In Curation We Trust: Generating Contextual & Actionable Threat Intelligence

Michel Coene
Bart Parys
Michel Coene

Bart Parys
Content

What we will dive into today

- Slides 4-7: Problem Statement & Examples
- Slides 8 - 14: The Curation Procedure... & More
- Slides 15-17: Lessons Learned & Roadmap
- Q&A
The problem
What everyone has done seen before, at least once

Indicator: 8.8.8.8
IDS: Enabled

SOC:  

Garbage
Enriched garbage
Correlated garbage
Sighting on garbage
Inflating balloon
## Threat Intelligence

**Consuming & producing**

<table>
<thead>
<tr>
<th>NVISO MDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Detect &amp; Respond</td>
</tr>
<tr>
<td>• TI consumer</td>
</tr>
<tr>
<td>• TI producer</td>
</tr>
<tr>
<td>• SOC monitoring of our clients</td>
</tr>
<tr>
<td>• Anonymized threat data is fed back in the MDR MISP instance for future correlation</td>
</tr>
<tr>
<td>• Threat hunting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NVISO CSIRT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Response Team</td>
</tr>
<tr>
<td>• TI consumer</td>
</tr>
<tr>
<td>• TI producer</td>
</tr>
<tr>
<td>• Incident response cases</td>
</tr>
<tr>
<td>• Malware analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NVISO CTI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Threat Intelligence</td>
</tr>
<tr>
<td>• TI consumer</td>
</tr>
<tr>
<td>• TI producer</td>
</tr>
<tr>
<td>• Threat intelligence integrations</td>
</tr>
<tr>
<td>• Threat Intel Feeds</td>
</tr>
<tr>
<td>• Tailored threat briefings</td>
</tr>
<tr>
<td>• Threat landscape reports</td>
</tr>
<tr>
<td>• Adversary emulation plans</td>
</tr>
<tr>
<td>• Vulnerability intelligence</td>
</tr>
</tbody>
</table>
The architecture

The first step in an attempt to solve the problem

Edge

Central

MDR + SOC

CSIRT
Problem exemplars
Recipe for sub-optimal detection

Potential false positives

Lack of contextualisation or inconsistencies

Actionable?

Warning: Potential false positives (show)
List of known Cloudflare IP ranges
List of known Office 365 URLs
Top 1,000,000 most-used sites from TrendKm
Top 10K most used sites from TrendKm
List of RFC 1918 CER blocks
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

- Add contextualization
  - Remove false positives
  - Verify relevance, completeness, and quality

Threat Intelligence

```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))
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Version</th>
<th>Description</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>145</td>
<td>List of Known CDN IPs</td>
<td>1</td>
<td>List of Known CDN IPs</td>
<td>False positive</td>
</tr>
<tr>
<td>144</td>
<td>NITRO URL False Positives</td>
<td>59</td>
<td>False Positive URL as observed by the NVISO Intelligence and Threat Response Operations.</td>
<td>False positive</td>
</tr>
<tr>
<td>143</td>
<td>NITRO Hosts False Positives</td>
<td>41</td>
<td>False Positive Hosts as observed by the NVISO Intelligence and Threat Response Operations.</td>
<td>False positive</td>
</tr>
<tr>
<td>142</td>
<td>NITRO Domain False Positives</td>
<td>38</td>
<td>False Positive Domains as observed by the NVISO Intelligence and Threat Response Operations.</td>
<td>False positive</td>
</tr>
<tr>
<td>141</td>
<td>NITRO Registry False Positive</td>
<td>38</td>
<td>False Positive Registry Keys as observed by the NVISO Intelligence and Threat Response Operations.</td>
<td>False positive</td>
</tr>
<tr>
<td>139</td>
<td>List of Known Azure IPs</td>
<td>2</td>
<td>Azure data centers, edge nodes etc.</td>
<td>False positive</td>
</tr>
<tr>
<td>138</td>
<td>NIVISO False Positive</td>
<td>6</td>
<td>Indicators that are found to be false positives by the CTT team</td>
<td>False positive</td>
</tr>
</tbody>
</table>

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

# 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!

ZMQ → Unpublish → Workflow → Source → TLP

Subscribe: "Incomplete"
Who?
Sanitize

ZeroMQ Server Status
Reply time: 2022-08-17 16:06:14
Start time: 2022-05-11 08:26:27
Events processed: 004
Messages processed: 240716

www.nviso.eu | 10
Manual Curation

Manual still comes into play

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

Unpublished | Warning lists | Target info | Usefulness

Published  No

Galaxies

- Attack Pattern
  - Standard Non-Application Layer Protocol - T1096
  - Malpedia
  - CHINACHOPPER

- Sector
  - Government, Administration
  - Telecom

www.nviso.eu | 11
No need repeating

“Offender list” and blocklist

One MISP to rule them all

Synchronise offender lists between MISP servers
Statistics

What have we seen so far?

- **3,219 events**
- **2,041,477 attributes**
- **16 blocklisted organisations**
### Other scripts to complement our curation

#### False positives
- Remove *or* tag NSRL matches
- Hashlookup CIRCL

#### Relevant indicators
- Inactivate indicators after a grace period
- Basic decaying of indicators

#### Scrape web sources
- Collect OSINT
- MISP reports

#### Bulk delete events
- Events with non-relevant information
- You need a backup plan
## Lessons Learned

### Key components to make this work

<table>
<thead>
<tr>
<th>Tooling</th>
<th>Documentation</th>
<th>Communication</th>
</tr>
</thead>
</table>
| • Customisation is key  
• Automate as much as possible  
• Extend what is available  
• ZMQ and Python  
• Platform features  
• Taxonomies (workflow)  
• Galaxies and clusters | • Server architecture  
• MISP synchronization data flows  
• There is a limit to what you can automate  
• Operating procedures for analysts  
• Multiple analysts – but same procedure | • Involve stakeholders at the appropriate time  
• Let TI consumers signal the quality of TI  
• Rinse and repeat |
**Future State**

**Roadmap**

**Integrate MISP workflows (New MISP feat.)**
- Shareable models

**Contribute back to community**
- Event proposals
- Sightings
- Resources
- Mature process

“Announcements”
- Create bot (Slack, Teams, …) that alert when new events are in

**Open source scripts**
- Generalise code for wider use
- https://github.com/NVISOsecurity/nviso-cti
THANK YOU!

Michel Coene
Bart Parys

threatintel@nviso.eu