Discovering MISP workflows

Improving automation in threat intelligence

CIRCL / Team MISP Project

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

EU MITRE ATT&CK
Community Workshop

MISP
Threat Sharing

Bringing workflows into threat intelligence platform

After multiple years, MISP users have reach a significant maturity level:

- Events with **complex TTPs, objects and attributes**;
- Exhaustive context such as **MITRE ATT&CK**, tags and relationships;
- Availability of **external modules and services** (e.g. from expansion services to third-party CTI);
- Comprehensive **processing pipelines** for threat intelligence are available;

Where is the glue?

- Initial idea came from GeekWeek7.5

- Experienced users wanted to have a way to **trigger actions and to modify to behavior of MISP** and especially leveraging what they have in their MISP platform.
- **Creating workflows for any of the steps** in MISP (creating attributes/objects, publishing and sharing information, ...).

Simplistic overview

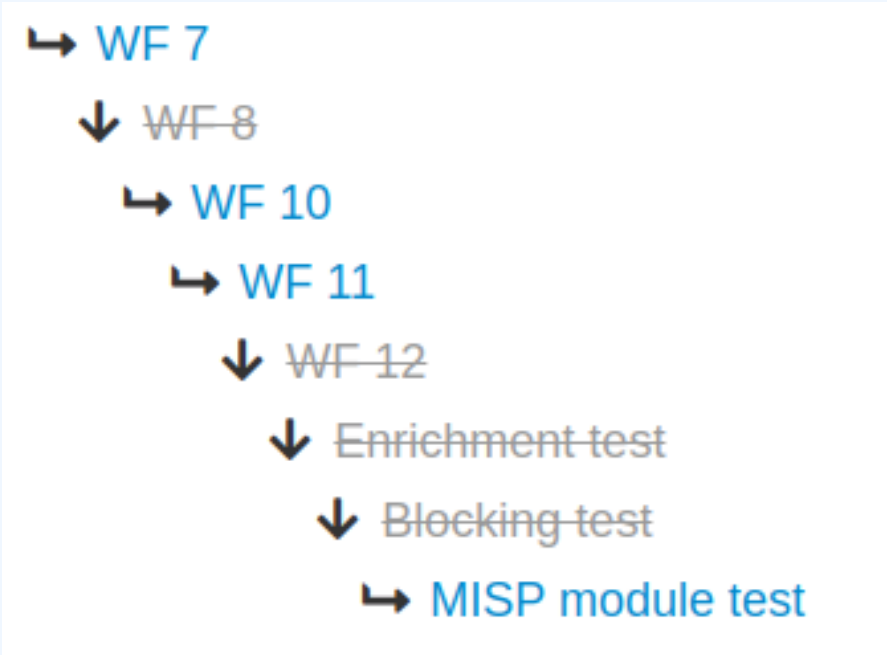
1. **User Interacts** with MISP using the UI or API
2. MISP handles the request, starts **preparing data** to perform the operation
3. MISP checks if there are workflows **listening to the trigger**
4. MISP fetches enabled workflows and **executes** them
5. If all went fine, MISP **continue** to perform the operation

Terminology

1. **workflow**: Sequence of actions to be executed
2. **execution path**: A path composed of actions to be executed sequentially
   - A workflow can contain more than one execution path
3. **trigger**: Starting point of an `execution path`. Triggers are called when specific action are done by MISP
   - A workflow can contain more than one trigger, but only one per type

Workflow execution in MISP

1. A trigger is called;
2. Collect workflows listening to called trigger;
3. Execute workflows in the saved order;



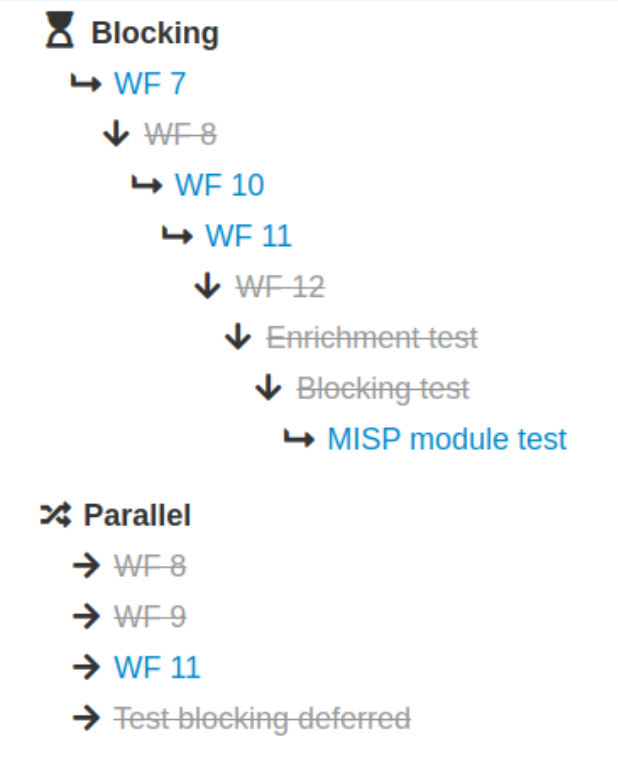
Execution Paths

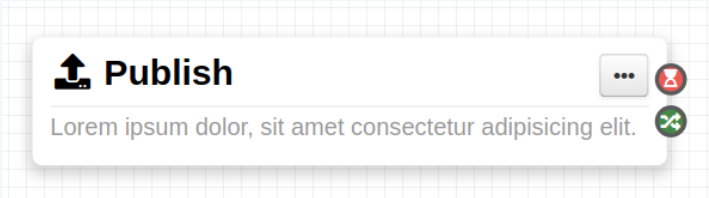
Currently 2 types of execution path:

- **Blocking**: Execution is stoped in case of error
  - Current workflow's blocking execution path is **stopped**
  - Any other blocking path of next workflows **will not be executed**
- **Non-blocking**/Deferred: Stop execution for current path only
  - Current execution path is **stopped**
  - **Resume** execution of remaining paths
  - Paths from other workflow will be **executed**

Execution Order and Execution Types

- **Blocking** paths from all workflows are executed first in the saved order
- If any blocking executions failed, the action that called the trigger will **be stopped**
- **Parallel/Deferred** paths from all workflows are executed. The order is irrelevant





Publishing example

Example:

1. An Event is published
2. MISP starts the publishing process
3. MISP executes a workflow listening to the trigger
   - **execution success**: Proceed publishing
   - **execution failure**: Stop publishing, log the reason and report the failure to the user

Execution context

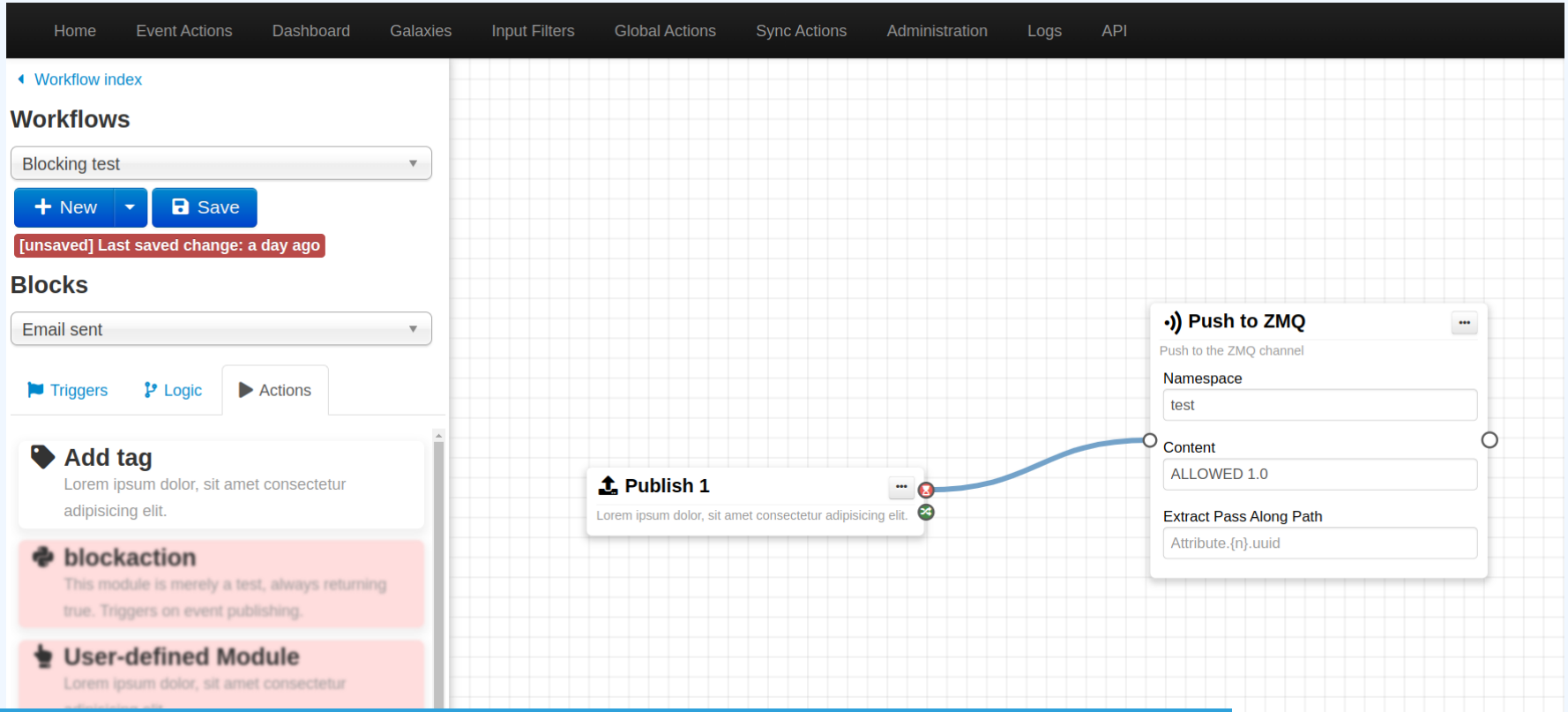
- Workflow can be triggered by any users
- However, the user for which the workflow executes is the workflow creator
- This is to make sure users with a higher privilege will have their workflow correctly executed

Workflow modules

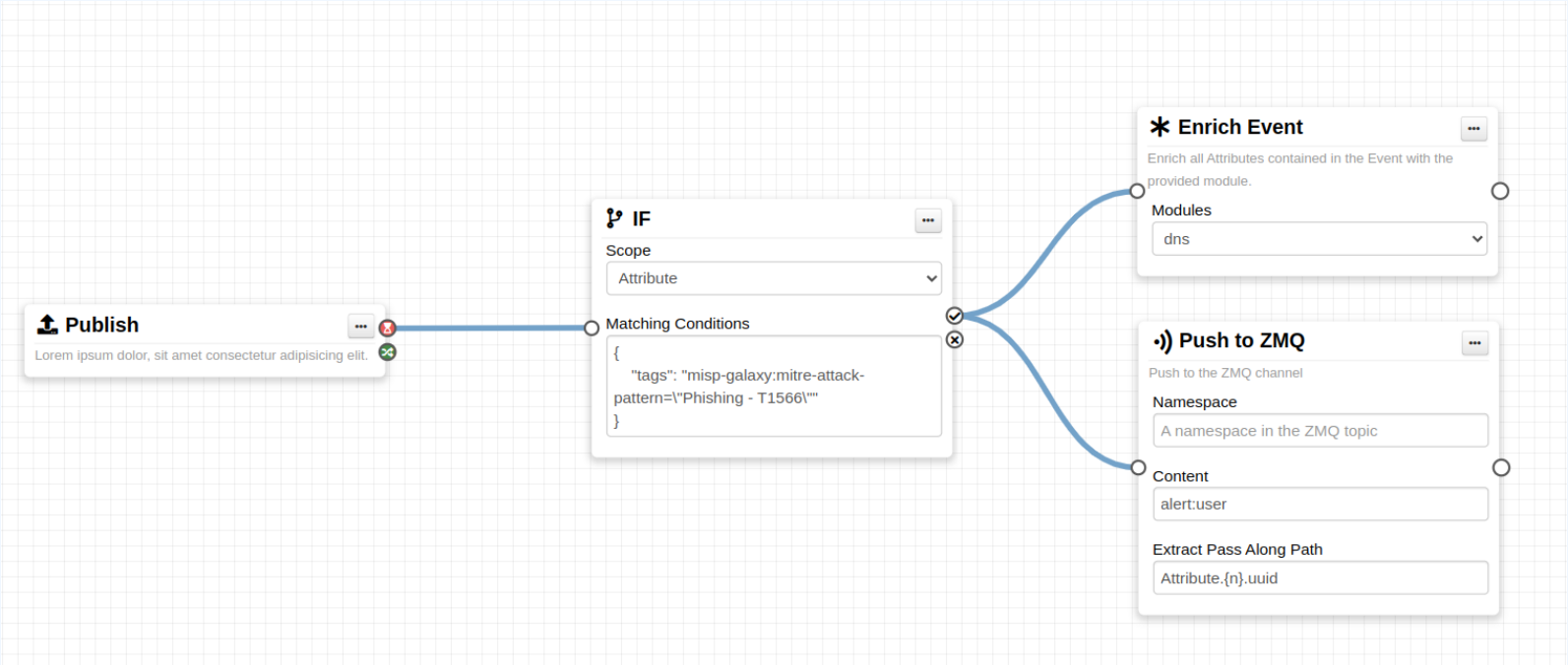
- 3 types of modules
  - `trigger`: Entry point of the execution
    - Event publish, email about to be sent, feed data about to be saved, ...
  - `logic`: Allow to redirect the execution flow.
    - IF condition, fork the blocking execution into a non-blocking one, ...
  - `action`: Modules that can modify data, prevent execution or perform additional actions
    - Publish to ZMQ, perform enrichments, block the execution, ...

Creating a workflow with the editor

1. Drag a `trigger` module from the side panel to the canvas
2. Drag an `action` module from the side panel to the canvas
3. From the `trigger` output, drag an arrow into the `action` input (left side)
   - You can choose between a `blocking` and `non-blocking` execution path by using the associated trigger output

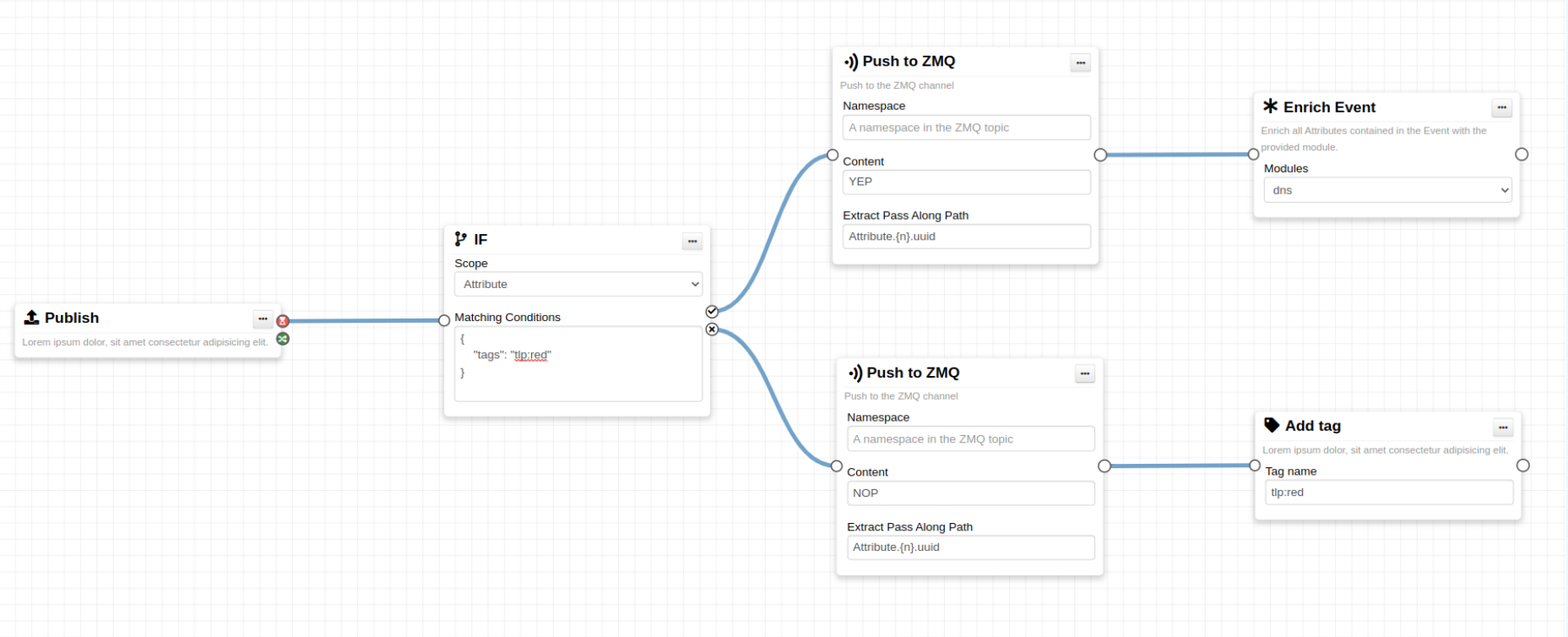


Workflow example with ATT&CK



1. Automatically processing phishing cases from ATT&CK context including enrichments and publishing pipelines.

Workflow - advanced example



Category	Type	Value	Tags
Network activity	ip-src	185.194.93.14	tlp:red x
Network activity	domain	circl.lu	tlp:white x

Ongoing developments

- First release of the workflow in MISP for the FIRST.org annual conference in Dublin (end of June).
- **Workflows are shareable** and a library of workflows will be available.
- Gathering ideas and requirements for new workflows from the threat intelligence community.
- Reviewing ATT&CK techniques to be mapped in the MISP workflows.