In Curation We Trust: Generating Contextual & Actionable Threat Intelligence

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

Inflating balloon

Sighting on garbage

Correlated garbage

Enriched garbage
### NVISO MDR
**Managed Detect & Respond**
- **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

### 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 integrations
- Threat Intel Feeds
- Tailored threat briefings
- Threat landscape reports
- Adversary emulation plans
- 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?

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 Tranco
- Top 10K most used sites from Tranco
- List of RFC 1918 C2R blocks

Potential false positives in traffic log:
- TLP: WHITE
- TLP: white
- CERT:TLP="white"
- Threat tip:White
- marking:TLPMarking="WHITE"
- TLPs="white"
- :traffic-light-protocol="WHITE"
- tip:white

Tags: amber, green, malware

#Attr.
86089
82870
76103
75742
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

# 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)

# Add source of this event
if include_source:
    servername = self.get_server(int(server))
    source_tag = self.source_tag.format(servername)
    self.misp.tag(uuid, source_tag)
Automated Curation

Automation is key!

ZMQ  Unpublish  Workflow  Source  TLP

Subscribe  "Incomplete"  Who?  Sanitize

ZeroMQ Server Status
Reply time: 2022-08-17 16:08:14
Start time: 2022-05-11 08:25:27
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 - T1095
  - Malpedia
  - CHINACHOPPER
- Sector
  - Finance
  - Government, Administration
  - Telecoms
No need repeating

“Offender list” and blocklist

One MISP to rule them all

MISP-1

MISP-2

MISP-3

Synchronise offender lists between MISP servers
Statistics

What have we seen so far?

3,219 events
2,041,477 attributes
16 blocklisted organisations

- Events: 3219
- Events this month: 114
- Events this month completed curation: 32
- Events this month waiting curation: 81
- Events this month without curation status: 1
- Events this month tip: white: 72
- Events this month tip: green: 27
- Events this month tip: amber: 14

- Attributes: 2,041,477
- Attributes this month: 73,991
- Attributes / event: 534
- Correlations: 39,084,20

- Users: 7
- Organisations: 588
- Blocklisted organisations: 16 (2.72%)
- Local organisations: 1
- Event creator orgs: 163
- Average users / org: 7
- Advanced authkeys: 15

- Disk usage: 39.22%
- Load: 0.43 - 0.16 - 0.12
- Memory: 4032.43 MB free (74.81% used)
### Other scripts to complement our curation

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>False positives</strong></td>
<td>• Remove <em>or</em> tag NSRL matches</td>
</tr>
<tr>
<td></td>
<td>• Hashlookup CIRCL</td>
</tr>
<tr>
<td><strong>Relevant indicators</strong></td>
<td>• Inactivate indicators after a grace period</td>
</tr>
<tr>
<td></td>
<td>• Basic decaying of indicators</td>
</tr>
<tr>
<td><strong>Scrape web sources</strong></td>
<td>• Collect OSINT</td>
</tr>
<tr>
<td></td>
<td>• MISP reports</td>
</tr>
<tr>
<td><strong>Bulk delete events</strong></td>
<td>• Events with non-relevant information</td>
</tr>
<tr>
<td></td>
<td>• You need a backup plan</td>
</tr>
</tbody>
</table>
## 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

www.nviso.eu | 16
THANK YOU!

Michel Coene
Bart Parys

threatintel@nviso.eu