

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

- The Analyst Data feature¹ 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.

¹Extending the MISP standard format

ANALYST OPINION AND NOTE VIEW

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

The image displays two screenshots from the MISP (Malware Information Sharing Platform) interface, illustrating the 'Analyst Opinion and Note View'.

Top Screenshot: OSINT - Advisory: Active exploitation of
(CVE-2024-24919)

Event Details:

- Event ID: 222826
- UUID: b1a150e-d143-4e93-9a8c-45968d29305
- Creator org: CIRCL
- Owner org: CIRCL
- Creator user: alexandre.dulaunoy@circl.lu
- Protected Event (experimental): Event is in unprotected mode. Switch to protected mode
- Tags: type:OSINT, osint:lifetime="perpetual", ftp:clear
- Date: 2024-05-31

Opinion View (Right Panel):

- Notes & Opinions: 1
- Outbound Relationships: 0
- Inbound Relationships: 0
- Filter: All notes (Organisation notes, Non-Org notes)
- Note by alexandre.dulaunoy@circl.lu (4 days ago): Strongly Agree (100%)
Exploited and many devices are available and vulnerable worldwide. (40K+)
- Buttons: + Add a note, + Add an opinion

Bottom Screenshot: UAVs/CAVs :: Bayraktar TB2

Cluster Details:

- Cluster ID: 213736
- Name: Bayraktar TB2
- Parent Galaxy: UAVs/CAVs
- Description: Bayraktar TB2
- Default: Yes
- Version: 1
- UUID: 6b4b821a-8900-47b4-b08e-451cd2017621
- Collection UUID: baf5c29d-d0db-4923-a984-80921126d3ab
- Source: Popular Mechanics
- Authors: Enes AYATA
- Distribution: All communities
- Owner Organisation: [Logo]
- Creator Organisation: [Logo]
- Connector tag: misp-galaxy:uavs="Bayraktar TB2"
- Events: 0

Opinion View (Right Panel):

- Notes & Opinions: 2
- Outbound Relationships: 0
- Inbound Relationships: 0
- Filter: All notes (Organisation notes, Non-Org notes)
- Note 1 by alexandre.dulaunoy@circl.lu (2 hours ago): Need to review the source of the information (Disagree 30%)
- Note 2 by alexandre.dulaunoy@circl.lu (2 hours ago): Metadata are incorrect and need to be reviewed (Disagree 30%)
- Buttons: + Add a note, + Add an opinion

Bottom Controls:

- Toggle ATT&CK Matrix
- Toggle Cluster relationships

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

UAVs/UCAVs :: Orlan-30

Cluster ID	213745
Name	Orlan-30
Parent Galaxy	UAVs/UCAVs
Description	Orlan-30
Default	Yes
Version	1
UUID	9536d2ee-e4a2-46ee-a4d2-313169312cd   
Collection UUID	beffc29d-b0db-4923-aaf8-80921126d3ab
Source	Popular Mechanics
Authors	Enes AYATA
Distribution	All communities
Owner Organisation	
Creator Organisation	
Connector tag	misp-galaxy:uavs="Orlan-30"
Events	0

 Toggle ATT&CK Matrix

 Toggle Cluster relationships

 Notes & Opinions **0**

 Outbound Relationships **1**

 Inbound Relationships **0**

CIRCL > 2 hours ago • 6/3/2024, 6:40:45 All

alexandre.dulaunoy@circl.lu PM

 related to → GalaxyCluster :: 4d604f05-80b2-45dc-ab2b-a4f9e787a0d

 Add a relationship

- 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

The screenshot displays the MITRE ATT&CK Workflows interface. The top navigation bar includes links for Home, Event Actions, Dashboard, Global Actions, Sync Actions, Administration, and Log out. The main header shows the workflow name 'Workflow: event-publish' and its status 'not saved'. The left sidebar lists several blueprints: 'PAP:RED and tip:red Blocking', 'Attach tip:clear on tip:white', 'Disable to_ids flag for existing hash in hashlookup', and 'Set tag based on BGP Ranking maliciousness level'. The main workspace shows a workflow diagram with the following steps: 1. 'Event Publish' (red box), 2. 'Attribute IDS Flag operation' (toggle to remove IDS flag), 3. 'Tag operation' (add tags), 4. 'Concurrent Task' (parallel execution), 5. 'Attach enrichment' (bgp ranking), and 6. 'Tag operation' (add tags). The right sidebar shows the configuration for the 'Tag operation' step, including Scope (Attributes), Action (Add Tags), Tag Locality (Local), and Tags (adversary infrastructure-state="active" X).

Workflow: event-publish

Event Publish

Attribute IDS Flag operation

Tag operation

Concurrent Task

Attach enrichment

Tag operation

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

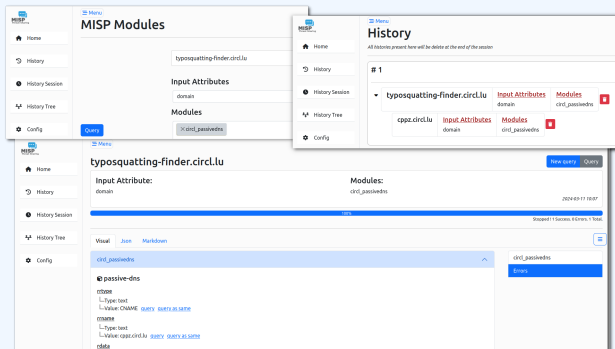
²<https://www.misp-project.org/security/>

- MISP modules³ 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 Modules⁴ 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/>

- 149 ready-to-use taxonomies are now available in MISP⁵ (used in MISP and many other tools)
- Improved **dark-web** taxonomy to map the use of JRC with the AIL project⁶
- Many improvements to the different taxonomies including **workflow**, **event-type**, and many others

⁵<https://github.com/MISP/misp-taxonomies/>

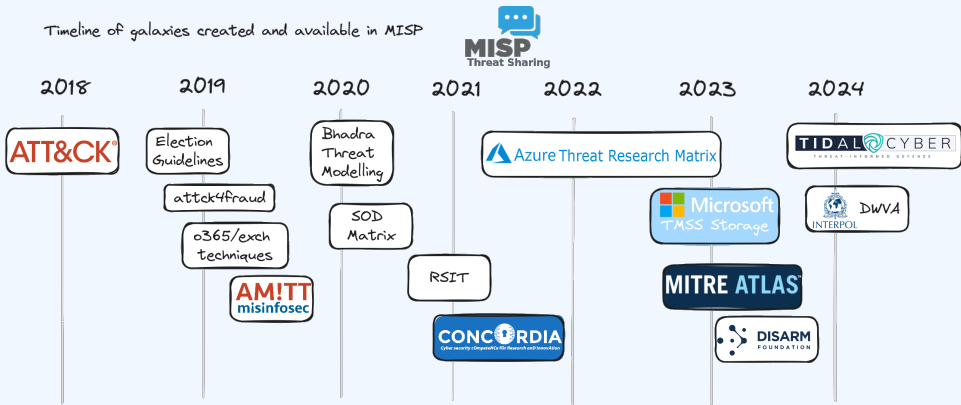
⁶<https://www.ail-project.org/>

- 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**

- New website for MISP galaxy⁷ 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



- 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 Flowintel⁸ 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-stix⁹ 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

[illegible][illegible]

- Extracting the complete description within the Cluster meta fields

The screenshot displays a list of STIX 2.1 Threats in the MISP interface, all belonging to the 'Ugly Gorilla' cluster. Each entry includes a globe icon and a plus sign. A detailed popup for one instance is shown, containing the following information:

- Ugly Gorilla**
- Description:** Ugly gorilla
- Synonyms:** Greenfield, JackWang, Wang Dong
- Source:**
- Primary Motivation:** organizational-gain
- Resource Level:** government
- Roles:** malware-author, agent, infrastructure-operator
- Threat Actor Types:** nation-state, spy

■ Ability to select the Clusters distribution

Import STIX 2.x JSON file

2.x JSON file

AA23-319A-StopRansomware-Rhysida-Ransomware.stix21.json

Distribution ⓘ

This community only



☐ Publish imported events

☒ Include the original imported file as attachment

How to handle Galaxies and Clusters ⓘ

As MISP standard format



Cluster distribution ⓘ

This community only



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

? 2 STIX 2.1 ACS Marking Q

isa:guide.19001.ACS3-9e0cd50e-6efc-45b3-8a3d-b6376541c9c5 Q ≡

STIX 2.1 Attack Pattern Q

- Masquerading Q ≡
- Command and Scripting Interpreter: PowerShell Q ≡
- Exploitation for Privilege Escalation Q ≡
- Valid Accounts Q ≡
- Exploit Public-Facing Application Q ≡
- Data Encrypted for Impact Q ≡
- Inhibit System Recovery Q ≡
- Impair Defenses: Disable or Modify Tools Q ≡
- Phishing Q ≡

? 1 STIX 2.1 ACS Marking Q

isa:guide.19001.ACS3-9e0cd50e-6efc-45b3-8a3d-b6376541c9c5

STIX 2.1 Attack Pattern Q

- OS Credential Dumping Q ≡

acs-marking:classification="U"

acs-marking:formal_determination="INFORMATION-DIRECTLY-RELAT

acs-marking:formal_determination="PUBREL" acs-marking:privi

tlp:white

isa:guide.19001.ACS3-9e0cd50e-6efc-45b3-8a3d-b6376541c9c5

Source:

IDentifier: isa:guide.19001.ACS3-9e0cd50e-6efc-45b3-8a3d-b6376541c9c5

Create Date Time: 2023-03-02T16:48:57.959Z

Responsible Entity Custodian: USA.DHS.NCCIC

Responsible Entity Originator: USA.DHS.NCCIC

Policy Reference: urn:isa:policy:acs:ns:v3.0?privdefault=deny&shareddefault=permit

Control Set.classification: U

Control Set.formal Determination: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT, PUBREL

- 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 v1.19¹⁰ 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:](https://www.cerebrate-project.org/2024/05/15/Cerebrate-version-1.19-released.html)

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

ONGOING REWORK

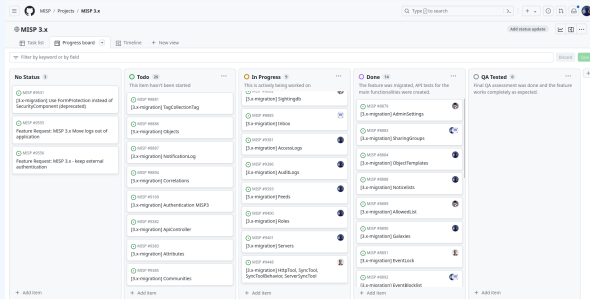
- Largest ongoing work is the work on **MISP3**
- Already announced long ago, development is now underway¹¹
- New **tech stack** based on Cerebrate's advances (CakePHP 4.x+, PHP 8.2+, Bootstrap 5+)
- Longer project, will bring long needed improvements

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 GitHub¹²



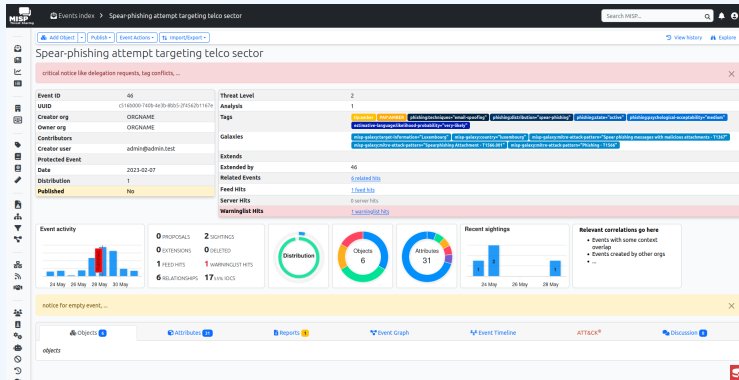
- 26 Pull Requests (1 Open, 1 Draft)
- **+105,165 lines of code added** and **20,992 lines of code removed**

¹²<https://github.com/orgs/MISP/projects/2/views/4>

- **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.

- **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 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 Airgap¹³ 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 MISPPProject

- ▶ <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>