MISP project new features and
Ongoing development activities

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
TLP:WHITE

MISP Summit 0x3 - 20171016

MISP development and CIRCL

- MISP is a **community-driven project**.
- CIRCL is the driving force behind the development of the MISP project as well as an active user of MISP operating multiple communities:
  - A large community of users including private CERTs, financial sector actors and various private organisations.
  - A publicly-funded CERT community (nren, n/g and sectorial CERTs).
  - A reversing community focusing on malware analysis and the sharing of ongoing analysis.
  - The FIRST.org MISP instance which includes FIRST members worldwide.
  - Multiple ISACs, other communities getting started with information sharing and exchange groups.

Funding aspects

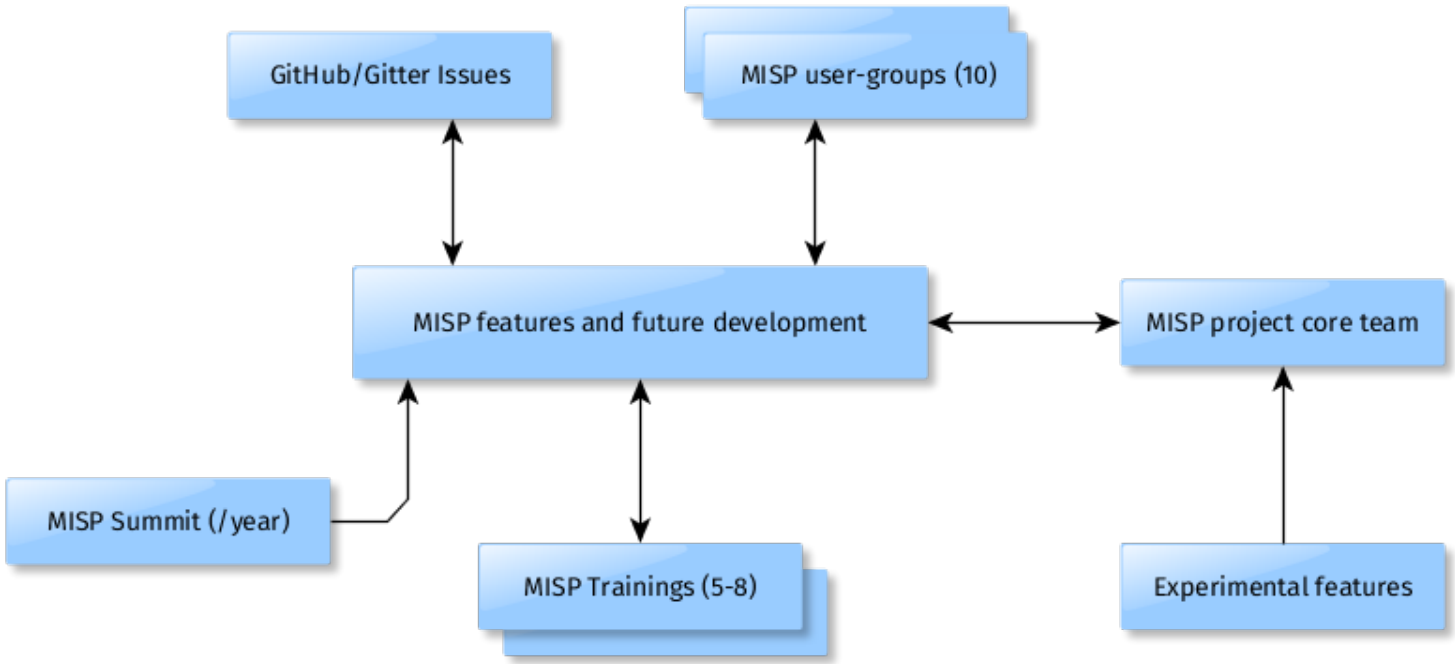
- **CIRCL financially supports MISP development** for the past years along with:
  - Co-funding on specific features
  - Research partnership
  - Additional development powered by third parties
  - Contributing organisations to integrate MISP standards into their tools
- Connecting Europe Facility funding 2016-LU-IA-0098[1] from 1st September 2017 until 31st August 2019 to improve MISP for n/g CSIRTs. The funding will cover integration with the CSP platform and support the MISP roadmap.

[1] *Improving MISP as building blocks for next-generation information sharing*

MISP team at CIRCL

- **Andras Iklody** (lead developer of the MISP core platform).
- **Alexandre Dulaunoy** (CIRCL MISP coord./OASIS CTI, misp-taxonomies, misp-modules, misp-objects).
- **Sascha Rommelfangen** (Lead of MISP QA)
- **Raphael Vinot** (PyMISP, misp-workbench and MISP viper/IntelMQ integration).
- **Gerard Wagener** (MISP research program (data-mining, academic use of MISP community dataset)).
- **Deborah Servili** (MISP Situational Awareness Project, galaxy classification and documentation).
- **Christian Studer** (MISP datamodel and OASIS CTI - STIX 2.x / MAEC and CASE-UCO project).
- **Steve Clement** - **Cedric Bonhomme** (MISP automation and automatic deployment)

MISP governance



Development based on practical user feedback

- There are many different types of users of an information sharing platform like MISP:
  - **Malware reversers** willing to share indicators of analysis with respective colleagues.
  - **Security analysts** searching, validating and using indicators in operational security.
  - **Intelligence analysts** gathering information about specific adversary groups.
  - **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
  - **Risk analysis teams** willing to know about the new threats, likelyhood and occurences.
  - **Fraud analysts** willing to share financial indicators to detect financial frauds.

MISP Project Overview

Galaxy

warning-lists

Taxonomies

modules (import, export, enrichment)

- The **core project**[a] (PHP/Python) supports the backend, API and UI.
- Modules (Python) to expand MISP functionalities.
- Taxonomies (JSON) to add categories and global tagging.
- Warning-lists (JSON) to help analysts to detect potential false-positives.
- Galaxy (JSON) to add threat-actors, tools or "intelligence".
- Objects (JSON) to allow for templated composition of security related atomic points of information.

2.4 development and release cycle

- Git tag are used for MISP release (2.4.x) are for **stable release**. We recommend MISP administrator to always run the latest release version.
- Development version is on the git HEAD of the MISP project.
- Major feature changes are created on git branches and regularly merged into the development version.
- Starting from 2.4, updates of the database schema are all done automatically at the first login.
- A MISP release[2] includes fixes, improvements and often new features (disabled by default if a change in the default MISP behaviour would occur).

[2] `http://www.misp-project.org/Changelog.txt`

New features after 2.4.69

- (2.4.70) 26 March 2017
  - MISP **user-interface has been improved** to support visually impaired users (significant in IC).
  - MISP API improved to add several attributes in go.
  - **MISP API extended** to add or edit MISP servers.
  - **Update of the software** can now be done via the diagnostic user-interface.
  - Many new attributes type added including **sigma** which is a generic for SIEM.
  - **MISP synchronization** improved on the debugging side along with a cleaner interface by removing old legacy sync 2.3.

New features after 2.4.69

- (2.4.71) 11 April 2017
  - Distribution can now be set in the free-text and modules import.
  - **API restsearch improved** allowing to support alternate download types from the restsearch output (OpenIOC in addition to MISP native format).
  - Auditing (via event history) is now accessible via the **API** in addition to the user-interface.
  - **Organisation blacklist is now enabled by default** including the sample UUIDs/organisations.
  - **Updated IETF Internet-Drafts** for MISP core format and taxonomy to support other tools to support the MISP format.

New features after 2.4.69

- (2.4.72) 14 April 2017
  - Major improvements to better support **large MISP instances** via additional flags to the index.
  - Enforce the hide tag directive. Allow to hide tag at instance level (by the MISP site admin). The tag is not removed but just hidden from the user-interface.
  - Client-side javascript has been improved.

New feature after 2.4.69

- (2.4.73) 09 May 2017
  - A new expansion protocol has been added to MISP to support TheHive[3] Cortex. You can now benefit from all expansion modules in TheHive into MISP. Cortex also integrated the support for the MISP expansion services.
  - MISP feeds (from remote url or file) have been completely rewritten to allow **caching of feeds** without importing these into MISP. So you can browse, cache and correlate information from feeds directly in your MISP instances. Feed overlap feature introduced.

Feed overlap analysis matrix

	1	2	3	4	5	6	7	8	10	11	12	15	16	18	19	20	21	24	25	27	29	30
1 CIRCL OSINT Feed	-	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%
2 The Botvrij.eu Data	49%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
3 ZeuS IP blocklist (Standard)	1%	1%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%
4 ZeuS compromised URL blocklist	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
5 blockrules of rules.emergingthreats.net	1%	0%	0%	0%	-	0%	0%	2%	0%	0%	0%	1%	10%	0%	0%	0%	0%	0%	0%	0%	0%	0%
6 Binary Defense Systems Artillery Threat Intelligence Feed and Banlist Feed	1%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
7 malwaredomainlist	2%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%
8 Tor exit nodes	19%	0%	0%	0%	5%	0%	0%	-	0%	0%	0%	1%	5%	0%	0%	0%	0%	0%	0%	0%	0%	0%
10 cybercrime-tracker.net - all	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
11 Phishtank online valid phishing	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
12 listdynamic dns providers	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
15 longtail.it.marist.edu	1%	0%	0%	0%	9%	1%	0%	3%	0%	0%	0%	-	27%	0%	0%	0%	0%	0%	0%	0%	0%	0%
16 longtail.it.marist.edu 7 days	1%	0%	0%	0%	9%	0%	0%	2%	0%	0%	0%	3%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%
18 diamondfox_panels	46%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%
19 Mirai-only-dec2016	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	9%	0%	0%	0%	0%	0%	0%
20 Mirai-only-jan2017																						
21 CIRCL - honeybot																						

New feature after 2.4.69

- (2.4.74) 30 May 2017
  - A new list of **default feeds** has been added to MISP including labs.snort.org, phishtank, abuse.ch, pan-unit42...
  - ZeroMQ pub-sub feature[4] has been significantly improved in MISP to allow for a **complete flexible notification scheme** for a host of actions which take place within a MISP instance including event publishing, attribute creation and update, sighting creation, user creation or modification.

[4] https://www.circl.lu/doc/misp/misp-zmq/

New feature after 2.4.69

- (2.4.75/2.4.76) 13 June 2017
  - **Performance improvement** released including memory usage of search API.
  - Fixing issues with older version of MySQL which could have introduced slowness.
  - Lookup and import is much faster (up-to 10 times faster).
  - Fixed multiple bugs in STIX export due to the change of library from MITRE.

New features after 2.4.69

- (2.4.77) 12 July 2017
  - Multiple security fixes and improvements (including **automatic bcrypt conversion of user's password**) from an external analysis done by cert.gov.nz.
  - Major speed enhancement for the CSV/freetext import in the feed interface.
  - Screenshots indicator improved to better support users actively sharing image artefacts using MISP.
  - Many usuability improvement in the user-interface.

New features after 2.4.69

- (2.4.78) 6 August 2017
  - **MISP roles can now be managed via the API**. Role functions such as add, delete, index, list and set_default are now accessible via the API. Useful for organisations requiring to manage a larget set of roles.
  - New MISP attribute types added like cookies to support the new MISP objects (released in 2.4.80).
  - An important security bug in the sharing groups and the attribute lookup was fixed[5] found by a contributor in Norway.

[5] `https://github.com/MISP/MISP/blob/2.4/CONTRIBUTING.md#reporting-security-vulnerabilities`

New features after 2.4.69

- (2.4.79) 25 August 2017
  - All taxonomies action (including index, view, enable, disable) are now accessible via the API. This allows organisations to better support their **tagging, marking and classification strategy** from a machine-to-machine interface.
  - Feeds preview are now exposed via the API in addition to the user-interface.
  - MISP galaxy now includes MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™).

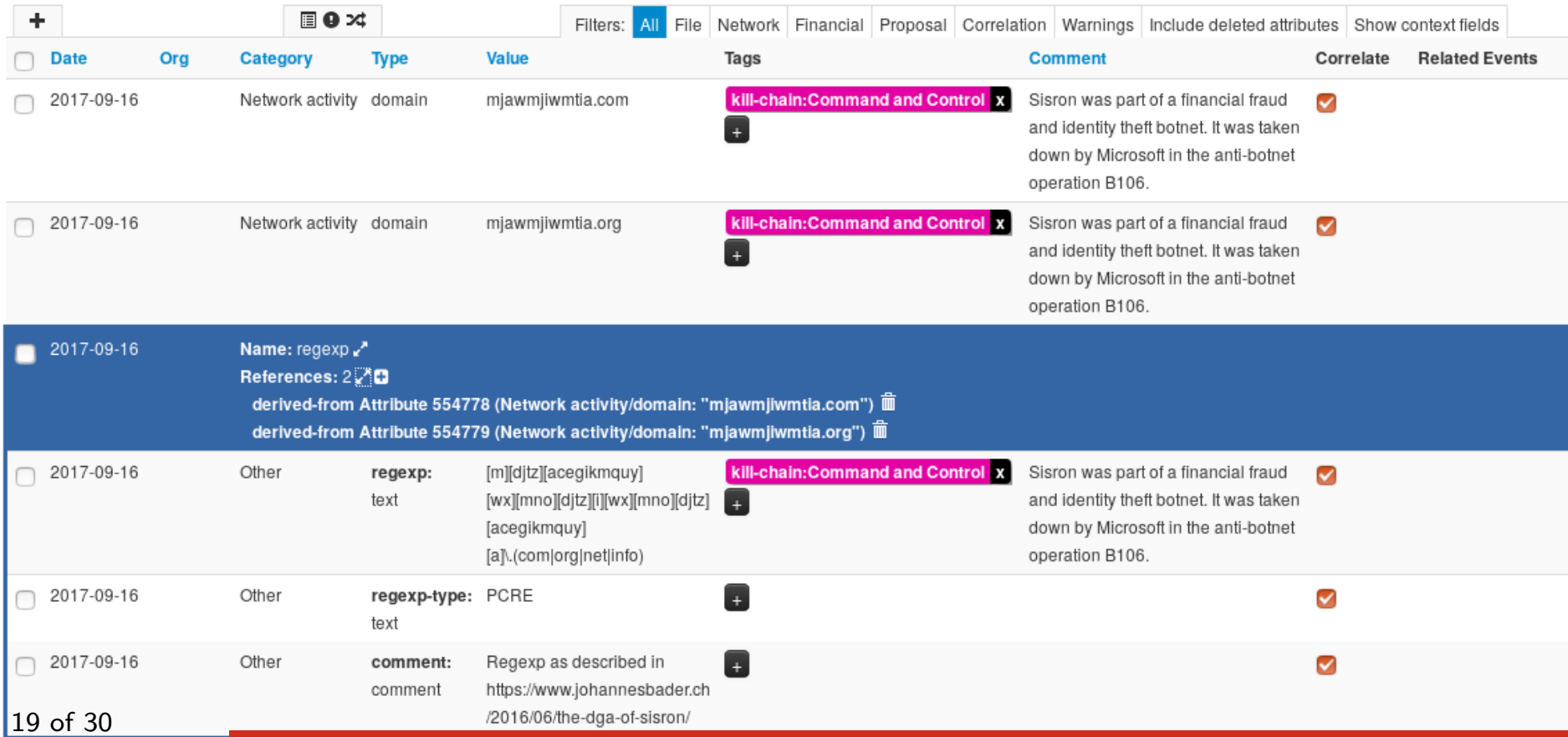
New features after 2.4.69

- (2.4.80) 18 September 2017
  - MISP now includes support for **MISP objects**. This allows MISP to support complex/combined objects in a flexible way along with their **relationships** towards other objects or even attributes. This is a major new extension in MISP.
  - Existing objects include **email, many binary file format (ELF, PE, MachO), geolocation, url, victim, phone or even person**[6].
  - MISP objects can be linked between each others or with attributes with **relationship types** (e.g. exfiltrates-to, identifies, beacons-to and so on).

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

Expressing DGA with MISP regexp object

- An example which describes a DGA (Domain Generation Algorithm) linked to two domain indicators using the MISP object functionality:



Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events
2017-09-16		Network activity	domain	mjawmjiwmtia.com	kill-chain:Command and Control	Sisron was part of a financial fraud and identity theft botnet. It was taken down by Microsoft in the anti-botnet operation B106.	✓	
2017-09-16		Network activity	domain	mjawmjiwmtia.org	kill-chain:Command and Control	Sisron was part of a financial fraud and identity theft botnet. It was taken down by Microsoft in the anti-botnet operation B106.	✓	
2017-09-16		**Name:** regexp **References:** 2 derived-from Attribute 554778 (Network activity/domain: "mjawmjiwmtia.com") derived-from Attribute 554779 (Network activity/domain: "mjawmjiwmtia.org")						
2017-09-16		Other	**regexp:** text	[m][djtz][acegikmquy][wx][mno][djtz][i][wx][mno][djtz][acegikmquy][a]\.(com|org|net|info)	kill-chain:Command and Control	Sisron was part of a financial fraud and identity theft botnet. It was taken down by Microsoft in the anti-botnet operation B106.	✓	
2017-09-16		Other	**regexp-type:** text	PCRE			✓	
2017-09-16		Other	**comment:** comment	Regexp as described in https://www.johannesbader.ch/2016/06/the-dga-of-sisron/			✓	

New features in 2.4.81

- Graphical representation of the MISP objects included in the event view.
- Significantly improvement in graphical visualisation including key shorcuts.
- STIX 2.0 experimental export added.

PyMISP updates in the past 8 months

- **Offline creation** of MISP event.
- Validation of the JSON based on the schema and MISP format Internet-Draft.
- **Neo4J, STIX and OpenIOC** format tooling added in PyMISP.
- Named attributes added to support the default MISP category and automatization flag. Code simplified.
- Data/sample upload from PyMISP is now supported.
- User Management and organisations API added.
- Support for the **digital signature** added (first beta version).

MISP Project (27) repositories updates 1/2

- misp-taxonomies includes more than **45+ vocabularies**.
- misp-warninglists includes more than **19+ default lists**.
- misp-STIX-Converter (MISP$\leftarrow\rightarrow$STIX) converter updated to support some standard STIX files.
- misp-taxii-server - TAXII server hooked up to MISP (STIX/inbox $\rightarrow$ automatic import to MISP).
- misp-workbench - includes misp-hashstore to **support local/disconnected lookup** against MISP.

MISP Project (27) repositories updates 2/2

- misp-galaxy includes more than **10 clusters** such as exploit-kit, microsoft-activity-group, preventive-measure, ransomware, remote access trojan, tds, **threat-actor and adversary tools**.
- misp-sighting-tools include sample scripts to sight attributes from pcap files to MISP.
- misp-rfc has been updated 4 IETF Internet-Drafts have been published for the MISP standards.

What's cooking?

MISP next features and work in progress

Improvement foreseen in MISP Objects

- Graphical representation of the MISP objects in the event view.
- Support of objects in the MISP modules.
- Tagging and adding galaxy at object level.
- Object editors from the user-interface.
- Expanding object to some of the API interface (depending of the capability of the exporting format).

Major features foreseen 1/2

- Distributed sighting (anonymized).
- Privacy-aware data-structure.
- Centralised opt-in organisations, feed registry and community discovery.
- User-specific UI settings.
- Supporting large evidence collection and sharing.
- Analyst annotation system.
- Tagging all-the-things project.
- STIX 2.x support.
- CASE/UCO support.
- Darwin project (technical to tactical).
- Integrate modules and API to feed ingestion.

Major features foreseen 2/2

- Gamification of the sharing aspect in MISP.
- Historical comparative feed analysis.
- Notification filtering and user-customised.
- Synchronisation and export improvements.
- Galaxy-based view.
- Authoring data via the graphical representation.
- UI and usuability improvement.
- Background worker migration to new MISP queueing library.
- API improvements to expose the complete functionalities.

PyMISP

- Integration of PyTaxonomies (and future) PyGalaxy in PyMISP to build and extend event in a single library.
- **async support** to be added (Python 3-only).
- Adding the support for MISP authority support in the digital signature (allowing trusted group to have their own key authority to validate the signature).

Conclusion

- Following the great feedback and contributions at the trainings and hackathons[7], a **MISP training** is organised the 21st November 2018 and the **MISP developer meeting** 22nd November 2017.
- MISP project evolves following direct **user feedback** and practices in information sharing.
- Don't hesitate to get in touch with us (via GitHub issues or directly) if you have some bug reports, ideas or contributions to share.
- If you would like to fund or support a specific feature, don't hesitate to get in touch.

[7] `https://hackathon.hack.lu/`

Q&A

- Follow @MISPProject on Twitter
- `https://github.com/MISP/MISP`
- `https://github.com/MISP/` for misp-modules, misp-galaxy, misp-objects and misp-taxonomies
- info@circl.lu (if you want to join one of the MISP community operated by CIRCL)
- PGP key fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5