10 years of MISP

What's next in threat intelligence information sharing?

CIRCL / Team MISP Project

ENISA CTI-EU

What is MISP?

- MISP is a **threat information sharing** platform that is free & open source software
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, **correlates**, **enriches** and **connects** the data
- Allows teams and communities to **collaborate** and **share**
- **Feeds** automated protective tools and analyst tools with the output
- MISP is a **complete threat intelligence platform** with strong sharing capabilities and extendability

Two years from now, threat intelligence will be easy.

Bill Gates if he did work in threat intelligence

The aim of this presentation

- Showing the **evolution of threat intelligence**[1] and
- **data-driven threat hunting** over the past years
- What can we expect in **the future**?

[1] based on our empirical view from users using/integrating MISP

From standalone indicator to advanced object data models

- In early 2010, MISP supported basic indicators sharing with a limited set of types
- In 2022, MISP integrates a dynamic object model with advanced custom relationships
- Why such evolution?
  - **Increase of intelligence usage in different sectors**. From threat-hunting[2] to risk assessment or strategic decisions
  - **Increased diversity[3] among analysts**

[2] With different types of threat hunts including TTP-driven, intelligence-driven, asset-driven...

[3] MISP object public store include 296 templates in 2022.

Multitude of intelligence models

- Chains, triangles, circles, diamonds, arrows, a mix or even a multi-layer matrix
- There is **no perfect intelligence models**
- Organisations invent their model, reuse existing ones or are even more creative
- Showing **how diverse[4] our societies are**

[4] Embrace the diversity of models, taxonomies. 146 taxonomies are available in MISP taxonomies.

But some models can be a game changer

- With the introduction of **MITRE ATT&CK(tm)** in 2013, this was a game changer. What makes it a successful model?
  - Based on real and actual data[5], not just theoritical
  - **Continuous updates** were performed on ATT&CK
  - Embraced and recommended by many communities (e.g. EU ATT&CK community)
  - Change in usage and practices take time[6]
  - **Percolate** to other models (e.g. reusing the same matrix-like format)

[5] FMX - Fort Meade Experiment

[6] On a MISP community, 1% of ATT&CK techniques attached in 2013. In 2022, it's 72%.

Unstructured versus structured intelligence

- **Building narratives is critical in threat intelligence**
  - Intelligence narrative can be described in structured format (e.g. course-of-action)
  - Or written in natural language used to describe higher-level (e.g. assesment, executive summary or strategic information)
- For years, many thought that narrative and structured intelligence were separated.
- Accepting that **structured and unstructed can be together**[7] became critical.

[7] Mixed free-text Markdown reports with graph-oriented intelligence sharing in MISP increased during the past year.

Automation processes - "playbooks"

- **Sharing detection engineering** information became more prevalent
  - Sharing only the resulting analysis (indicators) is the bare minimal requirement in various sharing communities
  - Sharing the complete detection process[8] increases[9]
  - Reproducible **workflows and playbooks** play an important to **actionable intelligence**[10]

[8] Detection rules, scripts and playbooks

[9] New object template to support advanced detection engineering or intelligene pipelines.

[10] MISP worflow blueprints

What's the future?

- **Sharing more** without disclosing the actual information[11]
- **Automatic data modeling** on unstructured intelligence
- Advanced sighting and **feedback on engineering detection rules**[12]
- Automation and sharing of the threat intelligence pipelines framework.

[11] Grow of research about PSI (private set intersection) and an increased usage of MISP feed caching

[12] Sharing back training-sets or dataset with the actual false-positive detection

Contact

- Contact CIRCL / MISP Project
  - mailto:info@circl.lu - mailto:info@misp-project.org
  - https://www.misp-project.org/
  - https://www.circl.lu/
  - Mastodon *@circl@social.circl.lu* - *@misp@misp-community.org*