



Curating CTI for an MDR service

MISP Summit 0x06

www.nviso.eu

About NVISO?

Introduction to NVISO



Our Company

NVISO is a pure play **Cyber Security consulting firm** of 90+ specialized security experts and founded in 2013.

Initially founded in **Belgium**, we opened offices in **Germany** (Frankfurt & Munich) in 2019!

Our mission is to **safeguard the foundations of European society from cyber attacks**.



Our DNA

Pride: we are proud of who we are and what we do.

We care: we care about our customers and people.

Break barriers: We challenge the status quo by continuous innovation.


No BS: We keep our promises and don't fool around.



Our Research

We invest 10% of our annual revenue in research of new security techniques and the development of new solutions.

Follow us on :

 @NVISOsecurity and @NVISO_Labs

 blog.nviso.be/



Our Services

We have a **strong track record** providing information and cyber security services to the **Financial Services, Government & Defense** and **Technology** sector. NVISO can **support you throughout the entire cyber security incident lifecycle**.

MDR, CSIRT, CTI ...



NVISO MDR
Managed Detect & Respond

- TI consumer
- TI producer
- SOC monitoring of our clients
- Anonymized threat data is fed back in the MDR MISP and intel events.

NVISO CSIRT
Incident Response Team

- TI consumer
- TI producer
- Incident response cases
- Malware analysis

NVISO CTI
Cyber Threat Intelligence

- TI consumer
- TI producer
- Threat intelligence integration
- Feeds
- Tailored threat briefings
- Threat landscape reports
- Adversary emulation plans
- Vulnerability intelligence



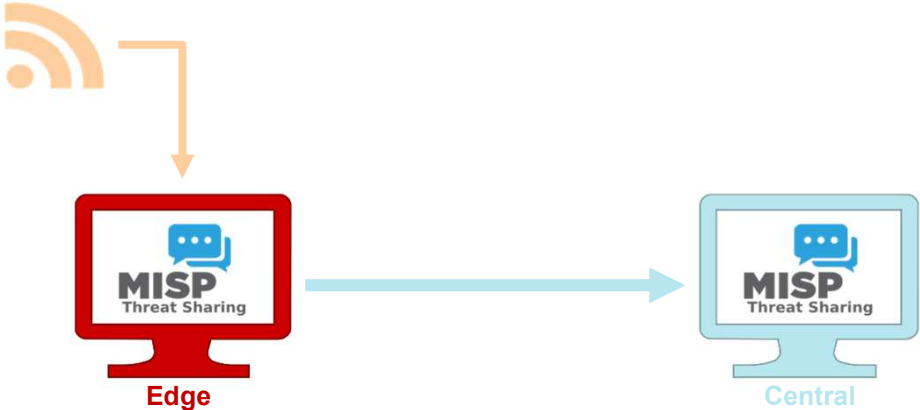
NVISO MISP setup



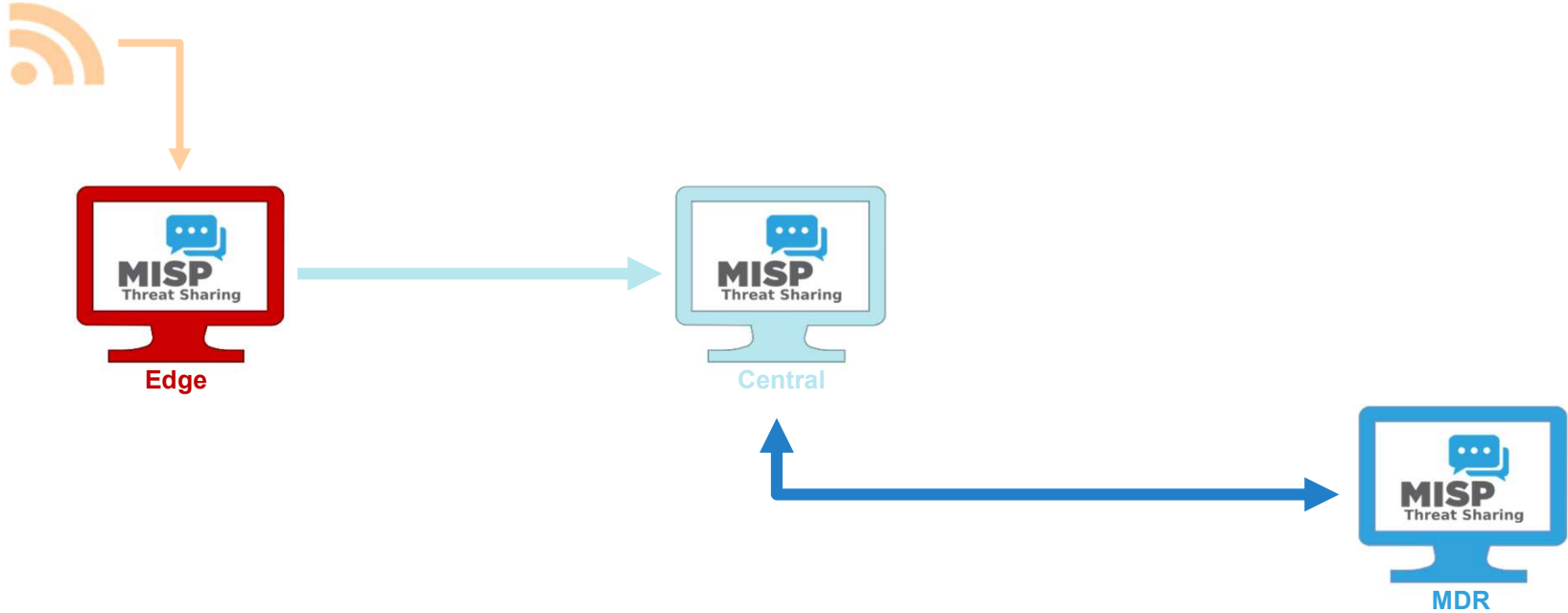
NVISO MISP setup



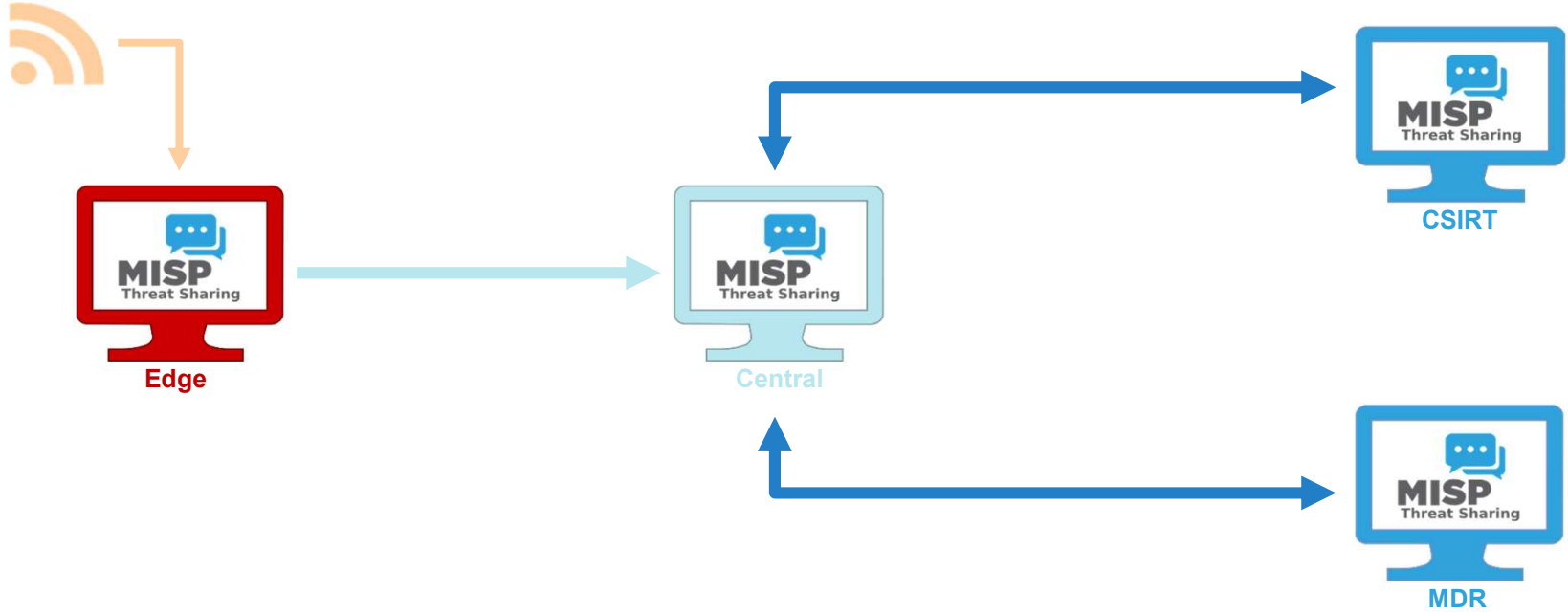
NVISO MISP setup



NVISO MISP setup



NVISO MISP setup

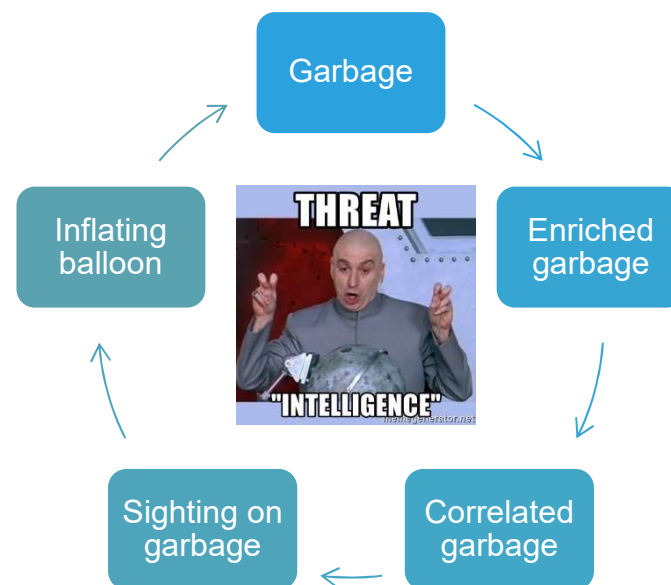


Everyone needs good threat intelligence

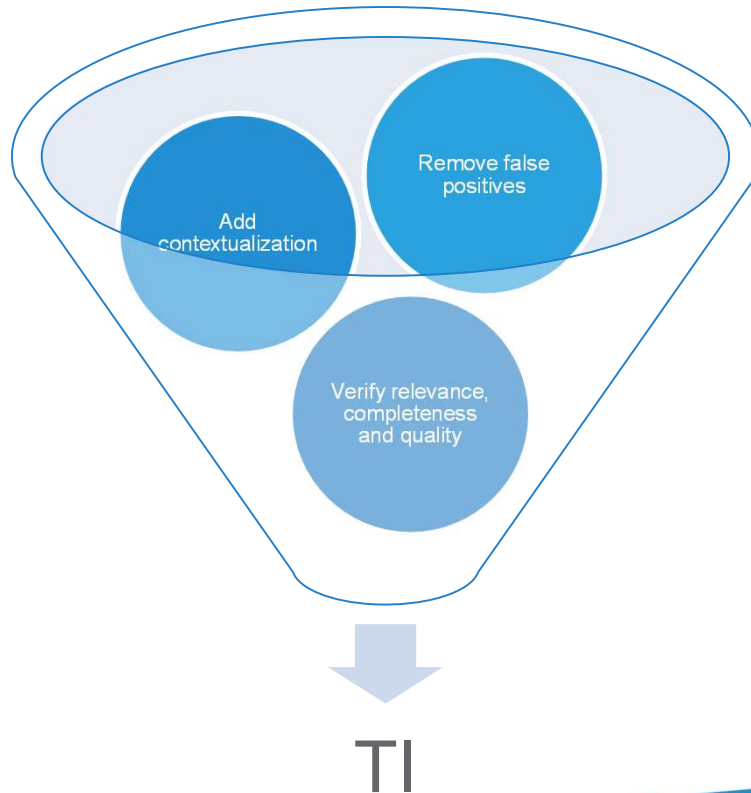


- In our case, not having good CTI means

Financial loss	Reputation loss	More reputation loss	Alert fatigue
<ul style="list-style-type: none">• MDR and CSIRT are searching for ghosts	<ul style="list-style-type: none">• We have a threat report on 8.8.8.8	<ul style="list-style-type: none">• Limited resources• We were so busy with FPs we missed the real campaigns	<ul style="list-style-type: none">• Time wasted on non-productive activities• Analysts start doubting the data coming from CTI



Curation procedure



- Remove **false positives**
 - MISP warninglists
 - Analyst judgement
- Add **contextualization**
 - Mandatory TLP tags
 - Intel source
 - Relations between attributes
 - Comments and objects
 - Target info, threat actor, sectors
- Verify **relevance**, completeness and **quality**
 - "Useful"
 - Sanity check

NVISO curation procedure (1)

The automatic (easy) part

ZMQ
• Subscribe to events



Unpublish



Workflow
• Set to incomplete



Source
• Who provided us this information?



TLP
• Sanitize different flavors

- Publish-subscribe model
- Real-time integration
- Available as a plugin
- Python examples available

```
if topic == 'misp_json_event':  
    payload = json.loads(message[len(topic)+1:])  
    action = payload["action"]  
    #self.logger.debug("ZMQ temp topic:{} action:{} payload:{}".format(topic, action, payload))  
    if action == "add_from_connected_server" or action == "edit_from_connected_server":  
        try:  
            result = nviso_curate.inbound_update(payload["Event"], payload["Server"])  
        except:  
            self.logger.critical("Exceptional error in ZMQ. Maybe missing event or server key?")  
    else:  
        self.logger.debug("Skip ZMQ action")
```



NVISO curation procedure (1)

The automatic (easy) part

ZMQ
• Subscribe to events



Unpublish



Workflow
• Set to incomplete



Source
• Who provided us this information?



TLP
• Sanitize different flavors

```
result_unpublish = self.misp.update_event(misp_event)
self.logger.debug("Unpublish event {} - {}".format(uuid, misp_event.info))
```



NVISO curation procedure (1)

The automatic (easy) part

ZMQ
• Subscribe to events



Unpublish



Workflow
• Set to incomplete



Source
• Who provided us this information?



TLP
• Sanitize different flavors

workflow



workflow namespace available in JSON format at [this location](#). The JSON format can be freely reused in your application or automatically enabled in [MISP taxonomy](#).

```
curator = nviso_curate(logger=subscriber.logger, custom_tag="workflow:state=\"incomplete\"", remove_tag="workflow:state=\"complete\"")
```

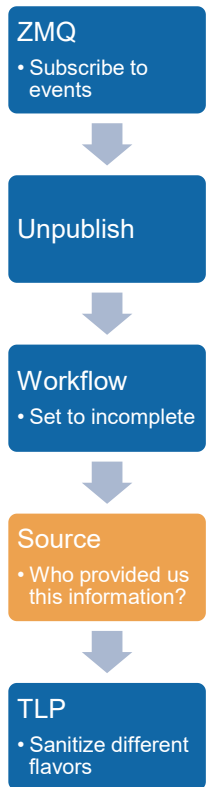
```
result_tag = self.misp.untag(uuid, self.remove_tag)  
self.logger.debug("Untag event {} - {} {}".format(uuid, misp_event.info, self.remove_tag))
```

```
# Add custom tag "incomplete"  
result_tag = self.misp.tag(uuid, self.custom_tag, local_tag)  
self.logger.debug("Tag event {} - {} with {}".format(uuid, misp_event.info, self.custom_tag))
```



NVISO curation procedure (1)

The automatic (easy) part

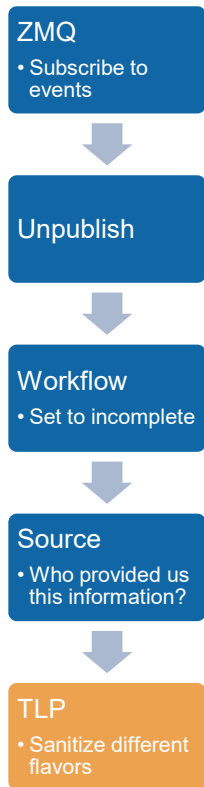


```
if action == "add_from_connected_server" or action == "edit_from_connected_server":  
    servername = self.get_server(int(server))  
    source_tag = self.source_tag.format(servername)  
    try:  
        result_tag = self.misp.tag(uuid, source_tag, False)
```



NVISO curation procedure (1)

The automatic (easy) part

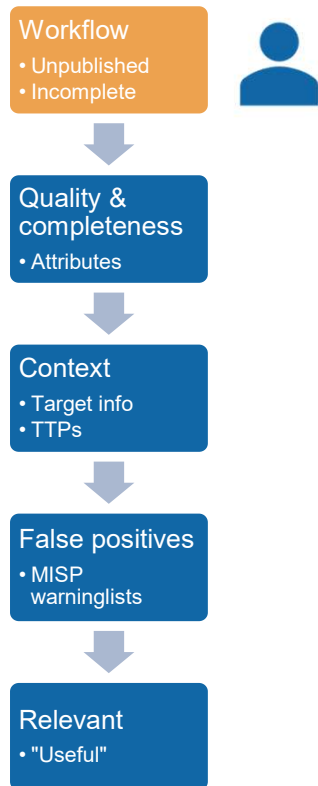


```
if tag.name.strip() == "TLP:Green" or tag.name.strip() == "TLP: Green" or tag.name.strip() == "TLP:GREEN" or tag.name.strip() == "Threat tlp:Green":  
    self.misp.untag(uuid, tag.id)  
    result_tag = self.misp.tag(uuid, "tlp:green")
```



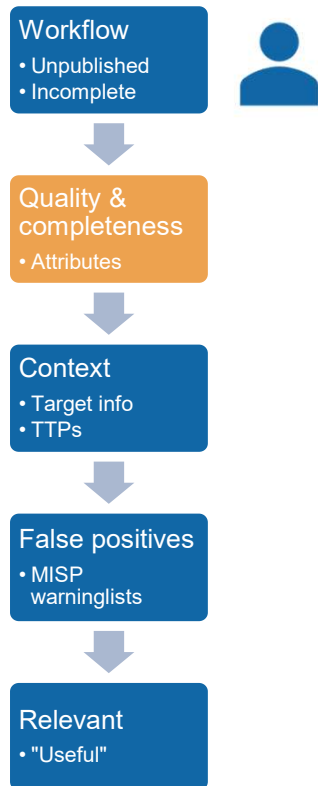
NVISO curation procedure (2)

The manual (hard) part



NVISO curation procedure (2)

The manual (hard) part

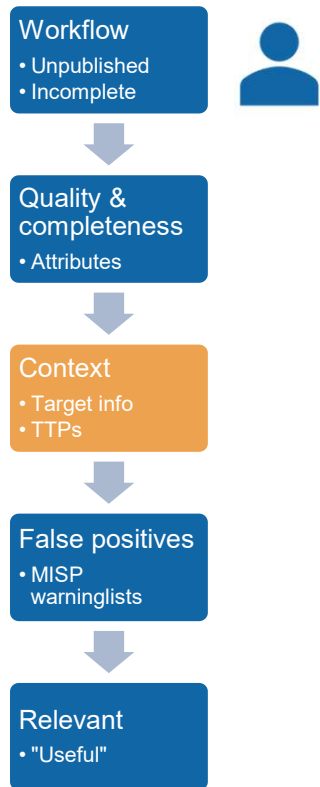


- Uncheck "to_ids" if attribute is too generic
 - Filenames ("start.bat")
 - Destination ("port 80")
 - ...
- Correct type and category
- Merge attributes into objects



NVISO curation procedure (2)

The manual (hard) part



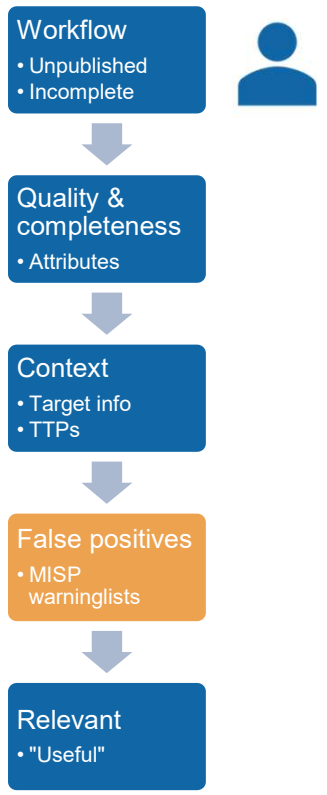
Galaxies

- Attack Pattern Q
 - Phishing - T1566 Q
- Sector Q
 - Bank Q
 - Finance Q



NVISO curation procedure (2)

The manual (hard) part

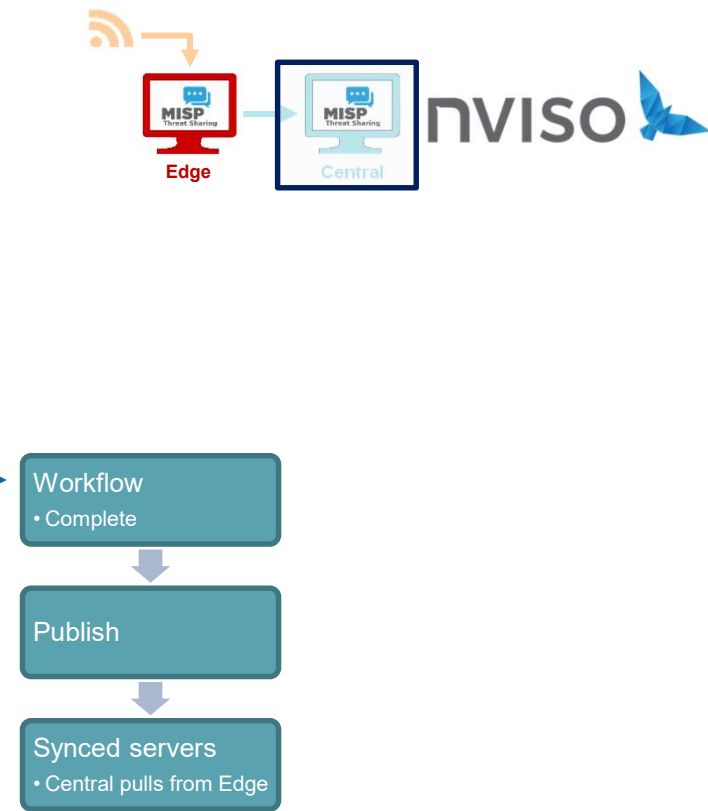
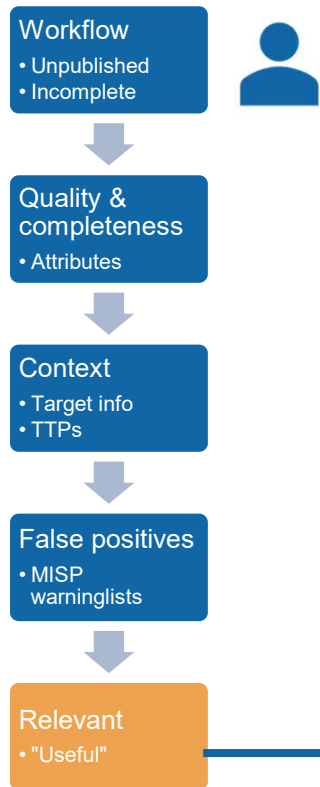


ID	Name
1	List of known Akamai IP ranges
4	List of known domains used by automated malware analysis services & security vendors
5	List of known bank domains
11	Common contact e-mail addresses
12	List of known hashes with common false-positives (based on Florian Roth input list)
13	Valid covid-19 related domains
17	List of known dax30 webpages
19	List of hashes for EICAR test virus
20	List of known hashes for empty files
22	List of known gmail sending IP ranges
23	List of known Googlebot IP ranges



NVISO curation procedure (2)

The manual (hard) part



NVISO curation procedure (3)

Avoid manual work



Blocklist event

- Events with ridiculous amount of attributes
- Not relevant or outdated

Blocklist organization

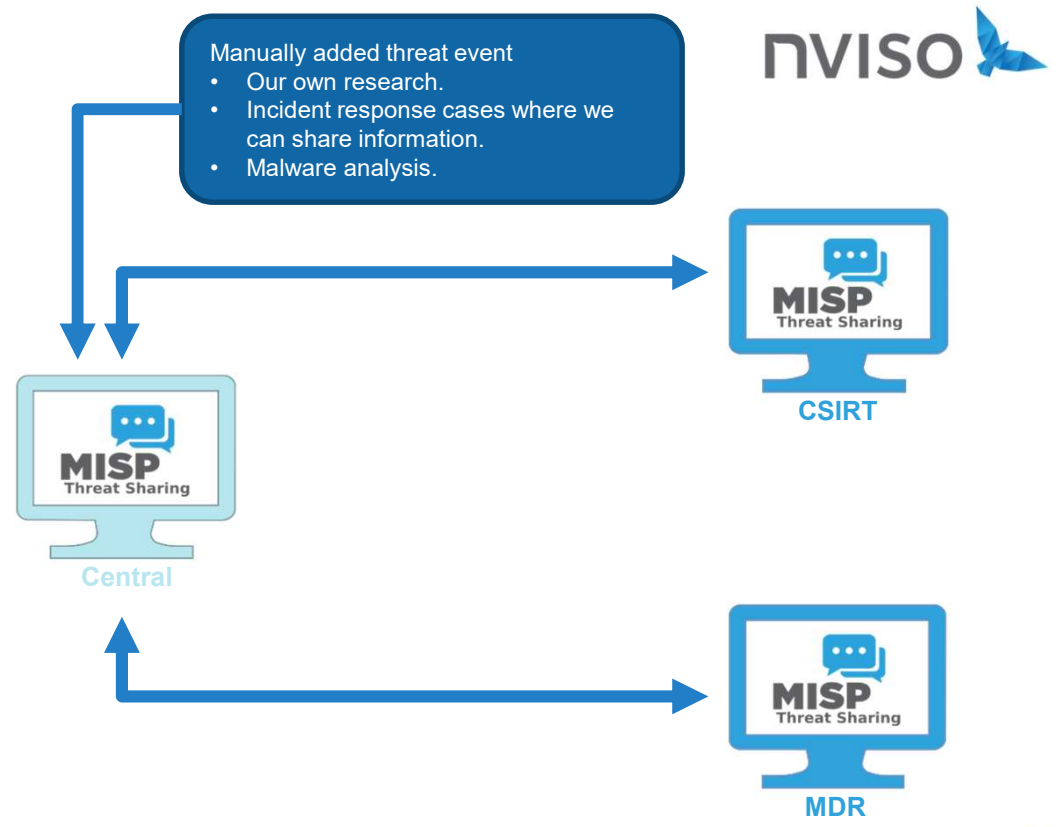
- Low quality events
- Public "sandbox" attributes
- "Internet scanner" IPs
- "Multiple" offenses

Comment
Low quality intel, no attributes marked or markable as IDS true
Lots of low quality cuckoo analysis events.
Low quality
Scanner / Source IPs > 1000 hits, low value

- Documentation in MISP and company documentation platform
 - Future:
 - update documentation when there are changes in MISP
 - inform colleagues via chatbot

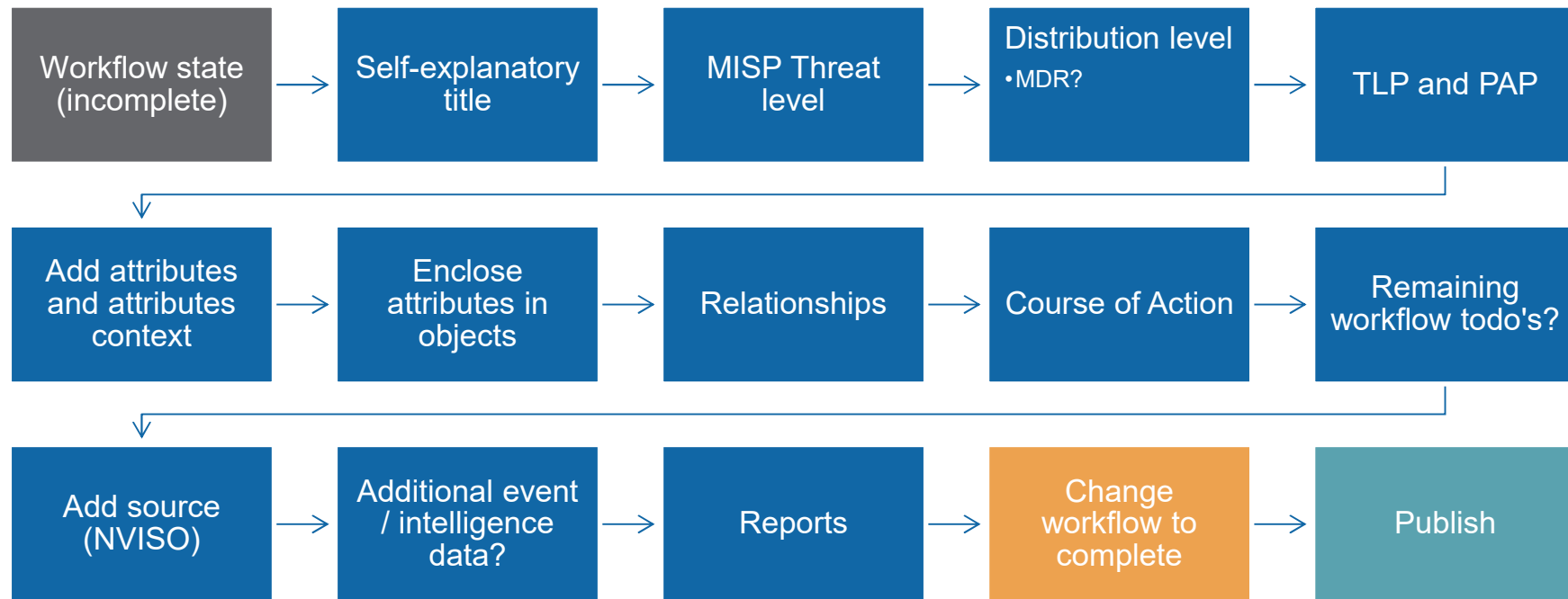
NVISO curation procedure (4)

Push to our Managed Detect and Respond service



NVISO curation procedure (5)

Manually adding threat events



Closing remarks



- Curation procedure
 - Automation
 - Manual process
 - ZMQ is magical
- We divide the load of the manual process between analysts
 - Divide and conquer
 - A curation workflow allows for a consistent approach
 - Favorite the tags you use the most to increase efficiency
 - Use tag collections to save time on a type of intel event such as phishing
- Balancing between different MISP instances
 - "Load" distribution
 - Have a clean set of data
 - Avoid over-sharing

Contact Information



- Koen Van Impe
 - Koen Van Impe kvanimpe@nviso.eu
 - @cudeso
- Bart Parys
 - Bart Parys bparys@nviso.eu
 - @bartblaze
- NVISO
 - <https://www.nviso.eu/>
 - @NVISOsecurity

HACKED ?

CALL

+32 (0)2 588 43 80

NVISO • Security. Research. Risk.

www.nviso.eu

