

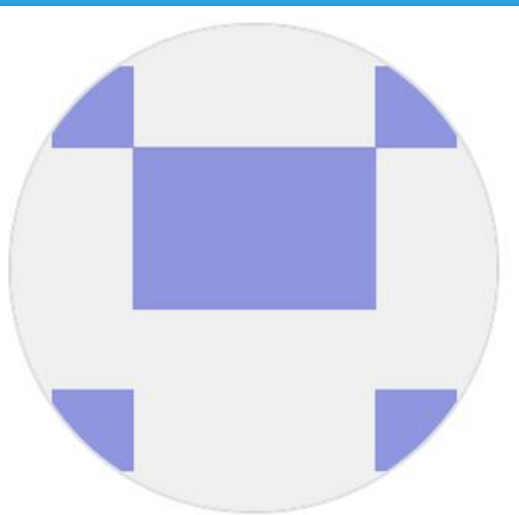


Integrating New Tools in Your Workflows Within Minutes in

MISP
Threat Sharing



Sami Mokaddem



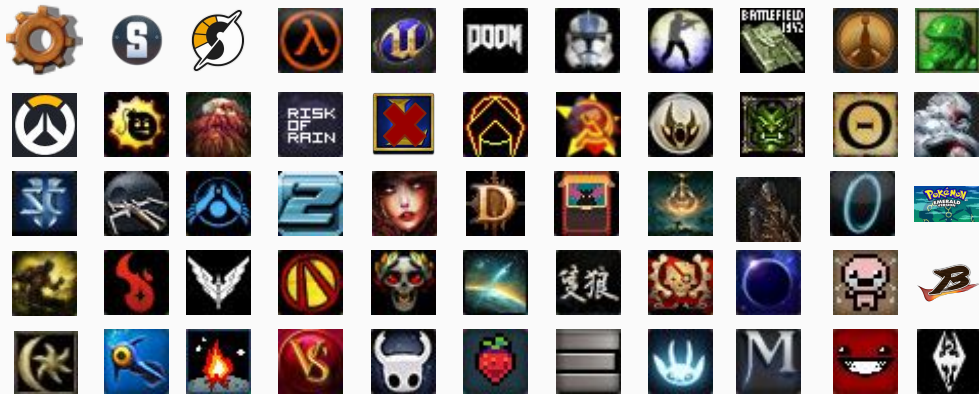
Sami Mokaddem
mokaddem

- Working at CIRCL since 2016
- Part of the MISP-Project team

Event graph viewer editor #3063

Merged adulau merged 27 commits into MISP:2.4 from mokaddem:ref_graph on 23 Mar 2018

- Love video games



Building MISP Features with Music...

AIL Project: Secrets in Squares - QR Codes



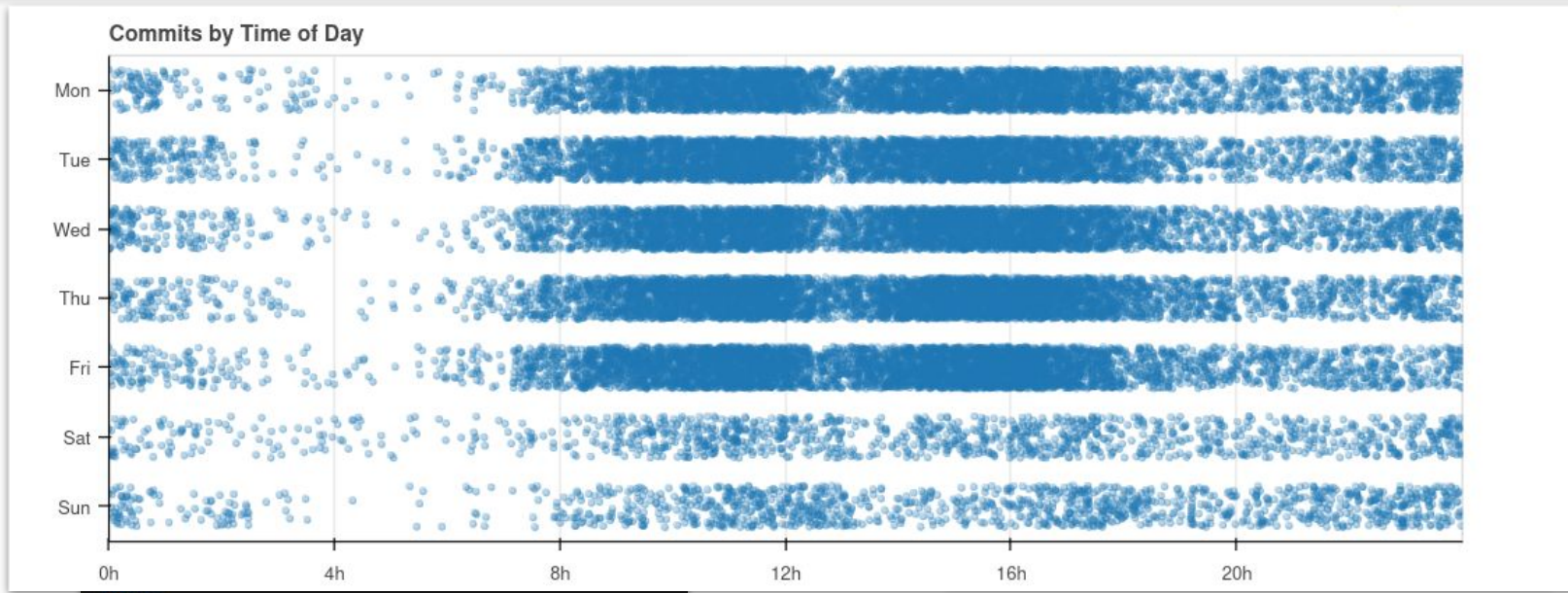
CIRCL

Computer Incident
Response Center
Luxembourg

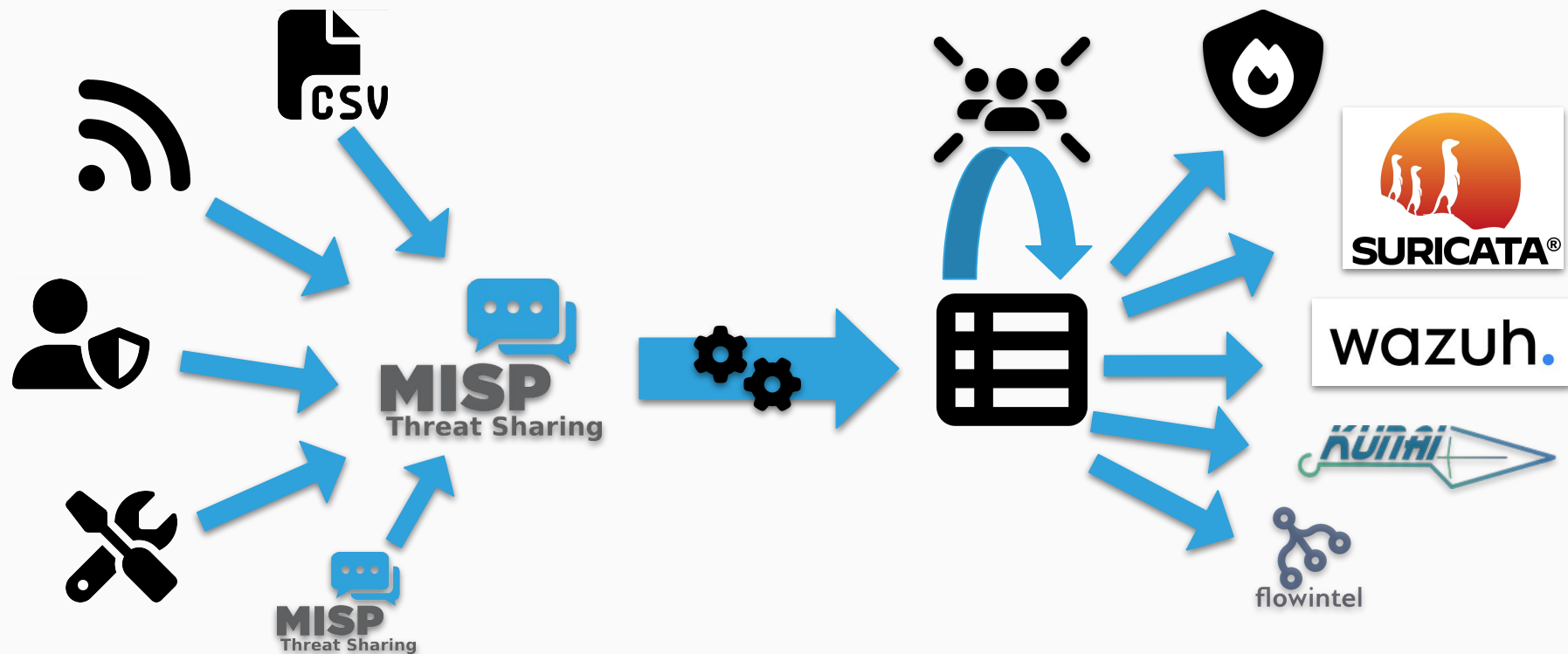
Aurelien Thirion
aurelien.thirion@circl.lu



Threat Intelligence Sharing Platform - TISP



MISP? What can I use it for?



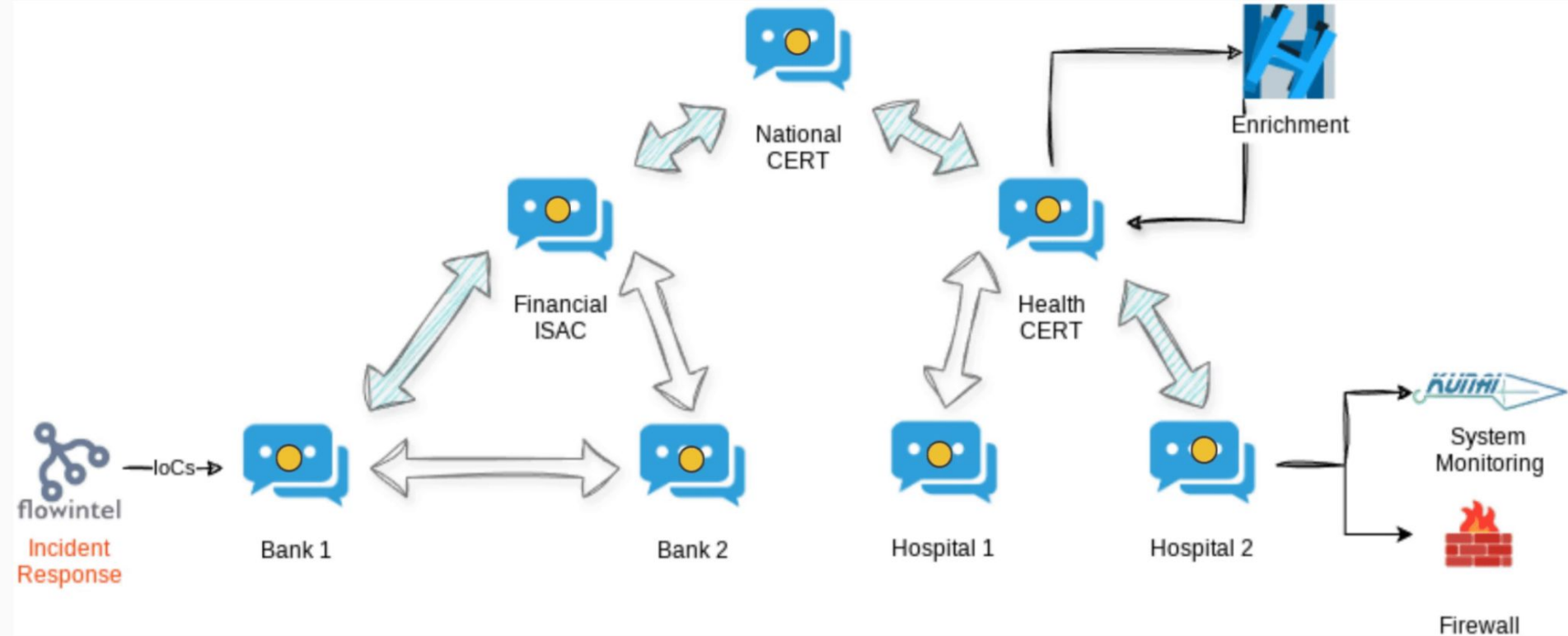
Collect

Normalise
/ Enrich

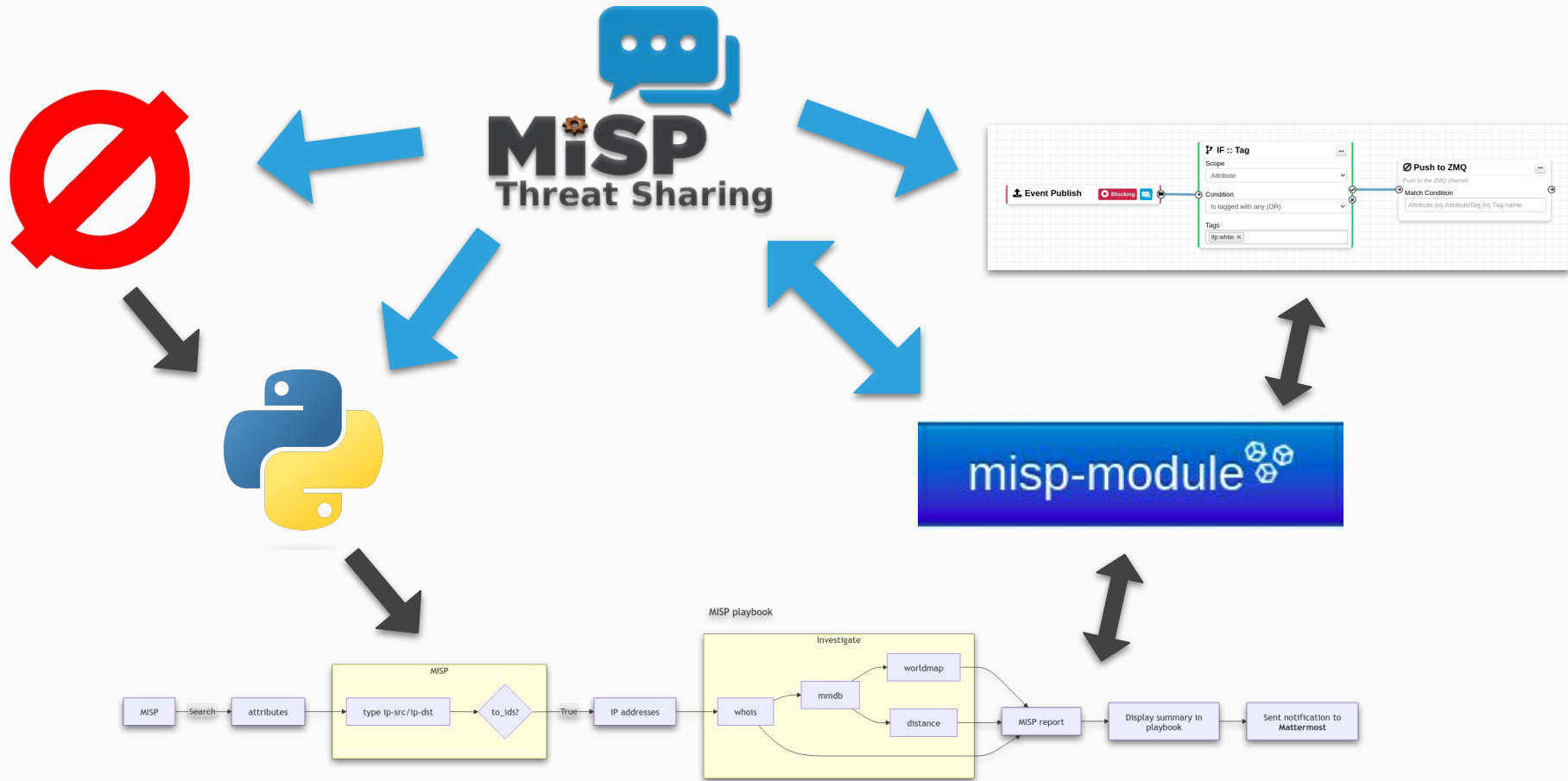
Collaborate

Feed /
Dissemination

MISP Community & Information Sharing



MISP Automation Ecosystem



Category	Type	Value
Network activity	ip-src	9.9.9.9 🔍

give_me_geolocation.py

Name: geolocation 📄

References: 1 📄

related-to Attribute 3d814069-8499-47f9-bd97-01050e264852 (ip-src: Network activity)

9.9.9.9: Inherit event ▼

Enriched via the mmdb_lookup module

<input checked="" type="checkbox"/>	Other	country text	Switzerland	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Inherit event ▼	
<input checked="" type="checkbox"/>	Other	countrycode text	CH	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Inherit event ▼	
<input checked="" type="checkbox"/>	Other	latitude float	47	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	Inherit event ▼	
<input checked="" type="checkbox"/>	Other	longitude float	8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	Inherit event ▼	
<input checked="" type="checkbox"/>	Other	text text	db_source: GeoOpen-Country, build_db: 2023-11-20 12:50:37. Latitude and longitude are country average.		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text"/>	Inherit event ▼

misp-module

```
root@sami-T14:/home/sami/git/misp-modules/misp_modules/modules/expansion# ls
abuseipdb.py                extract_url_components.py    malwarebazaar.py
apiosintds.py              farsight_passivedns.py     mcafee_insights_enrich.py
apivoid.py                 geoiip_asn.py              mmdb_lookup.py
assemblyline_query.py      geoiip_city.py             module_misp_standard.py.skeleton
assemblyline_submit.py     geoiip_country.py          module.py.skeleton
backscatter_io.py          google_safe_browsing.py    mwdb.py
btc_scam_check.py          google_search.py           ocr_enrich.py
btc_steroids.py            google_threat_intelligence.py
censys_enrich.py           greynoise.py               ods_enrich.py
circl_passivedns.py        hashdd.py                  odt_enrich.py
circl_passivessl.py        hashlookup.py              onyphe_full.py
clamav.py                  hibp.py                    onyphe.py
cluster25_expand.py        html_to_markdown.py        otx.py
convert_markdown_to_pdf.py hyasinsight.py             passive_ssh.py
countrycode.py             __init__.py                passivetotal.py
cpe.py                      intel471.py                 pdf_enrich.py
crowdsec.py                intelmq_eventdb.py.experimental
crowdstrike_falcon.py     ip2locationio.py          pptx_enrich.py
cuckoo_submit.py           ipasn.py                   __pycache__
custom_custom.py           ipinfo.py                  qintel_qsentry.py
cve_advanced.py            ipqs_fraud_and_risk_scoring.py
cve.py                      iprep.py                   qrcode.py
cytomic_orion.py           jinja_template_rendering.py
dbl_spamhaus.py            joesandbox_query.py        _ransomcoindb
_dnsdb_query               joesandbox_submit.py       ransomcoindb.py
dns.py                      lastline_query.py          rbl.py
docx_enrich.py             lastline_submit.py         recordedfuture.py
domaintools.py             macaddress_io.py           reversedns.py
eql.py                     macvendors.py              securitytrails.py
eupi.py                    malshare_upload.py         shodan.py
root@sami-T14:/home/sami/git/misp-modules/misp_modules/modules/expansion# ls | wc
120      120      1926
sigma_queries.py           sigma_syntax_validator.py   sigmf_expand.py
sigma_syntax_validator.py  socialscan.py               sophoslabs_intelix.py
sourcecache.py            stairwell.py                stix2_pattern_syntax_validator.py
threatcrowd.py            threatfox.py                 threatminer.py
triage_submit.py          trustar_enrich.py           urlhaus.py
urlscan.py                variotdbs.py                virustotal_public.py
virustotal.py             virustotal_upload.py       vmray_submit.py
vmware_nsx.py             vulndb.py                   vulnerability_lookup.py
_vulnerability_parser     vulners.py                  vysion.py
whoisfreaks.py            whois.py                    wiki.py
xforceexchange.py        xlsx_enrich.py              yara_query.py
yara_syntax_validator.py  yeti.py
```

MISP Workflow

Triggers

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

Missing a trigger? Feel free to open a [Github issue!](#)

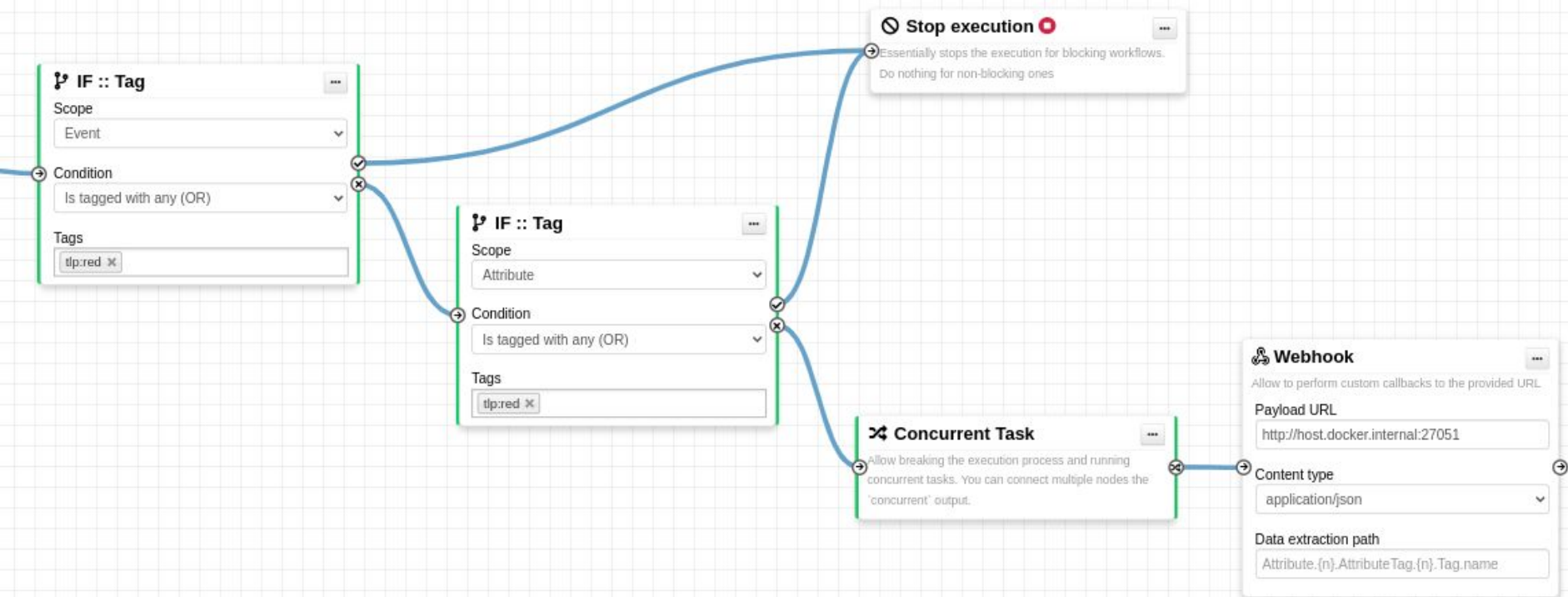
[Documentation and concepts](#)

« previous next »

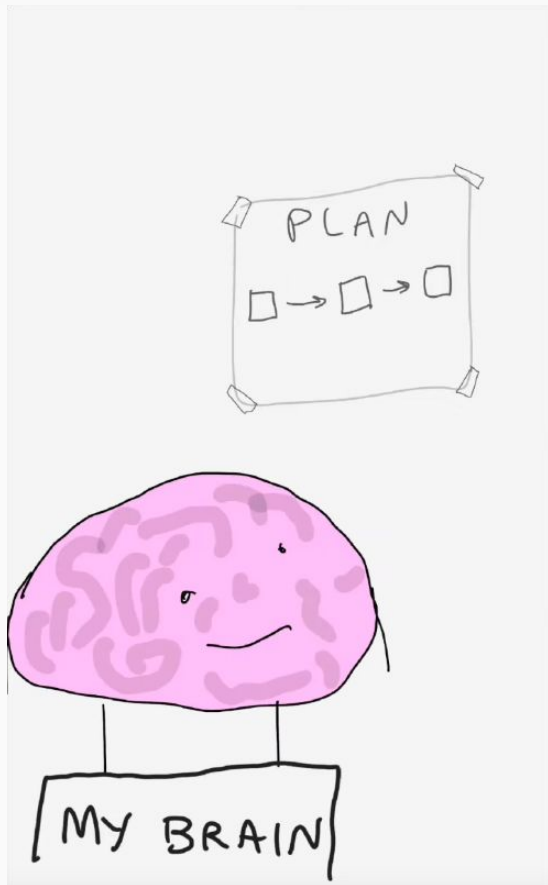
All attribute event event-report log object others post shadow-attribute sighting tag user Blocking Enabled Disabled

Trigger name	Scope	Trigger overhead	Description	Run counter	Blocking Workflow	MISP Core format	Workflow ID	Last Update	Debug enabled	Enabled	Actions
Attribute After Save	attribute	high	This trigger is called after an Attribute has been saved in the database	6075	×	✓	11	2024-10-18 09:03:37	<input type="checkbox"/>	✓	🔍 🔄 🗑️
Enrichment Before Query	others	low	This trigger is called just before a query against the enrichment service is done		✓	✓				×	▶ 🔄 🗑️
Event After Save	event	high	This trigger is called after an Event or any of its elements has been saved in the database	2	×	✓	8	2024-10-07 10:18:53	<input type="checkbox"/>	×	▶ 🔄 🗑️
Event After Save New	event	low	This trigger is called after a new Event has been saved in the database		×	✓				×	▶ 🔄 🗑️
Event After Save New From Pull	event	low	This trigger is called after a new Event has been saved in the database from a PULL operation. This trigger executes in place of 'event-after-save-new'	0	×	✓	2	2024-06-13 11:54:07	<input type="checkbox"/>	×	▶ 🔄 🗑️
Event Before Save	event	high	This trigger is called before an Event or any of its elements is about to be saved in the database		✓	✓				×	▶ 🔄 🗑️
Event Publish	event	low	This trigger is called just before a MISP Event starts the publishing process	50	✓	✓	1	2024-10-07 13:31:02	<input type="checkbox"/>	✓	🔍 🔄 🗑️
Event Report After Save	event-report	low	This trigger is called after an Event Report has been saved in the database	30	×	✓	5	2024-10-04 09:04:54	<input type="checkbox"/>	×	▶ 🔄 🗑️
Log After Save	log	high	This trigger is called after a Log event has been saved in the database	0	×	×	4	2024-07-18 09:02:02	<input type="checkbox"/>	×	▶ 🔄 🗑️
Object After Save	object	high	This trigger is called after an Object has been saved in the database	3	×	✓	12	2024-10-17 08:45:34	<input type="checkbox"/>	×	▶ 🔄 🗑️
Post After Save	post	low	This trigger is called after a Post has been saved in the database		×	×				×	▶ 🔄 🗑️
Shadow Attribute After Save	shadow-attribute	medium	This trigger is called just after a Shadow Attribute has been saved in the database	25	×	✓	7	2024-10-07 13:34:04	<input type="checkbox"/>	×	▶ 🔄 🗑️
Shadow Attribute Before Save	shadow-attribute	medium	This trigger is called just before a Shadow Attribute is saved in the database	0	✓	✓	6	2024-10-04 09:40:03	<input type="checkbox"/>	×	▶ 🔄 🗑️
Sighting After Save	sighting	medium	This trigger is called when a sighting has been saved	0	×	✓	3	2024-06-18 14:51:10	<input type="checkbox"/>	✓	🔍 🔄 🗑️
Tag Attached After Save	tag	high	This trigger is called just after a Tag has been attached to an Event or an Attribute.	3547	×	✓	9	2024-10-18 09:01:11	<input type="checkbox"/>	✓	🔍 🔄 🗑️
User After Save	user	low	This trigger is called after a user has been saved in the database	0	×	×	10	2024-10-07 13:38:26	<input type="checkbox"/>	×	▶ 🔄 🗑️
User Before Save	user	low	This trigger is called just before a user is save in the database		✓	×				×	▶ 🔄 🗑️

MISP Workflow



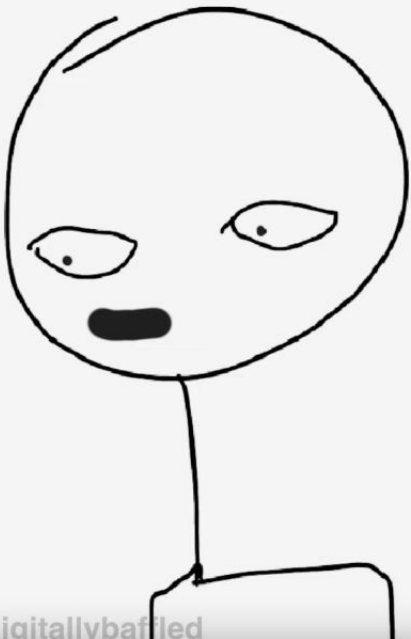
The plan



- We have an `.onion` address
 - We want to get more info about it → **enrichment**
- A. **Write the enrichment `onion_lookup.py`**
- We have a way to get more info
 - We want to automate that step → **workflow**
- B. **Design a workflow to remove user interaction**
1. Automatically enrich any `.onion` when they enter the tool
 2. Restrict sharing if `.onion` contains unwanted content
 3. For specific tags warn users on chat application / create a case

A. Write the enrichment `onion_lookup.py`

The doing Yes



- STEP 1: Duplicate the pre-made module skeleton

```
$ cp module_misp_standard.py.skeleton \
  onion_lookup.py
```

- STEP 2: Modify `onion_lookup.py`

```
$ emacs onion_lookup.py
```

- STEP 3: Restart `misp-module`
- STEP 4: Test it

Getting information about .onion

onion-lookup: Everything you've always wanted to know about a Tor hidden service.



onion-lookup

onion-lookup is a service for checking the existence of Tor hidden services and retrieving their associated metadata. onion-lookup relies on an private [AIL](#) instance to obtain the metadata.



API

An OpenAPI is also available to query onion-lookup.

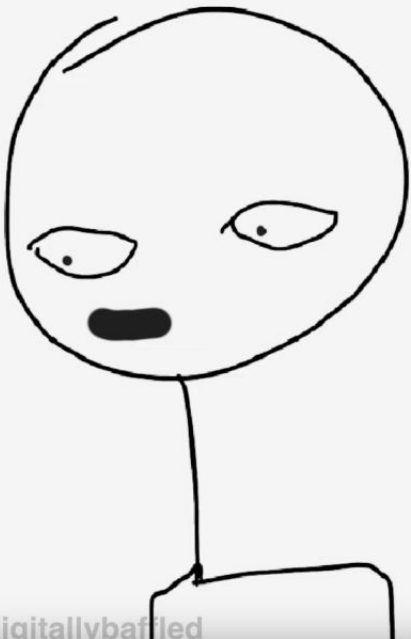
<https://onion.ail-project.org/>



onion-lookup is an open project part of the [AIL Project](#). Source code of the project is available at <https://github.com/ail-project/onion-lookup> released under the GNU Affero General Public License version 3.

A. Write the enrichment `onion_lookup.py`

The doing Yes



- STEP 1: Duplicate the pre-made module skeleton

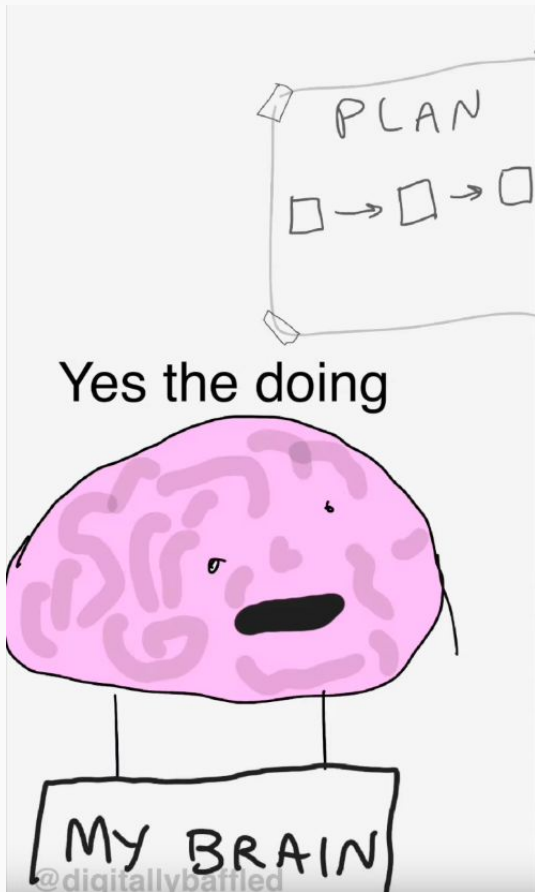
```
$ cp module_misp_standard.py.skeleton \
  onion_lookup.py
```

- STEP 2: Modify `onion_lookup.py`

```
$ emacs onion_lookup.py
```

- STEP 3: Restart [misp-module](#)
- STEP 4: Test it

B. Design a workflow to remove user interaction



1. Restrict sharing if .onion contains unwanted content

- Decision based on the tag

`dark-web:topic="pornography-child-exploitation"`



2. Automatically enrich any .onion when they enter the tool



3. For specific tags warn users on chat application / create a case

`infoleak:automatic-detection="credit-card"`

1. Restrict sharing if .onion contains unwanted content

Workflow that: automatically adjusts attribute's distribution to **Your Org Only**

When `dark-web:topic="pornography-child-exploitation"` is attached.



WHEN tag is attached to attribute

IF tag equals `dark-web:topic="pornography-child-exploitation"`

SET attribute distribution to **Your Org Only**

1. Restrict sharing if .onion contains unwanted content

Tag Attached After Save

Scope
Attributes

Tag Locality
Global

Tags
Type a tag

IF :: Tag

Scope
Attribute

Condition
Is tagged with any (OR)

Tags
dark-web:topic="pornography-child-exploitation"

Galaxy Clusters
Select Some Options

Attribute distribution operation

Set the Attribute's distribution to the selected level

Distribution
Organisation

2. Automatically enrich any .onion when they enter the tool

Workflow that: automatically run enrichment for any .onion



WHEN attribute is created

IF attribute is an



RUN enrichment onion_lookup.py

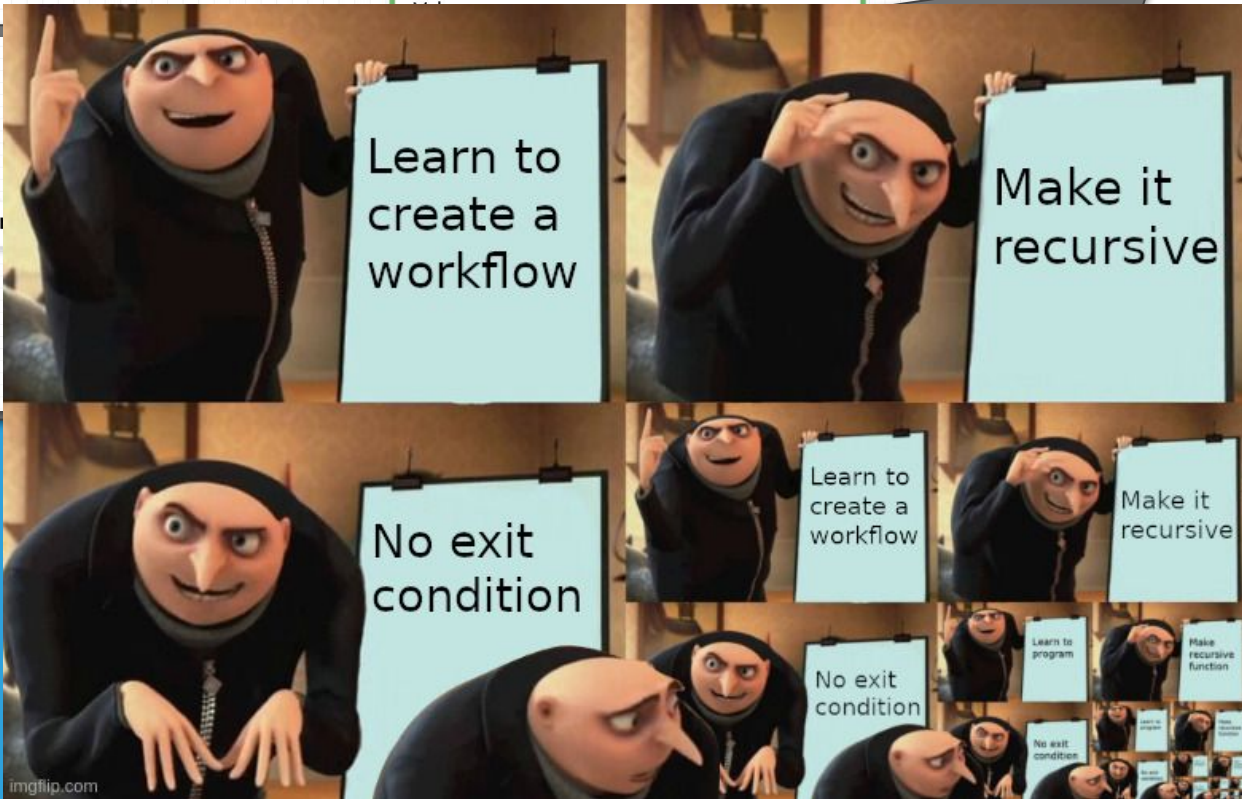
IF :: Generic

* Enrich Event

...utes contained in the Event with the

Att

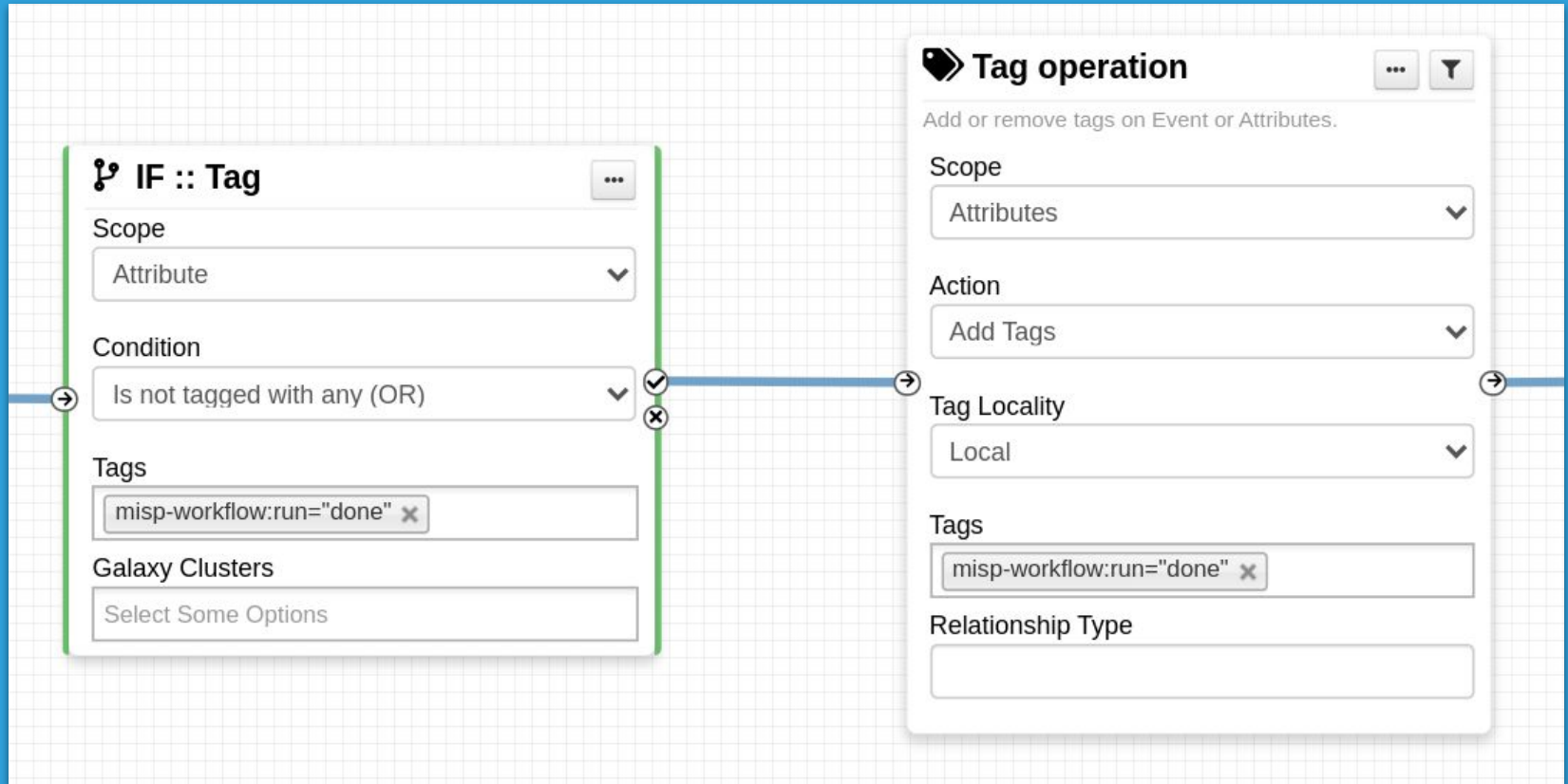
Att



How to solve that recursion?

1. Enforce the workflow **to run only once on the same Attribute**
 - Usage of local tags to indicate if it was run or not
2. Prevent the workflow **from running on new Attributes**
 - Only run the workflow on:
 - Attribute, not Object's Attribute
 - Will not work if an analyst creates an `.onion` Object
 - Attribute not having the comment "created via enrichment"
 - Requires `onion-lookup.py` to add a comment
 - Requires the workflow to add the comment to new Attributes
 - Attribute not having a dedicated tag
 - Same as above.

1. Enforce the workflow to run only once on the same Attribute



2. Prevent the workflow from running on new Attributes

IF :: Generic

Value

0

Operator

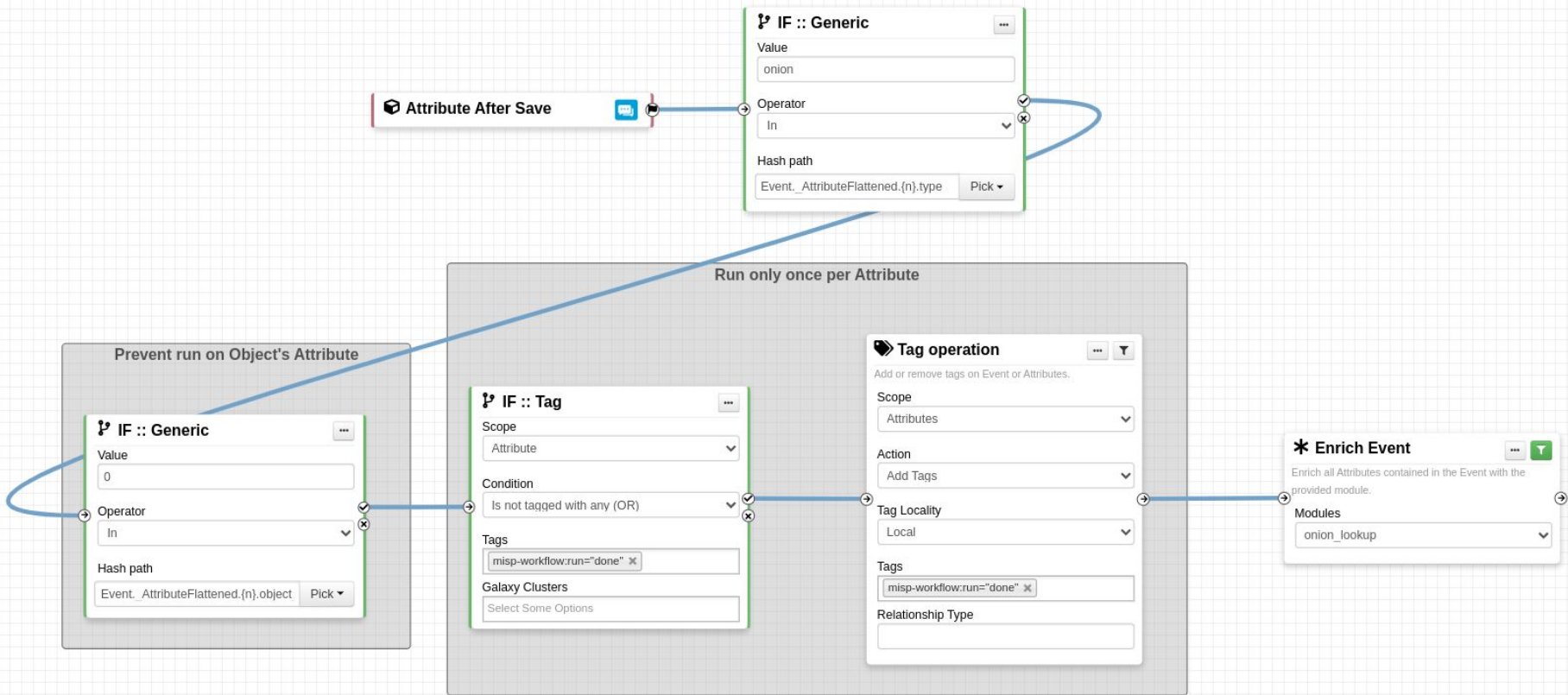
In

Hash path

Event._AttributeFlattened.{n}.object_id

Pick

Putting it all together



3. For specific tags warn users on chat application / create a case

`infoleak:automatic-detection="credit-card"`

The image shows a workflow configuration interface on a grid background. On the left is an 'IF :: Tag' node with the following settings:

- Scope: Attribute
- Condition: Is tagged with any (OR)
- Tags: `dark-web:topic="credit-card"`, `infoleak:analyst-detection="credit-card"`, and `infoleak:automatic-detection="credit-card"`
- Galaxy Clusters: Select Some Options

On the right is a 'Webhook' node with the following settings:

- Allow to perform custom callbacks to the provided URL
- Jinja URL: `https://enga9obul9m7l.x.pipedream.net/case-1`
- Content type: application/json
- HTTP Request Method: POST
- Self-signed certificates: Deny self-signed certificates
- Jinja Payload (leave empty for roaming data):

```
{
  "title": "onions to review",
  "event_title": "{{Event.info}}",
}
```
- Jinja Headers: Authorization: foobar

Blue arrows indicate connections: one from the 'Tags' section of the 'IF' node to the 'Webhook' node, and another from the 'infoleak:automatic-detection="credit-card"' tag in the 'IF' node to the 'infoleak:automatic-detection="credit-card"' text box at the top of the slide.

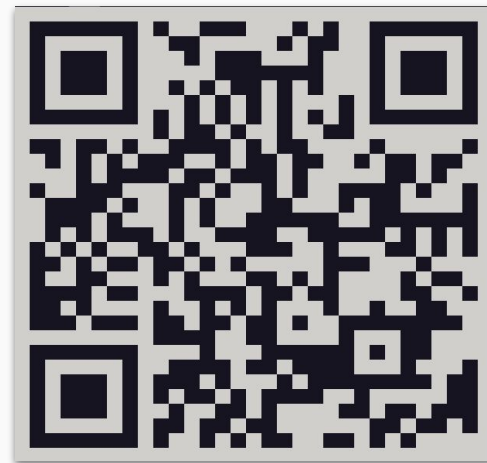
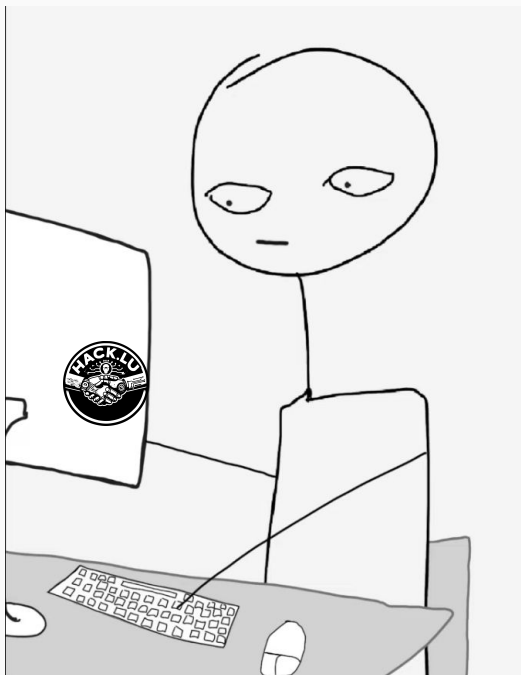
The way forward - How better handle recursion

1. Show warning that this workflow might cause a recursion
2. Triggerless workflows - Executed manually
 - Manually by an analyst (similar to publishing)
 - *Manually* by another workflow
3. Scheduled workflows - Time-based
 - Need to define how to feed data into the workflow (e.g. newly modified events)



Thank you!

misp-module



- All video game icons are sourced from SteamDB or Google Images and are the property of their respective owners.
- Font Awesome Free 6.6.0 by @fontawesome - <https://fontawesome.com> License - <https://fontawesome.com/license/free> Copyright 2024 Fonticons, Inc.
- "Doing the plan" from Digitally Baffled - <https://www.youtube.com/watch?v=xlmh4aGe3ok>

Conclusion