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

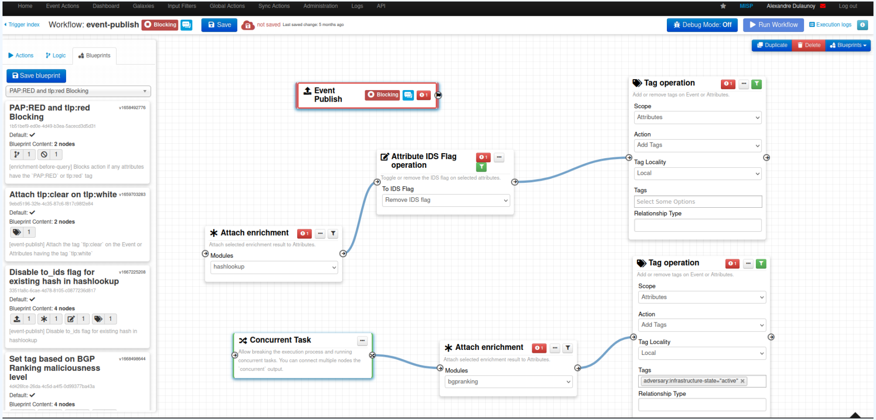
A topical listing of the new major features

- **Workflow** improvements
- **STIX 2.1** improvements along with TAXII integration
- **Freetext** import modernisation
- **Logging** and **security** improvements
- **Dashboard** rework
- **Security fixes** and other improvements

Workflows

- Continuous ongoing work
- Further addition of **logic nodes** for more advanced **branching** decision trees
- Additional **action nodes** (such as e-mailing improvements)
- The inclusion of new **triggers** based on community feedback
- **Filtered data** paths within workflows (e.g. Only execute this set of actions on a subset of the workflow's input data)

Workflows



Workflow: **event-publish**

not saved Last saved change: 5 months ago

PAP:RED and tlp:red Blocking

PAP:RED and tlp:red Blocking v1658492776
1b51bef9-ed0e-4d49-b3ea-5acecd3d5d31
Default: ✓
Blueprint Content: **2 nodes**
1 1
[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**
1
[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**
1 1 1 1
[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 1

Attach enrichment 1
Attach selected enrichment result to Attributes.
Modules: hashlookup

Attribute IDS Flag operation 1
Toggle or remove the IDS flag on selected attributes.
To IDS Flag: Remove IDS flag

Tag operation 1
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.

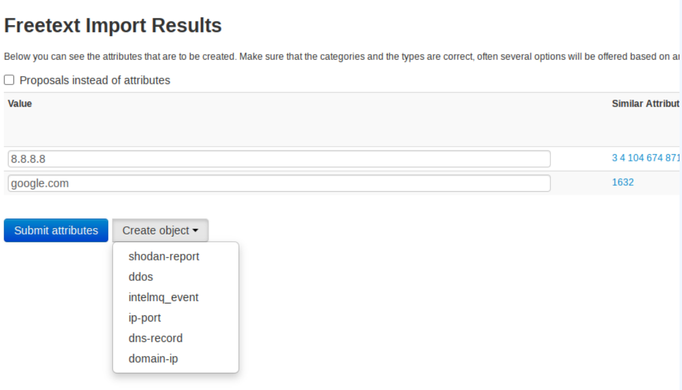
Attach enrichment 1
Attach selected enrichment result to Attributes.
Modules: bgpranking

Tag operation 1
Add or remove tags on Event or Attributes.
Scope: Attributes
Action: Add Tags
Tag Locality: Local
Tags: adversary:infrastructure-state="active" ×
Relationship Type:

Freetext import improvements

- The **freetext import** has been a powerful way of creating **attributes** parsed out of text
- Since 2.4.167, it can also be used to **create MISP objects**
- **Proposes** valid object **templates** for the given data-points
- New UI elements and parsing logic added
- Objects in general encouraged over flat attributes
- Goes hand-in-hand with new **object template** development

Freetext import improvements



Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on a

□ Proposals instead of attributes

Value	Similar Attribut
8.8.8.8	3 4 104 674 871
google.com	1632

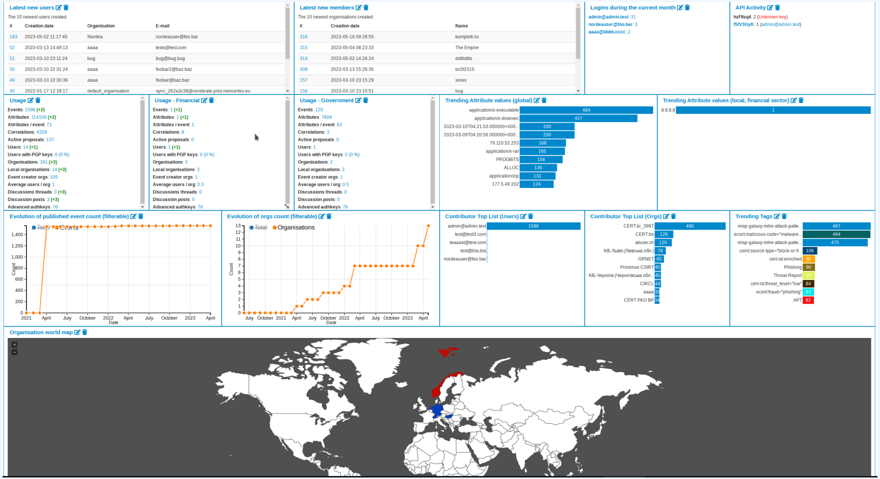
Logging rework

- **Logging concerns separated** into optional separate mechanisms
  - Separate Application, Audit, Access logs (thanks to Jakub Onderka)
- New user sanity checks on **prior authentications** and **associated IPs** (thanks to Christophe Vandeplas)
  - Allows users to audit their accounts' actions to catch abuse
- New internal logging of **authentication frequency**

Dashboard rework

- **Overhaul** of the **widget toolkit** for instance visibility
- New widgets to highlight **trends, community interactions and statistics**
- Focus on **customisation** and **bucketing** of organisation groups
  - Use Organisation meta-data, such as country, sector, org type
- Better defined **reporting periods**
  - Show data of current day, month, year or since an arbitrary date
- Rework of some existing widgets to be much more **performant**

Dashboard example



Latest new users

The 10 newest users created

#	Creation date	Organisation	E-mail
183	2023-05-02 11:17:45	Nordea	nordeauser@foo.bar
52	2023-03-13 14:49:13	aaaa	tests@test.com
51	2023-03-10 23:11:24	bug	bug@bug.bug
50	2023-03-10 22:31:24	aaaa	foobar2@baz.baz
49	2023-03-10 22:30:36	aaaa	foobar@baz.baz
45	2022-01-17 12:18:17	default_organisation	sync_262a3c38@cerebrate.pilot.melicertes.eu

Latest new members

The 10 newest organisations created

#	Creation date	Name
316	2023-05-16 09:28:55	komplett.no
315	2023-05-04 08:23:33	The Empire
314	2023-05-02 14:26:24	dsfdsfds
308	2023-03-13 15:26:35	bc5f2315
157	2023-03-10 23:15:29	xxxxx
156	2023-03-10 23:10:51	bug

Logins during the current month

admin@admin.test: 31
nordeauser@foo.bar: 3
aaaa@bbbb.cccc: 2

API Activity

hzFIlsq4: 2 (Unknown key)
f5fV3GyK: 1 (admin@admin.test)

Usage

Events: 1596 (+2)
Attributes: 114100 (+2)
Attributes / event: 71
Correlations: 6328
Active proposals: 137
Users: 14 (+1)
Users with PGP keys: 0 (0 %)
Organisations: 161 (+3)
Local organisations: 14 (+3)
Event creator orgs: 105
Average users / org: 1
Discussions threads: 3 (+3)
Discussion posts: 3 (+3)
Advanced authkeys: 76

Usage - Financial

Events: 1 (+1)
Attributes: 1 (+1)
Attributes / event: 1
Correlations: 8
Active proposals: 0
Users: 1 (+1)
Users with PGP keys: 0 (0 %)
Organisations: 3
Local organisations: 3
Event creator orgs: 1
Average users / org: 0.3
Discussions threads: 0
Discussion posts: 0
Advanced authkeys: 76

Usage - Government

Events: 120
Attributes: 7604
Attributes / event: 63
Correlations: 3
Active proposals: 0
Users: 1
Users with PGP keys: 0 (0 %)
Organisations: 2
Local organisations: 2
Event creator orgs: 1
Average users / org: 0.5
Discussions threads: 0
Discussion posts: 0
Advanced authkeys: 76

Trending Attribute values (global)

application/x-executable 484
application/x-dosexec 427
2023-03-10T04:21:03.000000+000... 200
2023-03-09T04:20:56.000000+000... 200
79.110.52.253 168
application/x-rar 165
PROGBITS 156
ALLOC 136
application/zip 131
177.5.49.202 124

Trending Attribute values (local, financial sector)

Evolution of published event count (filterable)

Evolution of orgs count (filterable)

Contributor Top List (Users)

Contributor Top List (Orgs)

Trending Tags

misp-galaxy:mitre-attack-patte... 497
ecsirt:malicious-code="malware... 494
misp-galaxy:mitre-attack-patte... 475
osint:source-type="block-or-fi... 106
cert-ist:enriched 90
Phishing 90
Threat-Report 89
cert-ist:threat_level="low" 84
ecsirt:fraud="phishing" 83
APT 82

Organisation world map

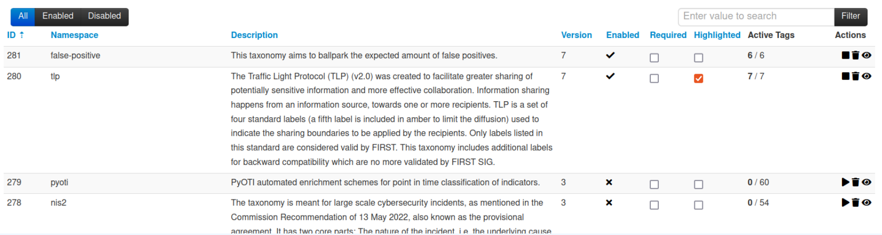
Security fixes and other improvements

- Long list of security fixes based on multiple external penetration tests
- **CVEs**[1] continuously reported for issues small and large
  - Make sure you're up to date!
- **Zigrin security**'s research funded by the **Luxembourg army** has been a massive help
- Long list of other improvements, quality of life changes, performance tuning

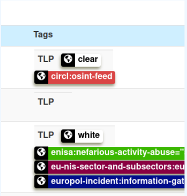
[1] `https://www.misp-project.org/security/`

Taxonomy highlight

- Many different taxonomies are used frequently in various organisations
- A new feature to highlight the important taxonomy in a MISP instance (community) is available
- Site admin user can select the **highlighted taxonomies**
- The taxonomy namespace will be highlight in a box on the index/event views



ID ⇡	Namespace	Description	Version	Enabled	Required	Highlighted	Active Tags	Actions
281	false-positive	This taxonomy aims to ballpark the expected amount of false positives.	7	✓	□	□	6 / 6	■ 🗑 👁
280	tlp	The Traffic Light Protocol (TLP) (v2.0) was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information sharing happens from an information source, towards one or more recipients. TLP is a set of four standard labels (a fifth label is included in amber to limit the diffusion) used to indicate the sharing boundaries to be applied by the recipients. Only labels listed in this standard are considered valid by FIRST. This taxonomy includes additional labels for backward compatibility which are no more validated by FIRST SIG.	7	✓	□	☑	7 / 7	■ 🗑 👁
279	pyoti	PyOTI automated enrichment schemes for point in time classification of indicators.	3	×	□	□	0 / 60	▶ 🗑 👁
278	nis2	The taxonomy is meant for large scale cybersecurity incidents, as mentioned in the Commission Recommendation of 13 May 2022, also known as the provisional agreement. It has two core parts: The nature of the incident, i.e. the underlying cause	3	×	□	□	0 / 54	▶ 🗑 👁



Tags
TLP clear circl:osint-feed
TLP
TLP white enisa:nefarious-activity-abuse=" eu-nis-sector-and-subsectors:eu europol-incident:information-gat

MISP modules

- MISP modules are companion to expansion, export, import for external services or tooling
- Extended to support the **MISP workflow actions**
- New modules include new import **extract_url_components**
- New expansion modules include **Crowdsec**, **ipinfo.io**
- Improved expansion modules **greynoise**, **VarIOT**
- Improved modules to support the MISP standard format

MISP TAXONOMIES

- 149 ready-to-use are now available in MISP taxonomies (used in MISP and many other tools)
- New **information-origin** taxonomy to classify AI-generated content with LLMs
- New **aviation** taxonomy developed by Eurocontrol to support labelling in the aviation sector
- New Microsoft **sentinel** taxonomy to support the MISP sentinel integration developed by Koen Van Impe
- Various fixes and improvement to taxonomies (e.g. the dark-web taxonomy due to updates in AIL 5.0)

MISP warning-lists

- New **captive-portal** warning-list added
- New known **parking page infrastructure** warning-list added
- New **google-chrome-crux-1million** warning-list added
- New **microsoft-azure-appid** warning-list added

MISP GALAXY

- New **sigma** galaxy added including relationships
- Latest MITRE ATT&CK version 13 updated for the MISP galaxy
- New microsoft threat actor taxonomy added including relationships with previous activity group and **threat-actor galaxy**
- Alignment of **ransomware galaxy** with the **ransomlook.io** project
- Major improvements in threat-actor galaxy including relationships with other galaxy clusters

MISP objects

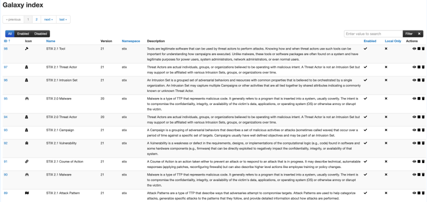
MISP STIX

- misp-stix[2] 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

[2] 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



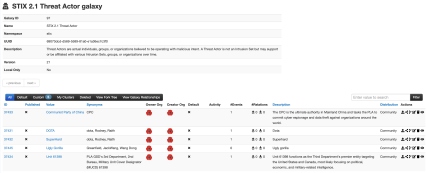
Galaxy index

« previous | 1 | 2 | next » | last »

All | Enabled | Disabled

Enter value to search | Filter | ✗

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

« previous | next »

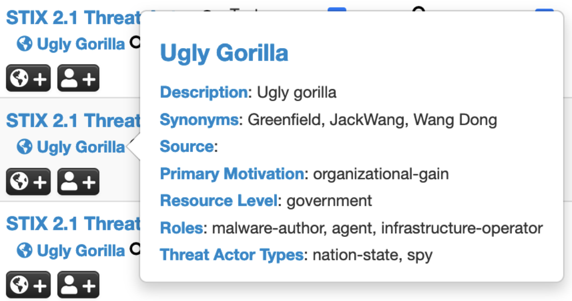
All | Default | Custom 5 | My Clusters | Deleted | View Fork Tree | View Galaxy Relationships

Enter value to search | Filter

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



STIX 2.1 Threat

Ugly Gorilla

STIX 2.1 Threat

Ugly Gorilla

STIX 2.1 Threat

Ugly Gorilla

Ugly Gorilla

Description: Ugly gorilla

Synonyms: Greenfield, JackWang, Wang Dong

Source:

Primary Motivation: organizational-gain

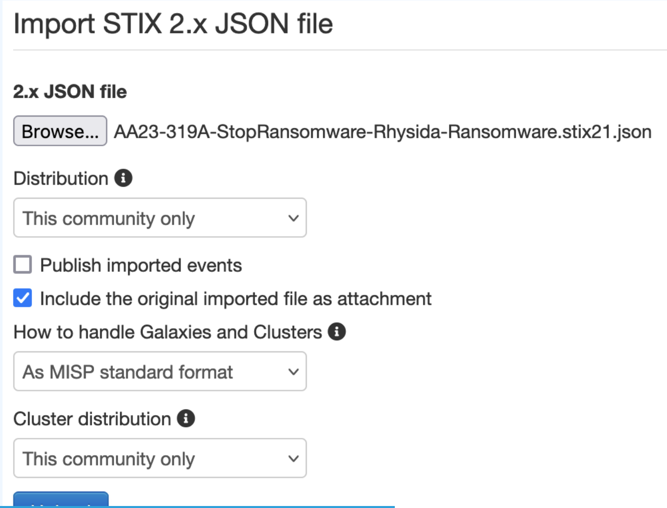
Resource Level: government

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

This community only

□ Publish imported events

☑ Include the original imported file as attachment

How to handle Galaxies and Clusters

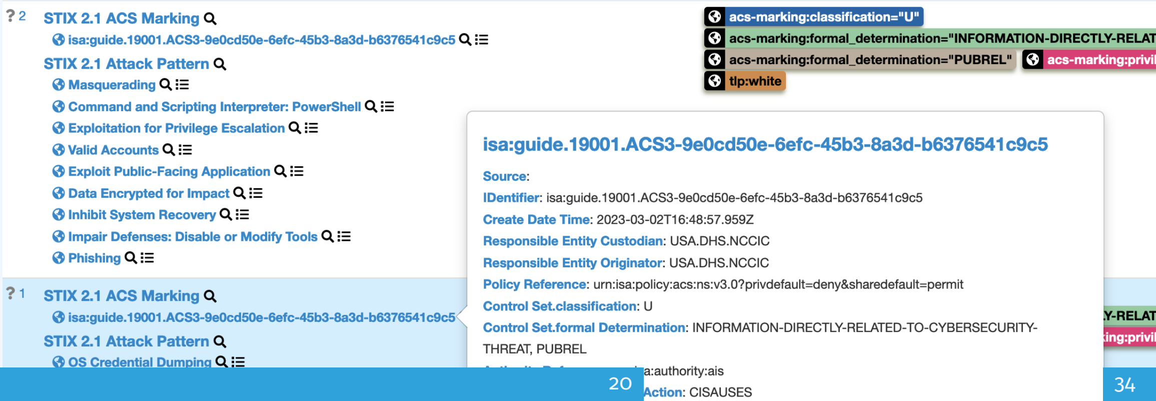
As MISP standard format

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
- 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:privil
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:privil

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

a:authority:ais

Action: 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

- New documentation for Cerebrate[3]
- Many **improvements and bugs fixed** following the feedback of different organisations deploying Cerebrate
- Deployment of the **PoC for NATO users is ongoing**
- Software stack of MISP 3 is tested on Cerebrate

[3] https://doc.cerebrate-project.org/

Ongoing rework

MISP 3

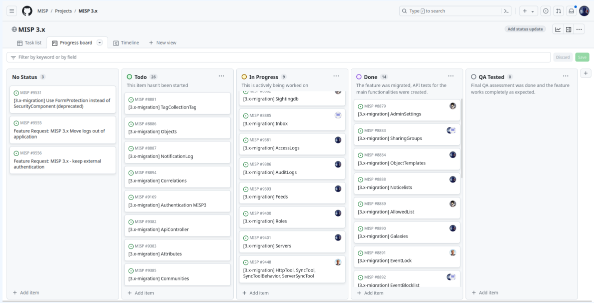
- Largest ongoing work is the work on **MISP3**
- Already announced long ago, development is now underway[4]
- New **tech stack** based on Cerebrate's advances (CakePHP 4.x+, PHP 8.2+, Bootstrap 5+)
- Longer project, will bring long needed improvements

[4] 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[5]



MISP / Projects / MISP 3.x

Type / to search

MISP 3.x

Add status update

Task list | Progress board | Timeline | + New view

Filter by keyword or by field

Discard | Save

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**

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

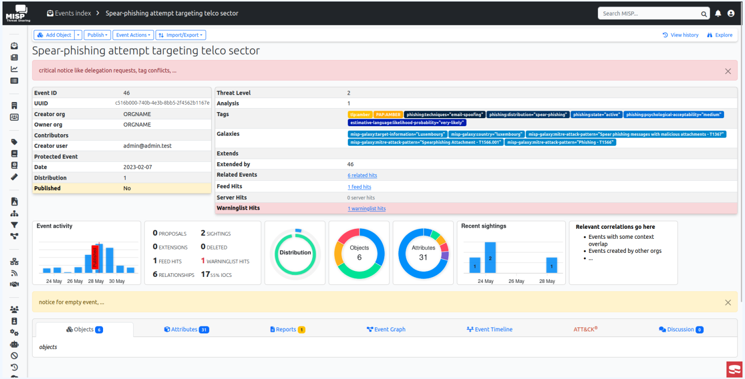
3.x - UI REVAMP

- **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 PLAYBOOKS

- A new project called MISP playbooks[6] has started
- MISP playbooks address **common use-cases** encountereted by **SOCs, CSIRTs and CTI teams**
- Covering all the activity such **detecting, reacting and analysing**
- Documentation in Markdown format and code in Python all in **Jupyter notebooks**

[6] https://www.github.com/MISP/misp-playbooks

MISP GUARD

- misp-guard[7] is a mitmproxy addon that inspects the synchronization traffic (via PUSH or PULL) between different MISP instances and applies a set of customizable rules defined in a JSON file
- **Simple code base for doing complementary filtering** between different MISPs for sensitive or classified networks
- misp-guard doesn’t depend on MISP to apply the filtering
- Next step code review and evaluate the different option for certification (ideas are welcome)

[7] https://github.com/MISP/misp-guard

Conclusions

To sum it all up...

- The MISP **developer/contributor community** continues to grow and is very active
- The main focus the past year was on the following
  - Performance, security, UX improvements
  - Customisations of workflow processes
  - Better operationalisation of MISP (community management, integration, monitoring)
  - Fleshing out the documentation and supporting materials
- Cerebrate is aiming to fill the void of community/fleet management that we currently have
- Definitely no lack of new ideas and improvements, if you want to participate, it's easy to **get involved**
- Prioritisation is hard. **Let us know what you think we should focus on**!

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