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

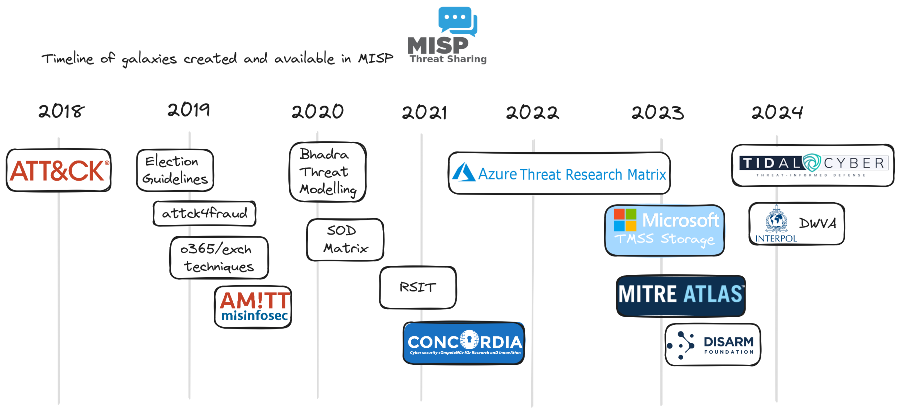
What is a MISP Galaxy?

- 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

MISP GALAXIES OVER TIME



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