SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

SAPPAN Project Presentation

Avikarsha Mandal (Fraunhofer FIT), Martin Zadnik (CESNET), Martin Laštovička (Masaryk University), Willie Victor (F-Secure)

2nd Joint Standardisation Workshop on Dynamic Countering Cyber-attacks

08.02.2022

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

SAPPAN (**S**haring and **A**utomation for **P**rivacy **P**reserving **A**ttack **N**eutralization)

H2020 Call SU-ICT-01-2018 (IA) - Dynamic countering of cyber-attacks

- **Scope:** Cyber-attacks management – advanced response and recovery
- **Timeline**: May 2019 until April 2022
- **Overall Budget:** € 4 700 053,39

Project Highlights:

- Support **SOC** to find optimal responses to and ways to recover from cyberattacks
- Platform for **privacy-preserving threat intelligence sharing** among organisations
- **Local and Federated detection tools** for effective response and recovery
- **Visual, interactive support tools** for SOC operators
- Improve **scalability** of massive data and logs processing for intrusion detection approaches
- Optimal **response recommendation** and **automation**

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

Consortium

Fraunhofer FIT

Hewlett Packard Enterprise

cesnet

F-Secure

DREAMLAB TECHNOLOGIES

Universität Stuttgart

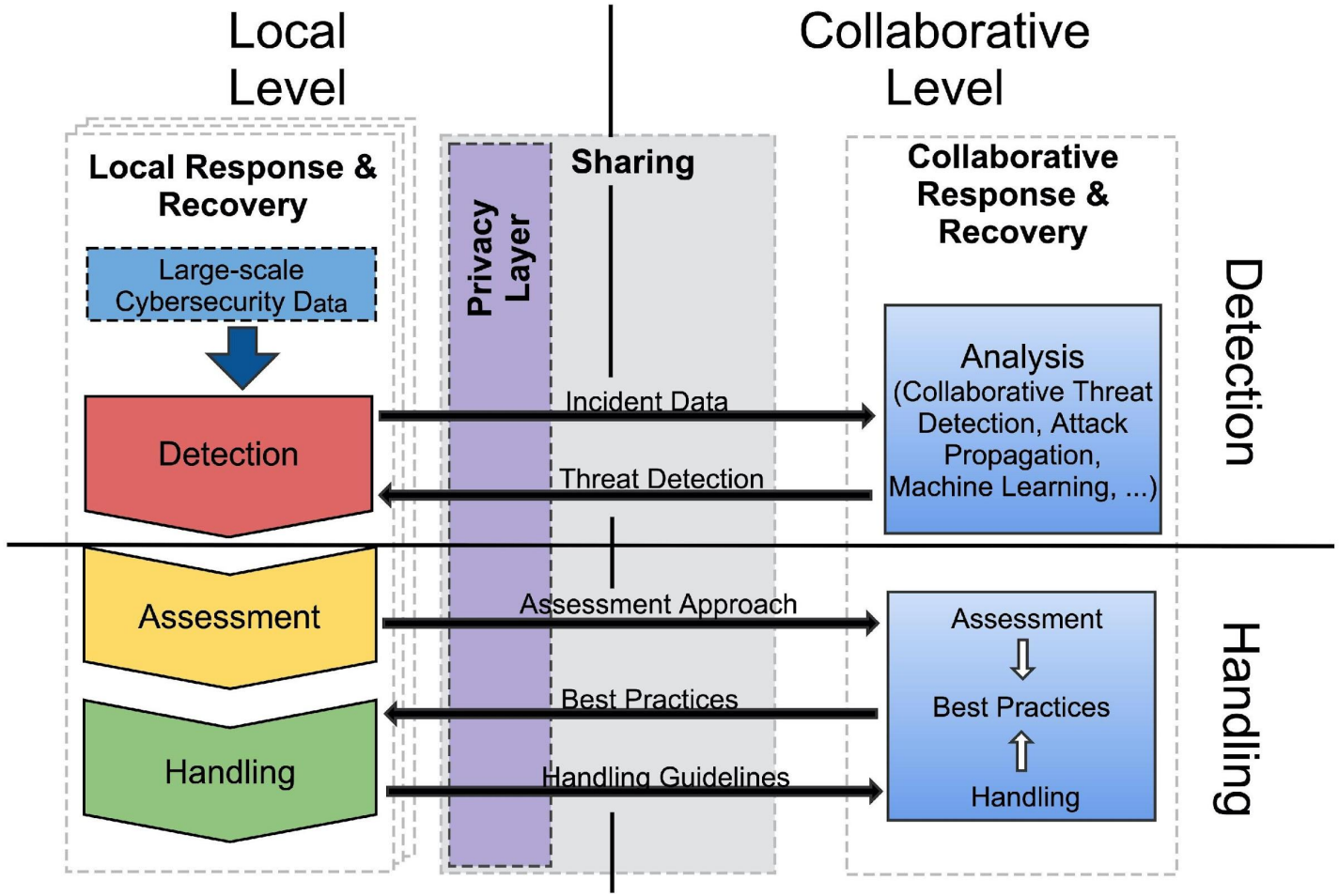
MUNI

RWTH AACHEN UNIVERSITY

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

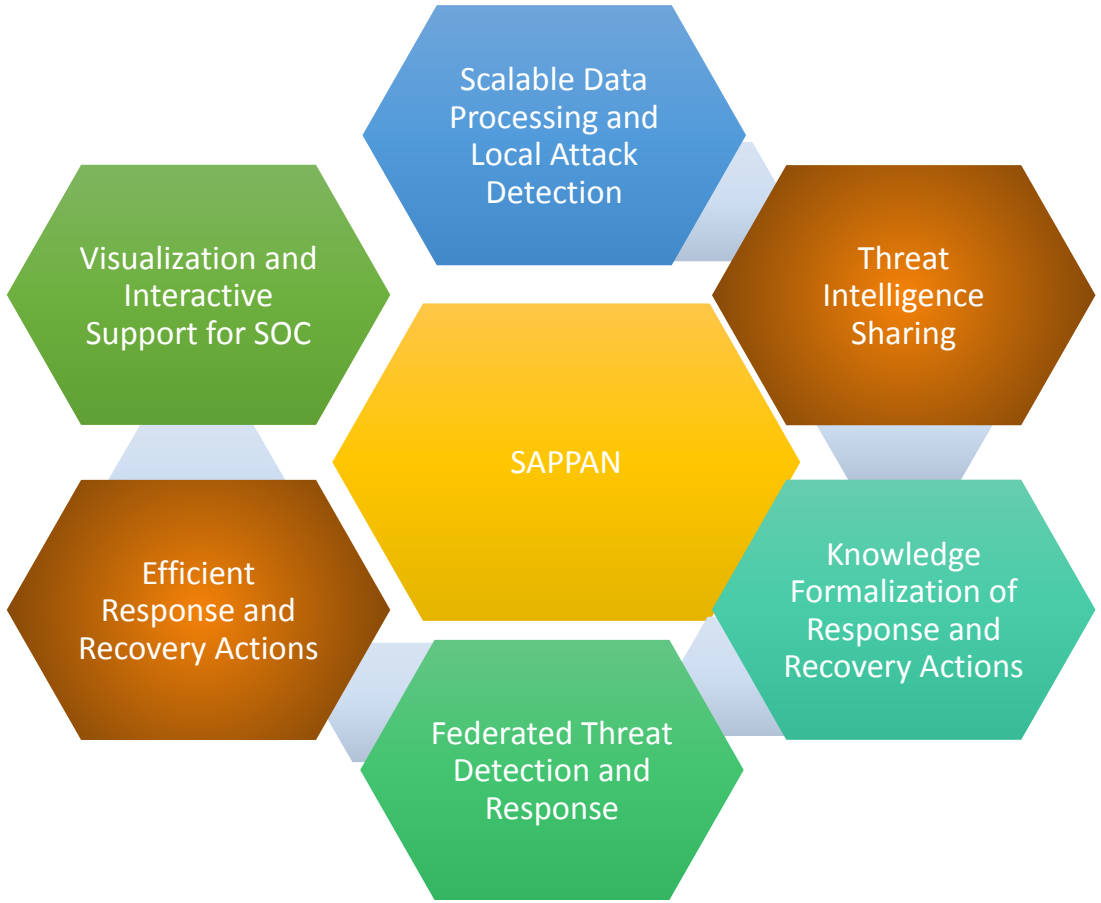
SAPPAN

SAPPAN Approach



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

SAPPAN Innovations



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

Selected SAPPAN Innovations

- Sharing Cybersecurity Playbooks (CESNET)
- Malware Analysis Automation Platform (Masaryk University)
- Response Recommendation Datasets (F-Secure)

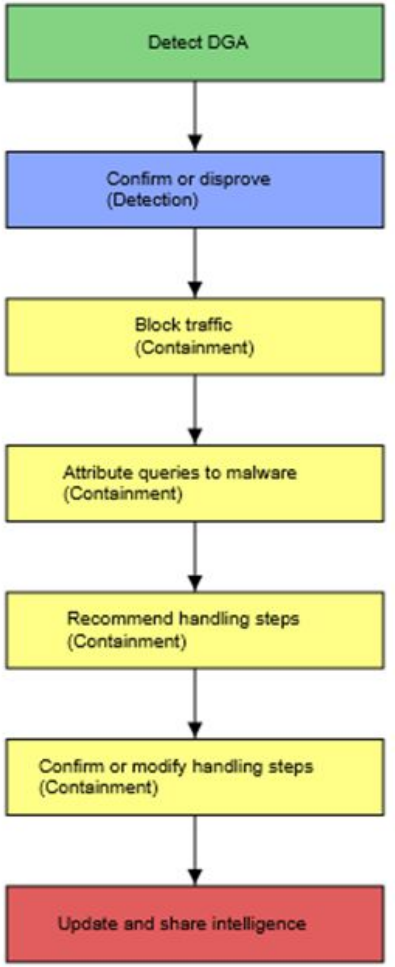
This project has received funding from the European Union's Horizon 2020 research and innovation
programme under grant agreement No 833418

Sharing Cybersecurity Playbooks

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

Sharing cybersecurity playbooks

- In order to distribute
  - response and recovery steps
  - semi/fully-automated workflows
- Create an ecosystem
  - commercial
  - community based



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

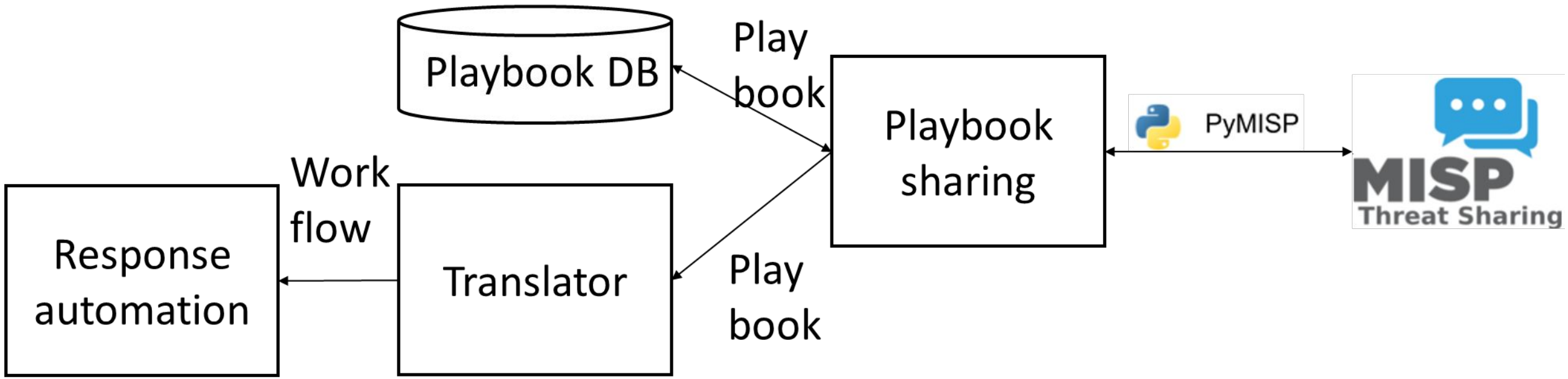
Sharing cybersecurity playbooks

- Multiple playbook formats
  - Workflows
  - SAPPAN
  - CACAO
- Uniform sharing format needed
  - CACAO covers it all
- MISP integration
- Table with metadata and playbook

Playbook standard
Playbook type
Description
Label
Abstraction
Validity
Playbook

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

Easy to use with MISP

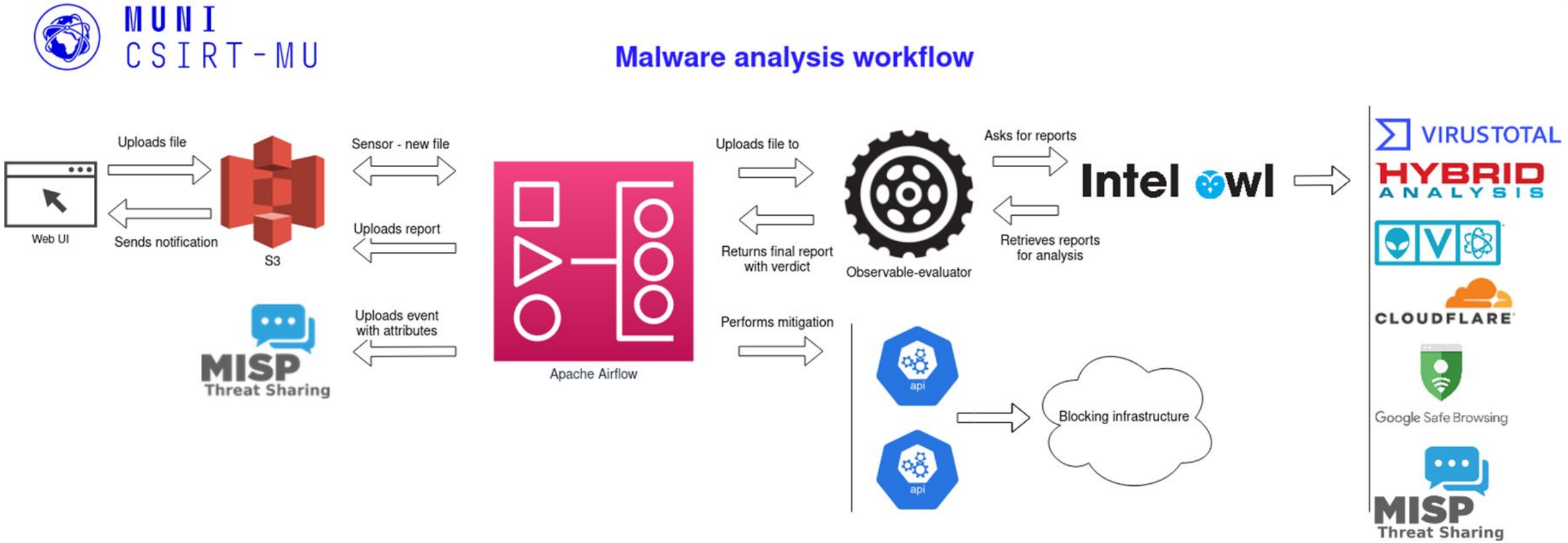


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Malware Analysis Automation Platform

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

Platform Architecture



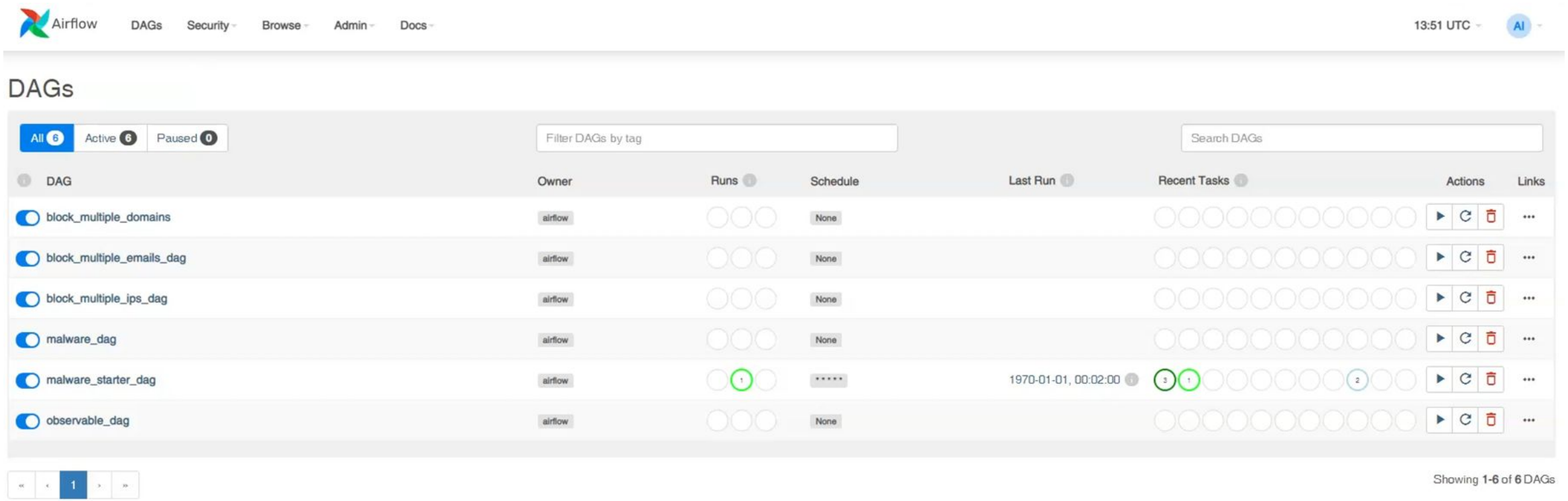
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

Deployment

1. Provide API keys to supported tools through config file
   - Public API without key may have limited services
2. Run Docker containers
   - Using Docker – docker-compose up
   - or Using Vagrant – vagrant up

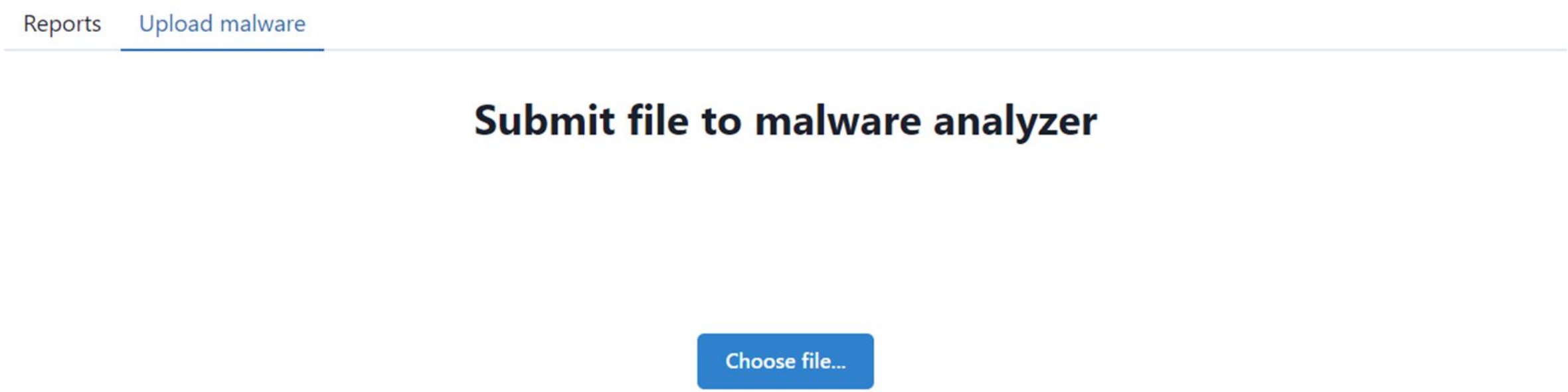
This project has received funding from the European Union's Horizon 2020 research and innovation
programme under grant agreement No 833418

Initial Airflow State



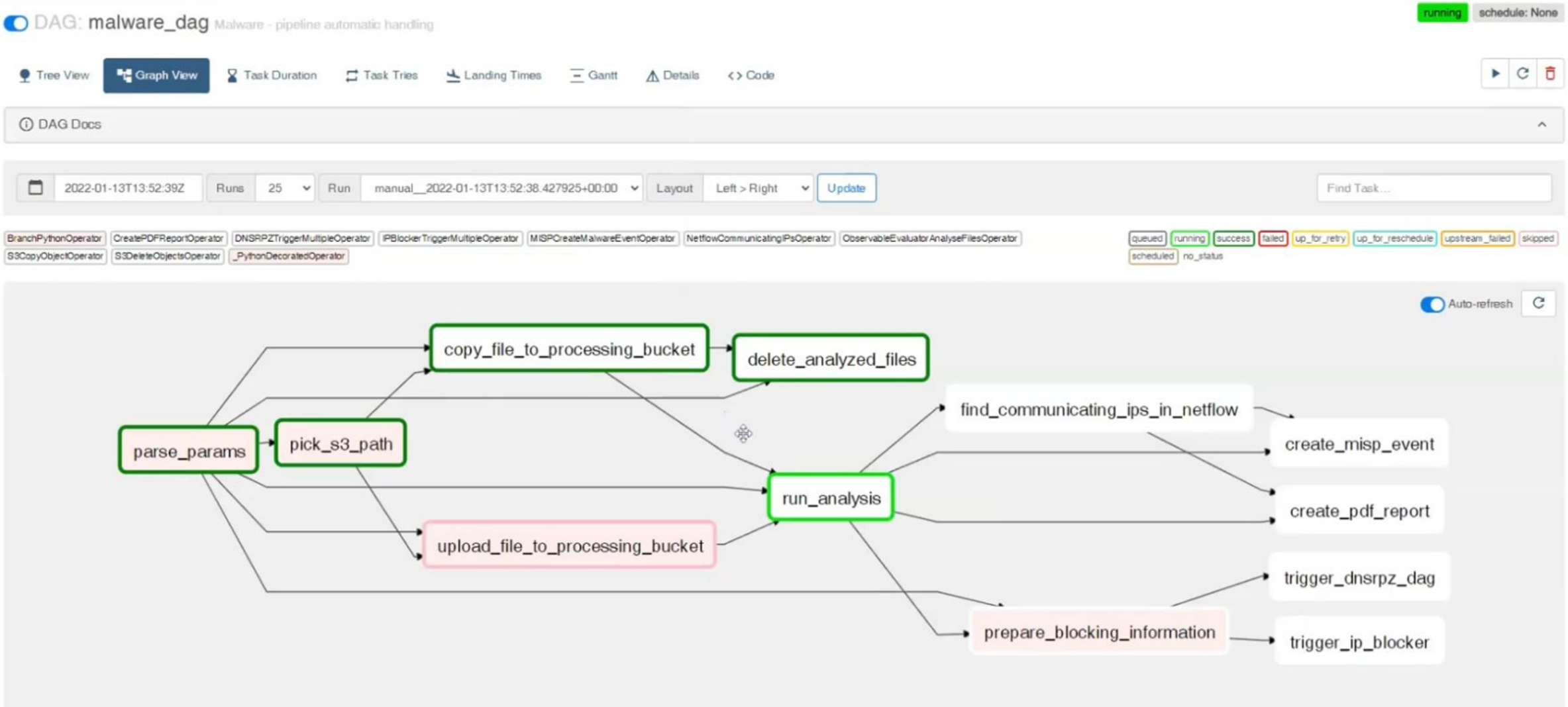
This project has received funding from the European Union's Horizon 2020 research and innovation
programme under grant agreement No 833418

Malware Gateway



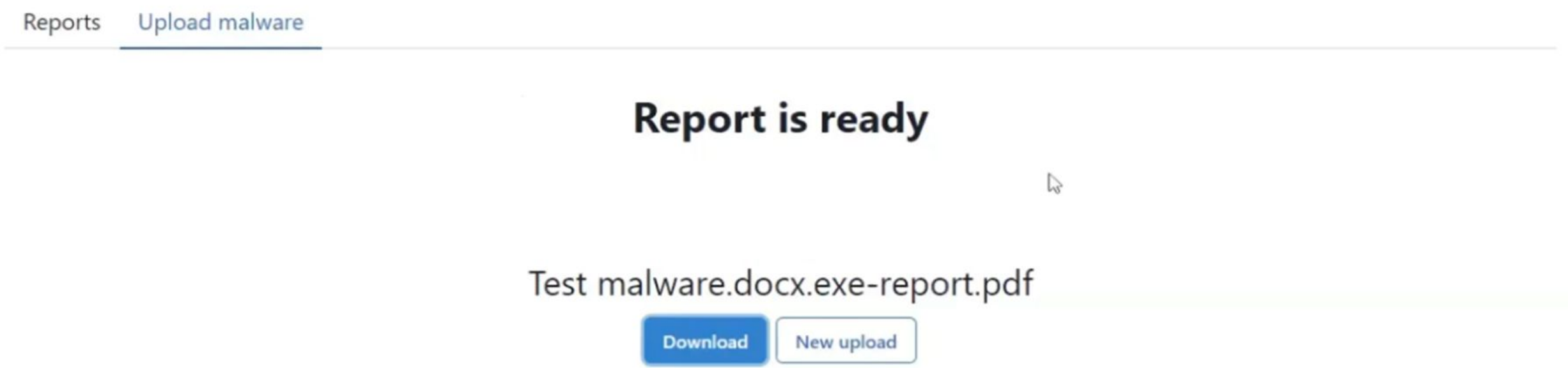
This project has received funding from the European Union's Horizon 2020 research and innovation
programme under grant agreement No 833418

Running Malware Analysis DAG



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

Report Download



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

Report for the File

Result

Malware-pipeline evaluated file Test malware.docx.exe as malicious.

Basic information

Name		Test malware.docx.exe
Hash	**MD5**	8d4b77fa3546149f25bd17357d41fbf0
	SHA1	7289737c1dc462726abbe89335a7702c130bbdcc
	SHA256	bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a
Aliases		myfile
		Andr.PegasusB_Pwk9fuo.apk
		TrojanSpyAndroidPegasus.32507731.apk
		bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a.apk
		bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a
		pegasus.apk
		Andr.PegasusB_6nFFeMO.apk
		6a3efdca-2465-460e-878e-3e6d52790c10
		Andr.PegasusB.apk
		base.apk
		bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a.exe
		pegasus2021_3.apk
Tagged as malicious		HybridAnalysis, OTX Alien Vault, VirusTotal
Tagged as harmless		MISP_Check_Hash

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

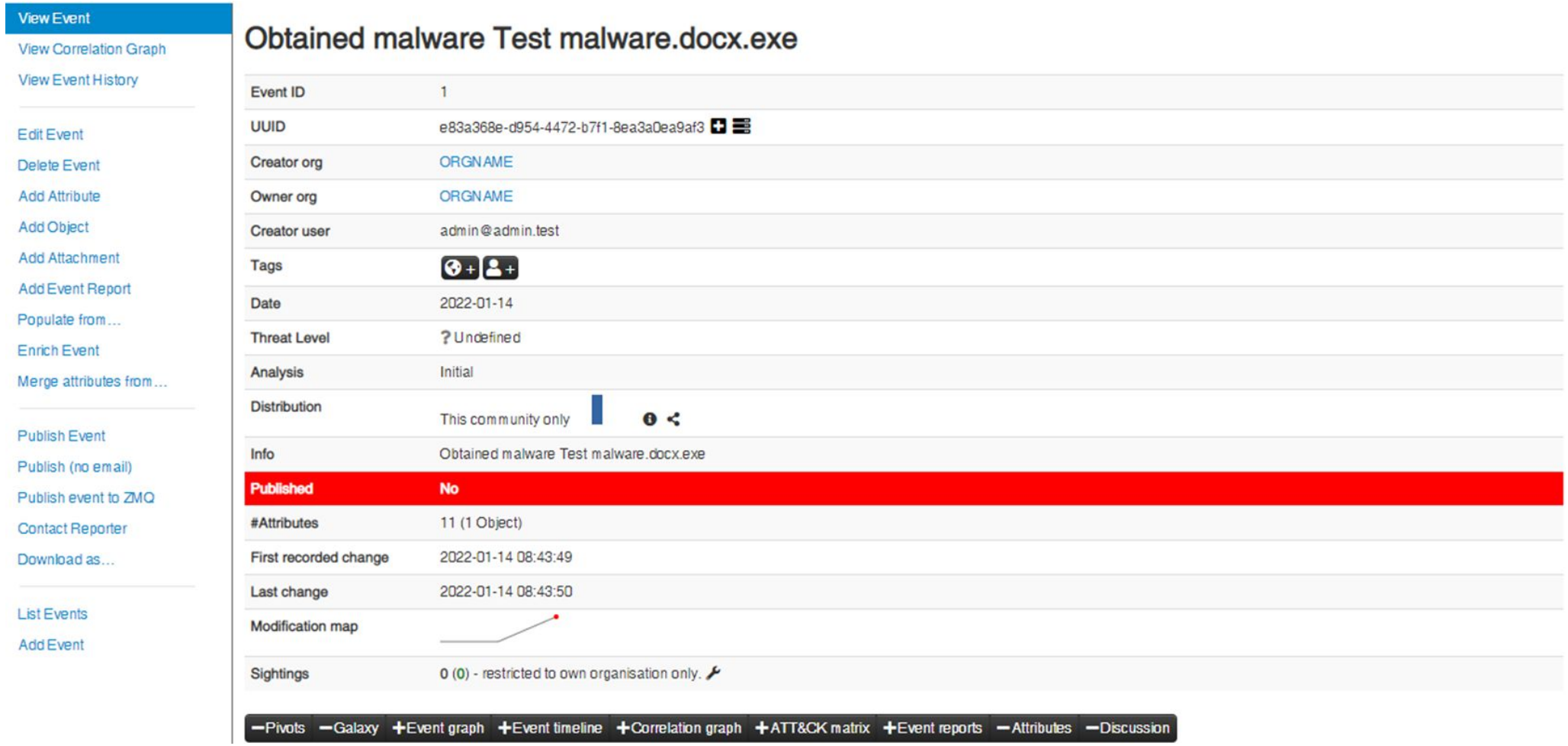
Observables in the Report

Found observables

Observable	Type	Malicious	Detected by	Tagged malicious	Tagged harmless
172.217.194.190	ip	Yes	VirusTotal	OTX Alien Vault	Google Safebrowsing, MISP
142.250.13.188	ip	Yes	VirusTotal	OTX Alien Vault	Google Safebrowsing, MISP
142.250.102.188	ip	Yes	VirusTotal	OTX Alien Vault	Google Safebrowsing, MISP
142.250.27.188	ip	No	VirusTotal		Google Safebrowsing, MISP

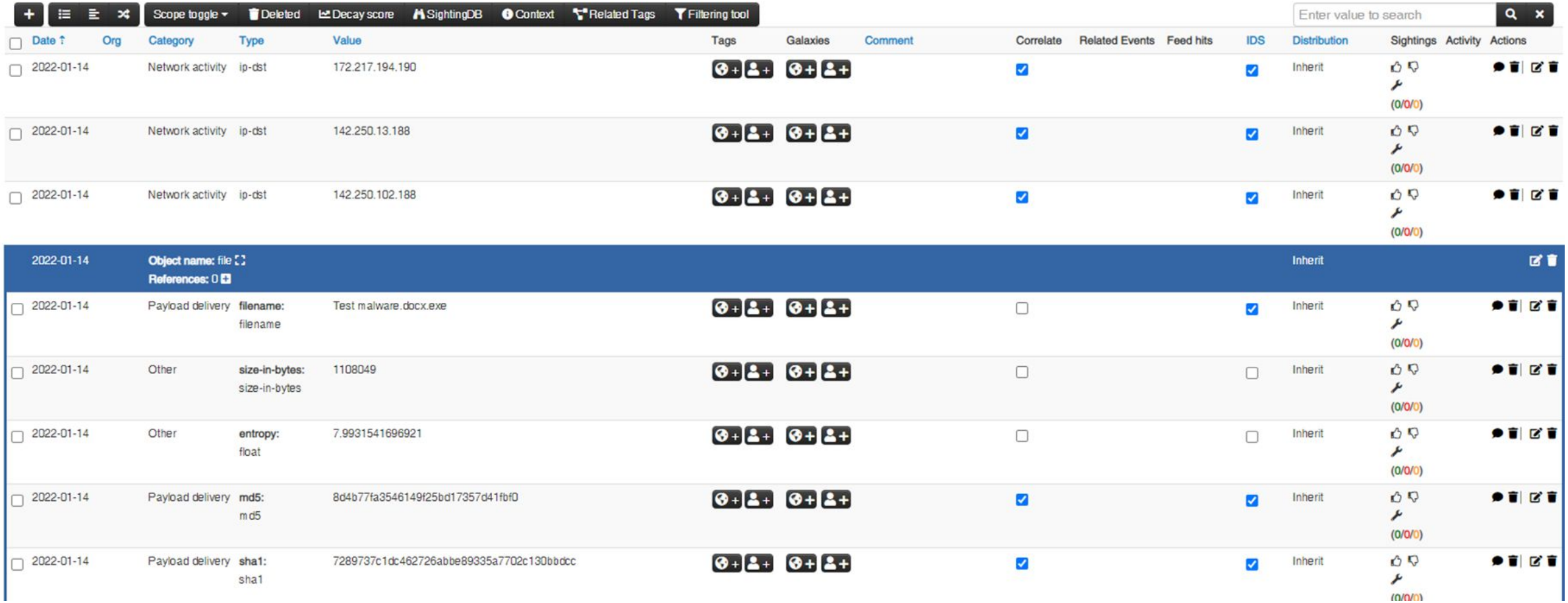
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833418

MISP Event



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

MISP Event Cont.



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

Mocked Blocking of Malicious Observables


```
{
  "count": 3,
  "results": [
    {
      "expires": "2022-01-21T08:43:55Z",
      "ip": "172.217.194.190",
      "listed": "2022-01-14T08:43:55Z",
      "reason": "Discovered in malware Test malware.docx.exe by VirusTotal",
      "who": "rtbh"
    },
    {
      "expires": "2022-01-21T08:43:55Z",
      "ip": "142.250.13.188",
      "listed": "2022-01-14T08:43:55Z",
      "reason": "Discovered in malware Test malware.docx.exe by VirusTotal",
      "who": "rtbh"
    },
    {
      "expires": "2022-01-21T08:43:56Z",
      "ip": "142.250.102.188",
      "listed": "2022-01-14T08:43:56Z",
      "reason": "Discovered in malware Test malware.docx.exe by VirusTotal",
      "who": "rtbh"
    }
  ]
}
```


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

Malware Analysis Automation Summary

- Platform independent
- One-command deployment
- Speeds-up the initial evaluation of a suspicious file
- Reduces possible mistakes as a human can overlook or forget to further investigate an observable
- Results are consistent across analysts, w. r. t. analysis times and results
  - Junior and senior analysts' results are the same

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

Response Recommendation Datasets

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

Response Recommendation Datasets

- Modern EDR products offer unprecedented insights into security events and ongoing attacks
- Enable remote investigations and real-time response
- Handling advanced attacks involves human Detection and Response teams
  - Specialist skills, so scalability remains a challenge
  - Assistive technologies and automation can help with this
  - Substantial progress has been made in attack detection through data science - Machine Learning techniques
  - Incident Investigation and Response remains largely manual process

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

Response Action Data

- Response workflows are generally well recorded
  - Needed for accountability, since response actions tend to be invasive
  - Also useful for personnel training purposes
- Specific actions can often be linked to elements of an incident *at a high level*
- Fine-grained *causal* relationships tend to be missing
  - "Response action X was directly related to observations A, B, and C in data"
- To enable effective and accurate assistive technologies for tactical incident response scenarios, strong "action -> cause" links are needed

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

Standards and Taxonomies

Existing industry initiatives to describe elements of incidents:

- Attack techniques and defensive measures: Mitre
- Incidents: STIX
- Response workflows: CACAO

Currently no open standards to record response actions and their causes

SAPPAN investigated the current feasibility of building detection-response datasets for AI-based assistive technologies for responders. Defining a fit-for-purpose standard structure was identified as essential future work.

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

Response Action Elements

- Essential elements of Detection-Response datasets:
  - Some security event(s) took place
  - Events have specific data associated with them
  - Investigation actions may reveal additional datapoints
  - One or more events or detections will lead a responder to a chain of actions to achieve containment and eradication
- Well-defined structure to contain the above is needed to enable research into machine learning applications in Detection-Response space
  - Should leverage existing standards where possible
  - Product independent, to enable sharing of data among contributors
  - Should lend itself to integration into EDR product technology stacks for automated data collection

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