ATT&CK and MISP Project

advanced features in MISP supporting your analysts and tools

@adulau

EU ATT&CK Community

What is MISP?

- Open source "TISP" - A TIP with a strong focus on sharing
- A tool that **collects** information from partners, your analysts, your tools, feeds
- Normalises, correlates, enriches the data
- Allows teams and communities to **collaborate**
- **Feeds** automated protective tools and analyst tools with the output
- A set of tools to manage sharing communities and interconnected MISP servers

The growing need to contextualise data

- Contextualisation became more and more important as we as a community matured
  - **Growth and diversification** of our communities
  - Distinguish between information of interest and raw data
  - **False-positive** management
  - TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
  - **Increased data volumes** leads to a need to be able to prioritise
- These help with filtering your TI based on your **requirements**...
- ...as highlighted by a great talk from Pasquale Stirparo titled *Your Requirements Are Not My Requirements*

The emergence of ATT&CK

- Standardising on high-level **TTPs** was a solution to a long list of issues
- Adoption was rapid, tools producing ATT&CK data, familiar interface for users
- A much better take on kill-chain phases in general
- Feeds into our **filtering** and **situational awareness**[1] needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns

[1] ATT&CK sighting is a standard export format in MISP

The emergence of ATT&CK and similar galaxies

- **attck4fraud** [2] by Francesco Bigarella from ING
- **Election guidelines** [3] by NIS Cooperation Group
- **AM!TT Misinformation pattern** [4] by the misinfosecproject
- Alternative ATT&CK models still on the rise

[2] https://www.misp-project.org/galaxy.html#_attck4fraud

[3] https://www.misp-project.org/galaxy.html#_election_guidelines

[4] https://github.com/MISP/misp-galaxy/blob/master/clusters/misinfosec-amitt-misinformation-pattern.json

Future of ATT&CK in MISP Project

- MISP Galaxy 2.0 will include **improved inter-linking between ATT&CK and other models** (other galaxy or matrix-like models)
- Those relationships will be also shareable within different MISP communities
- Improvement into ATT&CK sub-techniques integration within MISP

Get in touch if you have any questions

- Contact CIRCL
  - info@circl.lu
  - `https://twitter.com/circl_lu`
  - `https://www.circl.lu/`
- Contact MISPProject
  - `https://github.com/MISP`
  - `https://gitter.im/MISP/MISP`
  - `https://twitter.com/MISPProject`
- Join the COVID-19 MISP community
  - `https://covid-19.iglocska.eu`