MISP Project - One Year of Improvements

MISP core team

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

MISP Summit 0x5 - 21st October 2019

MISP
Threat Sharing

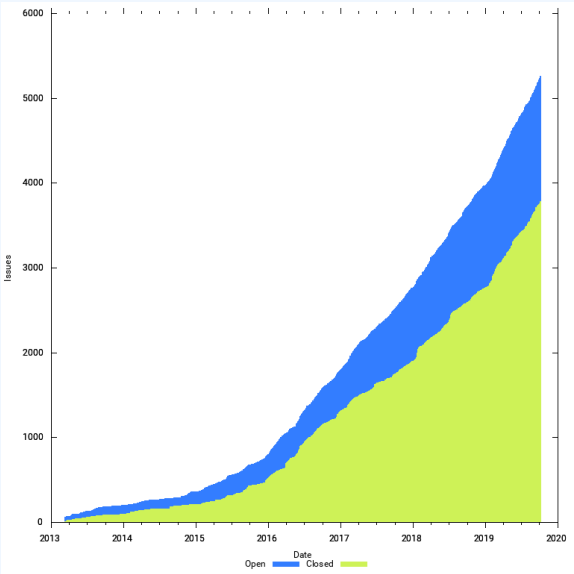
2019 - A successful year for the MISP project

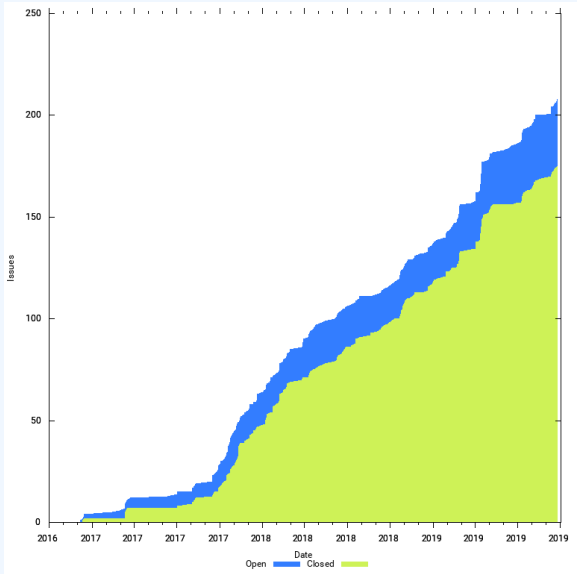
- **Improving and extending MISP project and information sharing practices** at a faster rate than expected
- Increasing reach out to collect ideas and inspirations from EU CSIRTs, the private sector and security professionals while doing trainings/workshops (thanks to the CEF funding)
- Integrate MISP 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 an European standard[2] and open source toolset for threat intelligence and information sharing**

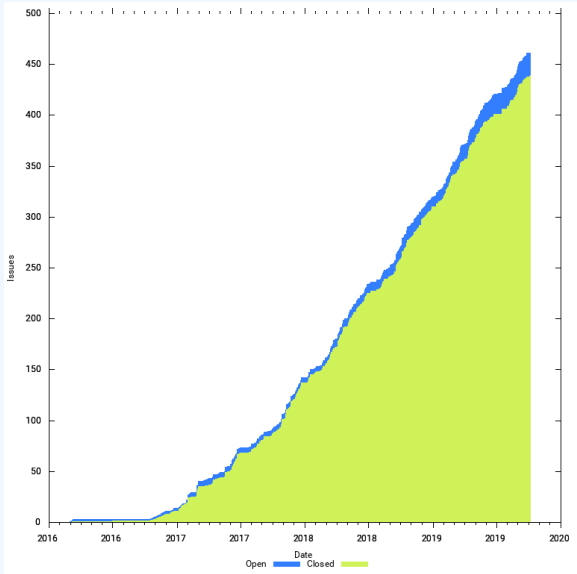
[1] https://www.x-isac.org/publication.html
[2] https://www.misp-standard.org/

Major outcomes in 2019

- 18 releases of the MISP core software which include 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).

Major outcomes in 2019

- Improved external tools were created during 2019 such as **misp-dashboard** (4 releases) - a new release is foreseen in the next weeks
- The decaying model for indicators described as a academic paper in 2018 is now part of the core MISP software[3]
- **All MISP training materials are released as open content**[4] and contain more than 36 hours of training (e.g. MISP usage, administration, OSINT analysis and collection, building sharing communities)
  - Source code is available and translation(s)/contribution(s) are welcome

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

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

MISP object templates

- From 89 (in 2018) to 147 (in 2019) object templates were added from many external contributors
- Object templates include updated **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 take over simple attributes in MISP to offer better contextualisation

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 improve the structure of the project (misp-standard.org is the first step)