MISP Project - One Year of Improvements

MISP core team

MISP Project
https://www.misp-project.org/

MISP Summit 0x5 - 21st October 2019

2019 - A successful year for the MISP project

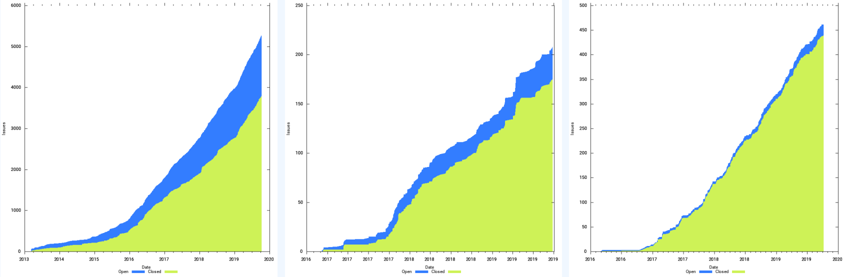
- **Improving and extending MISP project and information sharing practices** at a faster rate than expected
- Increasing the reach-out to collect ideas and inspirations from EU CSIRTs, the private sector and security professionals whilst doing trainings/workshops (thanks to the CEF funding)
- Integrate MISP at a rapid rate with **other standards** (such as MITRE ATT&CK sighting, STIX 2, GoAML and many others)
- Increased pan-European collaboration and information exchanged compared to 2018[1]
- Reaching the **establishment of a European standard**[2] **and open source toolset for threat intelligence and information sharing**

[1] https://www.x-isac.org/publication.html

[2] `https://www.misp-standard.org/`

Major outcomes in 2019

- 18 releases of the MISP core software which included more than 10 major new features. Attracting a large group of new users and contributors



- Increase of contributions during 2019 (MISP core, MISP objects and galaxy libraries)

Security vulnerabilities

- **"We love the smell of security vulnerabilities report in the morning, it smells like a great day!"**
- In 2019, we had 9 CVEs[3] for MISP core software
- If you find or have any ongoing security review of MISP, don't be afraid to contact us directly

[3] https://www.misp-project.org/security/

Major outcomes of 2019

- Improvements to external tools were created during 2019, such as those to the **misp-dashboard** (4 releases) - with a new release being foreseen within the next weeks
- The decaying model for indicators described as an academic paper in 2018 is now part of the core MISP software[4]
- **All MISP training materials are released as open content**[5] and contain more than 36 hours of training materials (e.g. MISP usage, administration, OSINT analysis and collection, building sharing communities)
  - Source code is available and translation(s)/contribution(s) are welcome

[4] https://www.misp-project.org/2019/09/12/Decaying-Of-Indicators.html

[5] https://github.com/MISP/misp-training

MISP OBJECT TEMPLATES

- The number of object templates rose from 89 (in 2018) to 147 (in 2019), thanks in a large part to the diligent work of many external contributors
- Object templates added include **telecom objects** (such as SS7, GTP, Diameter or IMSI-catcher output), **cyber security objects**, **security objects** (such as vehicule, interpol-notice)
- Objects are more and more used in different sharing communities and have overtaken simple attributes in MISP as the go-to data structure, offering better contextualisation for the data shared

MISP TAXONOMIES

- There are **102 taxonomies** available in MISP project contributed by various organisations and partners
- FIRST.org CTI SIG contributed an **ICS/OT Threat Attribution Industrial Control System taxonomy**
- MISP taxonomies[6] are common libraries and sharing communities select usually a subset to match their needs

[6] https://www.misp-project.org/taxonomies.html

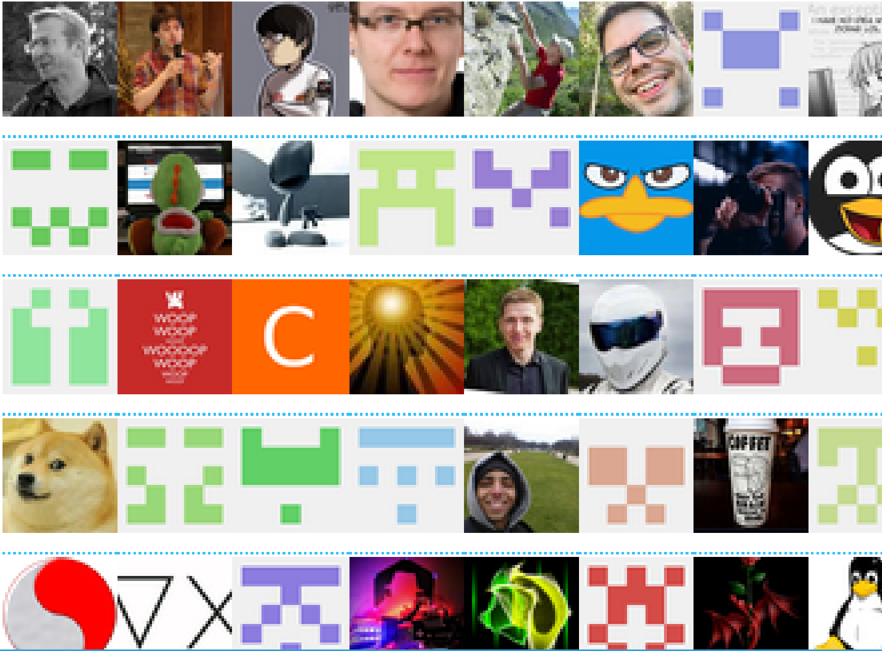
MISP galaxies

- There are **40 galaxies**[7] available in MISP project contributed by various organisations and partners
- We introduced a specific matrix-like format (such as MITRE ATT&CK model) and many new matrix-like were contributed such AM!TT Tactic (misinformation model), o365-exchange-techniques, attck4fraud, election guidelines

[7] https://www.misp-project.org/galaxy.html

Conclusion

- 2019 was a busy and successful year for the MISP project
- The 2-year CEF grant was a bootstrap to improve MISP to its next level
- New partnerships and projects are ongoing in 2020-2021 (such as the CEF VARIoT project or H2020 Enforce)
- As the MISP project becomes larger, we are **improving the structure of the project** (misp-standard.org is the first step)


WOOF
WOOF
WOOOOF
WOOF
C