MISP, the state of the art in cyber threat sharing

Andras Iklody @ CIRCL / Team MISP Project

MISP Project
https://www.misp-project.org/

Sikkerhetsfestivalen 2023

MISP
Threat Sharing

MISP in general

ABOUT CIRCL AND MISP

- CIRCL
  - National CERT for the private sector, communes, non-govermental entities in Luxembourg
  - Government-driven initiative, funded by the Ministry of Economy
  - Mission is to provide a systematic response facility to computer security threats and incidents
  - Open Source toolsmiths
- Our relationship with MISP has two sides
  - We **lead the development** of the MISP platform
  - We are also involved with and **run several communities**

Before we start - What is MISP?

- MISP is a **threat information sharing** platform
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, **correlates**, **enriches** the data
- Allows teams and communities to **collaborate**
- **Feeds** automated protective tools and analyst tools with the output

Before we start - what is MISP?

- It is also a set of **open standards** implemented both by MISP and other tools
- Additionally, it is an **ecosystem** of libraries, supporting tools
- A collection of guidance and best practice documentation by practitioners
- All of these are free & open source

What are the objectives of a modern TISP?

- A tool that **collects** information from partners, your analysts, your tools, sensors, feeds
- Normalises, **correlates**, **enriches** the data
- Manages your processes and automates tasks such as **notifications**, **data flow management**, **triaging** and so on
- Allows teams and communities to **collaborate** and rapidly **exchange knowledge**
- **Feeds** automated protective tools and analyst tools with the output
- **Presents** both individualised and community centric facts, trends, reports of the intelligence

MISP: Started from a practical use-case

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development** supporting different intelligence communities.

Development based on practical user feedback

- There are many different types of users of an information sharing platform like MISP:
  - **Malware reversers** willing to share indicators of analysis with respective colleagues.
  - **Security analysts** searching, validating and using indicators in operational security.
  - **Intelligence analysts** gathering information about specific adversary groups.
  - **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
  - **Risk analysis teams** willing to know about the new threats, likelyhood and occurences.
  - **Fraud analysts** willing to share financial indicators to detect financial frauds.
  - **Military** sharing highly specialised information.

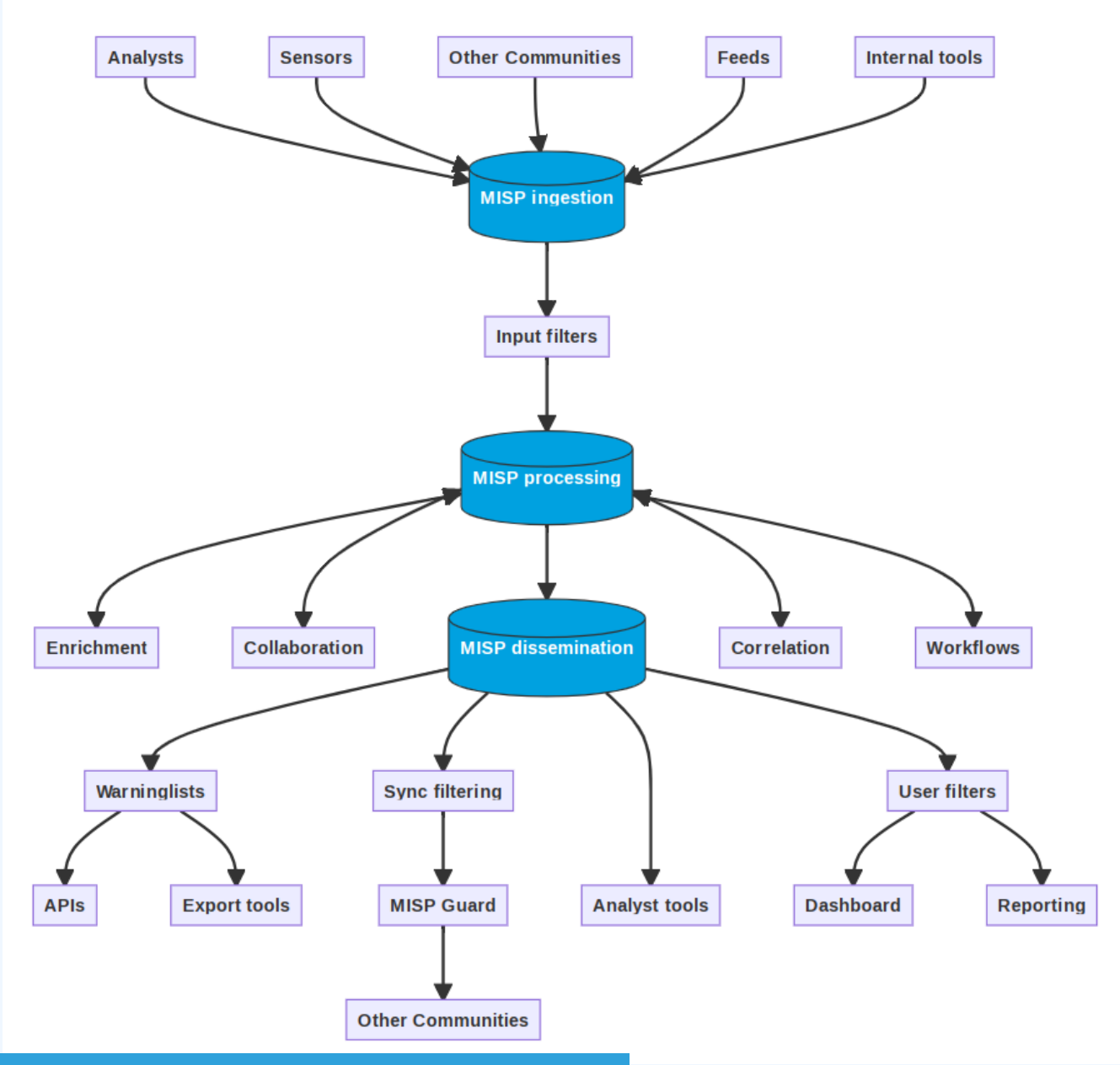
Why do we develop all of this?

- **Main goal**: Make our own lives and the lives of our constituency easier
  - Our central tool for ingesting, storing and disseminating information...
  - ...as well as to interact with organisations
  - By solving issues of other communities, we already have them prepared for information sharing with us when needed
- **Secondary**: Democratise threat intelligence for all
- **Stretch goal**: Build a full open-source tool-chain for CSIRTs / SoCs / etc

Communities using MISP

- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 2k organizations with close to 5k users).
- **Trust groups** running MISP communities in island mode (air gapped system) or partially connected mode.
- **Financial sector** (banks, ISACs, payment processing organizations) use MISP as a sharing mechanism.
- **Military and international organizations** (NATO, military CSIRTs, n/g CERTs,...).
- **Security vendors** running their own communities.
- **Sectorial communities** Telcoes, ISPs, Medical, ATF, ...
- **Topical communities** set up to tackle individual specific issues (disinformation, SIGINT, COVID-19, ...)

Information pipeline

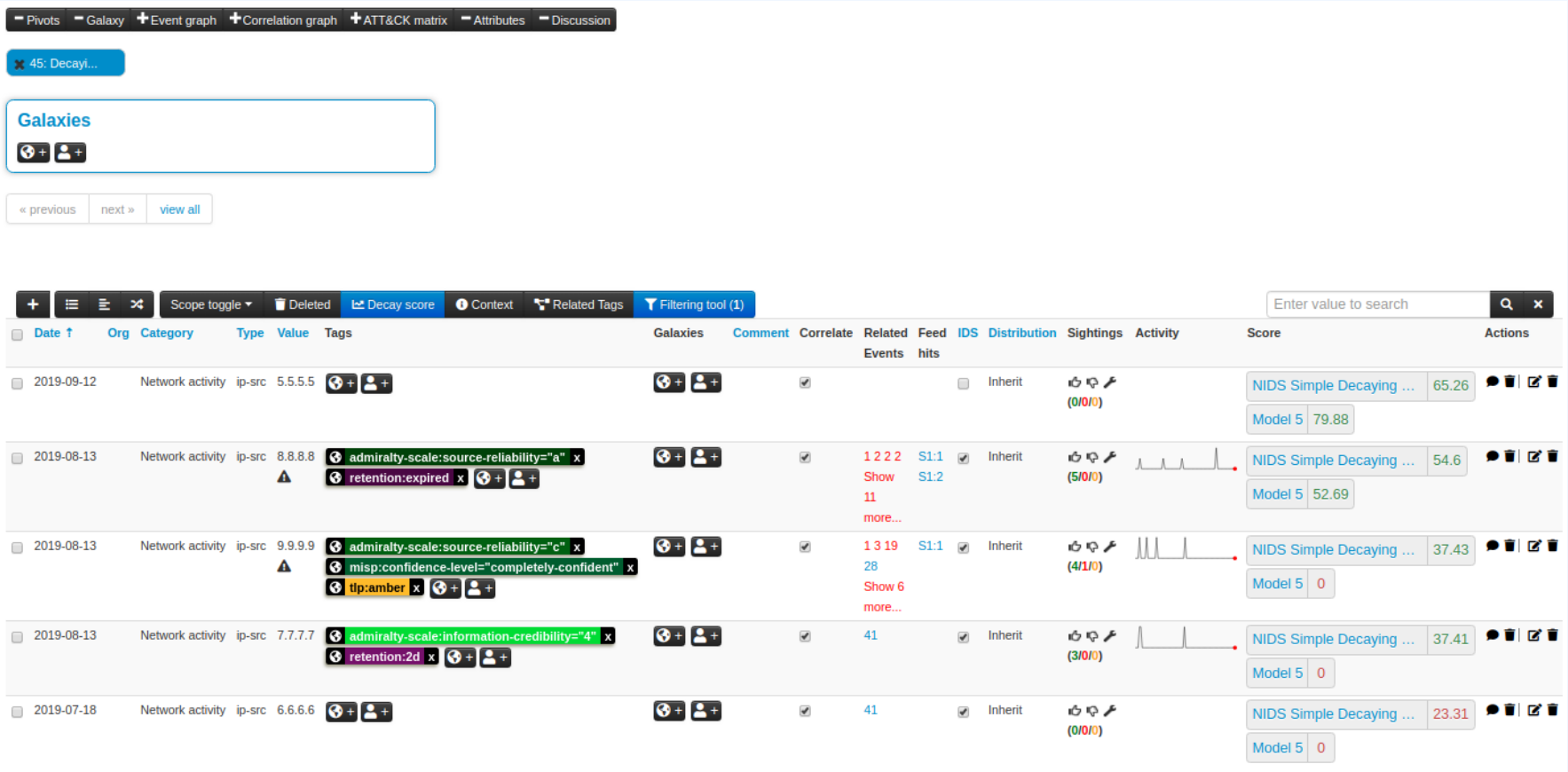


Some issues we try to tackle and their solutions

Information quality management

- What do we consider **actionable intelligence**?
  - Conflicting requirements - analyst work vs automated blocking for example
- **Filtering** both on **input** and on **output** separately
  - Lax on ingestion, strict on output mantra
  - Warninglists - sanitising obviously problematic data from output
  - Indicator scoring / lifecycle management

Information quality management



- **Decay score** calculated based on the enabled models
- Score takes into account **contextualisation, type, sightings**

Customisable lifecycle management

Home | Event Actions | Galaxies | Input Filters | Global Actions | Sync Actions | Administration | Audit | MISP

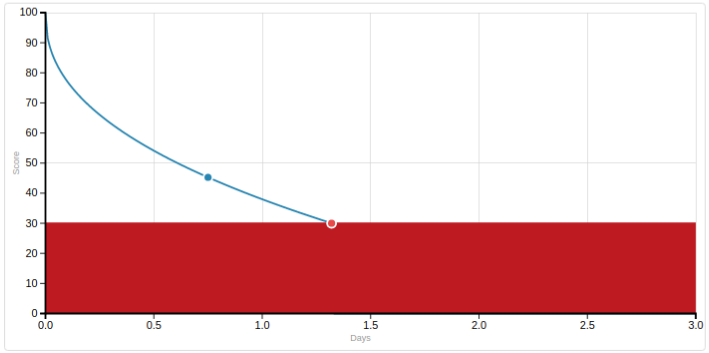
- Import Decaying Model
- Add Decaying Model
- Decaying Tool
- List Decaying Models

Decaying Of Indicator Fine Tuning Tool

Show All Types | Show MISP Objects | Search Attribute Type

	Attribute Type	Category	Model ID
	aba-rtn	Financial fraud	
	authentihash	Payload delivery	
	bank-account-nr	Financial fraud	
	bic	Financial fraud	
	bin	Financial fraud	
	bro	Network activity	10 11
	btc	Financial fraud	11
	cc-number	Financial fraud	
	cdhash	Payload delivery	
	community-id	Network activity	
✓	domain	Network activity	
✓	domain|ip	Network activity	10 84
	email-attachment	Payload delivery	
	email-dst	Network activity	11
	email-src	Payload delivery	
	filename	Payload delivery	
	filename|authentihash	Payload delivery	
	filename|impfuzzy	Payload delivery	
	filename|imphash	Payload delivery	
	filename|md5	Payload delivery	13
	filename|pehash	Payload delivery	13
	filename|sha1	Payload delivery	13

Polynomial



Lifetime	3	days
Decay speed	2.3	
Cutoff threshold	30	

Expire after (lifetime)	1 days and 7 hours
Score halved after (Half-life)	0 day and 6 hours

Adjust base score | Simulate this model

Phishing model | Simple model to rapidly decay | Edit

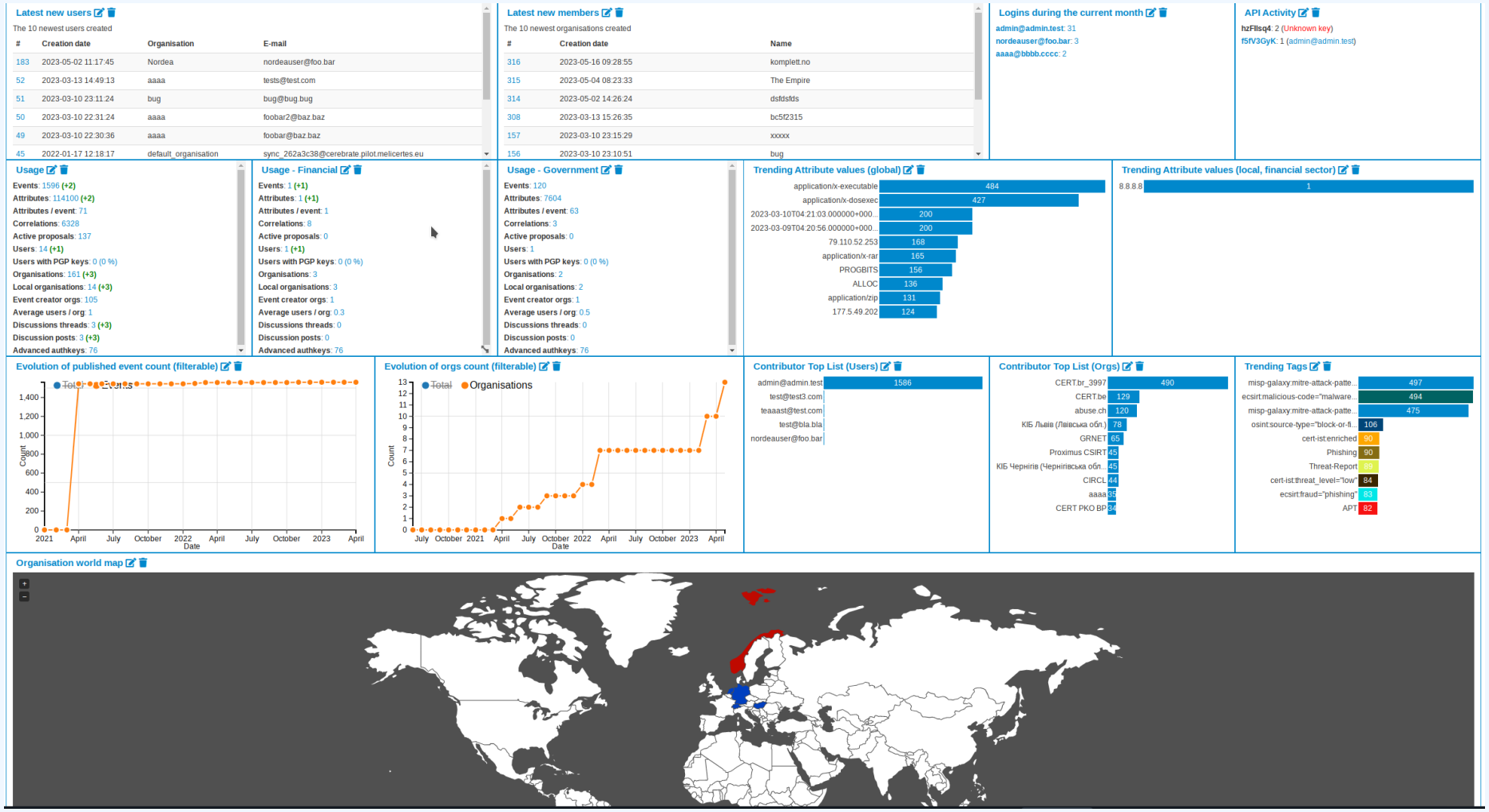
All available models | My models | Default models

	ID	Model Name	Org ID	Description	Formula	Parameters: Lifetime	Decay speed	Threshold	Default basescore	Basescore config	Settings	# Types	Enabled	Action
✓	29	Phishing model	1	Simple model to rapidly decay phishing website.	Polynomial	3	2.3	30	80	estimative-language 0.5; phishing 0.5		9	✓	Load model

Drilling down into our data

- Different use-cases require different tools.
- **Interactive interaction** with the data
  - "Event" tabular view
  - "Event" graph view
  - Correlation graphs
  - Various search interfaces
- **Trends and overviews**
  - Dashboarding
  - ATT&CK and similar frameworks based heatmaps
  - Alert e-mails and periodic reporting

Drilling down into our data



Drilling down into our data

- APIs
  - Long list of **filters**
  - **Complex queries**
  - Infusing queries with other tools (**warninglists, decaying**)
  - Interactive **UI query builder and tester**

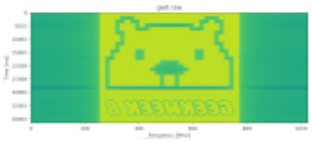
Data model management

- Three tier approach to information
- All three tiers are tightly integrated with one another
  - **Data** (Attributes, Objects, Relationships)
  - **Knowledge** ("Galaxies", Labels)
  - **Analyst reports** (Markdown reports)
- Different communities have wildly different requirements - extension mechanisms
  - **Object templates**
  - Custom **Galaxies**
  - **Taxonomies**

Data model management

2023-07-12 **Object name:** sigmf-expanded-recording

Dashboard | Galaxies | Input Filters | Global Actions | Sync Actions | Administration | Logs | API

		author: text	Luciano Mignetti	
2023-07-12	Other	**datatype:** text	cf32_le	
2023-07-12	Other	**license:** text	https://creativecommons.org/licenses/by/4.0/	
2023-07-12	Other	**recorder:** text	GNU Radio 3.8.2	
2023-07-12	Other	**sample_rate:** float	480000	
2023-07-12	Other	**sha512:** text	bb2f1f9222b172373e81d333a11a866d56611308fd481c7f9c2462e50fec62da1bddd93a94cd9b3e00dcaa6ba4ffe4546022aa50385bc582fc8dd7426740b564	
2023-07-12	Other	**version:** text	0.0.2	
2023-07-12	External analysis	**waterfall-plot:** attachment		

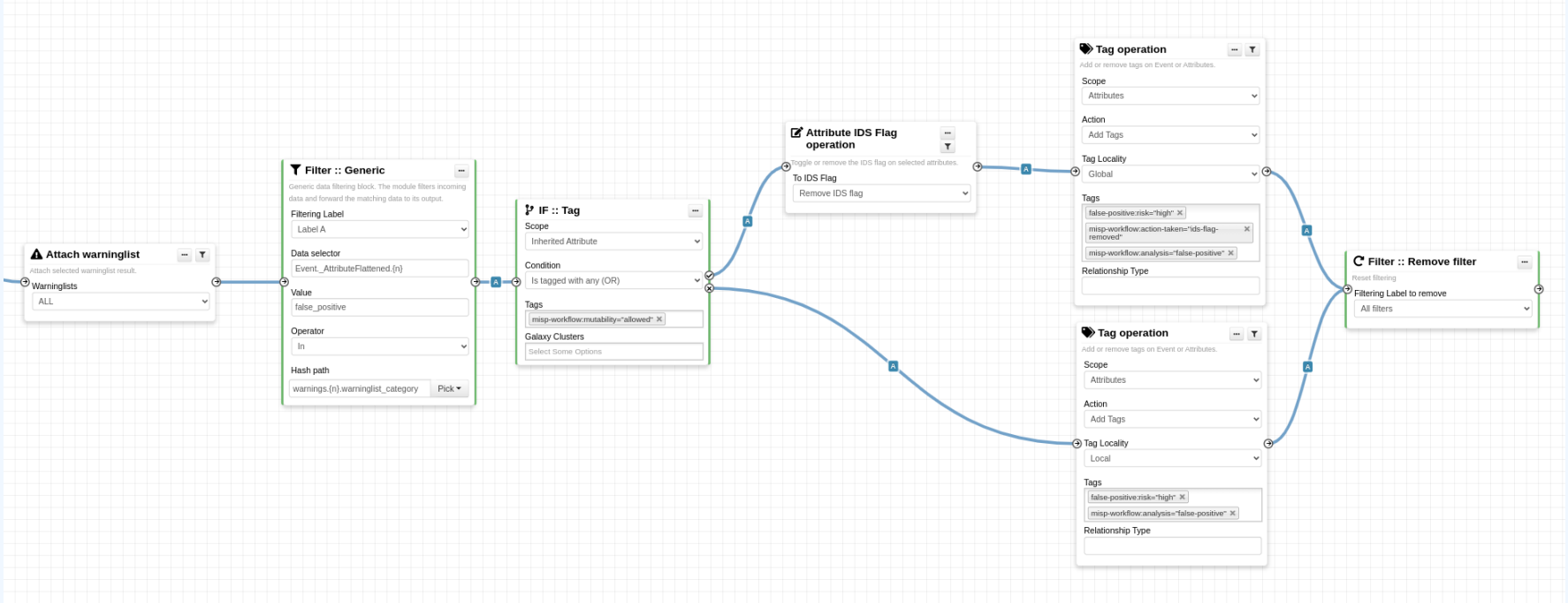
2023-07-12 **Object name:** sigmf-recording
References: 0
Referenced by: 1

2023-07-12	External analysis	**SigMF-data:** attachment	gw8.sigmf-data	
2023-07-12	External analysis	**SigMF-meta:** attachment	gw8.sigmf-meta	

Customising MISP

- Highly configurable per community need
  - Hundreds of **configuration options** to manage MISP behaviours
  - Hooking and modifying **core cuntionalities via Workflows**
  - Custom modules via companion system (**MISP-modules**)
  - **Modular** parts of the **codebase** (e-mail templates, dashboard elements, import/export functions)
  - If all of that is not enough - extensive **Python library** support for DIY fans :)

Customising MISP



Wrapping it all up

Community driven effort

- This concludes a **brief glimpse into what MISP is** and some of the key issues to tackle
- MISP is evolving based on **community efforts and needs**
- The outcome is a highly **versatile and customisable** system
- We all have different ideas of what we'd like to be able to do in our TISP
- **Prioritisation is hard** plus there are only so many hours in a day...
- ...**Get involved**, let us know how we can make it better or at least usable for your use-case!

Get in touch if you have any questions

- Contact me:
  - andras.iklody@circl.lu https://twitter.com/iglocska https://infosec.exchange/@iglocska
- Contact us:
  - info@circl.lu https://twitter.com/circl_lu https://www.circl.lu/
  - https://github.com/MISP https://www.misp-project.org/
  - https://twitter.com/MISPProject https://misp-community.org/@misp