MISP project & Cerebrate update

Update of the features & development efforts

CIRCL team

2023-06-04 NATO MUG

What has happened since the last MUG

Give you a brief update over the highlights

A Topical Listing of the New Major Features

- Improved data model in MISP to support **analyst data** including analyst notes, opinions, and relationships
- **Workflow** improvements and changes to support use-cases
- **STIX 2.1** improvements along with MISP galaxy 2.0 support
- Performance improvements including in the MISP sighting, synchronization, and ReST queries
- **Logging/Monitoring** and **security** improvements
- **MISP modules** are now autonomous
- **Security fixes** and other improvements

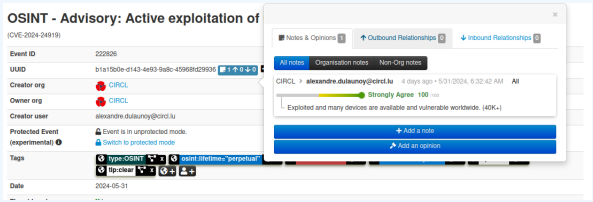
Analyst Data

- The Analyst Data feature[1] is an extended and shareable set of capabilities that allows analysts **to share and add their own analysis to any MISP event**.
- The Analyst Data feature comprises three main components:
  - Adding an **Analyst Note** to any element in MISP, such as Event, Event Report, Object, Attribute, or Galaxy Cluster.
  - Adding an **Analyst Opinion** with a rating (between 0 and 100) to any element in MISP, such as Event, Event Report, Object, Attribute, Galaxy Cluster, or Analyst Note.
  - Adding an **Analyst Relationship** from/to any element in MISP with a specified relationship type.

[1] Extending the MISP standard format

Analyst Opinion and Note View

- Showing/editing opinion on a MISP event or a MISP galaxy cluster



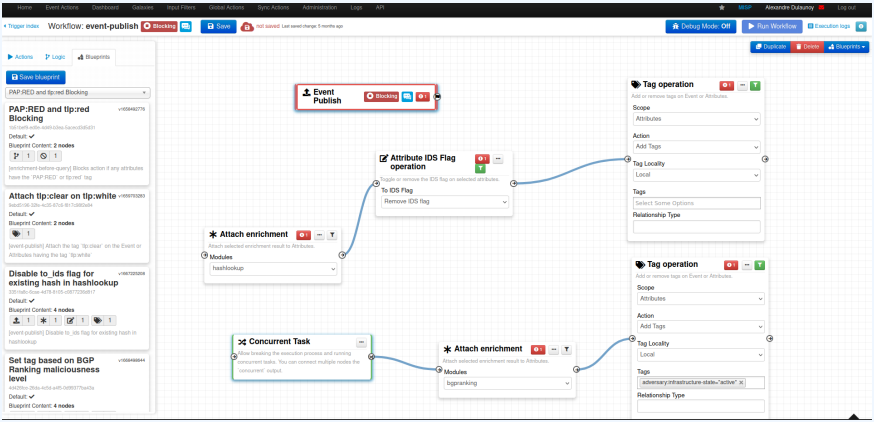
Analyst Relationship

- Showing/editing a relationship between a MISP galaxy cluster and another element

Workflows

- Additional **action nodes** like Slack added as action module in MISP modules
- Inclusion of new **triggers** based on community feedback
- Distribution-if module now includes sharing-group
- Various workflow bugs fixed following community feedback

Workflows


Home
Event Actions
Dashboard
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Logs
API
MISP
Alexandre Dulaunoy
Log out
Trigger index
Workflow: event-publish
Blocking
Save
not saved
Debug Mode: Off
Run Workflow
Execution logs
Duplicate
Delete
Blueprints
Actions
Logic
Blueprints
Save blueprint
PAP:RED and tlp:red Blocking
PAP:RED and tlp:red Blocking
Default: ✔
Blueprint Content: 2 nodes
Attach tlp:clear on tlp:white
Default: ✔
Blueprint Content: 2 nodes
Disable to_ids flag for existing hash in hashlookup
Default: ✔
Blueprint Content: 4 nodes
Set tag based on BGP Ranking maliciousness level
Default: ✔
Blueprint Content: 4 nodes
Event Publish
Blocking
Attribute IDS Flag operation
To IDS Flag
Remove IDS flag
Attach enrichment
Modules
hashlookup
Concurrent Task
Attach enrichment
Modules
bgpranking
Tag operation
Scope
Attributes
Action
Add Tags
Tag Locality
Local
Tags
Select Some Options
Relationship Type
Tag operation
Scope
Attributes
Action
Add Tags
Tag Locality
Local
Tags
adversary:infrastructure-state="active"
Relationship Type

Performance and Sightings

- Fast API authentication allowing the storage of hashed API keys in Redis (optional)
- Option to disable the loading of sightings via the API
- Support for a sighting policy (`getLastSighting`) and blocking sighting sync per organisation
- Attribute fetch refactored to simplify conditions and limit the loading of ACL
- Attribute search reworked for performance improvement
- New benchmarking suite added, collecting metrics, all accessible in the dashboard widget

Security Fixes and Other Improvements

- Long list of security fixes based on multiple external penetration tests
- **CVEs**[2] continuously reported for issues small and large
  - Make sure you're up to date and have TOTP active on your MISP instance.
- Research by **Zigrin Security**, funded by the **Luxembourg Army**, has been a massive help along with recent pentests from NATO
- Long list of other improvements, quality of life changes, and performance tuning

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

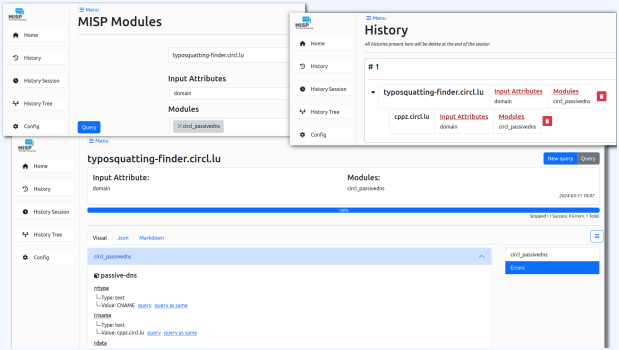
MISP Modules

- MISP modules[3] are companions for expansion, export, and import for external services or tooling
- New modules added, such as the **Google Threat Intelligence expansion module**
- New workflow action modules added, such as Slack, with improvements to the Mattermost module
- Many improvements and fixes to all the modules

[3] https://github.com/MISP/misp-modules/

MISP Modules are Now Standalone

- MISP Modules[4] can now function independently of the MISP platform.
- A versatile web interface is now available where you can query different modules, keep a history, and facilitate pivoting.



[4] https://www.misp-project.org/2024/03/12/Introducing.standalone.MISP.modules.html/

MISP Taxonomies

- 149 ready-to-use taxonomies are now available in MISP[5] (used in MISP and many other tools)
- Improved **dark-web** taxonomy to map the use of JRC with the AIL project[6]
- Many improvements to the different taxonomies including **workflow**, **event-type**, and many others

[5] https://github.com/MISP/misp-taxonomies/
[6] https://www.ail-project.org/

MISP Warning-Lists

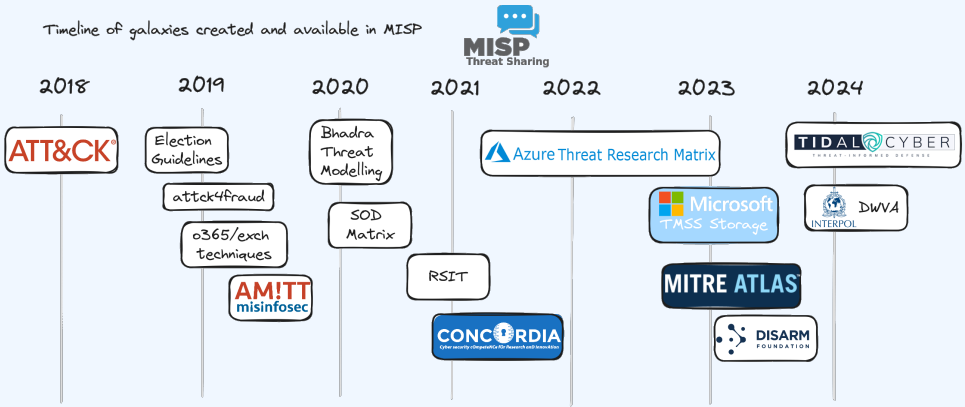
- New **check-host.net** warning-list added
- New **link-in-bio** warning-list added (similar to URL shortener)
- New **find-ip** known hostname used for querying your source IP (collected from our Passive DNS)
- Many updates in the existing warning-lists such as the **URL shortener**

MISP GALAXY

- New website for MISP galaxy[7] is now online including inter-relationship between galaxies
- Latest MITRE ATT&CK version 15.1 updated for the MISP galaxy
- New **producer** galaxy to facilitate the link to security reports with their respective producers
- New **INTERPOL Dark Web and Virtual Assets Taxonomies**, **UKHSA Culture Collections**, **Threat Matrix for Storage Services**, **Intel Agencies**, **Tidal**
- Major updates in **Disarm**, **threat-actor**, **Surveillance Vendor** and bf ransomware galaxies

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

Matrix-based MISP galaxy



MISP Objects

- Improvement in **cs-beacon-config** to map Shadow Server discovery service of CS
- Improvement of **ransomware-group-post** to map other discovery services such as ransomlook.io
- New objects to support Flowintel[8] cases and tasks
- New object **generalizing-persuasion-framework** requested for disinformation use-cases
- Many improvements to existing objects, including fixes for STIX 2.1 or CERT.PL use-cases
- Many new default relationships added to the MISP objects

[8] https://github.com/flowintel/flowintel-cm

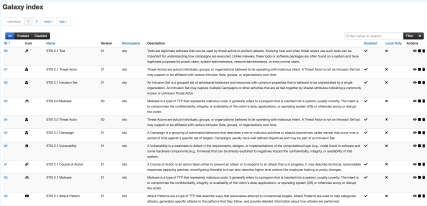
MISP STIX

- misp-stix[9] is standalone Python library support MISP standard format and all the STIX version (1.1.1, 1.2, 2.0 and 2.1)
- Two people from CIRCL are **co-sharing the OASIS Cyber Threat Intelligence (CTI) TC and CTI STIX subcommittee**
- Ensuring alignment between the standards, interoperability and an open source standard library

[9] https://github.com/MISP/misp-stix

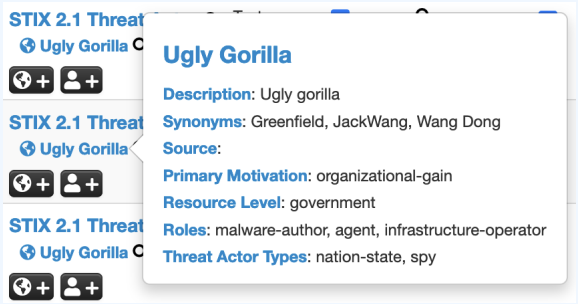
MISP stix - Custom Galaxy Cluster Import

- TTPs, Threat Actors and other contextual descriptions imported as Galaxy Clusters
- Generating specific Custom Galaxy Clusters from STIX directly

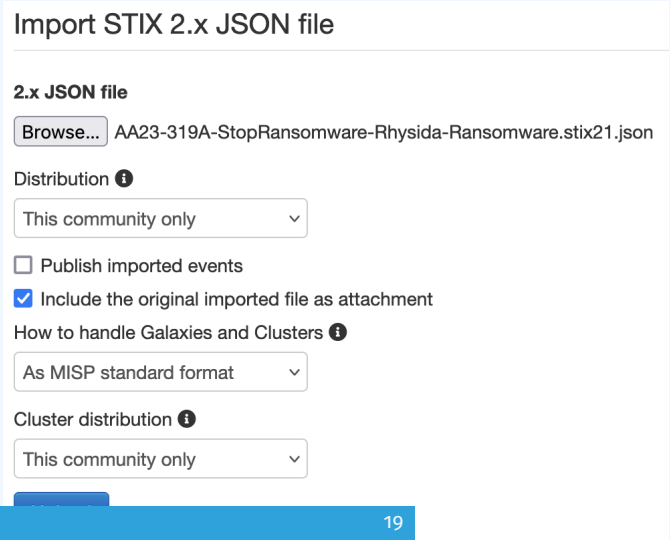


MISP stix - Custom Galaxy Cluster Import

- Extracting the complete description within the Cluster meta fields

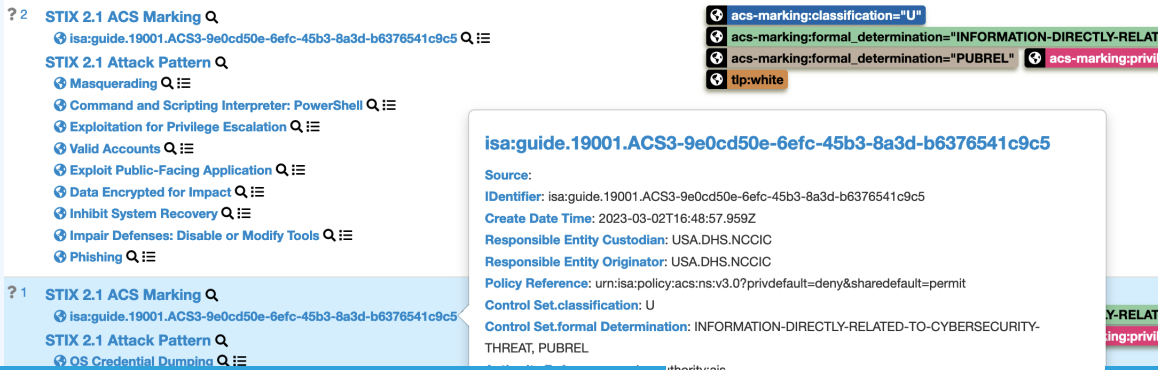


- Ability to select the Clusters distribution



MISP STIX - Support of ACS markings

- Generating a **Custom Galaxy Cluster** with the flattened description of the the Marking definition
- Extracting some of the fields as Tag to provide classification of the data marked with the Marking definition



Continuous improvement & Work in progress

- Import **Note & Opinion** objects using the recently released **Analyst Data** feature
- Filling the mapping gaps between **Indicators, Observed Data, Observable objects** and their MISP representation (**Attributes & Objects**)

Cerebrate

- Cerebrate v1.19[10] released with several usability and functionality fixes (v1.20 is expected this week)
- Many **improvements and bugs fixed** following feedback from various organizations deploying Cerebrate, such as the ENISA CSIRT network
- Deployment of the **PoC for NATO users is ongoing** - Cerebrate instance will be available on 15th September 2024

[10] https://www.cerebrate-project.org/2024/05/15/Cerebrate-version-1.19-released.html

Ongoing rework

MISP 3

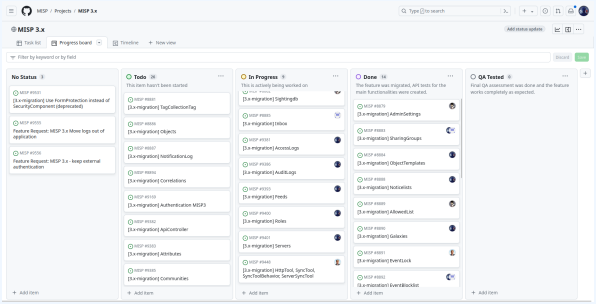
- Largest ongoing work is the work on **MISP3**
- Already announced long ago, development is now underway[11]
- New **tech stack** based on Cerebrate's advances (CakePHP 4.x+, PHP 8.2+, Bootstrap 5+)
- Longer project, will bring long needed improvements

[11] https://github.com/MISP/MISP/tree/3.x

MISP 3 Status

3.x Migration status

- Migration status is available online in the MISP project page on GitHub[12]



- 26 Pull Requests (1 Open, 1 Draft)
- **+105,165 lines of code added** and **20,992 lines of code removed**

[12] https://github.com/orgs/MISP/projects/2/views/4

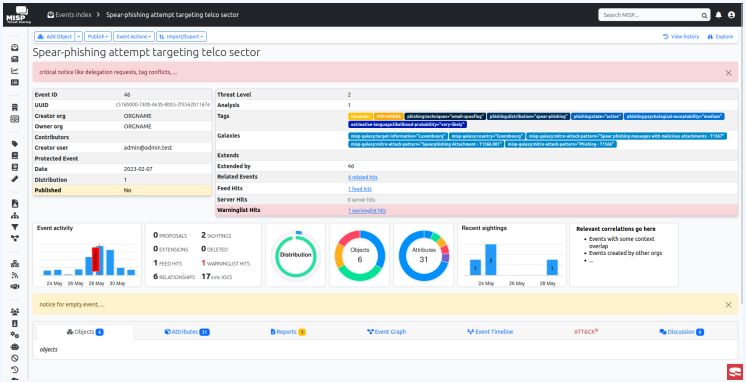
3.x - UI revamp

- **Event View Page Redesign** - We are working on a complete overhaul of this page, with a focus on catering to multiple use-cases for different user-personas, enhancing responsiveness, integrating multiple charts, and emphasizing critical elements of MISP events. We're also separating attributes and objects for clearer comprehension.
- **Navigation Menu Redesign** - We're restructuring the navigation menu for better organization, incorporating intuitive groupings, icons, and support for mobile devices through a hamburger menu.
- **Bootstrap Upgrade** - Moving from Bootstrap 2 to Bootstrap 4 ensures a more modern and adaptable framework.

3.x - UI revamp

- **Application-Wide Color Schemes** - We're introducing support for customizable color schemes, including the much-requested dark mode.
- **Settings and Diagnostics Page Redesign** - These sections will undergo a makeover to improve usability, accessibility and make them less overwhelming.
- **Removal of Deprecated Features** - We aim to focus MISP's functionality on core capabilities, we're eliminating deprecated features that are no longer actively used or supported. This includes functionalities like Discussions or Threads, News, Scheduled Tasks, and Populate Event from Template.

3.x - UI EXAMPLE



3.x - Improved developer/deployment experience

- Easy developer onboarding with dedicated readmes for development/testing.
- No more complex setup script, running docker development enviroment with just 3 commands:

```
$ git clone -b 3.x git@github.com:MISP/MISP.git MISP3
$ cd MISP3
$ docker-compose -f docker-compose.yml -f docker-compose.dev.yml --
    env-file="./docker/.env.dev" up
```

3.x - Automatic checks/fixes via via pre-commit hooks

- **phpcbf**: Code style beautifying.
- **phpcs**: Code style analysis PSR, naming conventions, etc.
- **phpstan**: Automatic static code analysis unused variables/imports, forbidden functions, etc.

3.x - New test suite

- Automatic API schema tests on requests/responses against OpenAPI spec.
- Code coverage.
- Testing sync and complex features mocking external http requests.
- Faster than previous PyMISP test suite.
- Reproducible, same tests are run by GitHub Actions on each PR.
- Easy to run, just one command:

```
docker-compose -f docker-compose.yml -f docker-compose.dev.yml --env
   -file="./docker/.env.test" exec misp vendor/bin/phpunit
```

MISP Airgap

- MISP Airgap[13] is a solution designed to **deploy MISP in air-gapped or isolated networks**.
- By leveraging the power of Linux containers (LXD), it ensures a secure, efficient, and manageable deployment of MISP instances.
- Furthermore, it enables users to frequently update their MISP instance in an environment cut off from the internet.

[13] https://www.misp-project.org/2024/01/12/MISP-airgap.html/

To Sum It All Up...

- The MISP **developer/contributor community** continues to grow and is very active.
- The main focus over the past months has been:
  - Performance, security, and monitoring
  - Improved deployment of MISP via the new misp-docker or misp-airgap
  - Enhancing the documentation and supporting materials such as misp-playbooks
  - Improving the MISP ecosystem, including misp-galaxy, misp-modules, and interconnectivity with new tools such as Flowintel
- There is definitely no lack of new ideas and improvements. If you want to participate, it's easy to **get involved**.

Get in touch if you have any questions

- Contact CIRCL
  - info@circl.lu
  - https://social.circl.lu/@circl
  - https://www.circl.lu/
- Contact MISPProject
  - https://github.com/MISP
  - https://gitter.im/MISP/MISP
  - https://misp-community.org/@misp
- Cerebrate project
  - https://github.com/cerebrate-project
  - https://github.com/cerebrate-project/cerebrate