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?

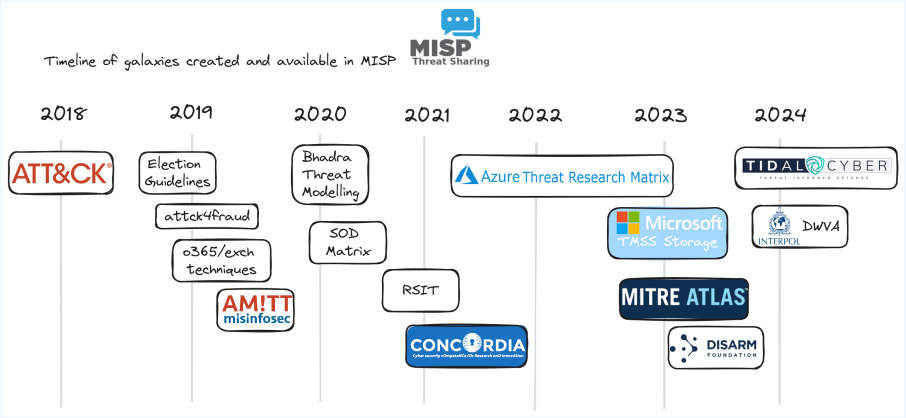
- MISP Galaxy is a feature in MISP and a MISP standard[1] format to create **contextualization libraries**.
  - There are two main types: **combined list** or **matrix-like list**.
- The first historical matrix-like galaxy was MITRE ATT&CK[2].
- Galaxies contain intelligence that can be **structured** 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/
[2] 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.

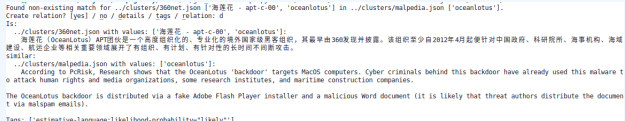
Conversion (or the Dirty Part)

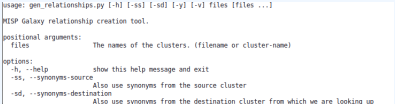
- Understand the topic.
- Understand the users and their use cases.
- Map to Matrix / Kill Chain.
- Handle **various formats**:
  - JSON, XLS, PDF, DOCX, Markdown, CSV, web scraping, Python, etc.
- Reverse engineer the data model.
- Manage UUIDs: existing vs. generating new.
- Handle duplicate values[3]:
  - Interaction with the framework owner.
- Create the conversion script.

[3] 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.





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