Developing a Threat Intelligence Model and Framework?

How You Can Promote Its Use in MISP and Other TIPs.

MISP Project

12th EU MITRE ATT&CK Community

Who is Who

- Alexandre Dulaunoy[1] (CIRCL, MISP, etc.)
- Christophe Vandeplas[2] (Consultant & Reservist, MISP, Sysdiagnose (EU), etc.)

[1] https://github.com/adulau

[2] https://github.com/cvandeplas

What is a MISP Galaxy?

- MISP Galaxy is a feature in MISP and a MISP standard[3] format to create **contextualization libraries**.
  - There are two main types: **combined list** or **matrix-like list**.
- The first historical matrix-like galaxy was MITRE ATT&CK[4].
- Galaxies contain intelligence that can be **structured** in a matrix-like format. Relationships between models can be created, and implementation such as in MISP allows for the **forking and sharing of information**. This is typically attached to intelligence in threat intelligence platforms to add context.

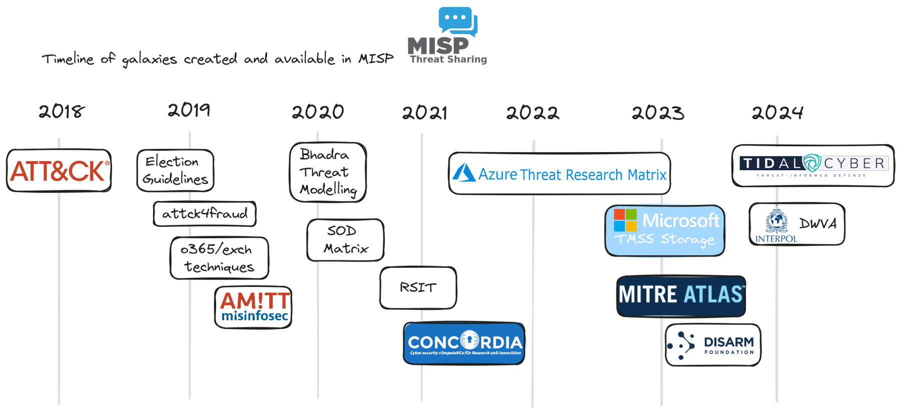
[3] https://www.misp-standard.org/

[4] Presented at the first EU ATT&CK community meeting in Luxembourg

Origins and Evolution

- Seeing the success of the ATT&CK framework in MISP gave rise to a host of matrix-based models:
  - Inflation? We don’t think so. There are **different models** because there are many **different use cases to be represented**.
  - We found this to be good as long as those models are maintained.

MISP GALAXIES OVER TIME



What Leads to Starting New Frameworks?

- New frameworks try to **fill gaps**.
- New ideas in different areas/domains.
- Small vs. large initiatives.
- **Collaboration is not always easy**.
    - Small contributors vs. large organizations.
    - Absence of guidance to contribute.
    - Closed models.
- Research & publication vs. practical use.
- Need for timely new data in a continuously evolving threat landscape.

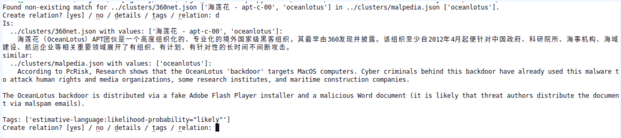
Conversion (or the Dirty Part)

- Understand the topic.
- Understand the users and their use cases.
- Map to Matrix / Kill Chain.
- Handle **various formats**:
  - JSON, XLS, PDF, DOCX, Markdown, CSV, web scraping, Python, etc.
- Reverse engineer the data model.
- Manage UUIDs: existing vs. generating new.
- Handle duplicate values[5]:
  - Interaction with the framework owner.
- Create the conversion script.

[5] In other words, many organizations didn't machine-validate their own model.

Relations (Where Are the Overlaps?)

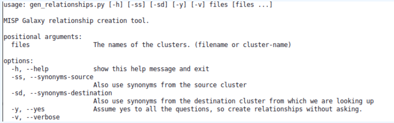
- Example relations: `similar`, `contains`, or lifecycle: `revoked-by`.
- Frameworks might contain internal relations.
- Relations between different frameworks:
  - **Native relationships**
  - **3rd party contributions**
- Create specific tooling to help or partially automate the creation of relations.



```
Found non-existing match for ../clusters/360net.json ['海莲花 - apt-c-00', 'oceanlotus'] in ../clusters/malpedia.json ['oceanlotus'].
Create relation? [yes] / no / details / tags / relation: d
Is:
  ../clusters/360net.json with values: ['海莲花 - apt-c-00', 'oceanlotus']:
    海莲花（OceanLotus）APT团伙是一个高度组织化的、专业化的境外国家级黑客组织，其最早由360发现并披露。该组织至少自2012年4月起便针对中国政府、科研院所、海事机构、海域
建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。
similar:
  ../clusters/malpedia.json with values: ['oceanlotus']:
    According to PcRisk, Research shows that the OceanLotus 'backdoor' targets MacOS computers. Cyber criminals behind this backdoor have already used this malware t
o attack human rights and media organizations, some research institutes, and maritime construction companies.

The OceanLotus backdoor is distributed via a fake Adobe Flash Player installer and a malicious Word document (it is likely that threat authors distribute the documen
t via malspam emails).

Tags: ['estimative-language:likelihood-probability="likely"']
Create relation? [yes] / no / details / tags / relation: 
```



```
usage: gen_relationships.py [-h] [-ss] [-sd] [-y] [-v] files [files ...]

MISP Galaxy relationship creation tool.

positional arguments:
  files                 The names of the clusters. (filename or cluster-name)

options:
  -h, --help            show this help message and exit
  -ss, --synonyms-source
                        Also use synonyms from the source cluster
  -sd, --synonyms-destination
                        Also use synonyms from the destination cluster from which we are looking up
  -y, --yes             Assume yes to all the questions, so create relationships without asking.
  -v, --verbose
```

Maintenance (Anyone on the Line?)

- **Frameworks have a lifecycle** - evolution of the model.
- Know when there is an update.
- **Deprecate, revoke, delete entries**.
- Change of UUID (UUIDv4 or UUIDv5) / value - may impact UUID.
  - Breaks relationships with UUIDs.
- Conversion script breaks.
- Keeping contributed relationships.

Opportunities (How Can It Help Me?)

- Structure new models: **Understand existing ones to identify gaps** and raise feature requests or pull requests on `misp-galaxy`.
- MISP Galaxy:
  - Open standard.
  - Data is CC0 - **reusable in any software**.
- Extend frameworks: Use one framework as a core library and build additional layers on top.
- Marketing and promotion: The more tools that use it, the **more widely the framework is adopted**.

Way Ahead for MISP Galaxy

- Add **more** frameworks and taxonomies.
- **Better mark revoked and deprecated** clusters in the galaxy.
- Automate the ingestion of updated third-party threat matrices.
- Improve the library for managing conversions to MISP Galaxy.

10 Golden Rules for Framework Creators (Technical)

- 1. Use a machine-readable format (JSON is preferred).
- 2. Ensure fixed and unique UUIDs.
- 3. Revoke entries, do not delete them.
- 4. Relate to UUIDs with relationship types.
- 5. Allow outbound relationships.

10 Golden Rules for Framework Creators (Community)

- 1. Publish and communicate.
- 2. Update regularly.
- 3. Encourage third-party contributions.
- 4. Expand existing frameworks.
- 5. Collaborate with other framework creators.

Get in touch if you have any questions

- MISP galaxy website https://www.misp-galaxy.org/
- Contact MISPProject
  - https://github.com/MISP
  - https://gitter.im/MISP/MISP
  - https://twitter.com/MISPProject