Turning data into actionable intelligence
advanced features in MISP supporting your analysts and tools

@adulau @Iglokska

FIRST Cyber Threat Intelligence Webinar
CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.

We lead the development of the Open Source MISP TISP which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.

CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing.
What is MISP?
Our initial scope
Why is contextualisation important?
What options do we have in MISP?
How can we leverage this in the end?
Open source "TISP" - A TIP with a strong focus on sharing

A tool that collects information from partners, your analysts, your tools, feeds

Normalises, correlates, enriches the data

Allows teams and communities to collaborate

Feeds automated protective tools and analyst tools with the output

A set of tools to manage sharing communities and interconnected MISP servers
There are many different types of users of an information sharing platform like MISP:

- **Malware reversers** willing to share indicators of analysis with respective colleagues.
- **Security analysts** searching, validating and using indicators in operational security.
- **Intelligence analysts** gathering information about specific adversary groups.
- **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
- **Risk analysis teams** willing to know about the new threats, likelihood and occurrences.
- **Fraud analysts** willing to share financial indicators to detect financial frauds.
The initial scope of MISP

- **Extract information** during the analysis process
- Store and **correlate** these datapoints
- **Share** the data with partners
- Focus on technical indicators: IP, domain, hostname, hashes, filename, pattern in file/memory/traffic
- Generate protective signatures out of the data: snort, suricata, OpenIOC
Contextualisation became more and more important as we as a community matured

- **Growth and diversification** of our communities
- Distinguish between information of interest and raw data
- **False-positive** management
- TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
- **Increased data volumes** leads to a need to be able to prioritise

These help with filtering your TI based on your requirements...

...as highlighted by a great talk from Pasquale Stirparo titled *Your Requirements Are Not My Requirements*
Different layers of context

- Context added by analysts / tools
- Data that tells a story
- Encoding analyst knowledge to automatically leverage the above
CONTEXT ADDED BY ANALYSTS / TOOLS
Expressing why data-points matter

- An IP address by itself is barely ever interesting
- We need to tell the recipient / machine why this is relevant
- All data in MISP has a **bare minimum required context**
- We differentiate between **indicators and supporting data**
Broadening the scope of what sort of context we are interested in

- **Who** can receive our data? **What** can they do with it?
- **Data accuracy, source reliability**
- **Why** is this data relevant to us?
- **Who** do we think is behind it, **what tools** were used?
- What sort of **motivations** are we dealing with? Who are the **targets**?
- How can we **block/detect/remediate** the attack?
- What sort of **impact** are we dealing with?
TAGGING AND TAXONOMIES

- Simple labels
- Standardising on vocabularies
- Different organisational/community cultures require different nomenclatures
- Triple tag system - taxonomies
- JSON libraries that can easily be defined without our intervention

<table>
<thead>
<tr>
<th>Tag</th>
<th>Events</th>
<th>Attributes</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>workflow:state=&quot;complete&quot;</td>
<td>11</td>
<td>0</td>
<td>workflow:state=&quot;complete&quot;</td>
</tr>
<tr>
<td>workflow:state=&quot;draft&quot;</td>
<td>0</td>
<td>0</td>
<td>workflow:state=&quot;draft&quot;</td>
</tr>
<tr>
<td>workflow:state=&quot;Incomplete&quot;</td>
<td>55</td>
<td>10</td>
<td>workflow:state=&quot;Incomplete&quot;</td>
</tr>
<tr>
<td>workflow:state=&quot;ongoing&quot;</td>
<td>0</td>
<td>0</td>
<td>workflow:state=&quot;ongoing&quot;</td>
</tr>
</tbody>
</table>
Galaxies

- Taxonomy tags often **non self-explanatory**
  - Example: universal understanding of tlp:green vs APT 28
- For the latter, a single string was ill-suited
- So we needed something new in addition to taxonomies - **Galaxies**
  - Community driven **knowledge-base libraries used as tags**
  - Including descriptions, links, synonyms, meta information, etc.
  - Goal was to keep it **simple and make it reusable**
  - Internally it works the exact same way as taxonomies (stick to JSON)
The emergence of ATT&CK

- Standardising on high-level **TTPs** was a solution to a long list of issues
- Adoption was rapid, tools producing ATT&CK data, familiar interface for users
- A much better take on kill-chain phases in general
- Feeds into our **filtering** and **situational awareness** needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns
The emergence of ATT&CK and similar galaxies

- attck4fraud ¹ by Francesco Bigarella from ING
- Election guidelines ² by NIS Cooperation Group
- AM!TT Misinformation pattern ³ by the misinfosecproject

¹https://www.misp-project.org/galaxy.html#_attck4fraud
²https://www.misp-project.org/galaxy.html#_election_guidelines
³https://github.com/MISP/misp-galaxy/blob/master/clusters/misinfosec-amitt-misinformation-pattern.json
FALSE POSITIVE HANDLING

- Low quality / false positive prone information being shared
- Lead to alert-fatigue
- Exclude organisation xy out of the community?
- FPs are often obvious - **can be encoded**
- **Warninglist system**\(^4\) aims to do that
- Lists of well-known indicators which are often false-positives like RFC1918 networks, ...

\(^4\)https://github.com/MISP/misp-warninglists
DATA THAT TELLS A STORY
Atomic attributes were a great starting point, but lacking in many aspects

**MISP objects** system

- Simple **templating** approach
- Use templating to build more complex structures
- Decouple it from the core, allow users to define their own structures
- MISP should understand the data without knowing the templates
- Massive caveat: **Building blocks have to be MISP attribute types**
- Allow **relationships** to be built between objects

---

5[https://github.com/MISP/misp-objects](https://github.com/MISP/misp-objects)
Supporting specific datamodels
Data shared was **frozen in time**

All we had was a creation/modification timestamp

Improved tooling and willingness allowed us to create a **feedback loop**

Lead to the introduction of the **Sighting system**

Signal the fact of an indicator sighting...

...as well as **when** and **where** it was sighted

Vital component for IoC **lifecycle management**

External **SightingDB** and standard - thanks to Sebastien Tricaud from Devo inc.
Continuous feedback loop (2)

Events

- Sightings
  CIRCL: 2 (2017-03-19 16:17:59)

- Inherit
  (2/0/0)

- No
  Inherit
  (0/0/0)

Tags
- Date: 2016-02-24
- Threat Level: High
- Analysis: Initial
- Distribution: Connected communities
- freetext test

- Sighting Details
  No
  MISP: 2
  CIRCL: 2

Discussion: 4 (2) - restricted to own organisation only.
Continuous feedback loop

- Monitor uptimes of infrastructure
- Make decisions on whether to action on an IoC
Data providers including the timing of the data has allowed us to include it directly in MISP

**First_seen** and **last_seen** data points

Along with a complete integration with the **UI**

Enables the **visualisation** and **adjustment** of indicators timeframes
The various ways of encoding analyst knowledge to automatically leverage our TI
Making use of all this context

- Providing advanced ways of querying data
  - Unified export APIs
  - Incorporating all contextualisation options into API filters
  - Allowing for an on-demand way of excluding potential false positives
  - Allowing users to easily build their own export modules feed their various tools
/attributes/restSearch
{
    "returnFormat": "netfilter",
    "enforceWarninglist": 1,
    "tags": {
        "NOT": [
            "tlp:white",
            "type:OSINT"
        ],
        "OR": [
            "misp-galaxy:threat-actor="Sofacy"",
            "misp-galaxy:sector="Chemical"
        ]
    }
}
Example query to generate ATT&CK heatmaps

/events/restSearch
{
    "returnFormat": "attack",
    "tags": [
        "misp-galaxy:sector="Chemical"
    ],
    "timestamp": "365d"
}
### A Sample Result for the Above Query

<table>
<thead>
<tr>
<th>Initial access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege escalation</th>
<th>Defense evasion</th>
<th>Credential access</th>
<th>Discovery</th>
<th>Lateral movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spearphishing via Service</td>
<td>Command-Line Interface</td>
<td>Login Item</td>
<td>AppOert DLLs</td>
<td>Code Signing</td>
<td>Vault Capture</td>
<td>System Network Configuration Discovery</td>
<td>Distributed Component Object Model</td>
<td>Data from Removable Media</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Communication Through Removable Media</td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>User Execution</td>
<td>Trap</td>
<td>Application Shimming</td>
<td>Rooter</td>
<td>Back History</td>
<td>Process Discovery</td>
<td>Pass the Hash</td>
<td>Man in the Browser</td>
<td>Data Compressed</td>
<td>Custom Command and Control Protocol</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Reversal/Rezumu</td>
<td>System Firmware</td>
<td>Scheduled Task</td>
<td>NTFS File Attributes</td>
<td>Exploitation for Credential Access</td>
<td>Network Share Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data Staged</td>
<td>Automated Exfiltration</td>
<td>Multi-Stage Channels</td>
</tr>
<tr>
<td>Spearphishing Link</td>
<td>Windows Management Instrumentation</td>
<td>LC_LOAD_DLLIB Addition</td>
<td>New Service</td>
<td>Network Share</td>
<td>Delete Force</td>
<td>Account Discovery</td>
<td>Pass the Ticket</td>
<td>Email Collection</td>
<td>Data Encrypted</td>
<td>Uncommonly Used Port</td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>Service Execution</td>
<td>LSASS Driver</td>
<td>Sudo Caching</td>
<td>Process Doppelganger</td>
<td>Password Filter DLL</td>
<td>System Information Discovery</td>
<td>Windows Remote Management</td>
<td>Clipboard Data</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Mulitlayer Encryption</td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>CMSTP</td>
<td>Rcommon</td>
<td>Process Injection</td>
<td>Disabling Security Tools</td>
<td>Two-Factor Authentication</td>
<td>System Network Connections Discovery</td>
<td>Windows Admin Shares</td>
<td>Video Capture</td>
<td>Exfiltration Over Physical Medium</td>
<td>Domain Fronting</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Control Panel Items</td>
<td>Authentication Package</td>
<td>Bypass User Account Control</td>
<td>Timestamp</td>
<td>LLMMRNBTS-NS Polishing</td>
<td>Network Service Scanning</td>
<td>Remote Services</td>
<td>Audio Capture</td>
<td>Data Transfer Size Limits</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Dynamic Data Exchange</td>
<td>Component Firmware</td>
<td>Extra Window Memory Injection</td>
<td>Modify Registry</td>
<td>Credentials in Files</td>
<td>File and Directory Discovery</td>
<td>Taint Shared Content</td>
<td>Data from Network Shared Drive</td>
<td>Connection Proxy</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>Source</td>
<td>Windows Management Instrumentation Event Subscription</td>
<td>Suid and Sgid</td>
<td>Indicator Removal from Tools</td>
<td>Forced Authentication</td>
<td>Security Software Discovery</td>
<td>Application Deployment Software</td>
<td>Data from Local System</td>
<td>Automated Collection</td>
<td>Data Encoding</td>
<td>Data Encoding</td>
</tr>
</tbody>
</table>
Decaying of indicators

- We were still missing a way to use all of these systems in combination to decay indicators.
- Move the decision making from complex filter options to complex decay models.
- The idea is to not modify our data, but to provide an overlay to make decisions on the fly.
- Decay models would take into account various available context:
  - Taxonomies
  - Sightings
  - Type of each indicator
  - Creation date
  - ...
### IMPLEMENTATION IN MISP: Event/view

<table>
<thead>
<tr>
<th>Date</th>
<th>Type</th>
<th>Category</th>
<th>Value</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-09-12</td>
<td>Network activity</td>
<td>p-src</td>
<td>5.5.5.5</td>
<td><img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /></td>
</tr>
<tr>
<td>2019-08-13</td>
<td>Network activity</td>
<td>p-src</td>
<td>8.8.8.8</td>
<td><img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /></td>
</tr>
<tr>
<td>2015-08-13</td>
<td>Network activity</td>
<td>p-src</td>
<td>5.9.9.9</td>
<td><img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /></td>
</tr>
<tr>
<td>2019-08-13</td>
<td>Network activity</td>
<td>p-src</td>
<td>7.7.7.7</td>
<td><img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /></td>
</tr>
<tr>
<td>2015-07-18</td>
<td>Network activity</td>
<td>p-src</td>
<td>6.6.6.6</td>
<td><img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /> <img src="image" alt="Galaxies" /></td>
</tr>
</tbody>
</table>

- **Decay score toggle button**
  - Shows Score for each *Models* associated to the *Attribute* type
Implementation in MISP: Fine Tuning Tool

Create, modify, visualise, perform mapping
Simulate Attributes with different Models
Monitor trends outside of MISP (example: dashboard)
A SMALL DETOUR - COVID-19 MISP
Using the new **built in dashboarding** system of MISP

**Customising MISP** for a specific use-case

We are focusing on four areas of sharing:

- Medical information
- Cyber threats related to / abusing COVID-19
- COVID-19 related disinformation
- Geo-political events related to COVID-19

Low barrier of entry, aiming for wide spread

Already a **massive community**

Register at https://covid-19.iglocska.eu
DASHBOARDING AND SITUATIONAL AWARENESS

Create, modify, visualise, perform mapping
To sum it all up...

- Massive rise in user capabilities
- Growing need for truly actionable threat intel

Lessons learned:
- **Context is king** - Enables better decision making
- **Intelligence and situational awareness** are natural by-products of context
- Don’t lock users into your workflows, build tools that enable theirs
Contact CIRCL
▶ info@circl.lu
▶ https://twitter.com/circl_lu
▶ https://www.circl.lu/

Contact MISPProject
▶ https://github.com/MISP
▶ https://gitter.im/MISP/MISP
▶ https://twitter.com/MISPProject

Join the COVID-19 MISP community
▶ https://covid-19.iglocska.eu