

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/>

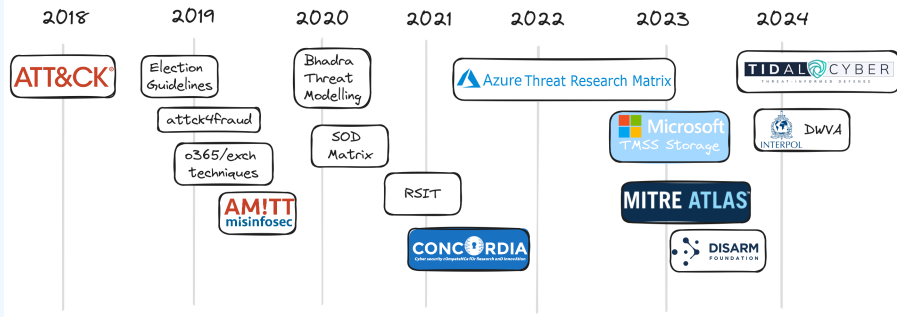
²Presented at the first EU ATT&CK community meeting in Luxembourg

- 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



Timeline of galaxies created and available in MISP



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.

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>