In Curation We Trust: Generating Contextual & Actionable Threat Intelligence

Michel Coene
Robert Nixon

2022-09-30
TLP:White

Michel Coene — **Robert Nixon**

Content

What we will dive into today

Slides 4 - 8	Problem Statement & Examples
Slides 9 - 17	The Curation Procedure… & More
Slides 18 - 19	Lessons Learned & Roadmap
Q&A	

Threat Intelligence Platform (TIP)

What is MISP?

MISP is an open-source threat intelligence and sharing platform.

Community project and co-financed by the European Union

Used by many organizations across the world to share threat related data

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

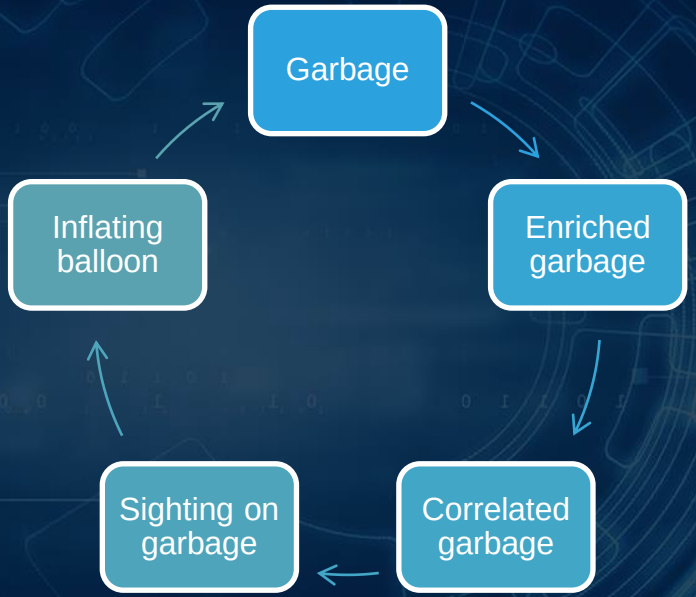
The problem

What everyone has ~~done~~ seen before, at least once

Indicator: 8.8.8.8

IDS: Enabled

SOC:



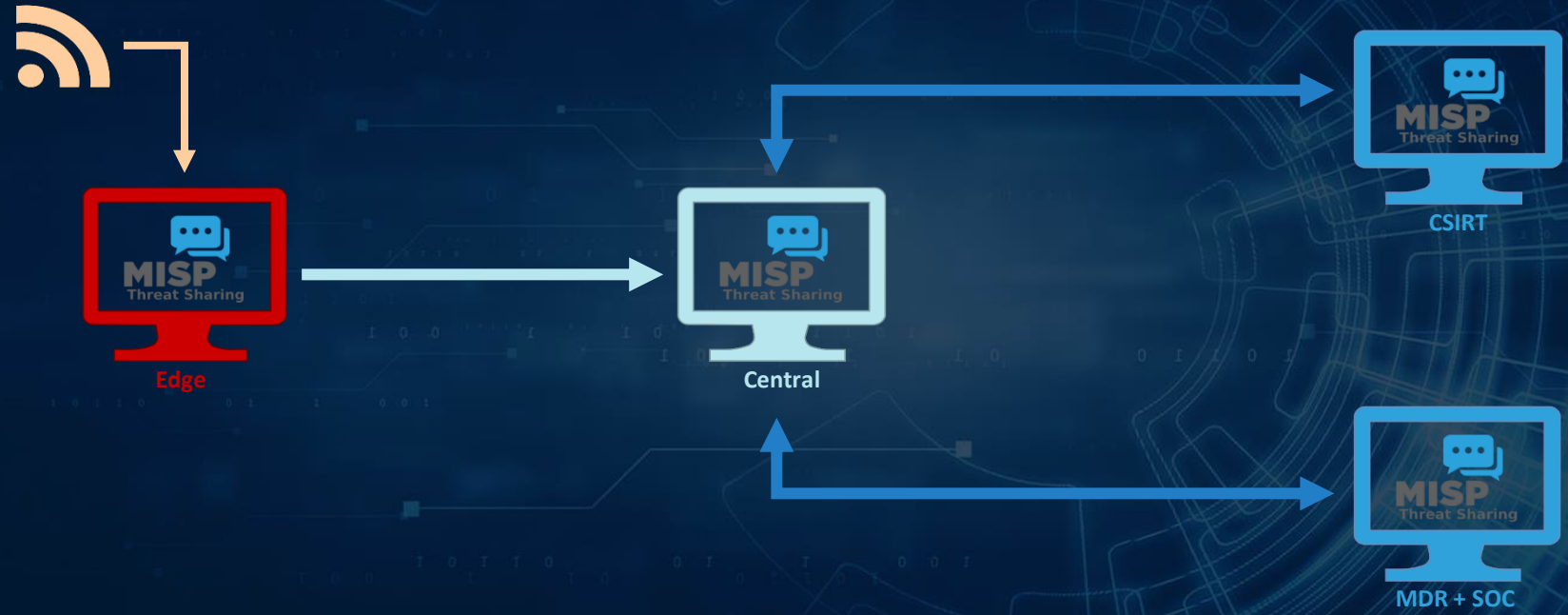
Threat Intelligence

Consuming & producing

NVISO MDR Managed Detect & Respond	NVISO CSIRT Incident Response Team	NVISO CTI Cyber Threat Intelligence
• **TI consumer** • **TI producer** • SOC monitoring of our clients • Anonymized threat data is fed back in the MDR MISP instance for future correlation • Threat hunting	• **TI consumer** • **TI producer** • Incident Response cases • Malware Analysis • Compromise Assessments	• **TI consumer** • **TI producer** • Threat intelligence integrations • TI Monitoring (Creds, Data Leakage) • Threat Intel Feeds • Tailored threat briefings • Threat landscape reports • Threat Intel based Red Teaming (TIBER) • Vulnerability intelligence

The architecture

The first step in an attempt to solve the problem



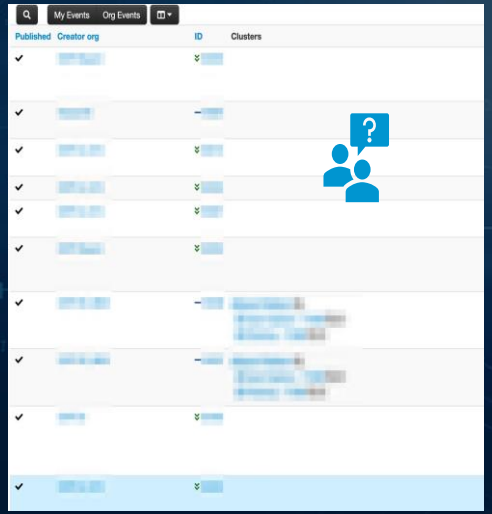
Problem exemplars

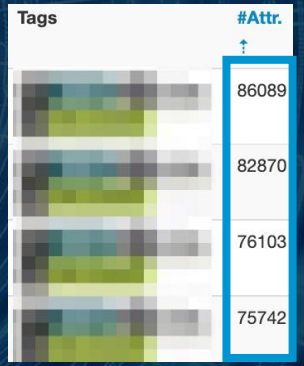
Recipe for sub-optimal detection

Potential false positives

Lack of contextualisation or inconsistencies

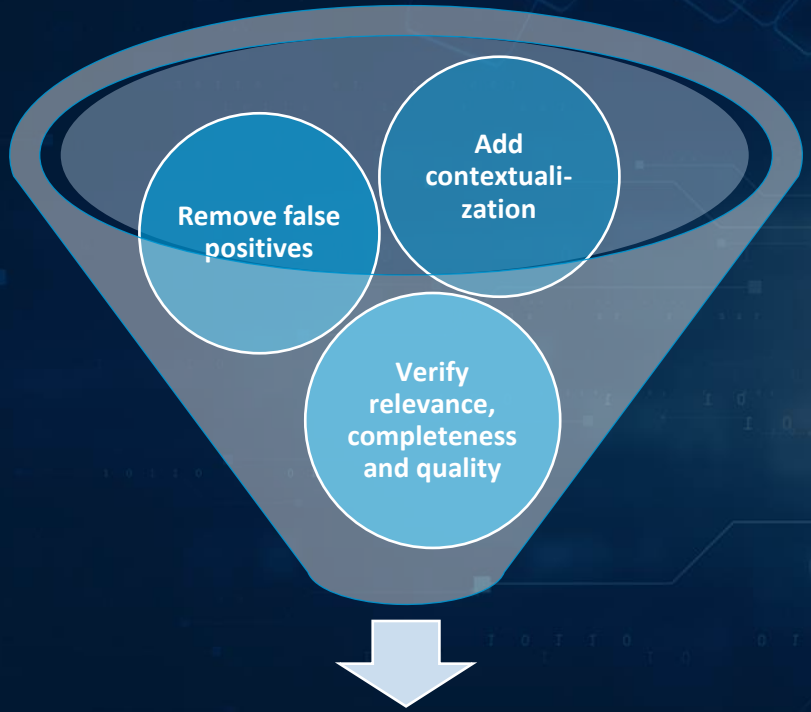
Actionable?





The curation procedure

In practical terms, what do we do?



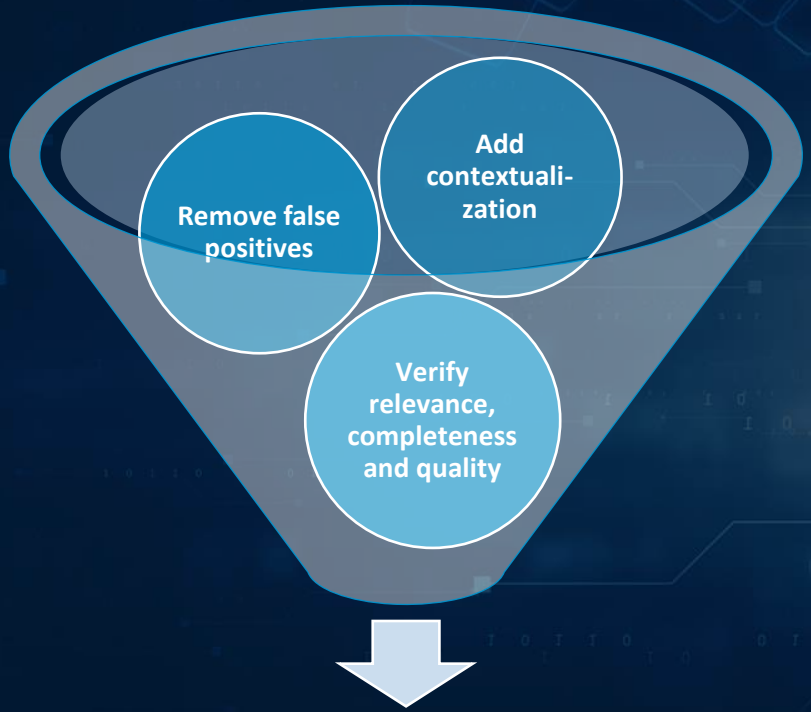
Remove **false positives**
- MISP warning lists
- Custom warning lists
- Analyst judgement

Add **contextualization**
- Mandatory TLP tags
- Intel source
- Relations, comments and objects
- Target info, threat actor, sectors, MITRE ATT&CK tags, ...

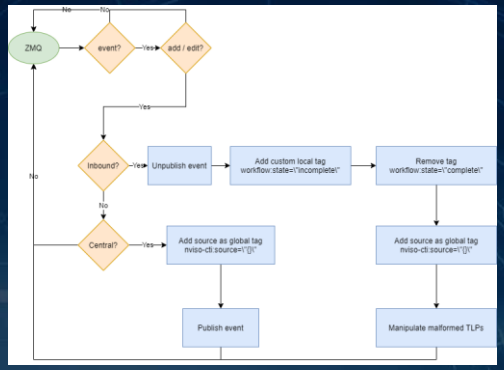
Verify **relevance**, completeness and **quality**
- "Useful"
- Sanity check
- If this alerts, is there enough context?

An attempt to solve the problem

Curation procedure



Threat Intelligence




```python
class nviso_curate:
    '''
    Class to curate NVISO events
    Curation depends on the server we're being executed

    :param logger: logger object
    :param custom_tag: Add this tag to events
    :param remove_tag: Remove this tag from events

    '''

    def __init__(self, logger, custom_tag, remove_tag):
        self.misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert,
        self.custom_tag = custom_tag
        self.logger = logger
        self.remove_tag = remove_tag
        self.source_tag = "nviso-cti:source=\"{}\""
```

```python
# Remove tag "complete"
if self.remove_tag:
    result_tag = self.misp.untag(uuid, self.remove_tag)
    self.logger.debug("Untag event {} - {} {}".format(uuid, misp_event.info, self.remove_tag))
```

ID ↑	Name	Version	Description	Category
145	List of known Limelight CDN IPs	1	List of known Limelight CDN IPs	False positive
144	NITRO URL False Positives	39	False Positive URLs as observed by the NVISO Intelligence and Threat Response Operations.	False positive
143	NITRO Hashes False Positives	41	False Positive Hashes as observed by the NVISO Intelligence and Threat Response Operations.	False positive
142	NITRO Domain False Positives	39	False Positive Domains as observed by the NVISO Intelligence and Threat Response Operations.	False positive
140	NITRO Registry False Positive	39	False Positive Registry Keys as observed by the NVISO Intelligence and Threat Response Operations.	False positive
139	List of known Azure IPs	2	Azure data centers, edge nodes etc.	False positive
136	NVISO False Positive List	6	Indicators that are found to be false positives by the CTI team	False positive

```python
elif tag.name.strip() == "TLP:White" or tag.name.strip() == "TLP: White"  or tag.name.strip() == "TLP:WHI
    self.misp.untag(uuid, tag.id)
    result_tag = self.misp.tag(uuid, "tlp:white")
```

```python
# Add source of this event
if include_source:
    servername = self.get_server(int(server))
    source_tag = self.source_tag.format(servername)
```

Automated Curation

Automation is key!

Edge

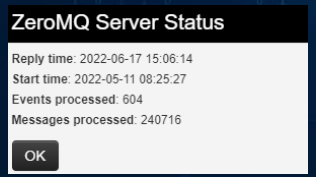
ZMQ → Unpublish → Workflow tags → Source → TLP 2.0?

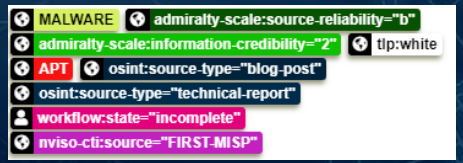
Subscribe

“Incomplete”

Who?

Sanitize





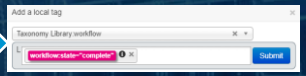
Manual Curation

Manual still comes into play

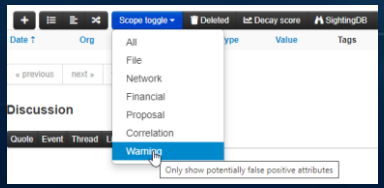
Edge

Central

Workflow → False Positives → Quality & Completeness → Context → Relevant

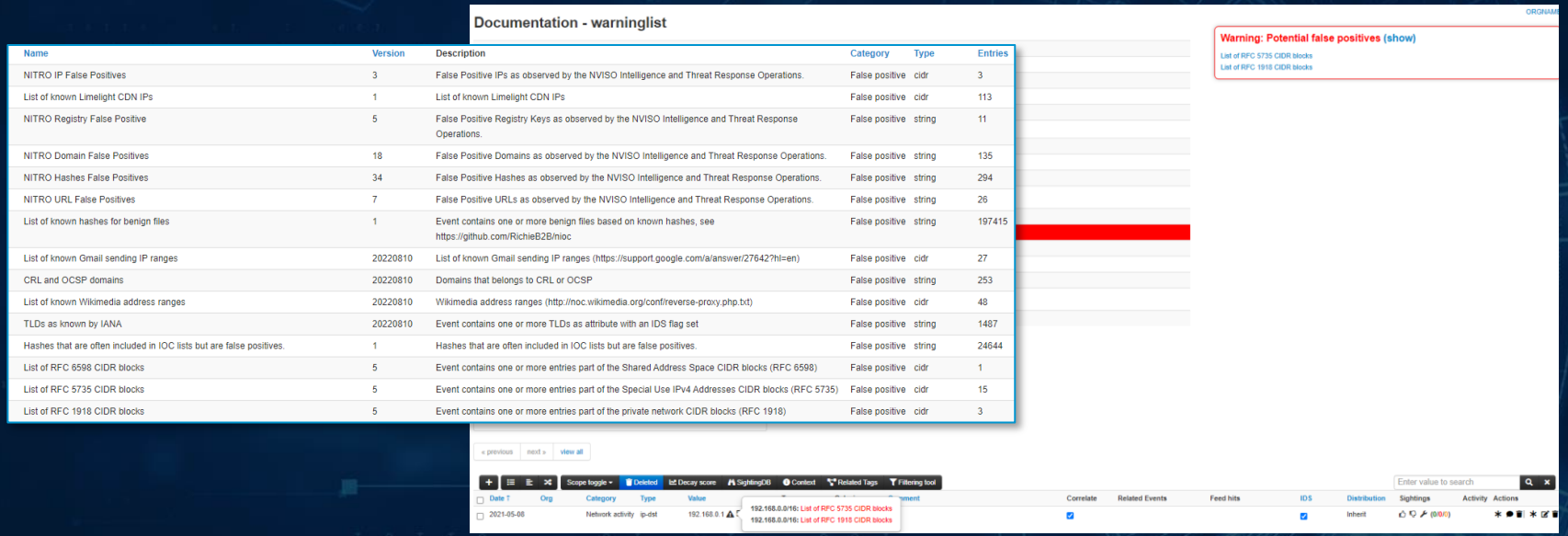


Unpublished | Warninglists | Target info | Usefulness



MISP Warninglists

Shareable lists of potential false positives



Documentation - warninglist

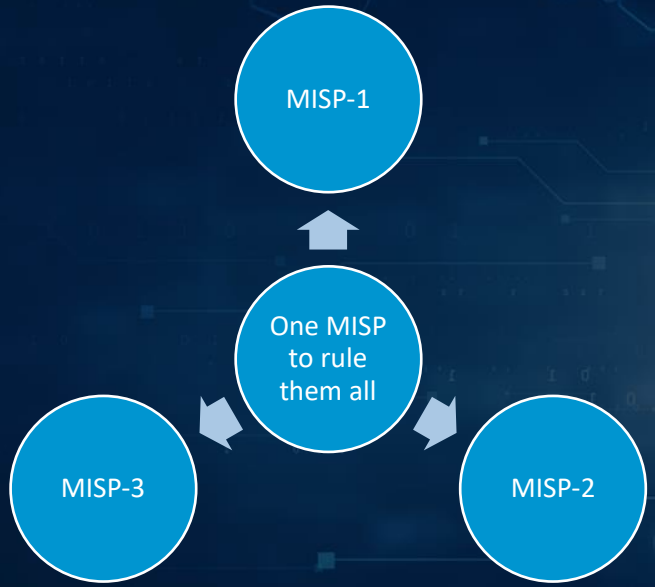
Name	Version	Description	Category	Type	Entries
NITRO IP False Positives	3	False Positive IPs as observed by the NVISO Intelligence and Threat Response Operations.	False positive	cidr	3
List of known Limelight CDN IPs	1	List of known Limelight CDN IPs	False positive	cidr	113
NITRO Registry False Positive	5	False Positive Registry Keys as observed by the NVISO Intelligence and Threat Response Operations.	False positive	string	11
NITRO Domain False Positives	18	False Positive Domains as observed by the NVISO Intelligence and Threat Response Operations.	False positive	string	135
NITRO Hashes False Positives	34	False Positive Hashes as observed by the NVISO Intelligence and Threat Response Operations.	False positive	string	294
NITRO URL False Positives	7	False Positive URLs as observed by the NVISO Intelligence and Threat Response Operations.	False positive	string	26
List of known hashes for benign files	1	Event contains one or more benign files based on known hashes, see https://github.com/RichieB2B/nioc	False positive	string	197415
List of known Gmail sending IP ranges	20220810	List of known Gmail sending IP ranges (https://support.google.com/a/answer/27642?hl=en)	False positive	cidr	27
CRL and OCSP domains	20220810	Domains that belongs to CRL or OCSP	False positive	string	253
List of known Wikimedia address ranges	20220810	Wikimedia address ranges (http://noc.wikimedia.org/conf/reverse-proxy.php.txt)	False positive	cidr	48
TLDs as known by IANA	20220810	Event contains one or more TLDs as attribute with an IDS flag set	False positive	string	1487
Hashes that are often included in IOC lists but are false positives.	1	Hashes that are often included in IOC lists but are false positives.	False positive	string	24644
List of RFC 6598 CIDR blocks	5	Event contains one or more entries part of the Shared Address Space CIDR blocks (RFC 6598)	False positive	cidr	1
List of RFC 5735 CIDR blocks	5	Event contains one or more entries part of the Special Use IPv4 Addresses CIDR blocks (RFC 5735)	False positive	cidr	15
List of RFC 1918 CIDR blocks	5	Event contains one or more entries part of the private network CIDR blocks (RFC 1918)	False positive	cidr	3

Source: https://www.circl.lu/doc/misp/warninglists/

https://github.com/MISP/misp-warninglists

No need repeating

"Offender list" and blocklist



Synchronise offender lists between MISP servers

Organisation Blocklists

« previous | next »

Id	Organisation name	UUID	Created ↑	Comment
[redacted]	[redacted]	[redacted]	2022-05-09 18:33:59	Very low quality, extremely large events with very high amount of FP's
[redacted]	[redacted]	[redacted]	2022-04-05 09:54:08	Generic sandbox output, non-filtered, nonsensical
[redacted]	[redacted]	[redacted]	2021-10-13 08:31:00	Low quality intel, no attributes marked or markable as IDS true
[redacted]		[redacted]	2021-09-22 08:48:29	
[redacted]	[redacted]	[redacted]	2021-07-29 14:39:57	Lots of low quality cuckoo analysis events.
[redacted]	[redacted]	[redacted]	2021-05-12 10:42:53	Low quality
[redacted]	[redacted]	[redacted]	2021-04-02 11:57:14	Scanner / Source IPs > 1000 hits, low value

```
for uuid in diff_source_blocklist_uuids:
    payload = json.dumps({"returnFormat": "json", "uuid": uuid})
    search_results = requests.request("POST", search_dest_url, headers=dest_headers, data=payload, verify=False)
    if len(search_results.json()['response']) != 0:
        try:
            delete_response = requests.request("DELETE", delete_dest_url + uuid, headers=dest_headers, verify=False)
            delete_response.raise_for_status()
            deleted_count += 1
        except requests.exceptions.HTTPError as err:
            print(err)
```

Statistics

What have we seen so far?

3,492 events

1,894,155 attributes

16 blocklisted organisations

Other scripts to complement our curation

False positives

- Remove *or* tag NSRL matches – Uses Hashlookup web service hosted by CIRCL
- Sync custom warninglists with NVISO NITRO MDR service

Relevant indicators

- Deactivate indicators after a grace period - cronjob to turn off IDS flag at a certain age
- Advanced decaying of indicators, can use Decaying Models in MISP

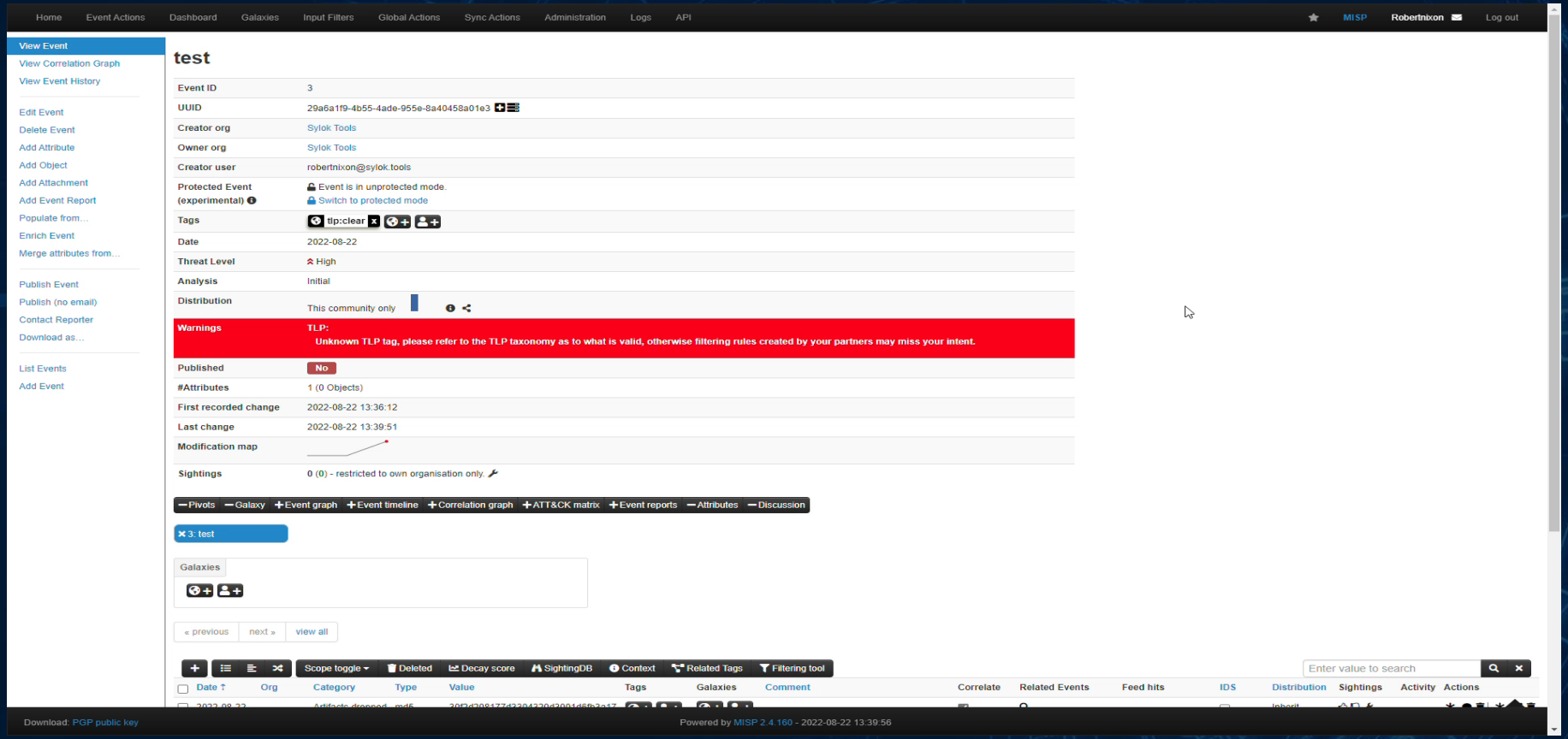
Scrape web sources

- Collect OSINT (RSS Feeds or Manually via URL submission)
- MISP reports generated automatically (html-to-markdown, supported via mermaid with IoC extraction and tagging!)
- https://www.misp-project.org/2022/08/08/MISP-scraper.html/

Bulk delete events

- Events with non-relevant information
- You need a backup plan

Workflows in MISP



Lessons Learned

Key components to make this work

Tooling

- **Customisation is key**
- **Automate as much as possible**
- **Extend what is available**

- ZMQ and Python
  - Some conflicts here with the new Workflow functionality
- Platform features
- Taxonomies (workflow tags)
- Galaxies and clusters

Documentation

- **Server architecture**
- **MISP synchronization data flows**

- There is a limit to what you can automate
- Operating procedures for analysts
- Multiple analysts – but same procedure

Communication

- **Involve stakeholders at the appropriate time**
- **Gather and validate your Primary Intelligence Requirement (PIRs)**
- **Let TI consumers signal the quality of TI**

- Rinse and repeat

Future State

Roadmap

Integrate MISP workflows (New MISP feat.)

- Shareable Workflow blueprints, there is a unique Github repo to share blueprints!
- Create new modules for Workflows
- Implement the new Periodic Notifications functionality

Contribute back to community

- Event proposals
- Sightings
- *Resources*
- *Mature processes*

"Announcements"

- Create bot (Slack, Teams, …) that alert when new events are in (Great place for a webhook using the new Workflows!)

Open source scripts

- Generalise code for wider use
- https://github.com/NVISOsecurity/nviso-cti


nviso
THANK YOU!
Q&A
Michel Coene
Robert Nixon
threatintel@nviso.eu
https://github.com/NVISOsecurity/nviso-cti
2022-09-30
TLP:White