Automation with Workflows in MISP

Short version

Sami Mokaddem

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

Content of the presentation

1. Automation in MISP
2. MISP Workflows
   - Fundamentals
   - Demo with examples
   - Using the system
   - How it can be extended

Automation in MISP: What already exists?

MISP API / PyMISP

- Needs CRON Jobs in place
- Potentially heavy for the server
- Not realtime

PubSub channels

- After the actions happen: No feedback to MISP
- Tougher to put in place & to share
- Full integration amounts to develop a new tool

→ No way to **prevent** behavior
→ Difficult to setup **hooks** to execute callbacks

Simple automation in MISP made easy

MISP
Threat Sharing

- **Visual** dataflow programming
- **Drag & Drop** editor
- Flexible **Plug & Play** system
- **Share** workflows, **debug** and **replay**

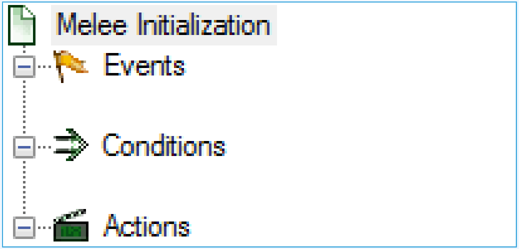
Example of use-cases

- **Notification** on specifc actions
  - New events matching criteria
  - New users
  - Automated alerts for high-priority IOCs
- **Extend** existing MISP behavior
  - Push data to another system
  - Automatic enrichment
  - Sanity check to block publishing / sharing
  - Curation pipelines
- **Hook** capabilities
  - Assign tasks and notify incident response team members
- ...

Workflow - Fundamentals

Objective: Start with the foundation to understand the basics

How does it work



Melee Initialization

Events

Conditions

Actions

1. An **event** happens in MISP
2. *(optional)* Check if all **conditions** are satisfied
3. Execute all **actions**
   - May prevent MISP to complete its original event

What kind of events?

Events

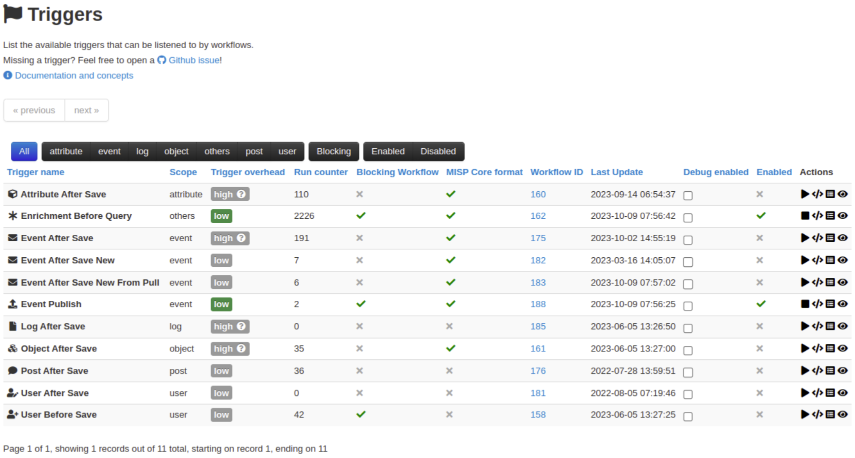
- New MISP Event
- Attribute has been saved
- New discussion post
- New user created
- Query against third-party services
- ...

? Supported events in MISP are called **Triggers**

? A **Trigger** is associated with **1-and-only-1 Workflow**

Triggers currently available

Currently 11 triggers can be hooked. 3 being Blocking.



Triggers

List the available triggers that can be listened to by workflows.

Missing a trigger? Feel free to open a Github issue!

Documentation and concepts

« previous | next »

All | attribute | event | log | object | others | post | user | Blocking | Enabled | Disabled

Trigger name	Scope	Trigger overhead	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Debug enabled	Enabled	Actions
Attribute After Save	attribute	high ?	110	×	✓	160	2023-09-14 06:54:37	☐	×	▶ </> ▤ 👁
Enrichment Before Query	others	low	2226	✓	✓	162	2023-10-09 07:56:42	☐	✓	■ </> ▤ 👁
Event After Save	event	high ?	191	×	✓	175	2023-10-02 14:55:19	☐	×	▶ </> ▤ 👁
Event After Save New	event	low	7	×	✓	182	2023-03-16 14:05:07	☐	×	▶ </> ▤ 👁
Event After Save New From Pull	event	low	6	×	✓	183	2023-10-09 07:57:02	☐	×	▶ </> ▤ 👁
Event Publish	event	low	2	✓	✓	188	2023-10-09 07:56:25	☐	✓	■ </> ▤ 👁
Log After Save	log	high ?	0	×	×	185	2023-06-05 13:26:50	☐	×	▶ </> ▤ 👁
Object After Save	object	high ?	35	×	✓	161	2023-06-05 13:27:00	☐	×	▶ </> ▤ 👁
Post After Save	post	low	36	×	×	176	2022-07-28 13:59:51	☐	×	▶ </> ▤ 👁
User After Save	user	low	0	×	×	181	2022-08-05 07:19:46	☐	×	▶ </> ▤ 👁
User Before Save	user	low	42	✓	×	158	2023-06-05 13:27:25	☐	×	▶ </> ▤ 👁

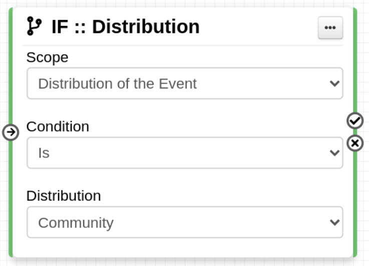
Page 1 of 1, showing 1 records out of 11 total, starting on record 1, ending on 11

What kind of conditions?

⇛ Conditions

- A MISP Event is tagged with `tlp:red`
- The distribution of an Attribute is a sharing group
- The creator organisation is `circl.lu`
- Or any other **generic** conditions

? These are also called **Logic modules**



IF :: Distribution

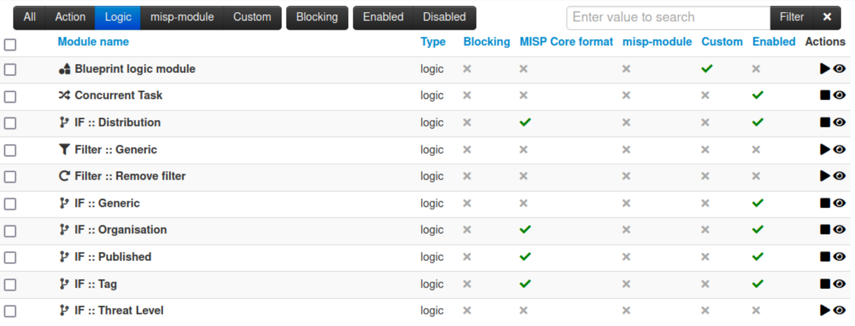
Scope: Distribution of the Event

Condition: Is

Distribution: Community

Workflow - Logic modules

- **logic** modules: Allow to redirect the execution flow.
  - IF conditions
  - Delay execution



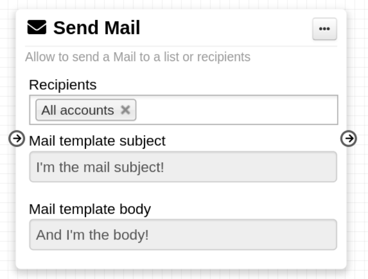
□	Module name	Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions
□	Blueprint logic module	logic	×	×	×	✓	×	▶ 👁
□	Concurrent Task	logic	×	×	×	×	✓	■ 👁
□	IF :: Distribution	logic	×	✓	×	×	✓	■ 👁
□	Filter :: Generic	logic	×	×	×	×	×	▶ 👁
□	Filter :: Remove filter	logic	×	×	×	×	×	▶ 👁
□	IF :: Generic	logic	×	×	×	×	✓	■ 👁
□	IF :: Organisation	logic	×	✓	×	×	✓	■ 👁
□	IF :: Published	logic	×	✓	×	×	✓	■ 👁
□	IF :: Tag	logic	×	✓	×	×	✓	■ 👁
□	IF :: Threat Level	logic	×	×	×	×	×	▶ 👁

What kind of actions?

Actions

- Send an email notification
- Perform enrichments
- Send a chat message on MS Teams
- Attach a local tag
- ...

These are also called **Action modules**



Send Mail

Allow to send a Mail to a list or recipients

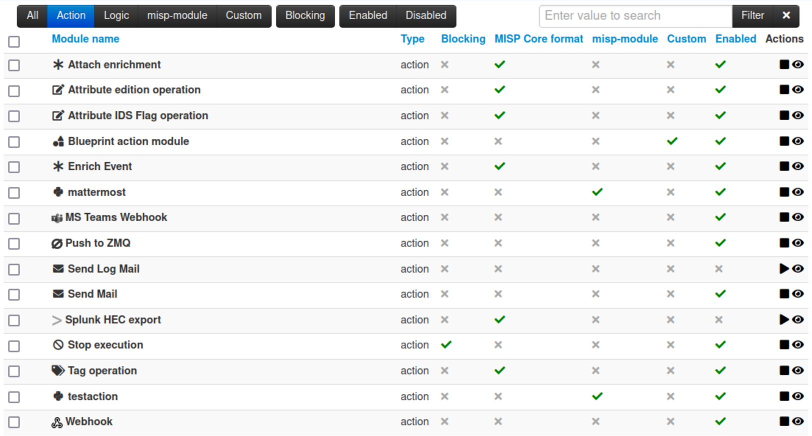
Recipients: All accounts ✕

Mail template subject: I'm the mail subject!

Mail template body: And I'm the body!

Workflow - Action modules

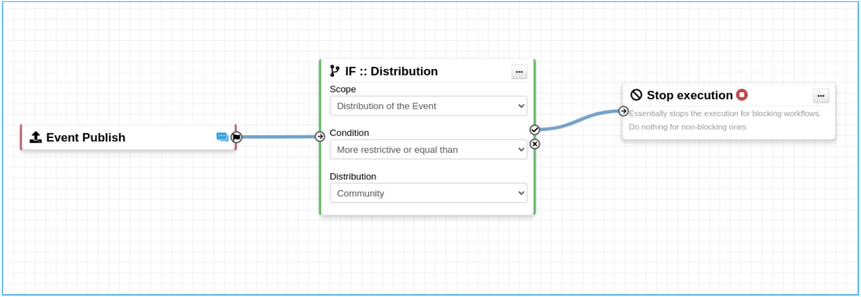
- **action** modules: Allow to executes operations
  - Tag operations
  - Send notifications
  - Webhooks & Custom scripts



□	Module name	Type	Blocking	MISP Core format	misp-module	Custom	Enabled	Actions
□	Attach enrichment	action	×	✓	×	×	✓	■ 👁
□	Attribute edition operation	action	×	✓	×	×	✓	■ 👁
□	Attribute IDS Flag operation	action	×	✓	×	×	✓	■ 👁
□	Blueprint action module	action	×	×	×	✓	✓	■ 👁
□	Enrich Event	action	×	✓	×	×	✓	■ 👁
□	mattermost	action	×	×	✓	×	✓	■ 👁
□	MS Teams Webhook	action	×	×	×	×	✓	■ 👁
□	Push to ZMQ	action	×	×	×	×	✓	■ 👁
□	Send Log Mail	action	×	×	×	×	×	▶ 👁
□	Send Mail	action	×	×	×	×	✓	■ 👁
□	Splunk HEC export	action	×	✓	×	×	×	▶ 👁
□	Stop execution	action	✓	×	×	×	✓	■ 👁
□	Tag operation	action	×	✓	×	×	✓	■ 👁
□	testaction	action	×	×	✓	×	✓	■ 👁
□	Webhook	action	×	×	×	×	✓	■ 👁

What is a MISP Workflow?

- Sequence of all nodes to be executed in a specific order
- Workflows can be enabled / disabled
- A Workflow is associated to **1-and-only-1 trigger**



Event Publish

IF :: Distribution

Scope: Distribution of the Event

Condition: More restrictive or equal than

Distribution: Community

Stop execution

Essentially stops the execution for blocking workflows.
Do nothing for non-blocking ones

Sources of Workflow modules (0)

Currently 36 built-in modules.

- **Trigger** module (11): built-in **only**
  - Get in touch if you want more
- **Logic** module (10): built-in & **custom**
- **Action** module (20): built-in & **custom**

Sources of Workflow modules (1)

- Built-in **default** modules
  - Part of the MISP codebase
  - Get in touch if you want us to increase the selection (or merge PR!)

Webhook v0.2
Allow to perform custom callbacks to the provided URL

Tag operation v0.2
Add or remove tags on Event or Attributes.

Stop execution v0.1
Essentially stops the execution for blocking workflows. Do nothing for non-blocking ones

Send Mail v0.1
Allow to send a Mail to a list or recipients

Enrich Event v0.1
Enrich all Attributes contained in the Event with the provided module.

MS Teams Webhook v0.2
Perform callbacks to the MS Teams webhook provided by the "Incoming Webhook" connector

Push to ZMQ v0.1
Push to the ZMQ channel

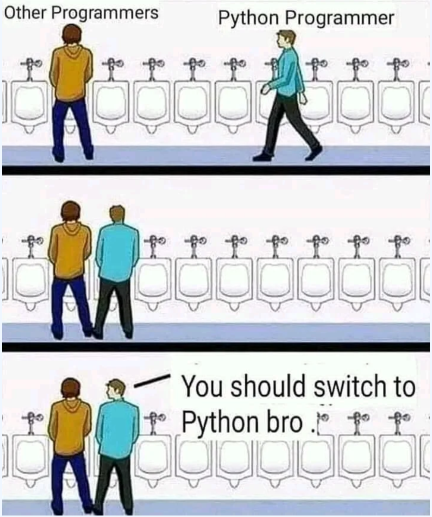
Sources of Workflow modules (2)

User-defined **custom** modules

- Written in PHP
- Extend existing modules
- MISP code reuse

Sources of Workflow modules (3)

Modules from the misp-module **enrichment service**



- Written in Python
- Can use any python libraries
- Plug & Play

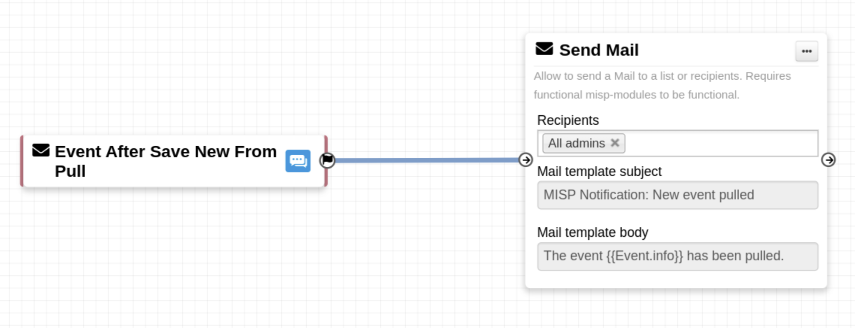
Demo by examples

WF-1. Send an email to **all admins** when a new event has been pulled

WF-2. Block queries on 3rd party services when **tlp:red** or **PAP:red**

- **tlp:red**: For the eyes and ears of individual recipients only
- **PAP:RED**: Only passive actions that are not detectable from the outside

Demo WF-1: Send an email to **all admins** when a new event has been pulled



Send Mail

Allow to send a Mail to a list or recipients. Requires functional misp-modules to be functional.

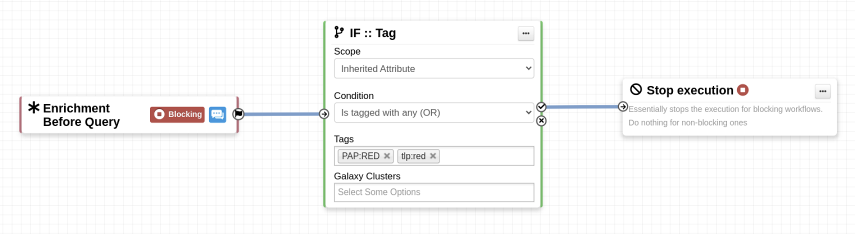
Recipients: All admins ✕

Mail template subject: MISP Notification: New event pulled

Mail template body: The event {{Event.info}} has been pulled.

Demo WF-2: Block queries on 3rd party services when **tlp:red** or **PAP:red**

- **tlp:red**: For the eyes and ears of individual recipients only
- **PAP:RED**: Only passive actions that are not detectable from the outside



Scope: Inherited Attribute

Condition: Is tagged with any (OR)

Tags: PAP:RED ✕ tlp:red ✕

Galaxy Clusters: Select Some Options

Stop execution

Essentially stops the execution for blocking workflows. Do nothing for non-blocking ones

Getting started with workflows

Everything is ready?

Let’s see how to build a workflow!

🛠

Creating a workflow with the editor

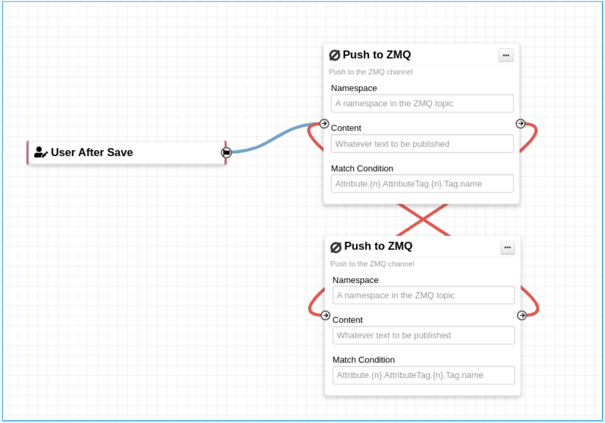
1. Prevent event publication **if tlp:red** tag
    - Send a mail to `admin@admin.test` about potential data leak
2. **else**, send a notification on Mattermost

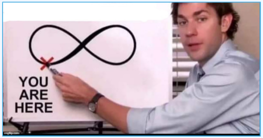
Considerations when working with workflows

Objective: Overview of some common pitfalls

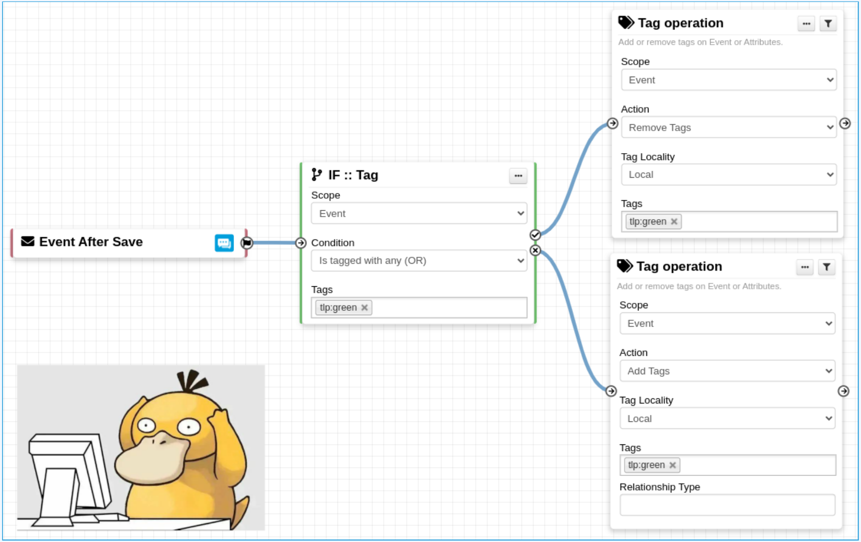
Working with the editor - Operations not allowed

Execution loop are not authorized


User After Save
Push to ZMQ
Push to the ZMQ channel
Namespace
A namespace in the ZMQ topic
Content
Whatever text to be published
Match Condition
Attribute.{n}.AttributeTag.{n}.Tag.name
Push to ZMQ
Push to the ZMQ channel
Namespace
A namespace in the ZMQ topic
Content
Whatever text to be published
Match Condition
Attribute.{n}.AttributeTag.{n}.Tag.name



Recursive workflows



Event After Save

IF :: Tag

Scope: Event

Condition: Is tagged with any (OR)

Tags: tlp:green

Tag operation

Add or remove tags on Event or Attributes.

Scope: Event

Action: Remove Tags

Tag Locality: Local

Tags: tlp:green

Tag operation

Add or remove tags on Event or Attributes.

Scope: Event

Action: Add Tags

Tag Locality: Local

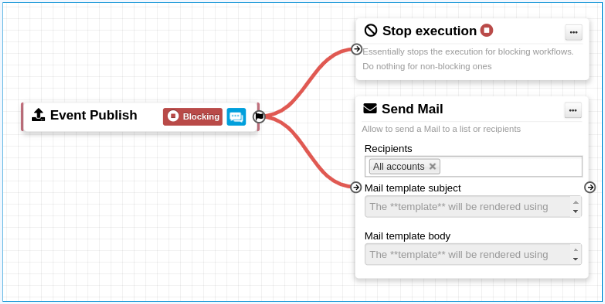
Tags: tlp:green

Relationship Type:

⚠Recursion: If an action re-run the workflow

Working with the editor - Operations not allowed

Multiple connections from the same output



Event Publish

Blocking

Stop execution

Essentially stops the execution for blocking workflows.
Do nothing for non-blocking ones

Send Mail

Allow to send a Mail to a list or recipients

Recipients

All accounts

Mail template subject

The **template** will be rendered using

Mail template body

The **template** will be rendered using

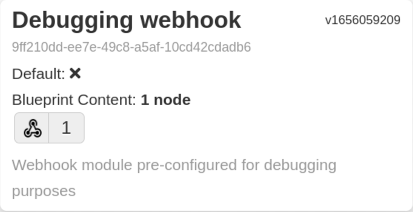
- Execution order not guaranted
- Confusing for users

Advanced usage

Objective: Overview of Blueprints, Data format and Filtering

Workflow blueprints

1. Blueprints allow to **re-use parts** of a workflow in another one
2. Blueprints can be saved, exported and **shared**



Debugging webhook

v1656059209

9ff210dd-ee7e-49c8-a5af-10cd42cdadb6

Default: ✗

Blueprint Content: **1 node**

Webhook module pre-configured for debugging purposes

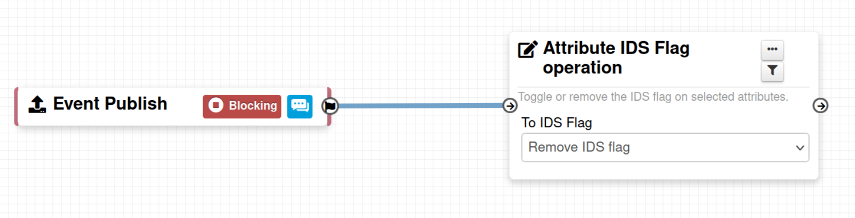
Blueprints sources: `MISP/misp-workflow-blueprints` repository[1]

- Block actions if any attributes have the `PAP:RED` or `tlp:red` tag
- Curation pipeline
- Enrich data from 3rd-party

[1] https://github.com/MISP/misp-workflow-blueprints

Fitlering data on which to apply a module

What is the outcome of executing this workflow?

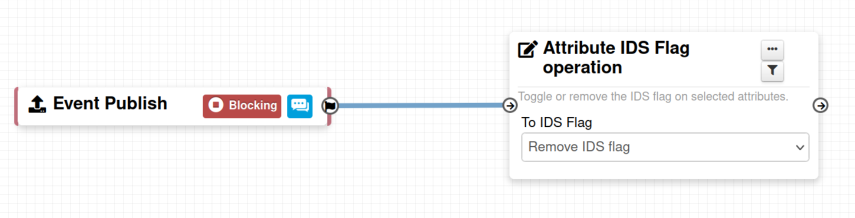


Toggle or remove the IDS flag on selected attributes.

To IDS Flag: Remove IDS flag

FITLERING DATA ON WHICH TO APPLY A MODULE

What is the outcome of executing this workflow?



Event Publish

Blocking

Attribute IDS Flag operation

Toggle or remove the IDS flag on selected attributes.

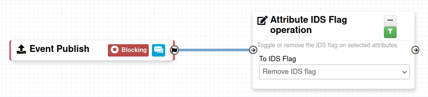
To IDS Flag: Remove IDS flag

All Attributes get their `to_ids` turned off.

How could we force that action only on Attribute of type `comment`?

→ Hash path filtering!

Fitlering data on which to apply a module

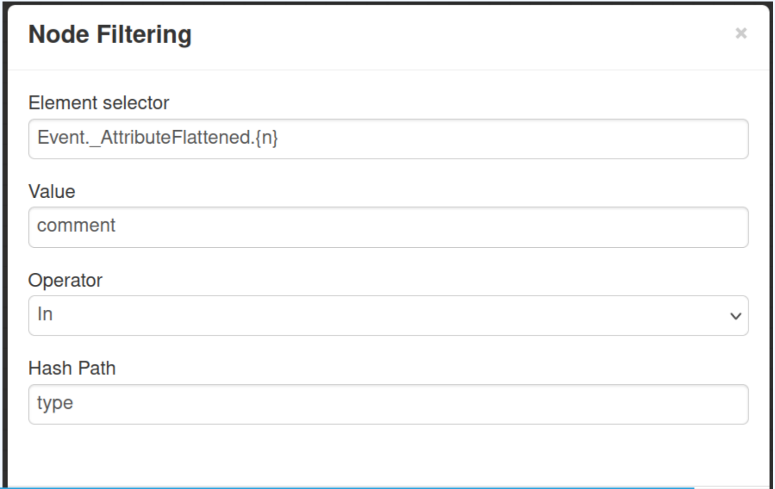


Attribute IDS Flag operation

Toggle or remove the IDS flag on selected attributes.

To IDS Flag

Remove IDS flag



Node Filtering

Element selector

Event._AttributeFlattened.{n}

Value

comment

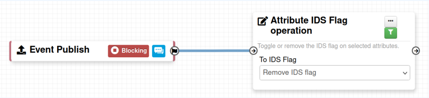
Operator

In

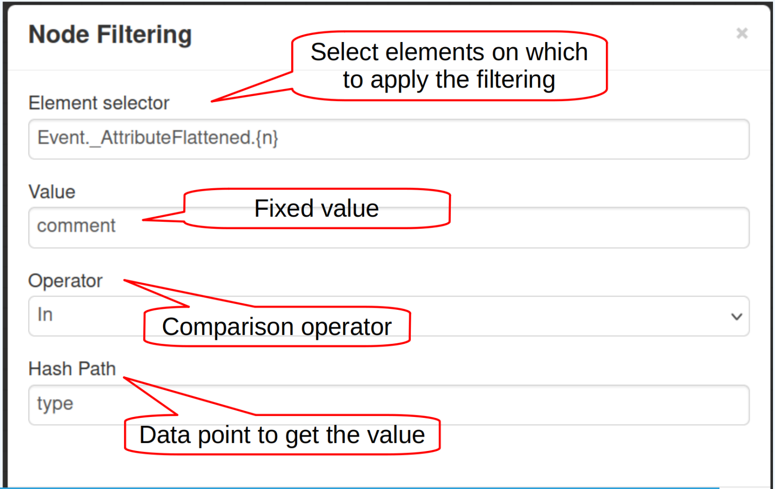
Hash Path

type

Fitlering data on which to apply a module



Event Publish
Blocking
Attribute IDS Flag operation
Toggle or remove the IDS flag on selected attributes.
To IDS Flag
Remove IDS flag



Node Filtering

Element selector: Event._AttributeFlattened.{n}

Value: comment

Operator: In

Hash Path: type

Select elements on which to apply the filtering

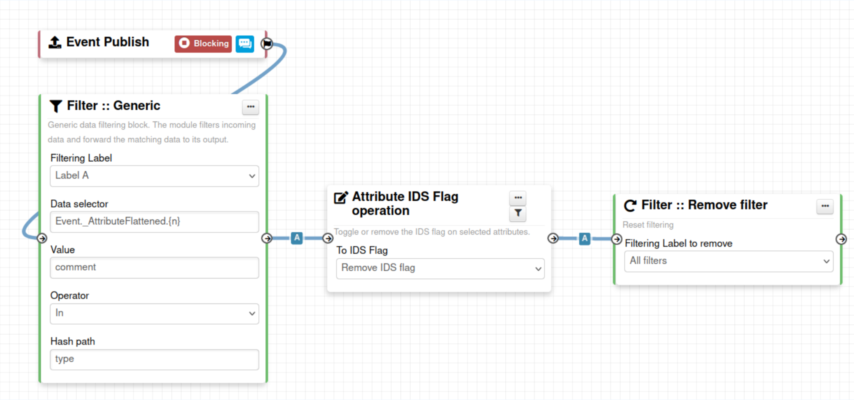
Fixed value

Comparison operator

Data point to get the value

Fitlering data on which to apply on multiple modules

New feature as of **v2.4.171** allows setting filters on a path.



Event Publish

Blocking

Filter :: Generic

Generic data filtering block. The module filters incoming data and forward the matching data to its output.

Filtering Label: Label A

Data selector: Event._AttributeFlattened.{n}

Value: comment

Operator: In

Hash path: type

Attribute IDS Flag operation

Toggle or remove the IDS flag on selected attributes.

To IDS Flag: Remove IDS flag

Filter :: Remove filter

Reset filtering

Filtering Label to remove: All filters

Should I migrate to MISP Workflows

I have automation in place using the API/ZMQ. Should I move to Workflows?

- I have a curation pipeline using the API, should I port it to workflows?
  - **No** in general, but WF can be used to start the curation process or perform simple pre-processing
- What if I want to **block** some actions
  - Put the blocking logic in the WF, keep the remaining outside
- Bottom line is **Keep it simple** for you to maintain

Future works

- More modules
- More modules
- More triggers
- Recursion prevention system

Final words

- Designed to **quickly** and **cheaply** integrate MISP in CTI pipelines
- **Beta** Feature unlikely to change. But still..
- Waiting for feedback!
  - New triggers?
  - New modules?