysis



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Domain Generation Algorithms (DGA)

A typical setup of modern, remote controlled malware



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Domain Generation Algorithms (DGA)

Goal: Reaching the C2-Proxy in the internet to:

- Receive new instructions
- Deliver data to attacker

Old days:

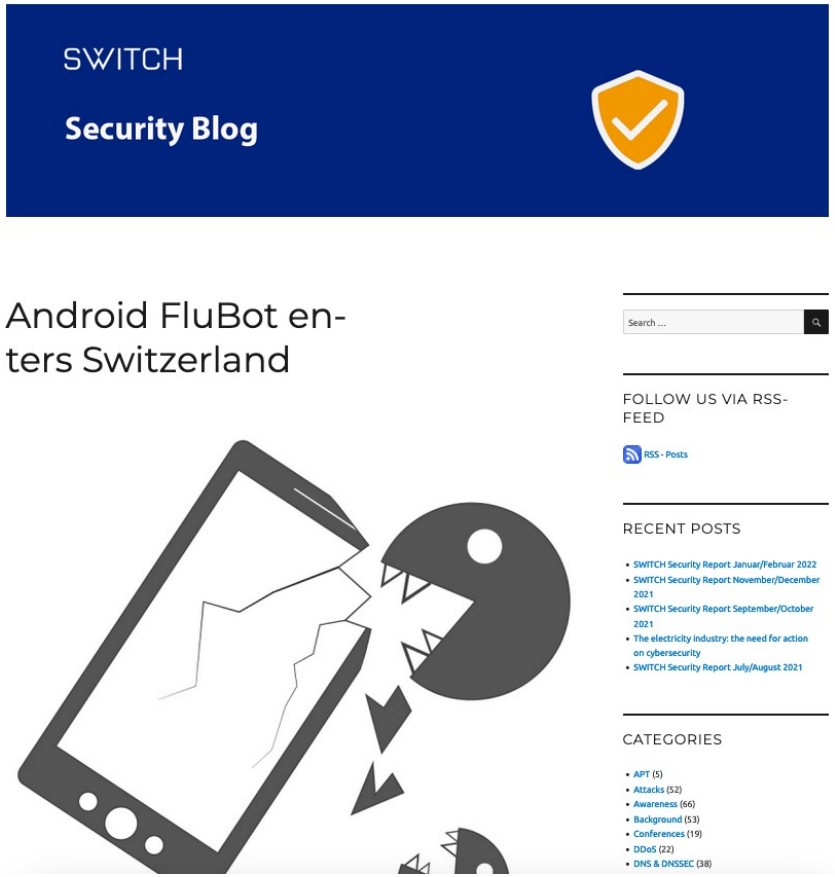
- Hardcoded IP-addresses / URLs

Today / modern aproach:

- Dynamic creation of domain names / URLs
- BPredefined schema / algorithm
  - ➔ Algorithmically generated domains (AGDs)
  - ➔ Domain Generating Algorithms (DGAs)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Domain Generation Algorithms (DGA)



Example:
https://securityblog.switch.ch/2021/06/19/android-flubot-enters-switzerland/

Resulting examples:

- *generate_domain(2020,11,12) ➔ ovyvwnkjserklcrj.com*
- *generate_domain(2020,10,1) ➔ mlnmewqrfchttjcl.com*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

DGA detection - Results

Finding 9 needles in the *.ch domain haystack

Detecting suspicious *.ch-domains using deep neural networks

30 August 2021

By Mischa Obrecht

We have recently witnessed the advent of artificial intelligence, machine and deep learning technologies, which have led to a tremendous amount of interest from almost every other area of science, technology and business. The area of cyber-security is no exception. It is however interesting, that most security vendors and consultants keep a cloak of silence around specific AI-enabled cyber-security use cases and thus specific examples of how AI and machine learning are used in the context of cyber-security are rather scarce.

This blog post is about introducing such a use case where we successully attempt to use deep neural networks to identify suspicious domains in the full *.ch domain-space.

https://dreamlab.net/en/blog/post/detecting-suspicious-ch-domains-using-deep-neural-networks/

Model Input	Model Output	Analysis / Conclusion (Analyst)
Domain	Certainity	
abcdefghijklmnopqrstuvwxyz.ch	100%	Likely malicious
adslkfalkfjlkfjdsalkfafljflsa.ch	100%	Unclear, no IP resolution
8qswldnsrvb73xkczdyj.ch	99.90%	Likely malicious
rgdfgdfgdfgdf.ch	99.90%	no suspicious observations
utitan101310bgfhnythjdukfdyjt.ch	99.80%	no suspicious observations
sfdfgdfgdfgdfgdfg.ch	99.80%	Unclear, no IP resolution
n7q9ipiddq9ihtx.ch	99.10%	Likely malicious
testhgfjdgdfxhgxdfhx12.ch	99.10%	Likely malicious
oiqweurpui345345jk.ch	94.10%	no suspicious observations
ymfvrcnwyw.ch	92.50%	Unclear, no IP resolution
aqddddwxszedc.ch	84.80%	Unclear, no IP resolution
ihjj8qltfyfe.ch	82.20%	Likely malicious
asdfjkhdsfajdfsajhsadf.ch	77.10%	no suspicious observations
7as6q796d6s98q6qd6sdq.ch	72.60%	Likely malicious
rggrgrgrgrgrgr.ch	66.50%	Unclear, no IP resolution
fj6f8j1gbwzl.ch	54.60%	Likely malicious
fdsafdahkjfdhajkfdas.ch	52.20%	Likely malicious
xczjhkgdsadsa.ch	51.30%	Likely malicious
ik48lsu5dww485letzk9m7f.ch	51.10%	no suspicious observations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

DGA detection - Results

Improving state of the art and going from binary to multiclass classification

arXiv > cs > arXiv:2006.11103

Computer Science > Cryptography and Security

[Submitted on 19 Jun 2020]

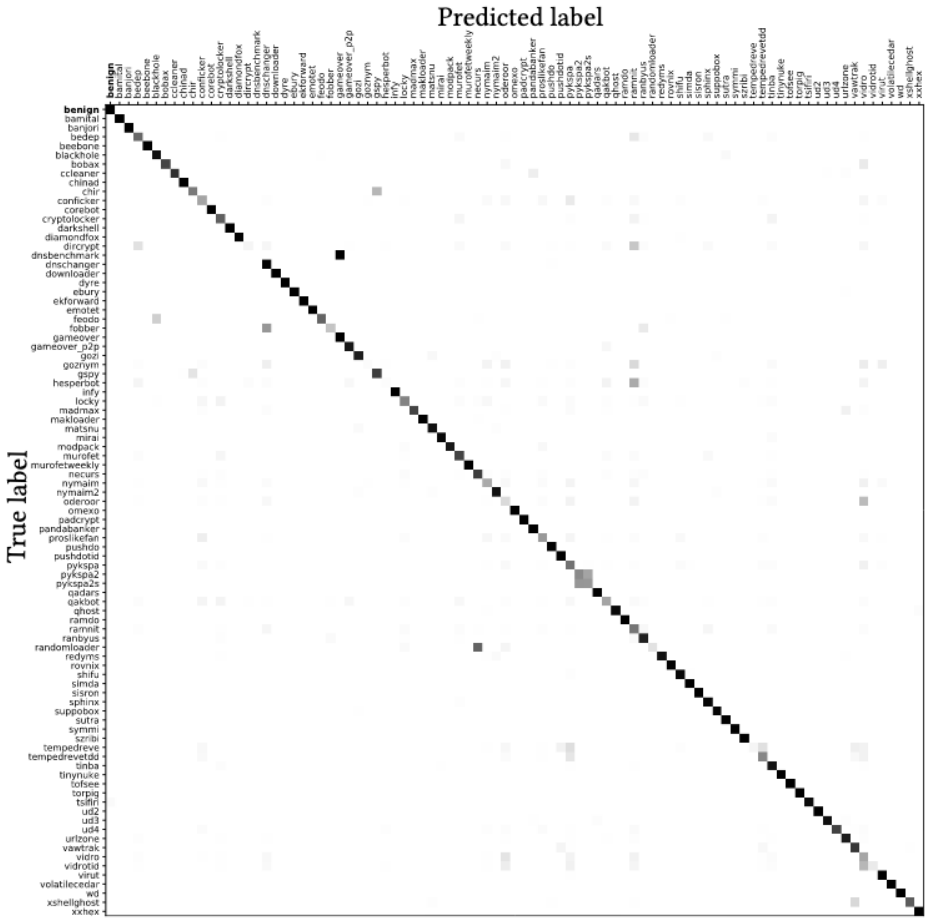
Analyzing the Real-World Applicability of DGA Classifiers

Arthur Drichel, Ulrike Meyer, Samuel Schüppen, Dominik Teubert

Separating benign domains from domains generated by DGAs with the help of a binary classifier is a well-studied exact DGA that generated a domain enabling targeted remediation measures is less well studied. Selecting the m far. These include the questions on which traffic to train in which network and when, just as well as how to assess classifiers are real-time capable. In this paper, we address these issues and thus contribute to bringing DGA dete each of the two tasks and extensively evaluate them as well as previously proposed classifiers in a unified setting training and classification speed. Finally, we show that our newly proposed binary classifier generalizes well to ot

Comments: Accepted at The 15th International Conference on Availability, Reliability and Security (ARES 2020)
Subjects: **Cryptography and Security (cs.CR)**; Machine Learning (cs.LG)
Cite as: arXiv:2006.11103 **[cs.CR]**
(or arXiv:2006.11103v1 **[cs.CR]** for this version)
https://doi.org/10.48550/arXiv.2006.11103
Journal reference: In The 15th International Conference on Availability, Reliability and Security (ARES 2020), ACM, 11 pages
Related DOI: https://doi.org/10.1145/3407023.3407030

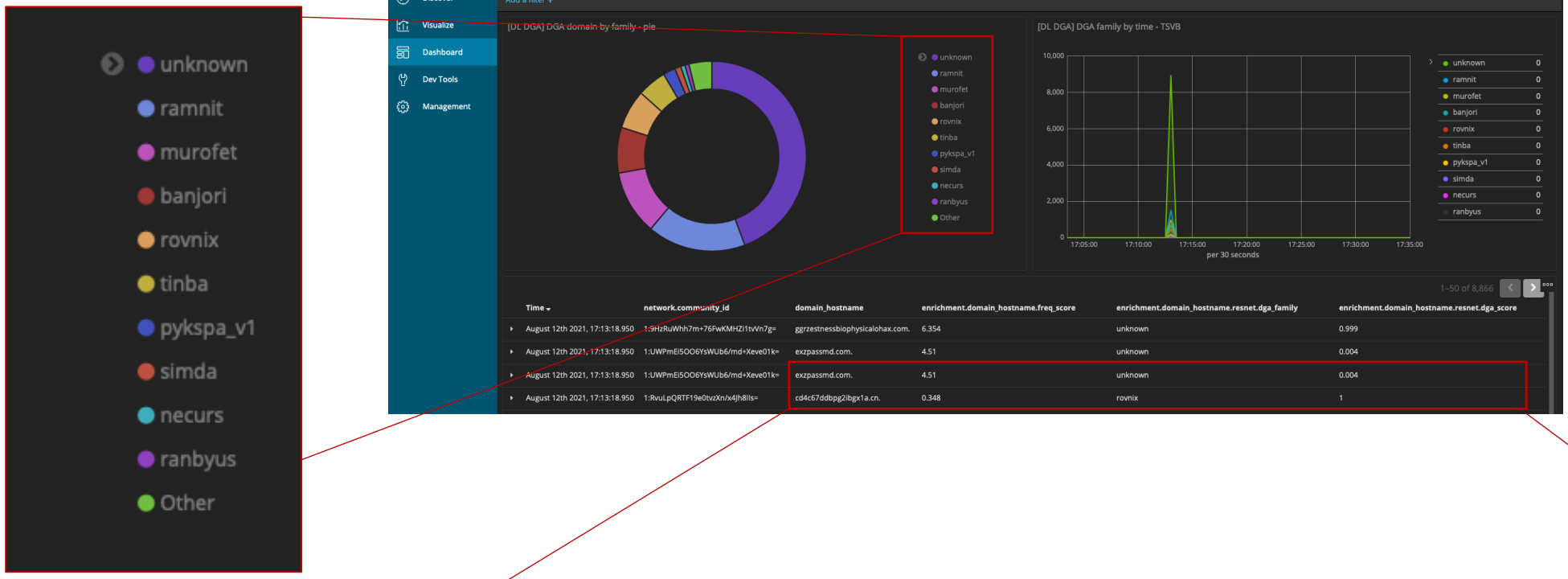
https://arxiv.org/abs/2006.11103



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

DGA detection - Results

POC Implementation in SIEM solution



exzpassmd.com.	4.51	unknown	0.004
cd4c67ddbpg2ibgx1a.cn.	0.348	rovnix	1

DGA detection - Conclusion

Improvements in accuracy and step beyond state of the art

POC Implementation done, adaption underway

➔ Real world applicability

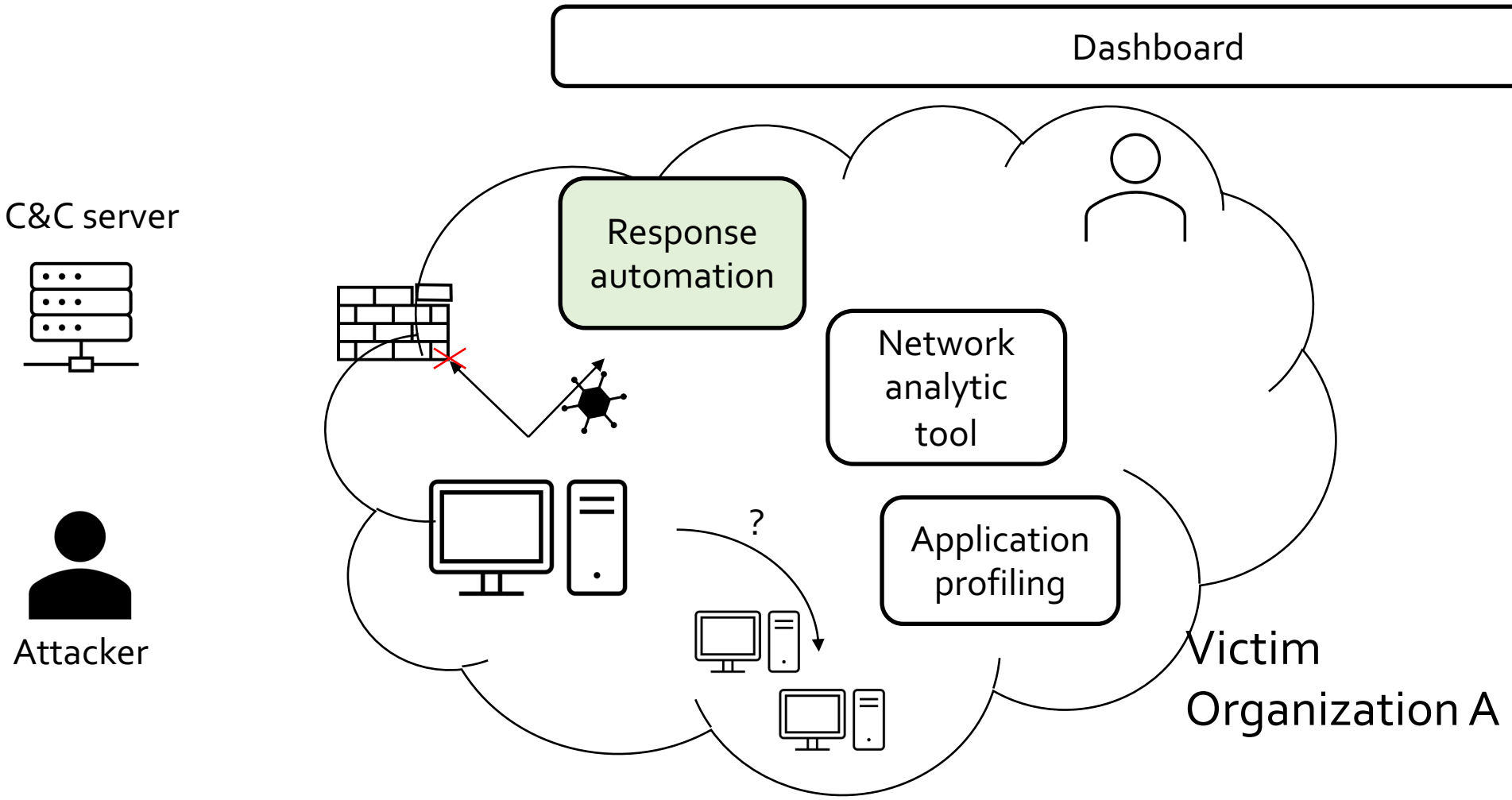
Other exciting innovations:

- Explainable AI: https://gitlab.com/rwth-itsec/explain
- Visualizations of neural networks[1]
- Collaboration / federated machine learning[1]
- Anonymization techniques for sharing of data[1]

[1]not yet published

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

SAPPAN Response



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Response automation

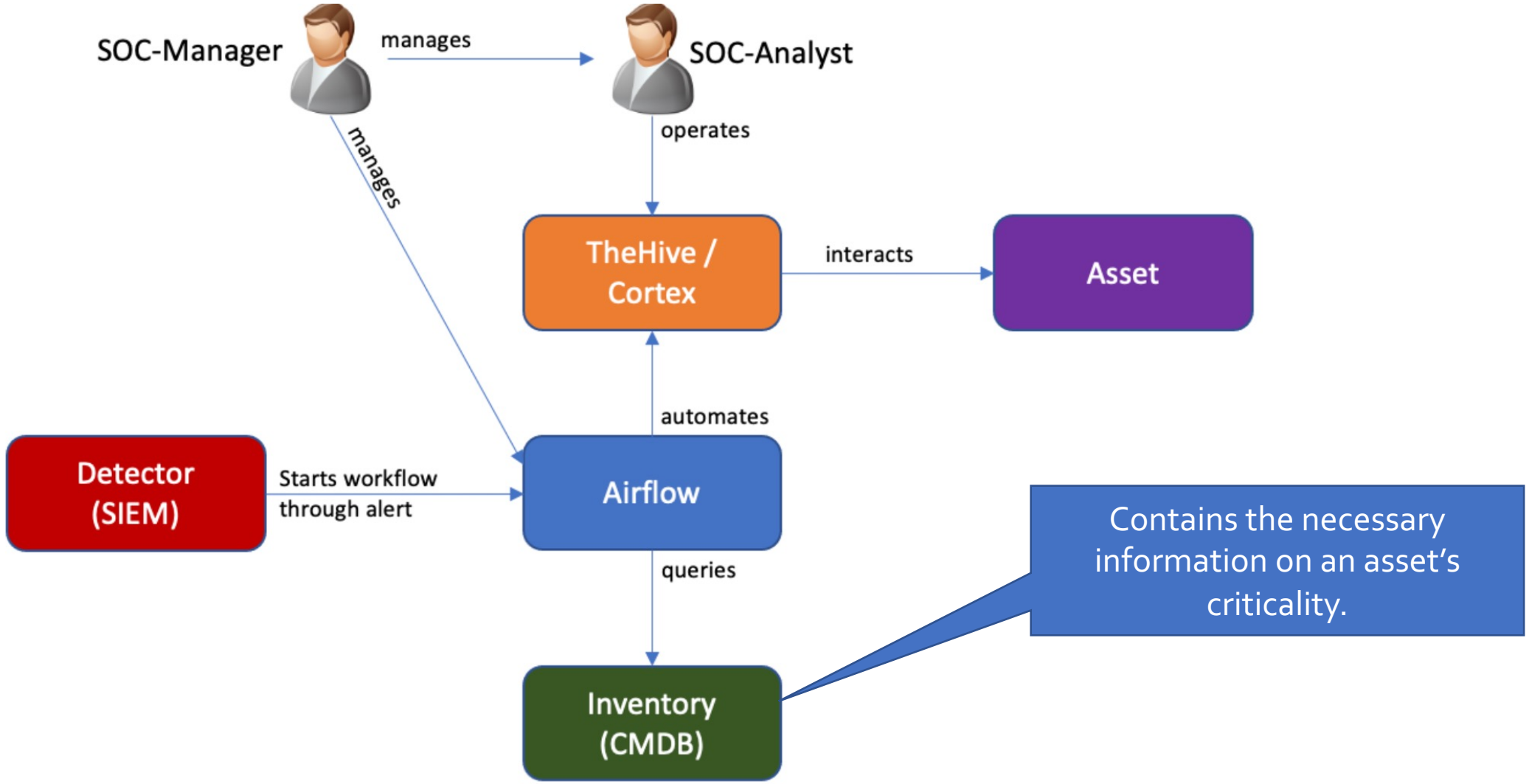
TheHive

Cortex

Airflow

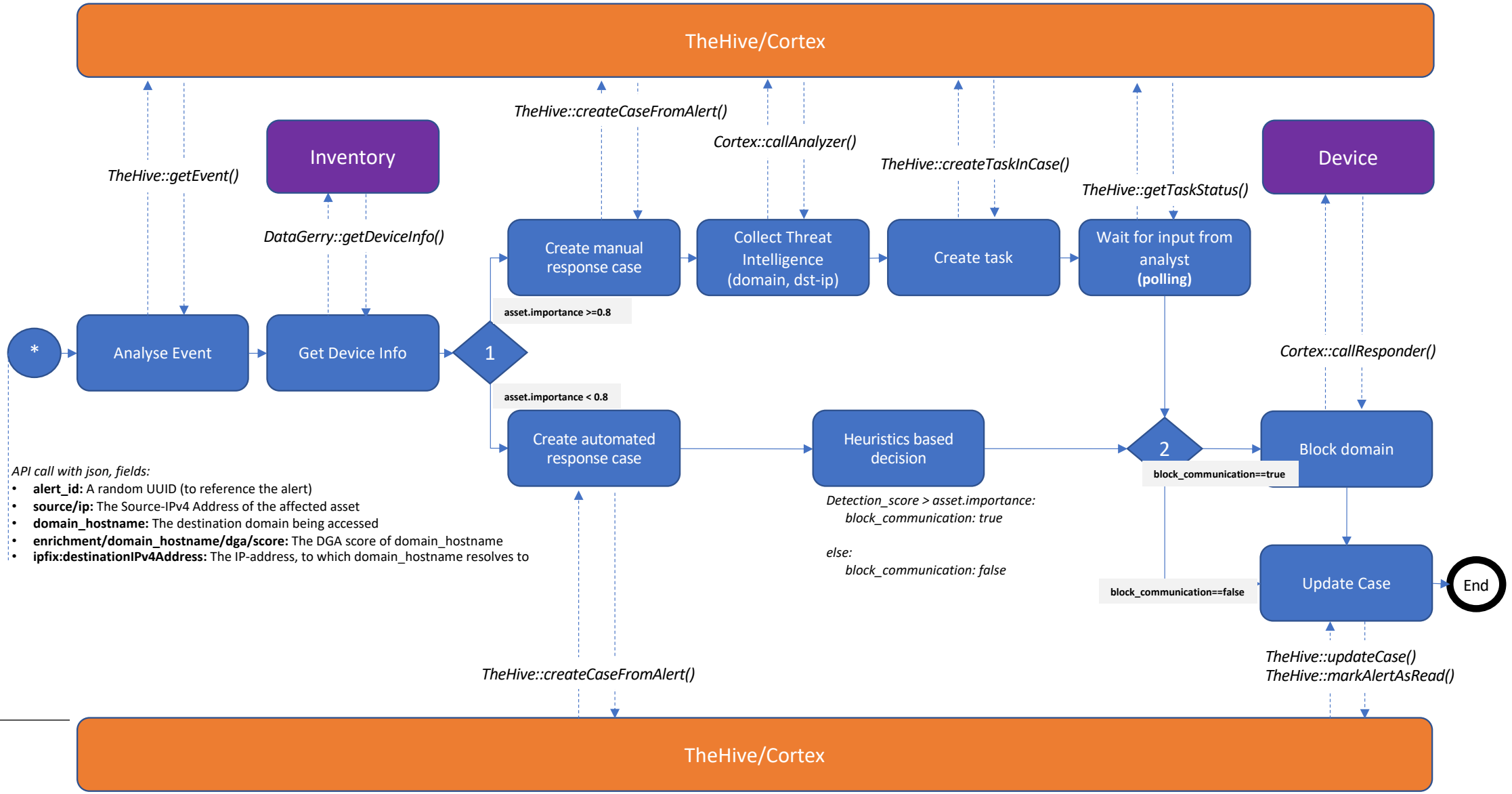
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Response automation



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Response automation



Response automation - Conclusion

What did we learn?

- Automation of incident response is possible but requires a good risk mitigation strategy.
- The implemented workflow must be use case and even organization specific.
- The devil is in the detail of workflow design, not the implementation.

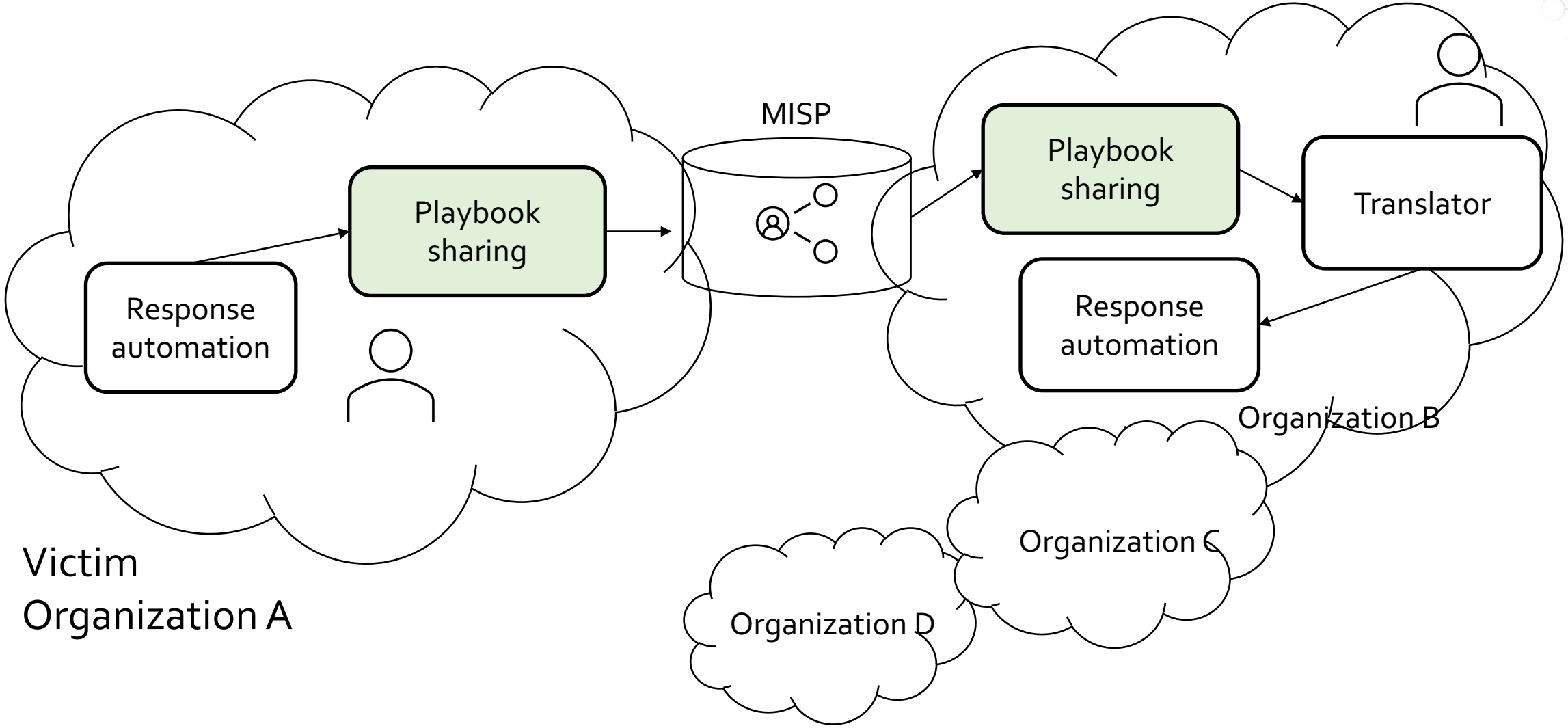
Other exciting innovations:

- Malware Analysis Platform [1]
- Incident similarity and response recommendation[1]

[1]not yet published

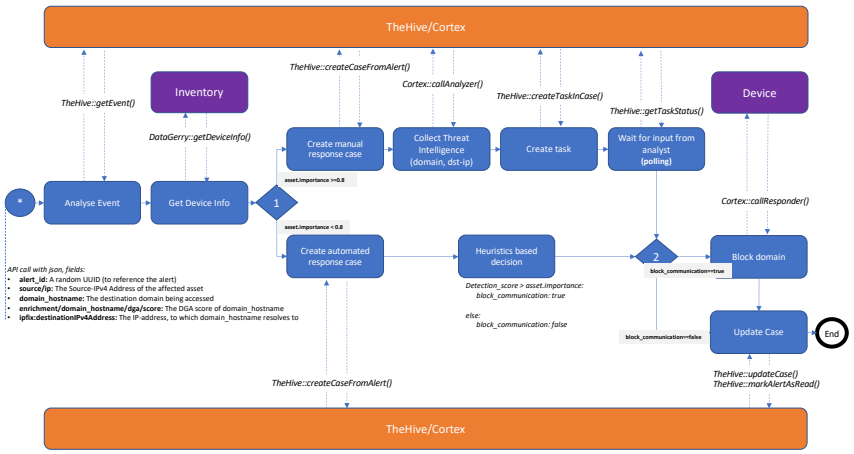
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

SAPPAN Post-incident/preparation



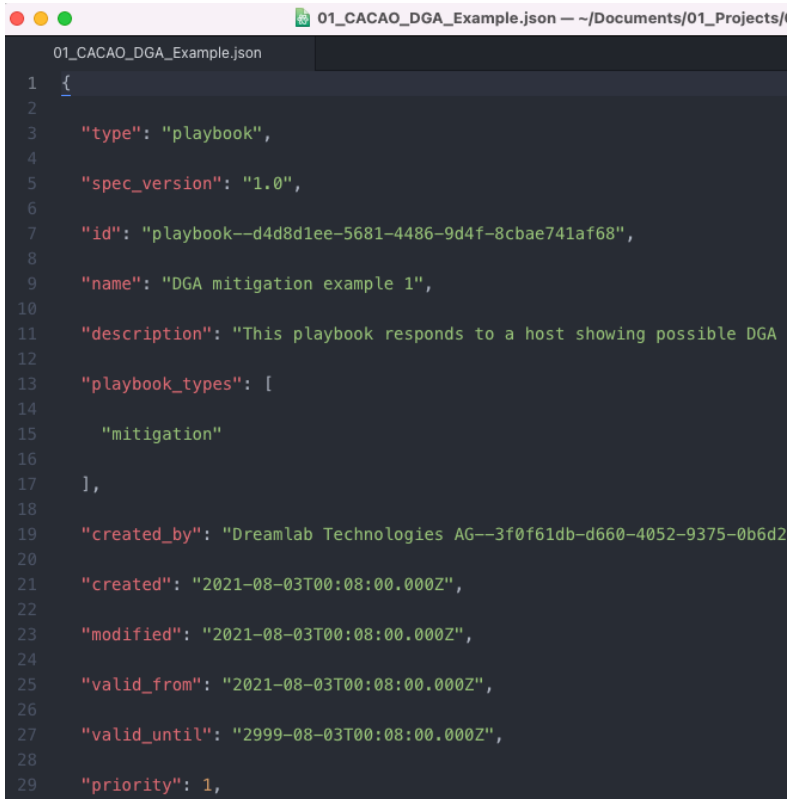
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Playbook sharing



Implementation in Apache Airflow (Python)

Translator



JSON Representation according to CACAO Standard

https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Playbook sharing through MISP

MISP / misp-objects Public

Code | Issues 43 | Pull requests 2 | Actions | Security | Insights

main | misp-objects / objects / security-playbook / definition.json

whoisroot Add sane default for boolean objects ✓

4 contributors

189 lines (189 sloc) | 6.15 KB

```
{
  "attributes": {
    "created": {
      "categories": [
        "Other"
      ],
      "description": "The time at which the playbook was originally created.",
      "disable_correlation": true,
      "misp-attribute": "datetime",
      "ui-priority": 1
```

https://github.com/MISP/misp-objects/blob/main/objects/security-playbook/definition.json

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Playbook sharing - Conclusion

Contribution to CACAO standard

Creation of new MISP object

Other exciting innovations:

- Translator to transform CACAO Playbooks (json) into Airflow skeleton (Python)[1]

[1]not yet published

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

SAPPAN - Summary

Results addressing multiple particular issues in NIST IH lifecycle

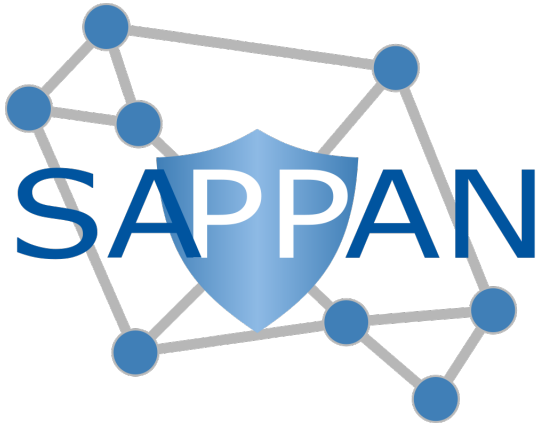
Contributions:

- Academic research
- Standardization (CACAO & MISP)
- Improvement of Security Products (F-Secure & Dreamlab)

Going beyond what is available

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Thank you for your attention!



SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

Entering the rabbit hole:

- https://sappan-project.eu/
- https://www.youtube.com/channel/UCrqc_Tzt6nU3ks1nrkRnq2g (The SAPPAN Youtube Channel)
- https://ercim-news.ercim.eu/en129/special/from-collaboration-to-automation-a-proof-of-concept-for-improved-incident-response

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418