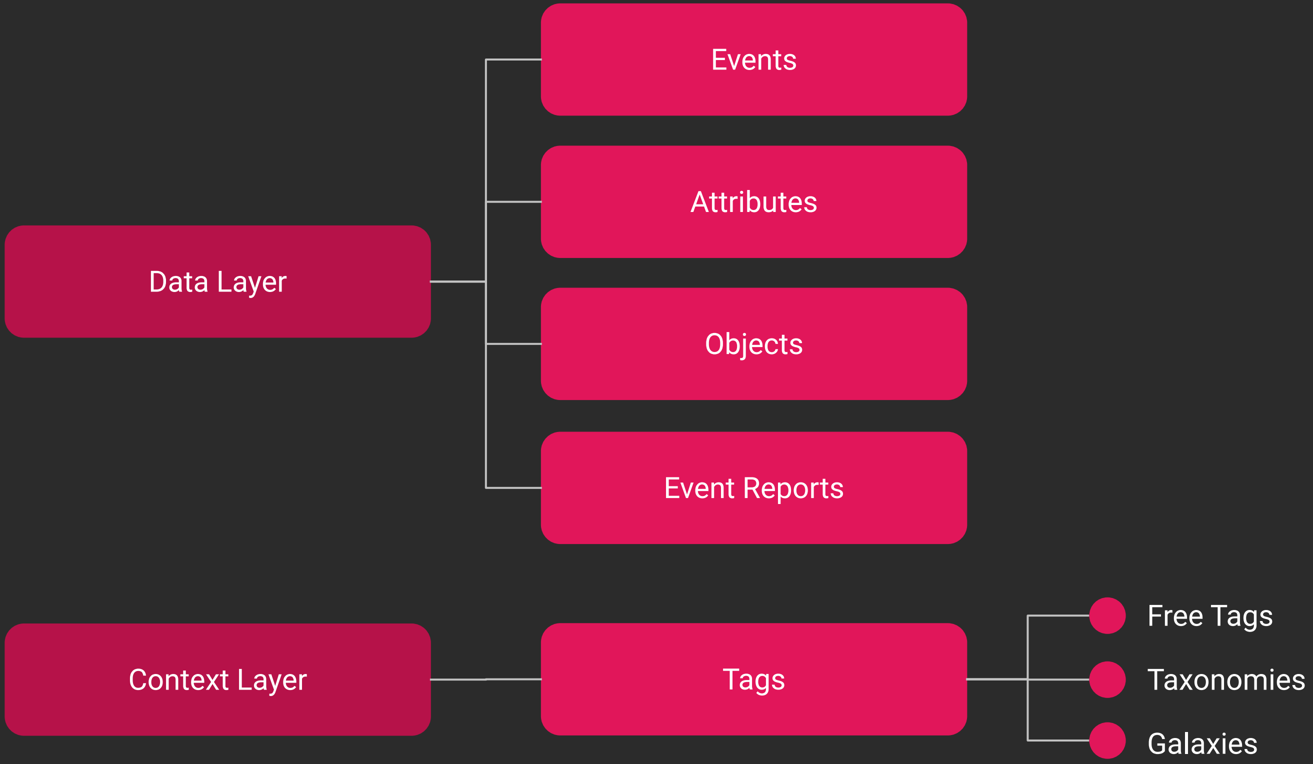
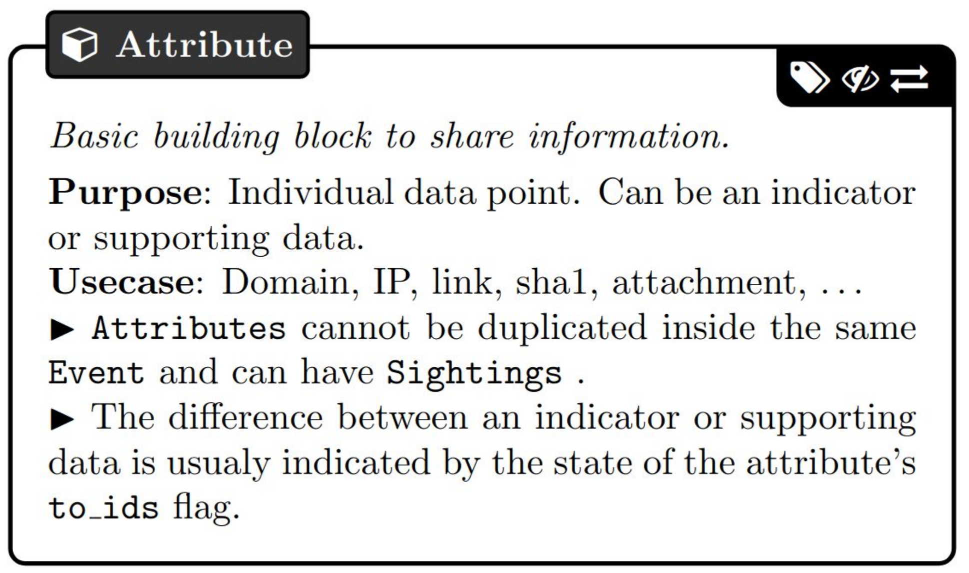
MISP Data model overview

Type of Data model



Data Layer

MISP Attributes



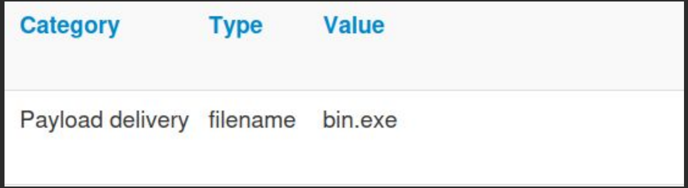
Attribute

Basic building block to share information.

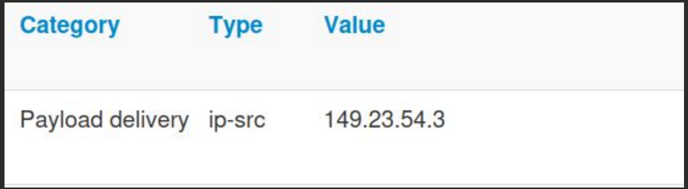
Purpose: Individual data point. Can be an indicator or supporting data.

Usecase: Domain, IP, link, sha1, attachment, . . .

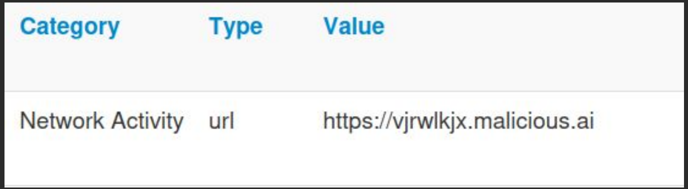
- `Attributes` cannot be duplicated inside the same `Event` and can have `Sightings` .
- The difference between an indicator or supporting data is usualy indicated by the state of the attribute's `to_ids` flag.



Category	Type	Value
Payload delivery	filename	bin.exe

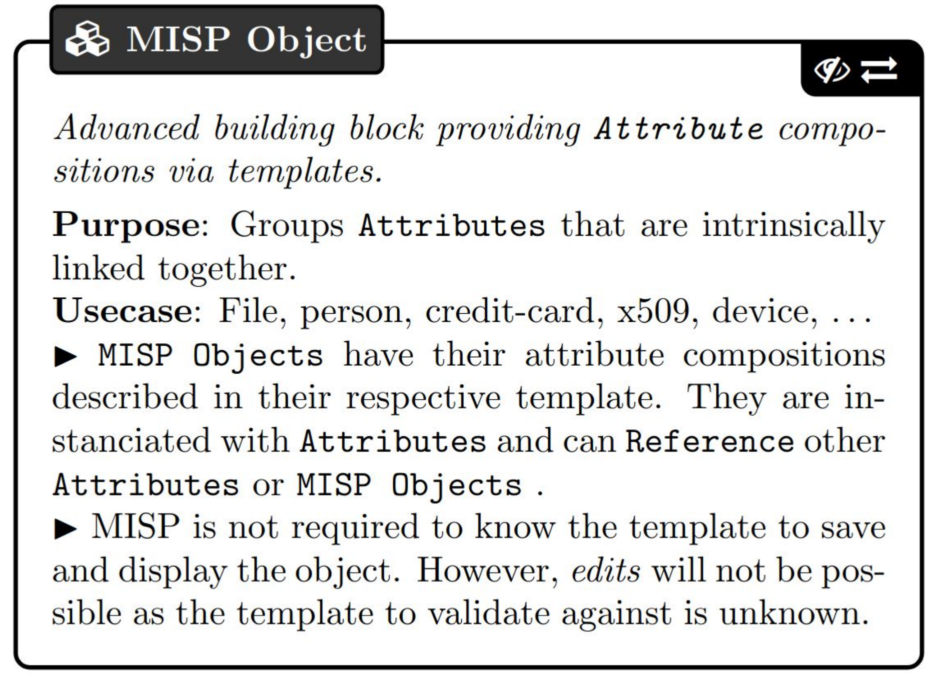


Category	Type	Value
Payload delivery	ip-src	149.23.54.3



Category	Type	Value
Network Activity	url	https://vjrwlkjx.malicious.ai

MISP Objects



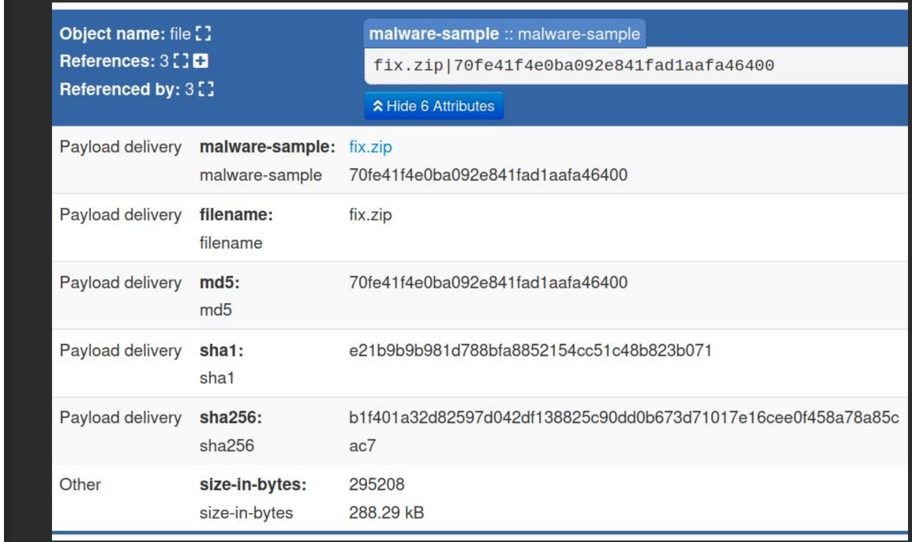
MISP Object

Advanced building block providing **`Attribute`** *compositions via templates.*

Purpose: Groups **`Attributes`** that are intrinsically linked together.

Usecase: File, person, credit-card, x509, device, . . .

- ▶ `MISP Objects` have their attribute compositions described in their respective template. They are instanciated with **`Attributes`** and can **`Reference`** other **`Attributes`** or `MISP Objects` .
- ▶ MISP is not required to know the template to save and display the object. However, *edits* will not be possible as the template to validate against is unknown.



Object name: file
References: 3
Referenced by: 3

malware-sample :: malware-sample

`fix.zip|70fe41f4e0ba092e841fad1aafa46400`

Payload delivery	**malware-sample:** malware-sample	fix.zip 70fe41f4e0ba092e841fad1aafa46400
Payload delivery	**filename:** filename	fix.zip
Payload delivery	**md5:** md5	70fe41f4e0ba092e841fad1aafa46400
Payload delivery	**sha1:** sha1	e21b9b9b981d788bfa8852154cc51c48b823b071
Payload delivery	**sha256:** sha256	b1f401a32d82597d042df138825c90dd0b673d71017e16cee0f458a78a85c ac7
Other	**size-in-bytes:** size-in-bytes	295208 288.29 kB

MISP Events

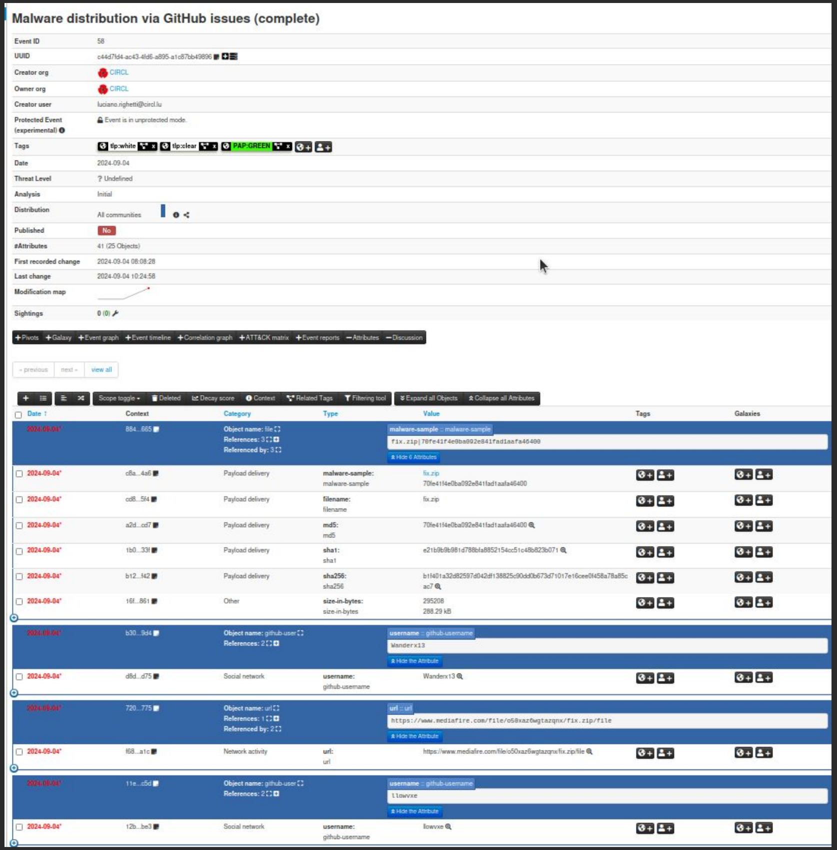
Event

Encapsulations for contextually linked information.

Purpose: Group datapoints and context together. Acting as an envelop, it allows setting distribution and sharing rules for itself and its children.

Usecase: Encode incidents/events/reports/...

- Events can contain other elements such as `Attributes` , `MISP Objects` and `Event Reports` .
- The distribution level and any context added on an `Event` (such as `Taxonomies`) are propagated to its underlying data.

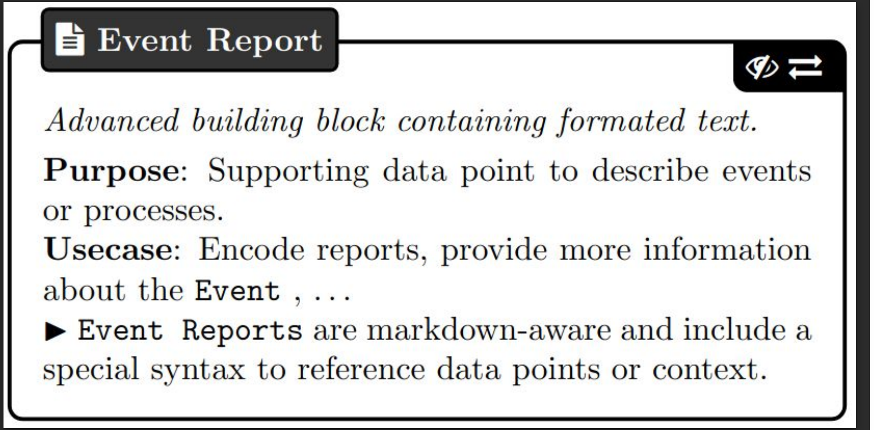


Malware distribution via GitHub issues (complete)

Event ID	58
UUID	c44d7fd4-ac43-4fd6-a895-a1c87bb49896
Creator org	CIRCL
Owner org	CIRCL
Creator user	luciano.righetti@circl.lu
Protected Event (experimental)	Event is in unprotected mode.
Tags	tlp:white x tlp:clear x PAP:GREEN x
Date	2024-09-04
Threat Level	? Undefined
Analysis	Initial
Distribution	All communities
Published	No
#Attributes	41 (25 Objects)
First recorded change	2024-09-04 08:08:28
Last change	2024-09-04 10:24:58
Modification map	
Sighting	0 (0)

Date ↑	Context	Category	Type	Value	Tags	Galaxies
2024-09-04*	884...665	Object name: file References: 3 Referenced by: 3		malware-sample :: malware-sample fix.zip|70fe41f4e0ba092e841fad1aafa46400 Hide 6 Attributes		
2024-09-04*	c8a...4a6	Payload delivery	malware-sample: malware-sample	fix.zip 70fe41f4e0ba092e841fad1aafa46400		
2024-09-04*	cd8...5f4	Payload delivery	filename: filename	fix.zip		
2024-09-04*	a2d...cd7	Payload delivery	md5: md5	70fe41f4e0ba092e841fad1aafa46400		
2024-09-04*	1b0...33f	Payload delivery	sha1: sha1	e21b9b9b981d788bfa8852154cc51c48b823b071		
2024-09-04*	b12...f42	Payload delivery	sha256: sha256	b1f401a32d82597d042df138825c90dd0b673d71017e16cee0f458a78a85cac7		
2024-09-04*	16f...861	Other	size-in-bytes: size-in-bytes	295208 288.29 kB		
2024-09-04*	b30...9d4	Object name: github-user References: 2		username :: github-username Wanderx13 Hide the Attribute		
2024-09-04*	d8d...d75	Social network	username: github-username	Wanderx13		
2024-09-04*	720...775	Object name: url References: 1 Referenced by: 2		url :: url https://www.mediafire.com/file/o50xaz6wgtazqnx/fix.zip/file Hide the Attribute		
2024-09-04*	f68...a1c	Network activity	url: url	https://www.mediafire.com/file/o50xaz6wgtazqnx/fix.zip/file		
2024-09-04*	11e...c5d	Object name: github-user References: 2		username :: github-username llowvxe Hide the Attribute		
2024-09-04*	12b...be3	Social network	username: github-username	llowvxe		

MISP Event Report



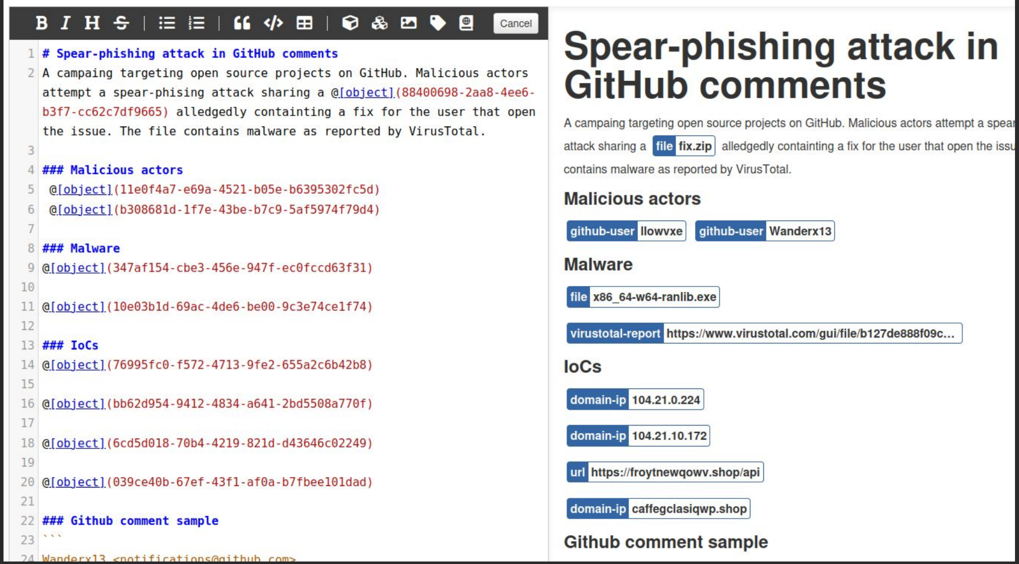
Event Report

Advanced building block containing formated text.

Purpose: Supporting data point to describe events or processes.

Usecase: Encode reports, provide more information about the `Event` , . . .

▶ `Event Reports` are markdown-aware and include a special syntax to reference data points or context.



~~~
# Spear-phishing attack in GitHub comments
A campaing targeting open source projects on GitHub. Malicious actors attempt a spear-phising attack sharing a @[object](88400698-2aa8-4ee6-b3f7-cc62c7df9665) alledgedly containting a fix for the user that open the issue. The file contains malware as reported by VirusTotal.

### Malicious actors
 @[object](11e0f4a7-e69a-4521-b05e-b6395302fc5d)
 @[object](b308681d-1f7e-43be-b7c9-5af5974f79d4)

### Malware
@[object](347af154-cbe3-456e-947f-ec0fccd63f31)

@[object](10e03b1d-69ac-4de6-be00-9c3e74ce1f74)

### IoCs
@[object](76995fc0-f572-4713-9fe2-655a2c6b42b8)

@[object](bb62d954-9412-4834-a641-2bd5508a770f)

@[object](6cd5d018-70b4-4219-821d-d43646c02249)

@[object](039ce40b-67ef-43f1-af0a-b7fbee101dad)

### Github comment sample
```
Wanderx13 <notifications@github.com>
~~~

Spear-phishing attack in GitHub comments

A campaing targeting open source projects on GitHub. Malicious actors attempt a spear
attack sharing a file fix.zip alledgedly containting a fix for the user that open the issu
contains malware as reported by VirusTotal.

Malicious actors

github-user llowvxe github-user Wanderx13

Malware

file x86_64-w64-ranlib.exe

virustotal-report https://www.virustotal.com/gui/file/b127de888f09c...

IoCs

domain-ip 104.21.0.224

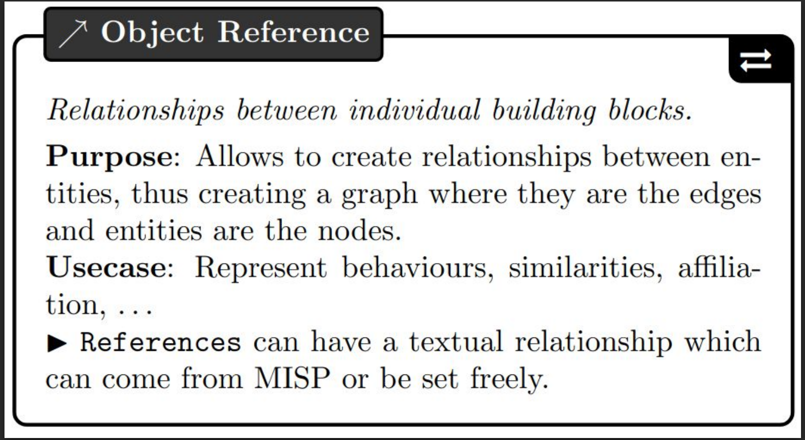
domain-ip 104.21.10.172

url https://froytnewqowv.shop/api

domain-ip caffegclasiqwp.shop

Github comment sample

Object Reference



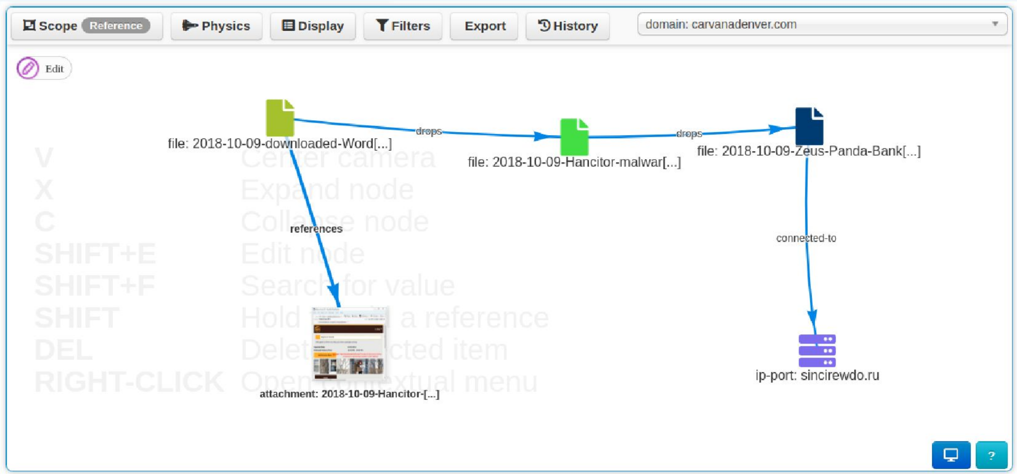
↗ Object Reference ⇄

Relationships between individual building blocks.

Purpose: Allows to create relationships between entities, thus creating a graph where they are the edges and entities are the nodes.

Usecase: Represent behaviours, similarities, affiliation, ...

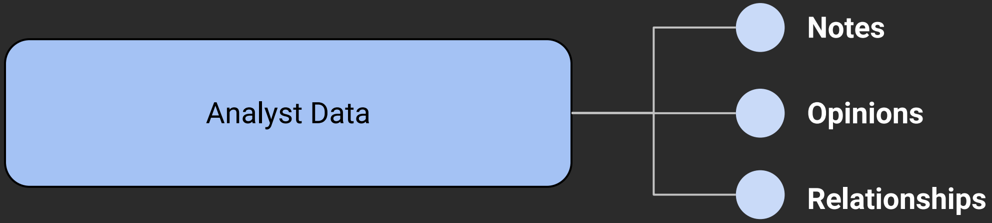
- ▶ `References` can have a textual relationship which can come from MISP or be set freely.

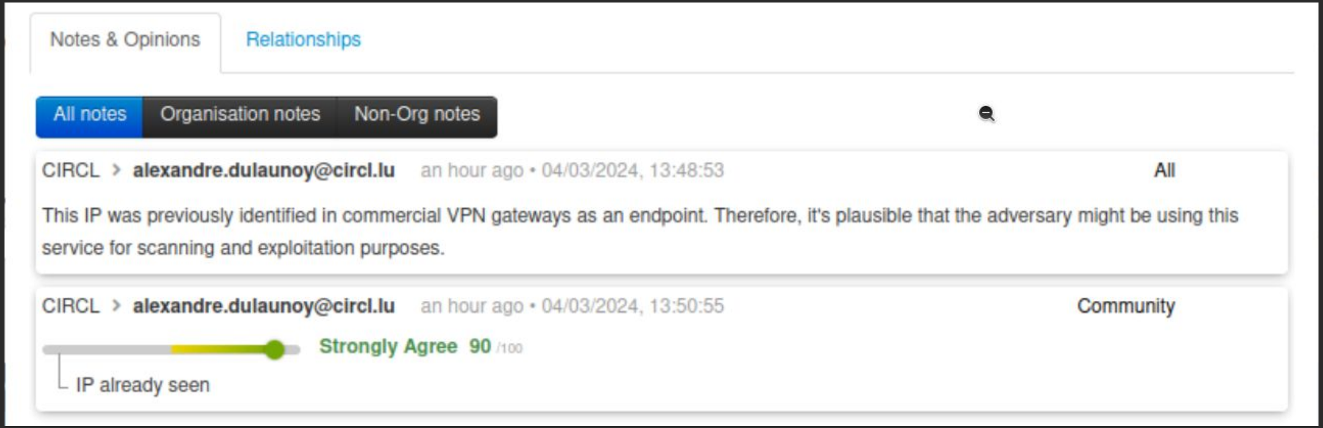


Scope
Reference
Physics
Display
Filters
Export
History
domain: carvanadenver.com
Edit
file: 2018-10-09-downloaded-Word[...]
drops
file: 2018-10-09-Hancitor-malwar[...]
drops
file: 2018-10-09-Zeus-Panda-Bank[...]
references
connected-to
attachment: 2018-10-09-Hancitor-[...]
ip-port: sincirewdo.ru
?

V	Center camera
X	Expand node
C	Collapse node
SHIFT+E	Edit node
SHIFT+F	Search for value
SHIFT	Hold [illegible] a reference
DEL	Delete selected item
RIGHT-CLICK	Open contextual menu

Analyst Data





CIRCL › **alexandre.dulaunoy@circl.lu** an hour ago • 04/03/2024, 13:48:53 All

This IP was previously identified in commercial VPN gateways as an endpoint. Therefore, it's plausible that the adversary might be using this service for scanning and exploitation purposes.

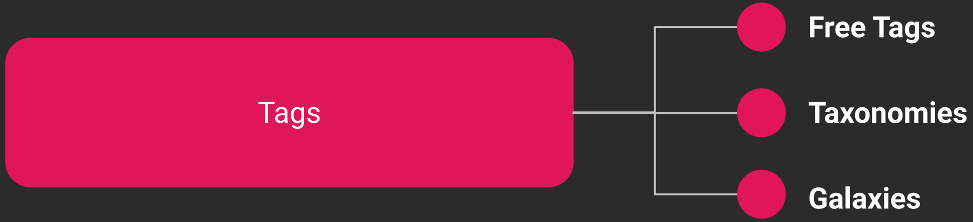
CIRCL › **alexandre.dulaunoy@circl.lu** an hour ago • 04/03/2024, 13:50:55 Community

Strongly Agree 90 /100

└ IP already seen

Context Layer

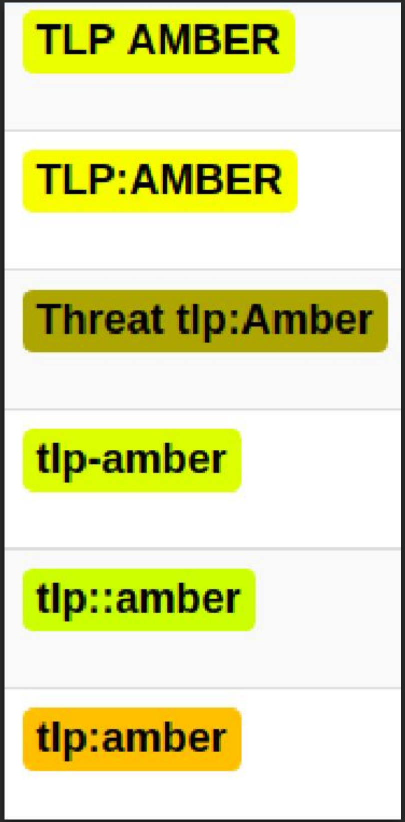
Tags



- **Free Tags**: Label where the text can be set without restriction
- **Taxonomies**: Normalized classification to express the same vocabulary
- **Galaxies**: Normalized classification boosted by meta-data

Free Tags

- Label where the text can be set without restriction
- Simplest form of contextualization
- Can make automation and understanding difficult



TLP AMBER

TLP:AMBER

Threat tlp:Amber

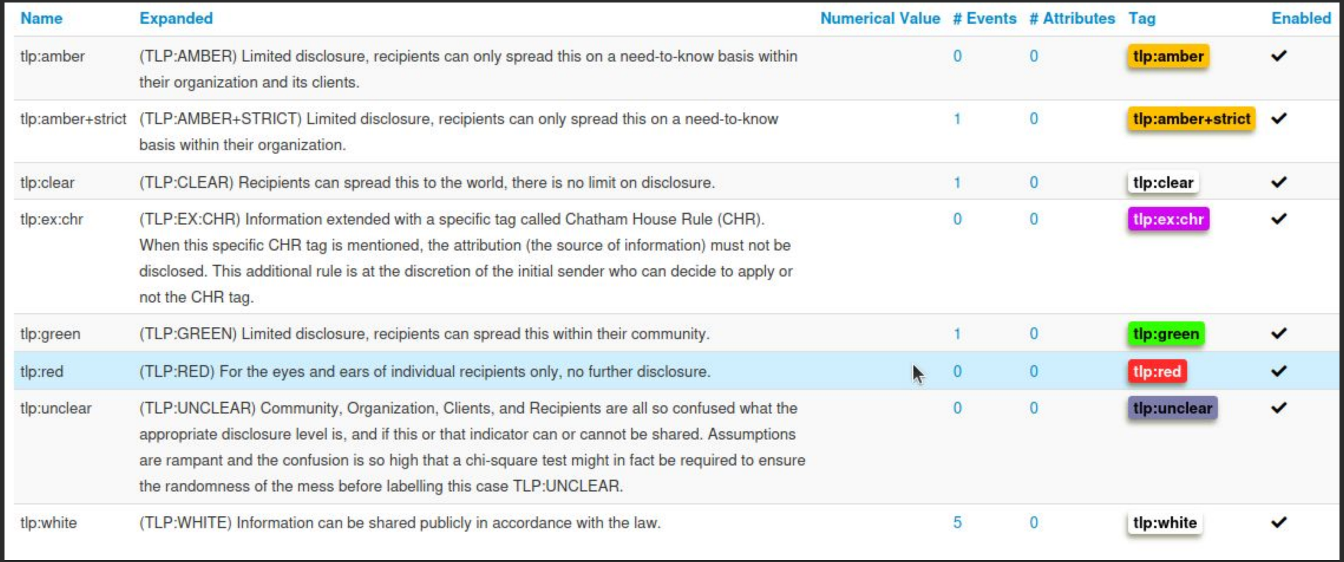
tlp-amber

tlp::amber

tlp:amber

Taxonomies

- Simple label standardised on common set of vocabularies
- Efficient classification globally understood
- Ease consumption and automation



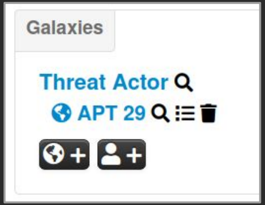
Name	Expanded	Numerical Value	# Events	# Attributes	Tag	Enabled
tlp:amber	(TLP:AMBER) Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.		0	0	tlp:amber	✓
tlp:amber+strict	(TLP:AMBER+STRICT) Limited disclosure, recipients can only spread this on a need-to-know basis within their organization.		1	0	tlp:amber+strict	✓
tlp:clear	(TLP:CLEAR) Recipients can spread this to the world, there is no limit on disclosure.		1	0	tlp:clear	✓
tlp:ex:chr	(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.		0	0	tlp:ex:chr	✓
tlp:green	(TLP:GREEN) Limited disclosure, recipients can spread this within their community.		1	0	tlp:green	✓
tlp:red	(TLP:RED) For the eyes and ears of individual recipients only, no further disclosure.		0	0	tlp:red	✓
tlp:unclear	(TLP:UNCLEAR) Community, Organization, Clients, and Recipients are all so confused what the appropriate disclosure level is, and if this or that indicator can or cannot be shared. Assumptions are rampant and the confusion is so high that a chi-square test might in fact be required to ensure the randomness of the mess before labelling this case TLP:UNCLEAR.		0	0	tlp:unclear	✓
tlp:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.		5	0	tlp:white	✓

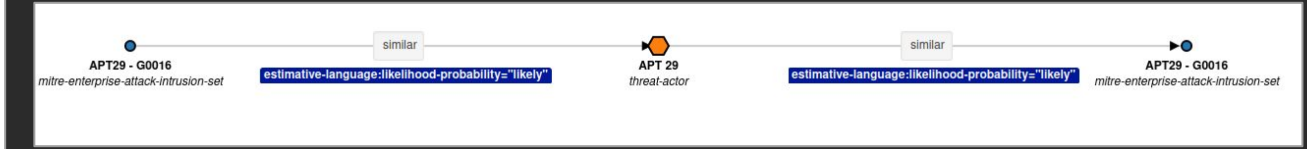
MISP Galaxies & Clusters

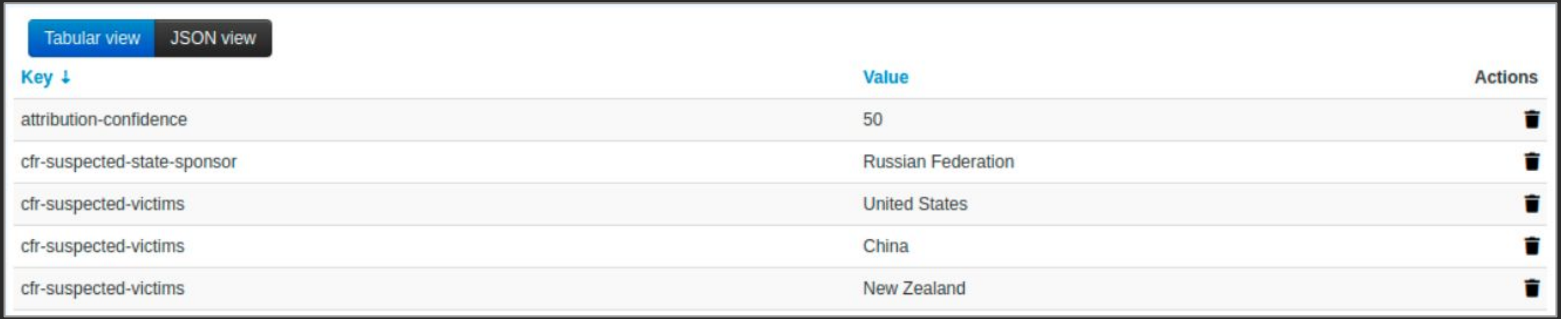
- **Galaxies** = Collection, **Cluster** = Item in the Collection

Example: Country Luxembourg

- Normalized classification boosted by meta-data
- Enable description of complex high-level information
- Supports relationships to other Clusters




APT29 - G0016
mitre-enterprise-attack-intrusion-set
similar
estimative-language:likelihood-probability="likely"
APT 29
threat-actor
similar
estimative-language:likelihood-probability="likely"
APT29 - G0016
mitre-enterprise-attack-intrusion-set



Key ↓	Value	Actions
attribution-confidence	50	🗑
cfr-suspected-state-sponsor	Russian Federation	🗑
cfr-suspected-victims	United States	🗑
cfr-suspected-victims	China	🗑
cfr-suspected-victims	New Zealand	🗑

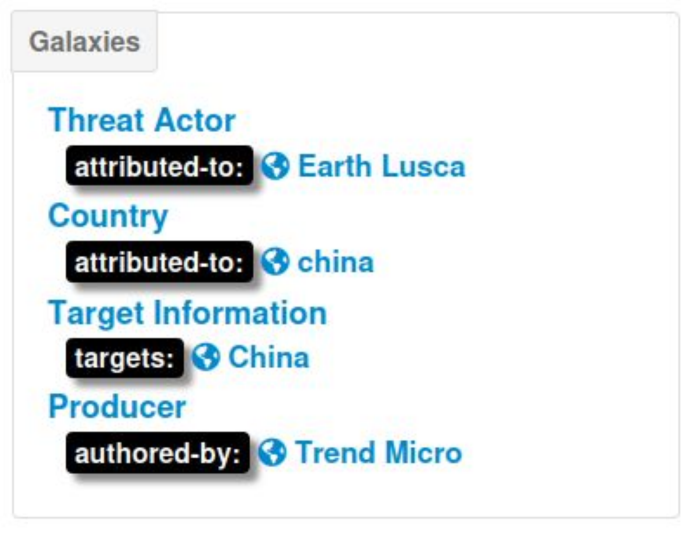
Galaxies VS Taxonomies

Taxonomies	Galaxies
Normalized Classification	
Self-explanatory	Describe high-level information
Used for Categorization	Provide Contextual Information

Examples	
● TLP / PAP ● adversary ● phishing ● false-positive	● Country ● Threat Actors ● MITRE ATT&CK ● Malpedia / MoTIF / Tidal

Tag Usage

- Tags can be attached on many elements:
  - Events, Attributes, …
- Tags can have a **Relationship Verb**
- Tags can be **Global** or **Local**



Galaxies

Threat Actor

attributed-to: Earth Lusca

Country

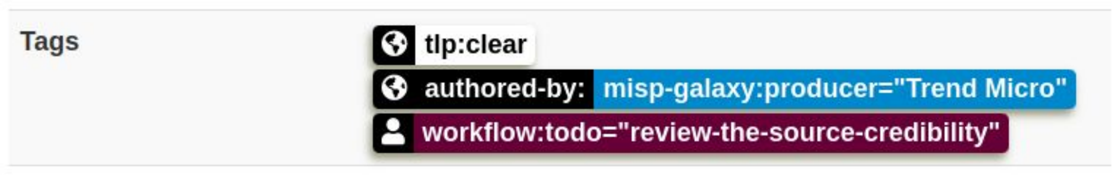
attributed-to: china

Target Information

targets: China

Producer

authored-by: Trend Micro



Tags

tlp:clear

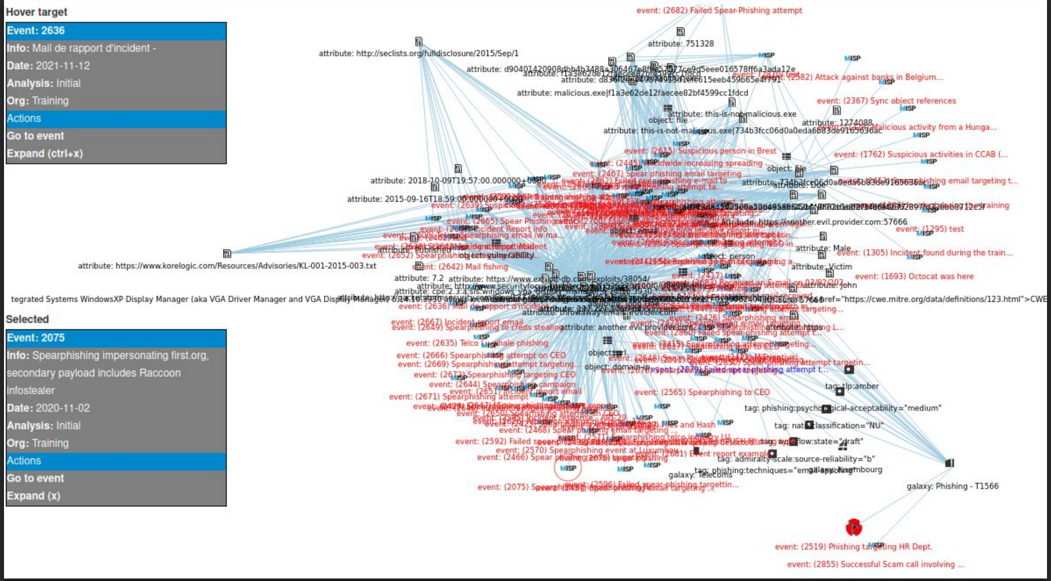
authored-by: misp-galaxy:producer="Trend Micro"

workflow:todo="review-the-source-credibility"

Correlation in MISP

Correlation in MISP

- Correlations
  - Links created automatically whenever an Attribute is created or modified. They allow interconnection between Events based on their attributes
- Correlation Engine
  - Is the system used by MISP to create correlations between Attribute 's value



Hover target

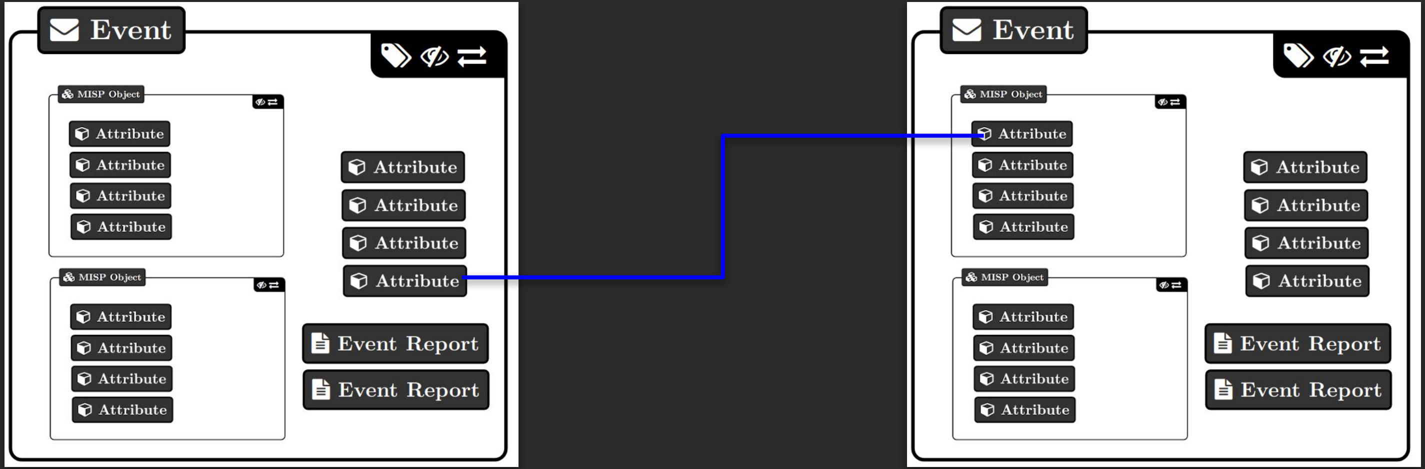
Event: 2636
Info: Mail de rapport d'incident -
Date: 2021-11-12
Analysis: Initial
Org: Training
Actions
Go to event
Expand (ctrl+x)

Selected

Event: 2075
Info: Spearphishing impersonating first.org, secondary payload includes Raccoon infostealer
Date: 2020-11-02
Analysis: Initial
Org: Training
Actions
Go to event
Expand (x)

event: (2682) Failed Spear-Phishing attempt
attribute: 751328
attribute: http://seclists.org/fulldisclosure/2015/Sep/1
event: (2582) Attack against banks in Belgium...
attribute: malicious.exe|f1a3e62de12faecee82bf4599cc1fdcd
event: (2367) Sync object references
attribute: this-is-not-malicious.exe
object: file
attribute: 1274088
attribute: this-is-not-malicious.exe|734b3fcc06d0a0eda6b83de916563 6ac
Malicious activity from a Hunga...
event: (2615) Suspicious person in Brest
event: (1762) Suspicious activities in CCAB (...
event: (2467) Spear phishing email targeting ...
attribute: 2018-10-09T19:57:00.000000+0000
attribute: 2015-09-16T18:59:00.000000+0000
attribute: https://another.evil.provider.com:57666
event: (2665) Spear Phishing
event: (1295) test
object: email
attribute: Male
event: (1305) Incident found during the train...
event: (2652) Spearphishing
object: vulnerability
object: person
attribute: https://www.korelogic.com/Resources/Advisories/KL-001-2015-003.txt
event: (2642) Mail fishing
attribute: Victim
attribute: 7.2
event: (1693) Octocat was here
attribute: John
tegrated Systems WindowsXP Display Manager (aka VGA Driver Manager and VGA Display Manager
ref="https://cwe.mitre.org/data/definitions/123.html">CWE
event: (2636) Mail de rapport d'incident
event: (2667) Incident report email
event: (2649) Spearphishing to creds stealing
attribute: another.evil.provider.com
event: (2635) Telco whale phishing
event: (2666) Spearphishing attempt on CEO
event: (2669) Spearphishing attempt targeting...
object: domain-ip
event: (2673) Spearphishing targeting CEO
event: (2644) Spearphishing campaign
tag: tlp:amber
event: (2671) Spearphishing attempt
event: (2565) Spearphishing to CEO
tag: phishing:psychological-acceptability="medium"
tag: nato:classification="NU"
event: (2592) Failed spear-phishing
tag: workflow:state="draft"
event: (2570) Spearphishing event at Luxembourg
event: (2466) Spear phishing
tag: admiralty-scale:source-reliability="b"
tag: phishing:techniques="email-spoofing"
galaxy: Telecoms
galaxy: Luxembourg
galaxy: Phishing - T1566
event: (2075) Spearphishing
event: (2596) Failed spear-phishing targettin...
event: (2519) Phishing targeting HR Dept.
event: (2855) Successful Scam call involving ...
MISP

Correlation in MISP



01 String Value

- Exact match on the value
- `DEADBEEF` <-> `DEADBEEF`

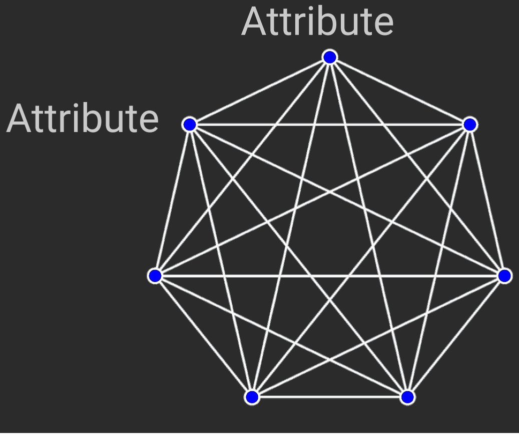
02 CDIR Block

- If an IP is contained in the CIDR block
- `1.1.1.0/24` <-> `1.1.1.128`

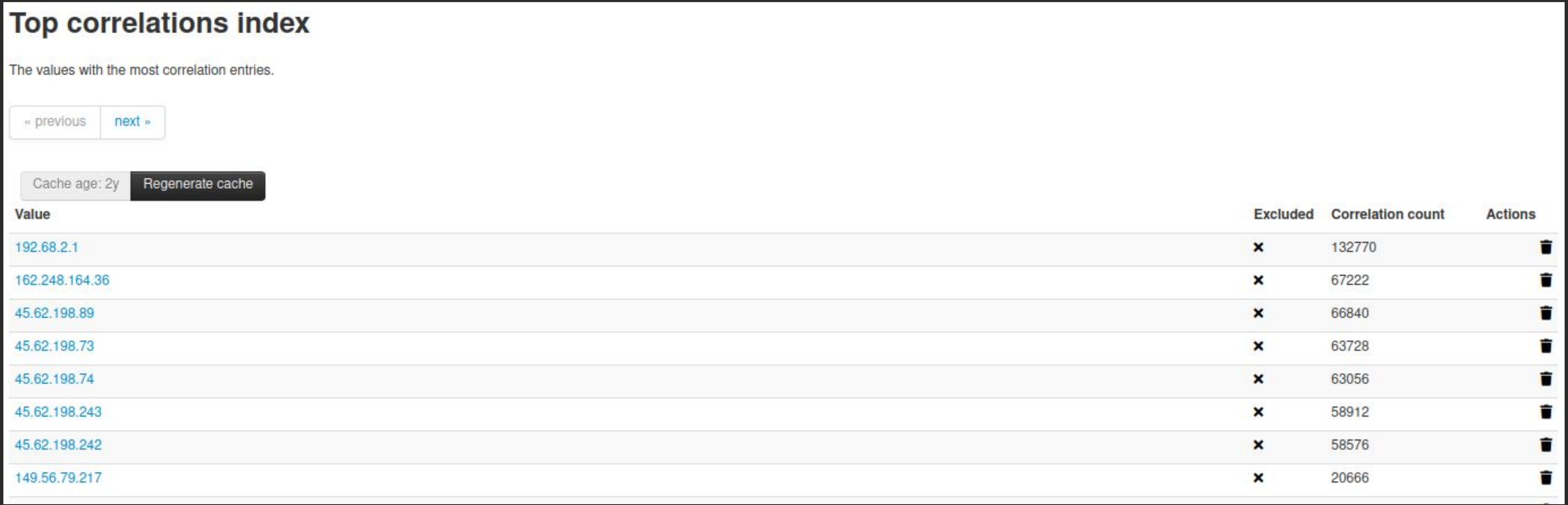
03 SSDEEP Hash

- Algorithm computing fuzzy-hashes
- `3:q8wK6FuFWcEqlv:3wK6FN1I,"stdin"`
- `ssdeep-1.1/cycles.c matches md5deep-1.12/cycles.c (94)`
- Setting: MISP.ssdeep_correlation_threshold

Correlation in MISP



- Correctly clustering data is important
  - Use extended events if applicable
  - Split data per incident or based on time
- Be careful when configuring non-MISP feed



Top correlations index

The values with the most correlation entries.

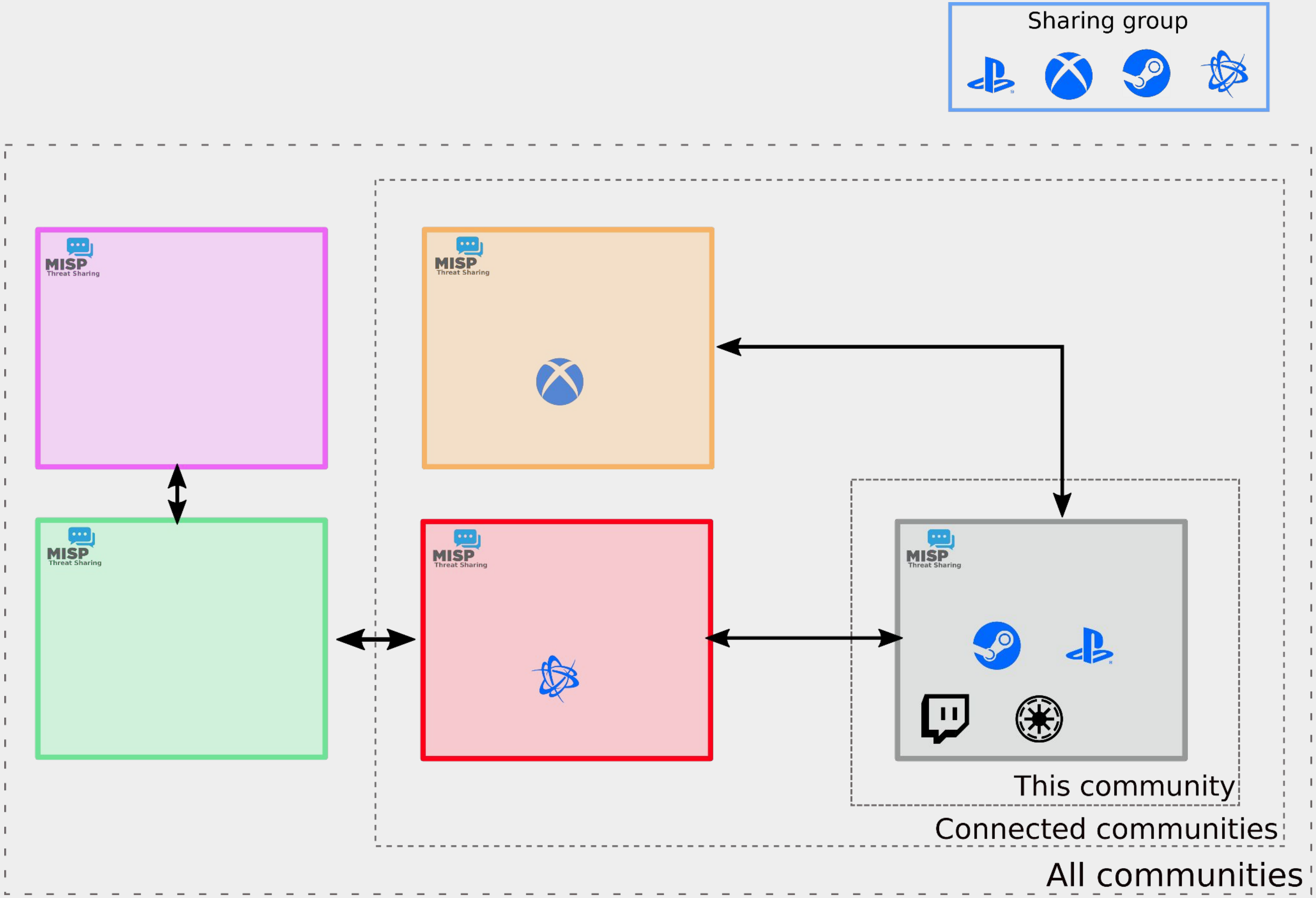
Value	Excluded	Correlation count	Actions
192.68.2.1	×	132770	🗑
162.248.164.36	×	67222	🗑
45.62.198.89	×	66840	🗑
45.62.198.73	×	63728	🗑
45.62.198.74	×	63056	🗑
45.62.198.243	×	58912	🗑
45.62.198.242	×	58576	🗑
149.56.79.217	×	20666	🗑

Distribution levels

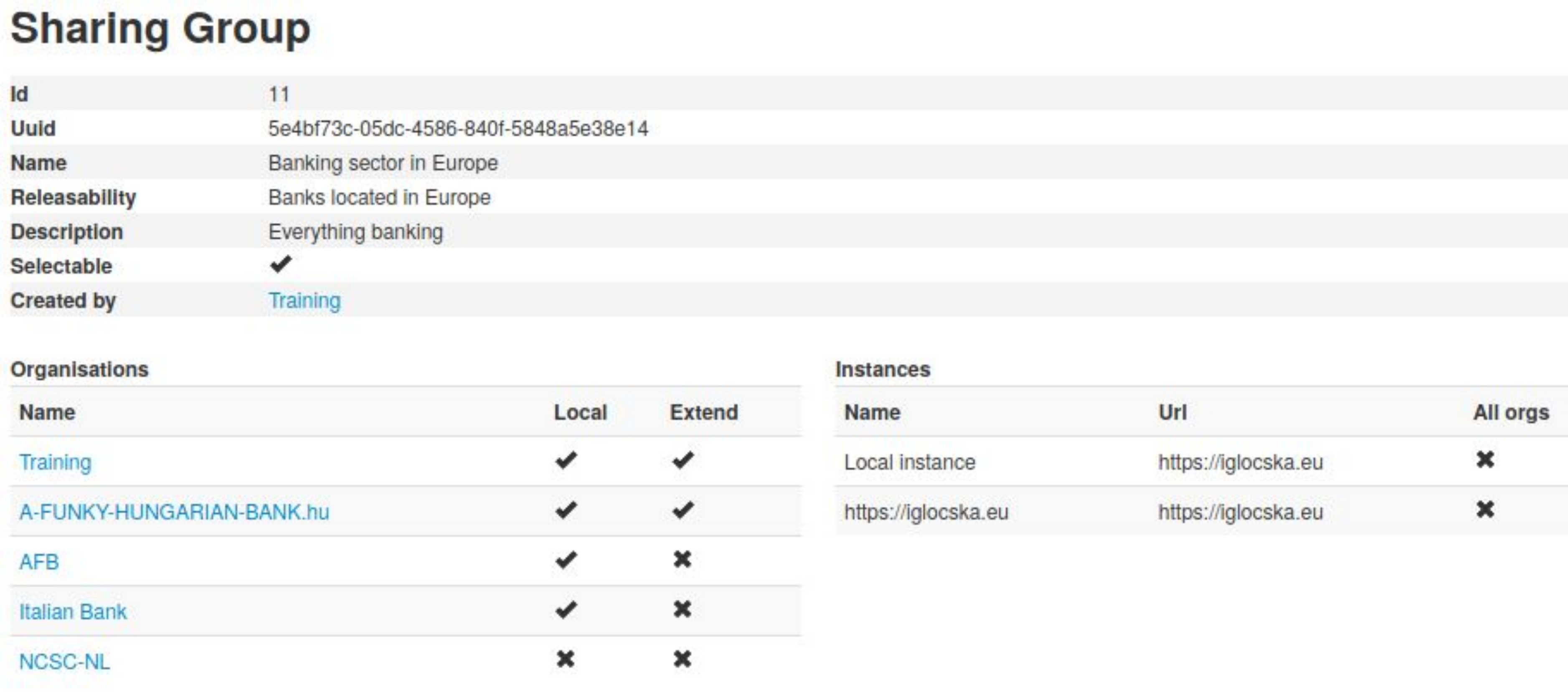
Distribution levels

MISP has multiple distribution settings:

- Organisation only
- This community
  - The server on which you’re on
- Connected communities
  - This community + any connected servers; but not further
- All communities
  - No restriction on propagation as long as there is a connection
- Distribution lists / **Sharing groups**
- Inherit event
  - Will default to the distribution of the event


Sharing group
MISP Threat Sharing
MISP Threat Sharing
MISP Threat Sharing
MISP Threat Sharing
MISP Threat Sharing
This community
Connected communities
All communities

Distribution lists / Sharing groups



Sharing Group

Id	11
Uuid	5e4bf73c-05dc-4586-840f-5848a5e38e14
Name	Banking sector in Europe
Releasability	Banks located in Europe
Description	Everything banking
Selectable	✓
Created by	Training

Organisations

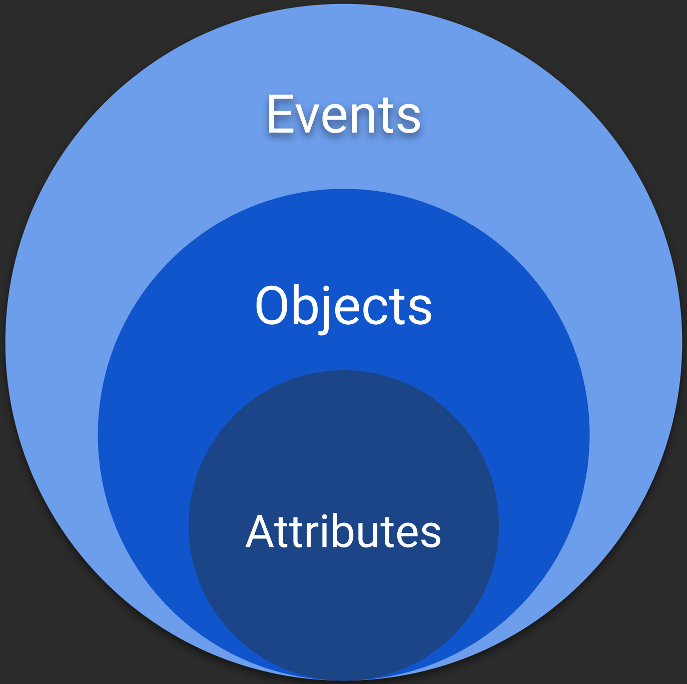
Name	Local	Extend
Training	✓	✓
A-FUNKY-HUNGARIAN-BANK.hu	✓	✓
AFB	✓	✖
Italian Bank	✓	✖
NCSC-NL	✖	✖

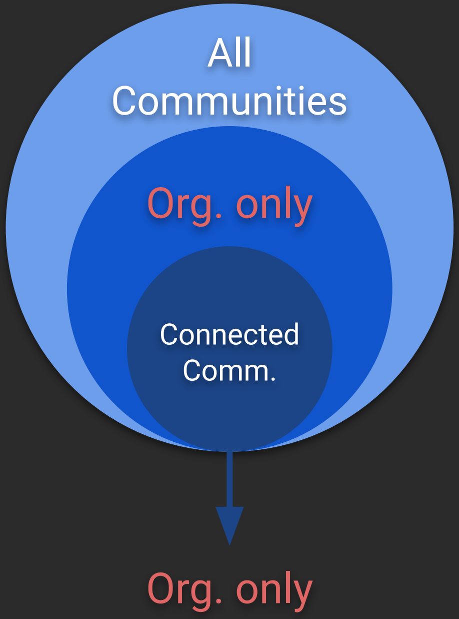
Instances

Name	Url	All orgs
Local instance	https://iglocska.eu	✖
https://iglocska.eu	https://iglocska.eu	✖

Propagation of Distribution

The final distribution level is the most restrictive one


Events
Objects
Attributes


All Communities
Org. only
Connected Comm.
Org. only