MISP Project

Latest Features and Development Efforts

Team CIRCL

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

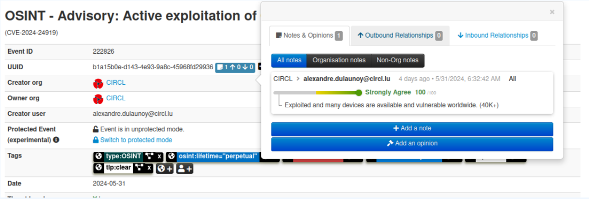
Analyst Data

- 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



OSINT - Advisory: Active exploitation of

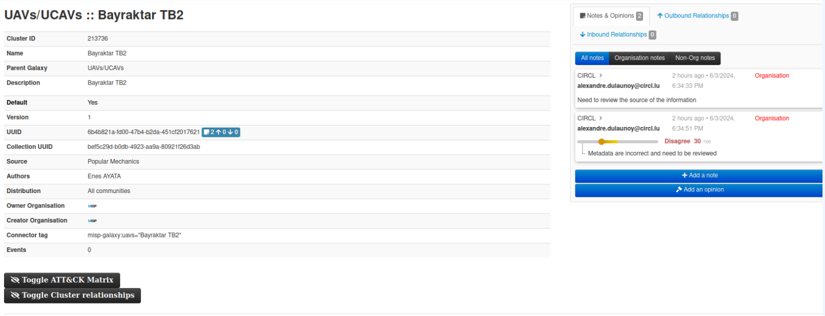
(CVE-2024-24919)

Event ID	222826
UUID	b1a15b0e-d143-4e93-9a8c-45968fd29936 1 ↑0 ↓0
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 x osint:lifetime="perpetual" tlp:clear x
Date	2024-05-31

CIRCL › alexandre.dulaunoy@circl.lu 4 days ago • 5/31/2024, 6:32:42 AM All

Strongly Agree 100 /100

Exploited and many devices are available and vulnerable worldwide. (40K+)



UAVs/UCAVs :: Bayraktar TB2

Cluster ID	213736
Name	Bayraktar TB2
Parent Galaxy	UAVs/UCAVs
Description	Bayraktar TB2
Default	Yes
Version	1
UUID	6b4b821a-fd00-47b4-b2da-451cf2017621 2 ↑0 ↓0
Collection UUID	bef5c29d-b0db-4923-aa9a-80921f26d3ab
Source	Popular Mechanics
Authors	Enes AYATA
Distribution	All communities
Owner Organisation	
Creator Organisation	
Connector tag	misp-galaxy:uavs="Bayraktar TB2"
Events	0

Toggle ATT&CK Matrix
Toggle Cluster relationships
Notes & Opinions 2
↑ Outbound Relationships 0
↓ Inbound Relationships 0
All notes
Organisation notes
Non-Org notes

CIRCL › alexandre.dulaunoy@circl.lu 2 hours ago • 6/3/2024, 6:34:33 PM Organisation

Need to review the source of the information

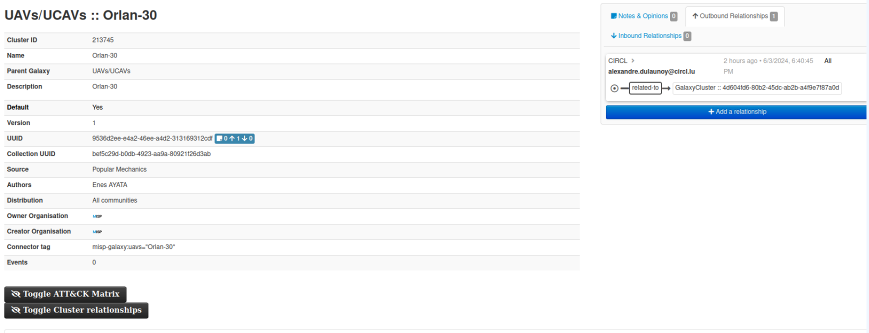
CIRCL › alexandre.dulaunoy@circl.lu 2 hours ago • 6/3/2024, 6:34:51 PM Organisation

Disagree 30 /100

Metadata are incorrect and need to be reviewed

Analyst Relationship

- 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-a4d2-313169312cdf 0 ↑ 1 ↓ 0
Collection UUID	bef5c29d-b0db-4923-aa9a-80921f26d3ab
Source	Popular Mechanics
Authors	Enes AYATA
Distribution	All communities
Owner Organisation	MISP
Creator Organisation	MISP
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

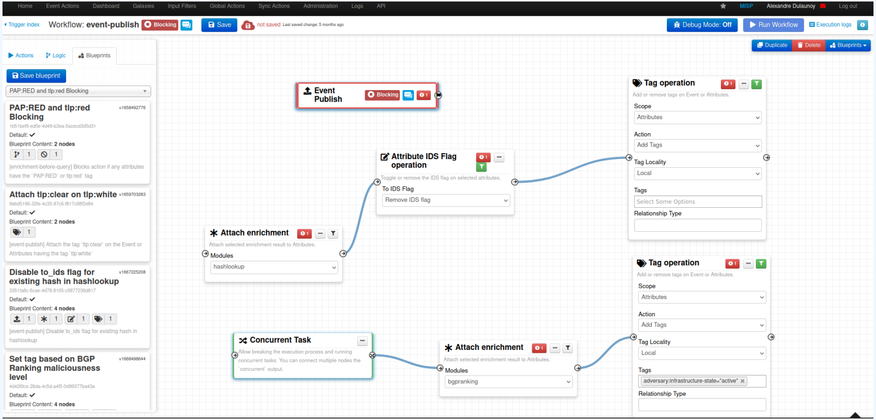
CIRCL ›
alexandre.dulaunoy@circl.lu
2 hours ago • 6/3/2024, 6:40:45 PM
All

⊙ — related-to → GalaxyCluster :: 4d604fd6-80b2-45dc-ab2b-a4f9e7f87a0d

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



Workflow: event-publish Blocking Save not saved Last saved change: 5 months ago

Save blueprint

PAP:RED and tlp:red Blocking

PAP:RED and tlp:red Blocking v1658492776
1b51bef9-ed0e-4d49-b3ea-5acecd3d5d31
Default: ✓
Blueprint Content: **2 nodes**
[enrichment-before-query] Blocks action if any attributes have the `PAP:RED` or tlp:red` tag

Attach tlp:clear on tlp:white v1659703283
9ebd5196-32fe-4c35-87c6-f817c98f2e84
Default: ✓
Blueprint Content: **2 nodes**
[event-publish] Attach the tag `tlp:clear` on the Event or Attributes having the tag `tlp:white`

Disable to_ids flag for existing hash in hashlookup v1667225208
3351fa8c-6cae-4d78-8105-c0877236d817
Default: ✓
Blueprint Content: **4 nodes**
[event-publish] Disable to_ids flag for existing hash in hashlookup

Set tag based on BGP Ranking maliciousness level v1668498644
4d426fce-26da-4c5d-a4f5-0d99377ba43a
Default: ✓
Blueprint Content: **4 nodes**

Event Publish Blocking

Attach enrichment
Attach selected enrichment result to Attributes.
Modules: hashlookup

Attribute IDS Flag operation
Toggle or remove the IDS flag on selected attributes.
To IDS Flag: Remove IDS flag

Tag operation
Add or remove tags on Event or Attributes.
Scope: Attributes
Action: Add Tags
Tag Locality: Local
Tags: Select Some Options
Relationship Type:

Concurrent Task
Allow breaking the execution process and running concurrent tasks. You can connect multiple nodes the `concurrent` output.

Attach enrichment
Attach selected enrichment result to Attributes.
Modules: bgpranking

Tag operation
Add or remove tags on Event or Attributes.
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/

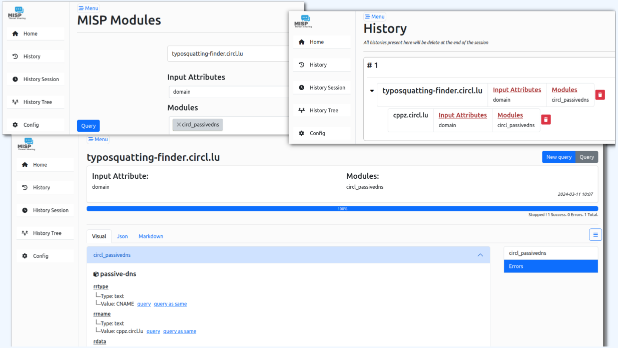
MISP Modules

- 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.



MISP Modules

typosquatting-finder.circl.lu

Input Attributes

domain

Modules

× circl_passivedns

History

All histories present here will be delete at the end of the session

1

typosquatting-finder.circl.lu | Input Attributes: domain | Modules: circl_passivedns

cppz.circl.lu | Input Attributes: domain | Modules: circl_passivedns

typosquatting-finder.circl.lu

Input Attribute: domain

Modules: circl_passivedns

2024-03-11 10:07

100%

Stopped ! 1 Success. 0 Errors. 1 Total.

circl_passivedns

passive-dns

rrtype
└Type: text
└Value: CNAME query query as same

rrname
└Type: text
└Value: cppz.circl.lu query query as same

rdata

[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**

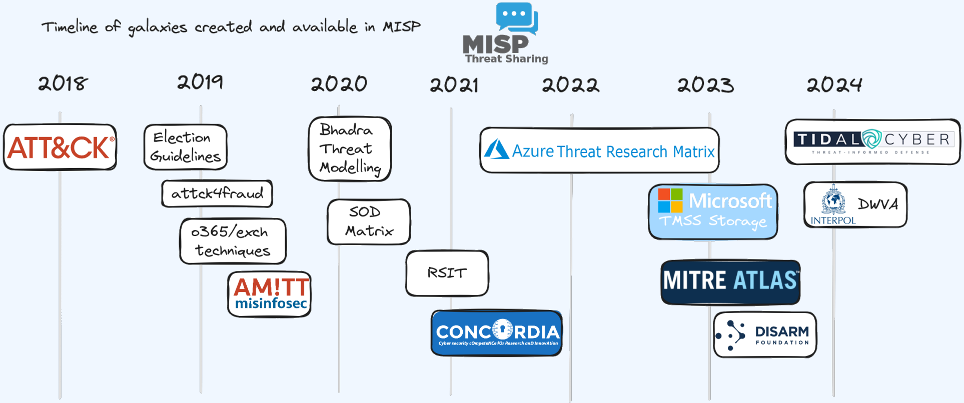
MISP GALAXY

- 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

Timeline of galaxies created and available in MISP



MISP Threat Sharing

2018

ATT&CK

2019

Election Guidelines

attck4fraud

o365/exch techniques

AM!TT misinfosec

2020

Bhadra Threat Modelling

SOD Matrix

2021

RSIT

CONCORDIA Cyber security cOmpeteNCe fOr Research anD InnovAtion

2022

Azure Threat Research Matrix

2023

Microsoft TMSS Storage

MITRE ATLAS

DISARM FOUNDATION

2024

TIDAL CYBER THREAT-INFORMED DEFENSE

INTERPOL DWVA

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

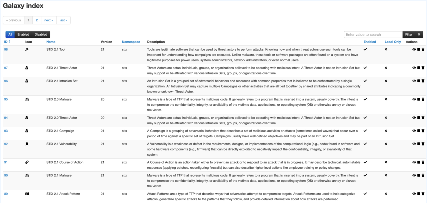
MISP STIX

- 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

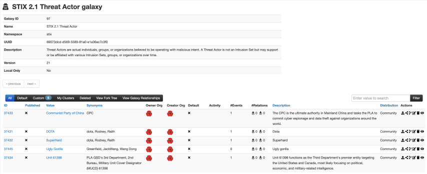
MISP STIX - Custom Galaxy Cluster Import

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



Galaxy index

ID ↑	Icon	Name	Version	Namespace	Description	Enabled	Local Only	Actions
98		STIX 2.1 Tool	21	stix	Tools are legitimate software that can be used by threat actors to perform attacks. Knowing how and when threat actors use such tools can be important for understanding how campaigns are executed. Unlike malware, these tools or software packages are often found on a system and have legitimate purposes for power users, system administrators, network administrators, or even normal users.	✓	✗	
97		STIX 2.1 Threat Actor	21	stix	Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.	✓	✗	
96		STIX 2.1 Intrusion Set	21	stix	An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor.	✓	✗	
95		STIX 2.0 Malware	20	stix	Malware is a type of TTP that represents malicious code. It generally refers to a program that is inserted into a system, usually covertly. The intent is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or otherwise annoy or disrupt the victim.	✓	✗	
94		STIX 2.0 Threat Actor	20	stix	Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.	✓	✗	
93		STIX 2.1 Campaign	21	stix	A Campaign is a grouping of adversarial behaviors that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets. Campaigns usually have well defined objectives and may be part of an Intrusion Set.	✓	✗	
92		STIX 2.1 Vulnerability	21	stix	A Vulnerability is a weakness or defect in the requirements, designs, or implementations of the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system.	✓	✗	
91		STIX 2.1 Course of Action	21	stix	A Course of Action is an action taken either to prevent an attack or to respond to an attack that is in progress. It may describe technical, automatable responses (applying patches, reconfiguring firewalls) but can also describe higher level actions like employee training or policy changes.	✓	✗	
90		STIX 2.1 Malware	21	stix	Malware is a type of TTP that represents malicious code. It generally refers to a program that is inserted into a system, usually covertly. The intent is to compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or otherwise annoy or disrupt the victim.	✓	✗	
89		STIX 2.1 Attack Pattern	21	stix	Attack Patterns are a type of TTP that describe ways that adversaries attempt to compromise targets. Attack Patterns are used to help categorize attacks, generalize specific attacks to the patterns that they follow, and provide detailed information about how attacks are performed.	✓	✗	



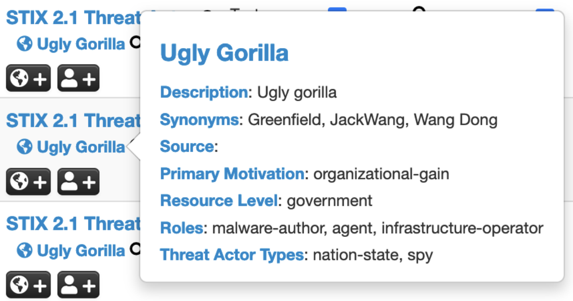
STIX 2.1 Threat Actor galaxy

Galaxy ID	97
Name	STIX 2.1 Threat Actor
Namespace	stix
UUID	69073dcd-d569-5589-81a0-e1a36ec7c3f0
Description	Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.
Version	21
Local Only	No

ID	Published	Value	Synonyms	Owner Org	Creator Org	Default	Activity	#Events	#Relations	Description	Distribution	Actions
37433	✗	Communist Party of China	CPC			✗		1	⇧ 0 ⇩ 0	The CPC is the ultimate authority in Mainland China and tasks the PLA to commit cyber espionage and data theft against organizations around the world.	Community	
37431	✗	DOTA	dota, Rodney, Raith			✗		1	⇧ 0 ⇩ 0	Dota	Community	
37432	✗	SuperHard	dota, Rodney, Raith			✗		1	⇧ 0 ⇩ 0	Superhard	Community	
37445	✗	Ugly Gorilla	Greenfield, JackWang, Wang Dong			✗		0	⇧ 0 ⇩ 0	Ugly gorilla	Community	
37434	✗	Unit 61398	PLA GSD's 3rd Department, 2nd Bureau, Military Unit Cover Designator (MUCD) 61398			✗		1	⇧ 0 ⇩ 0	Unit 61398 functions as the Third Department's premier entity targeting the United States and Canada, most likely focusing on political, economic, and military-related intelligence.	Community	

MISP stix - Custom Galaxy Cluster Import

- Extracting the complete description within the Cluster meta fields



Ugly Gorilla

Description: Ugly gorilla

Synonyms: Greenfield, JackWang, Wang Dong

Source:

Primary Motivation: organizational-gain

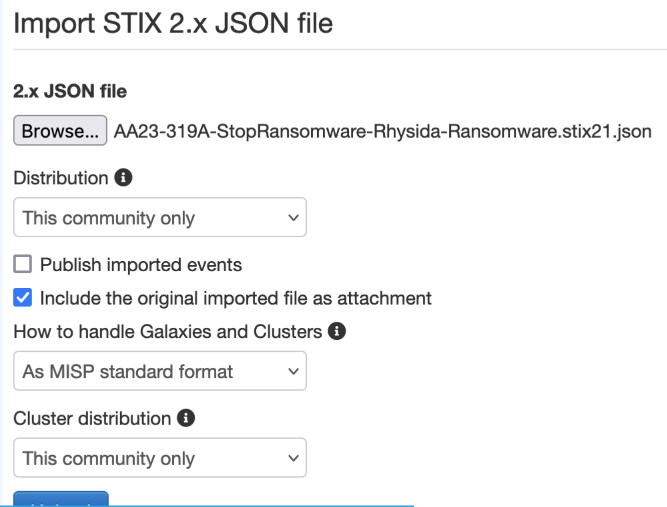
Resource Level: government

Roles: malware-author, agent, infrastructure-operator

Threat Actor Types: nation-state, spy

MISP STIX - Distribution and MISP Galaxy 2.0

- Ability to select the Clusters distribution



Import STIX 2.x JSON file

2.x JSON file

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

Distribution ℹ

This community only

□ Publish imported events

☑ Include the original imported file as attachment

How to handle Galaxies and Clusters ℹ

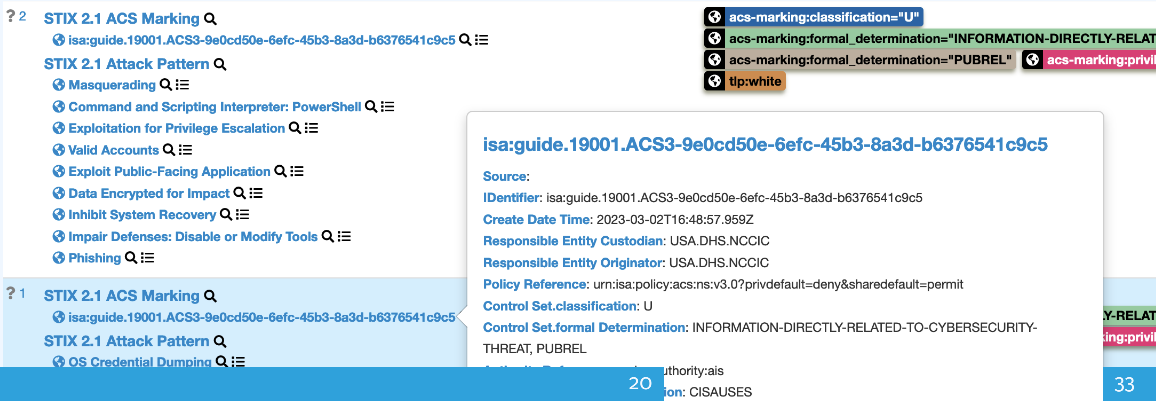
As MISP standard format

Cluster distribution ℹ

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

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

STIX 2.1 Attack Pattern

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

acs-marking:classification="U"
acs-marking:formal_determination="INFORMATION-DIRECTLY-RELAT
acs-marking:formal_determination="PUBREL"
acs-marking:privi
tlp:white

? 1 STIX 2.1 ACS Marking

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

STIX 2.1 Attack Pattern

- OS Credential Dumping

Y-RELAT
king:privi

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&sharedefault=permit
Control Set.classification: U
Control Set.formal Determination: INFORMATION-DIRECTLY-RELATED-TO-CYBERSECURITY-THREAT, PUBREL
uthority:ais
ion: CISAUSES

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

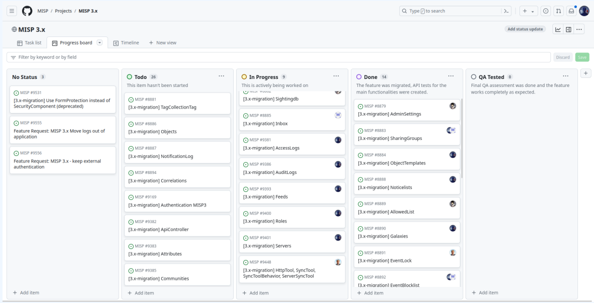
- Largest ongoing work is the work on **MISP3**
- Already announced long ago, development is now underway[11]
- New **tech stack** based on Cerebrate's advances (CakePHP 4.x+, PHP 8.2+, Bootstrap 5+)
- Longer project, will bring long needed improvements

[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]



No Status 3

- MISP #9531 — [3.x-migration] Use FormProtection instead of SecurityComponent (deprecated)
- MISP #9555 — Feature Request: MISP 3.x Move logs out of application
- MISP #9556 — Feature Request: MISP 3.x - keep external authentication

+ Add item

Todo 26

This item hasn't been started

- MISP #8881 — [3.x-migration] TagCollectionTag
- MISP #8886 — [3.x-migration] Objects
- MISP #8887 — [3.x-migration] NotificationLog
- MISP #8894 — [3.x-migration] Correlations
- MISP #9169 — [3.x-migration] Authentication MISP3
- MISP #9382 — [3.x-migration] ApiController
- MISP #9383 — [3.x-migration] Attributes
- MISP #9385 — [3.x-migration] Communities

+ Add item

In Progress 9

This is actively being worked on

- [3.x-migration] Sightingdb
- MISP #8885 — [3.x-migration] Inbox
- MISP #9381 — [3.x-migration] AccessLogs
- MISP #9386 — [3.x-migration] AuditLogs
- MISP #9393 — [3.x-migration] Feeds
- MISP #9400 — [3.x-migration] Roles
- MISP #9401 — [3.x-migration] Servers
- MISP #9448 — [3.x-migration] HttpTool, SyncTool, SyncToolBehavior, ServerSyncTool

+ Add item

Done 14

The feature was migrated, API tests for the main functionalities were created.

- MISP #8879 — [3.x-migration] AdminSettings
- MISP #8883 — [3.x-migration] SharingGroups
- MISP #8884 — [3.x-migration] ObjectTemplates
- MISP #8888 — [3.x-migration] Noticelists
- MISP #8889 — [3.x-migration] AllowedList
- MISP #8890 — [3.x-migration] Galaxies
- MISP #8891 — [3.x-migration] EventLock
- MISP #8892 — [3.x-migration] EventBlocklist

+ Add item

QA Tested 0

Final QA assessment was done and the feature works completely as expected.

+ Add item

- 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`

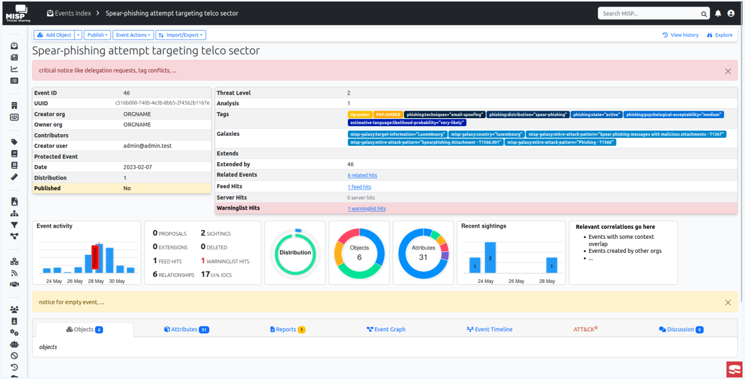
3.x - UI revamp

- **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



Spear-phishing attempt targeting telco sector

critical notice like delegation requests, tag conflicts, ...

Event ID	46
UUID	c516b000-740b-4e3b-8bb5-2f4562b1167e
Creator org	ORGNAME
Owner org	ORGNAME
Contributors	
Creator user	admin@admin.test
Protected Event	
Date	2023-02-07
Distribution	1
Published	No

Threat Level	2
Analysis	1
Tags	tlp:amber PAP:AMBER phishing:techniques="email-spoofing" phishing:distribution="spear-phishing" phishing:state="active" phishing:psychological-acceptability="medium" estimative-language:likelihood-probability="very-likely"
Galaxies	misp-galaxy:target-information="Luxembourg" misp-galaxy:country="luxembourg" misp-galaxy:mitre-attack-pattern="Spear phishing messages with malicious attachments - T1367" misp-galaxy:mitre-attack-pattern="Spearphishing Attachment - T1566.001" misp-galaxy:mitre-attack-pattern="Phishing - T1566"
Extends	
Extended by	46
Related Events	6 related hits
Feed Hits	1 feed hits
Server Hits	0 server hits
Warninglist Hits	1 warninglist hits

0 PROPOSALS
2 SIGHTINGS
0 EXTENSIONS
0 DELETED
1 FEED HITS
1 WARNINGLIST HITS
6 RELATIONSHIPS
17 55% IOCS

Relevant correlations go here

- Events with some context overlap
- Events created by other orgs
- ...

notice for empty event, ...

objects

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