

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



WHAT IS A MISP GALAXY?

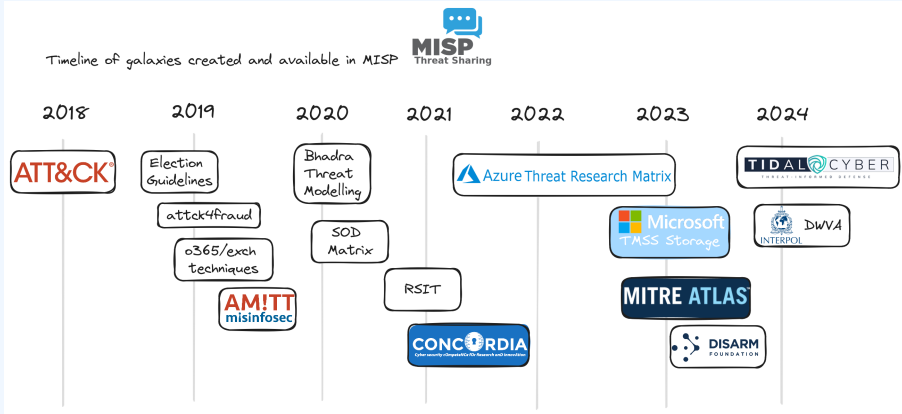
- MISP Galaxy is a feature in MISP and a MISP standard¹ format to create **contextualization libraries**.
 - ▶ There are two main types: **combined list** or **matrix-like list**.
- The first historical matrix-like galaxy was MITRE ATT&CK².
- Galaxies contain intelligence that can be **structured** in 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.

¹<https://www.misp-standard.org/>

²Presented at the first EU ATT&CK community meeting in Luxembourg

- 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 values³:
 - ▶ Interaction with the framework owner.
- Create the conversion script.

³In 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、专业化的境外国家背景客组织，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 to 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 document via malware emails).
Tags: l'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.

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>