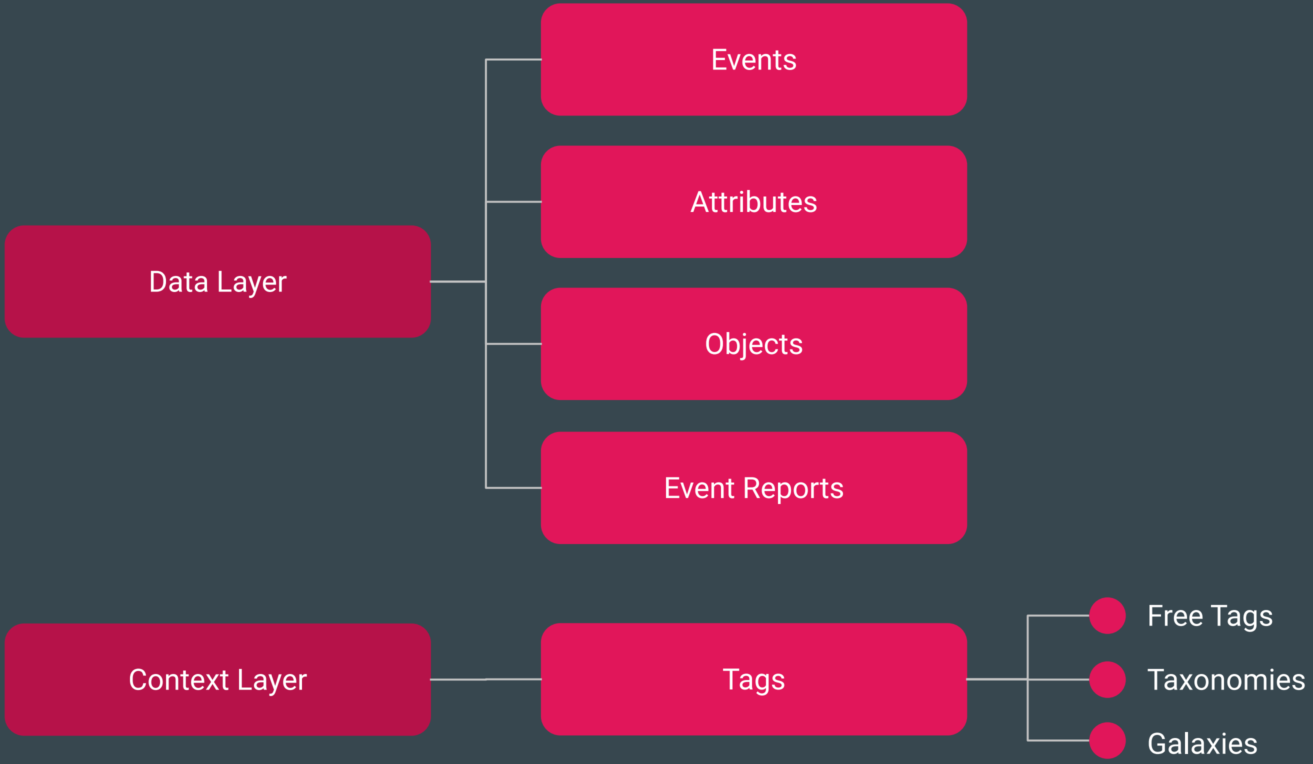
MISP Data model overview

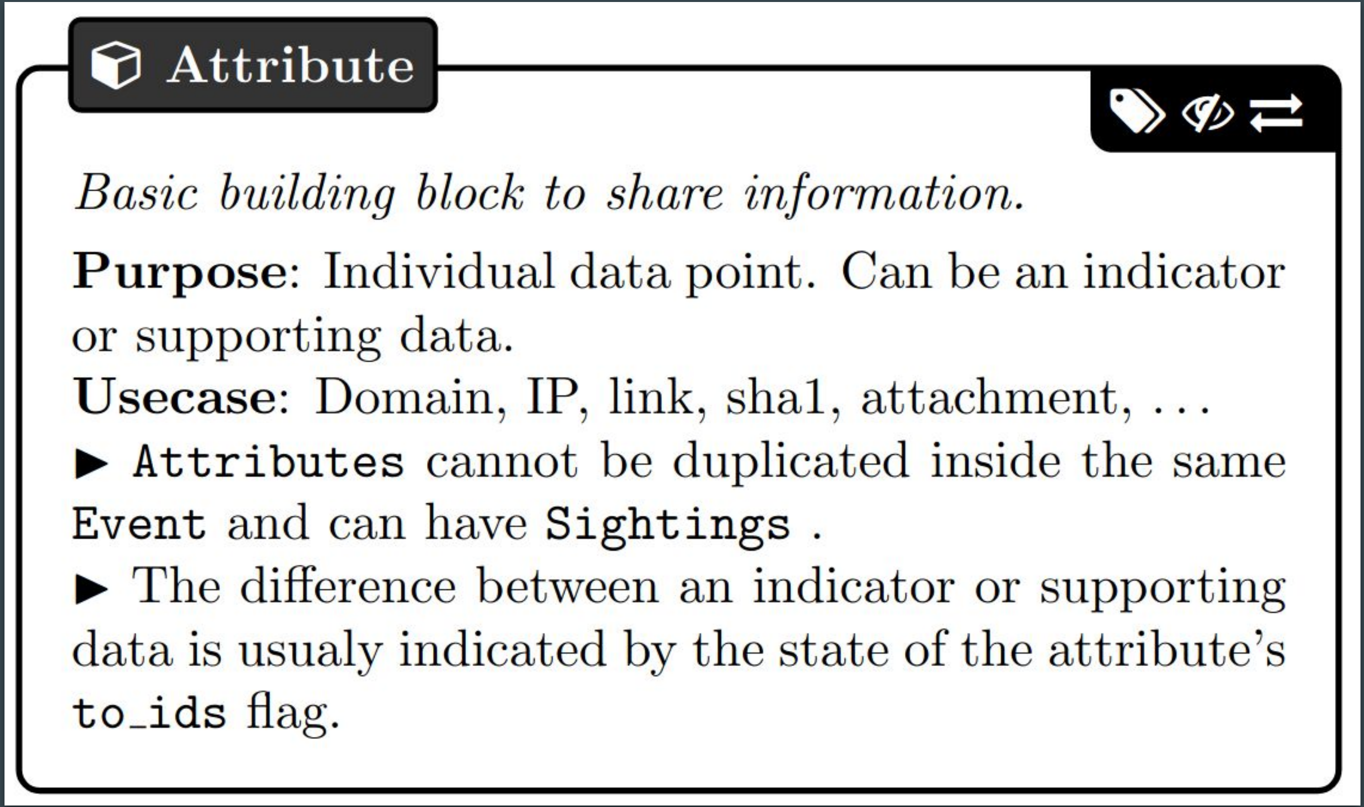
MISP
Threat Sharing

Type of Data model



Data Layer

MISP Attributes



Attribute

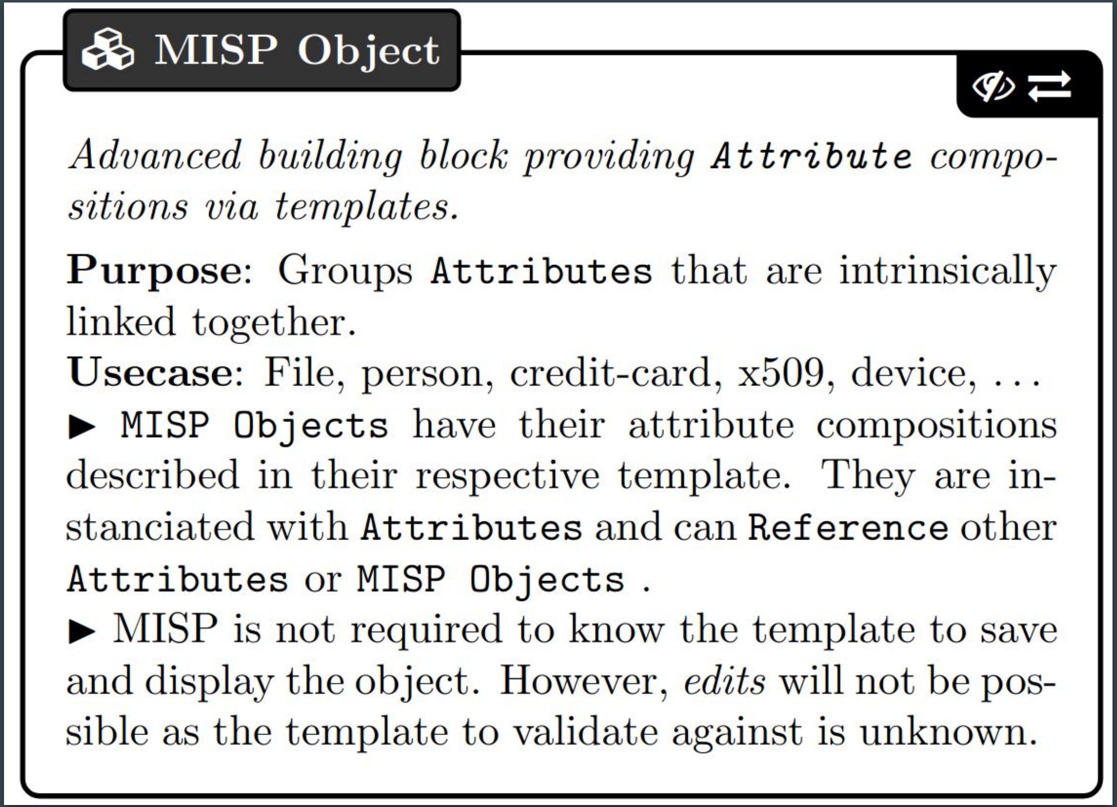
Basic building block to share information.

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.

MISP Objects



MISP Object

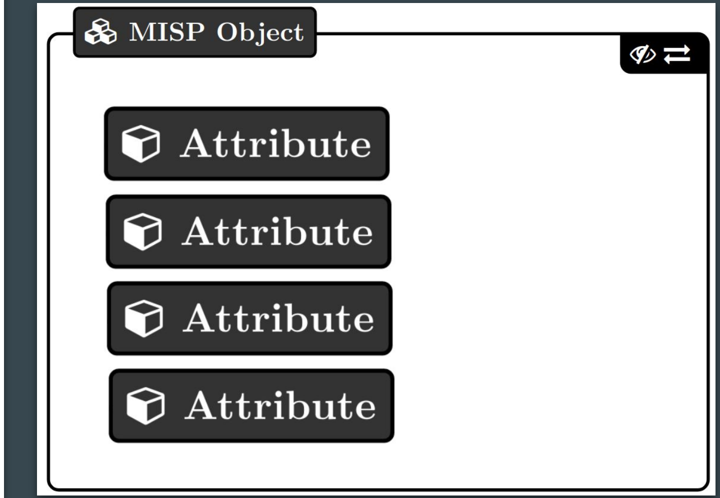
Advanced building block providing `Attribute` *compositions via templates.*

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

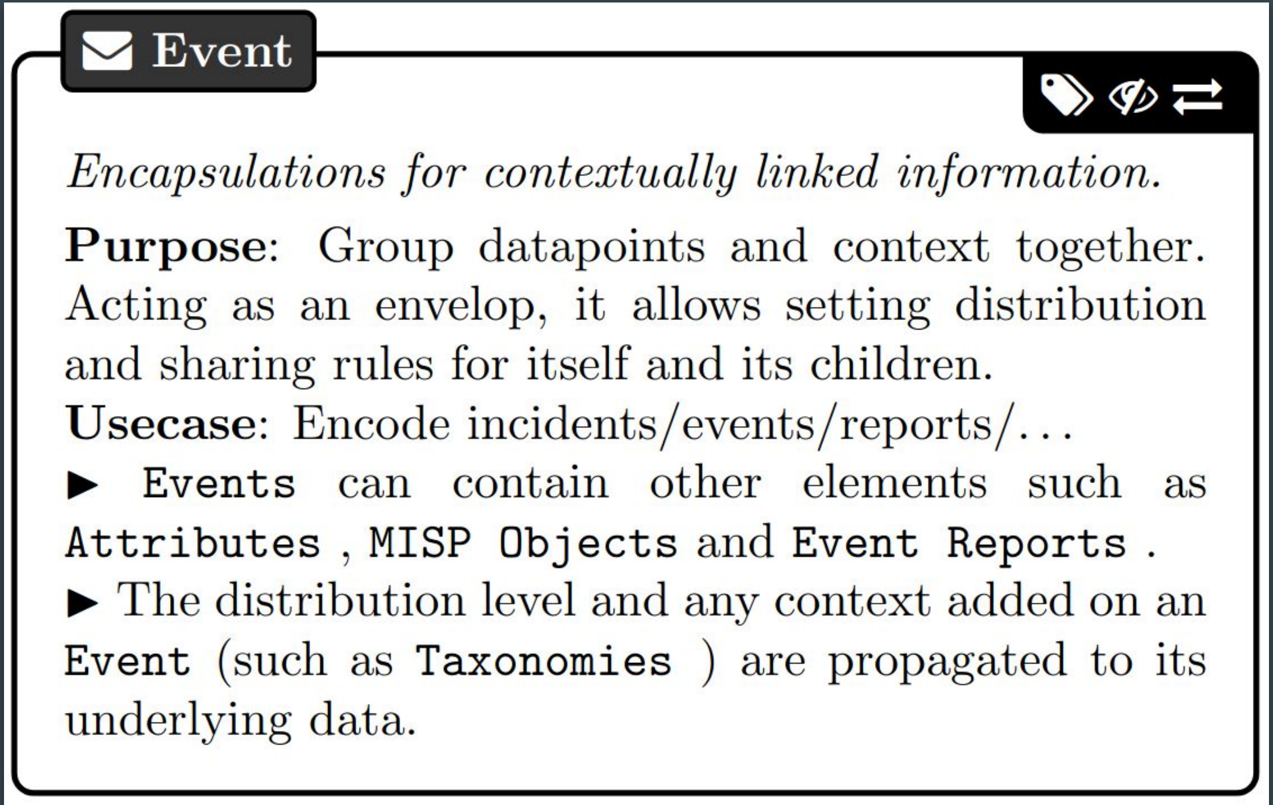
Usecase: File, person, credit-card, x509, device, ...

▶ `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.



MISP Events



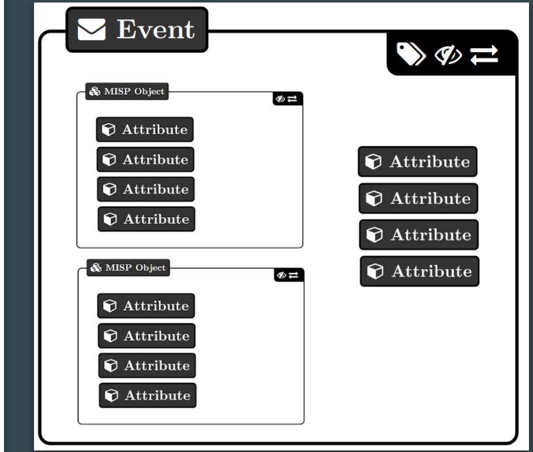
Event

Encapsulations for contextually linked information.

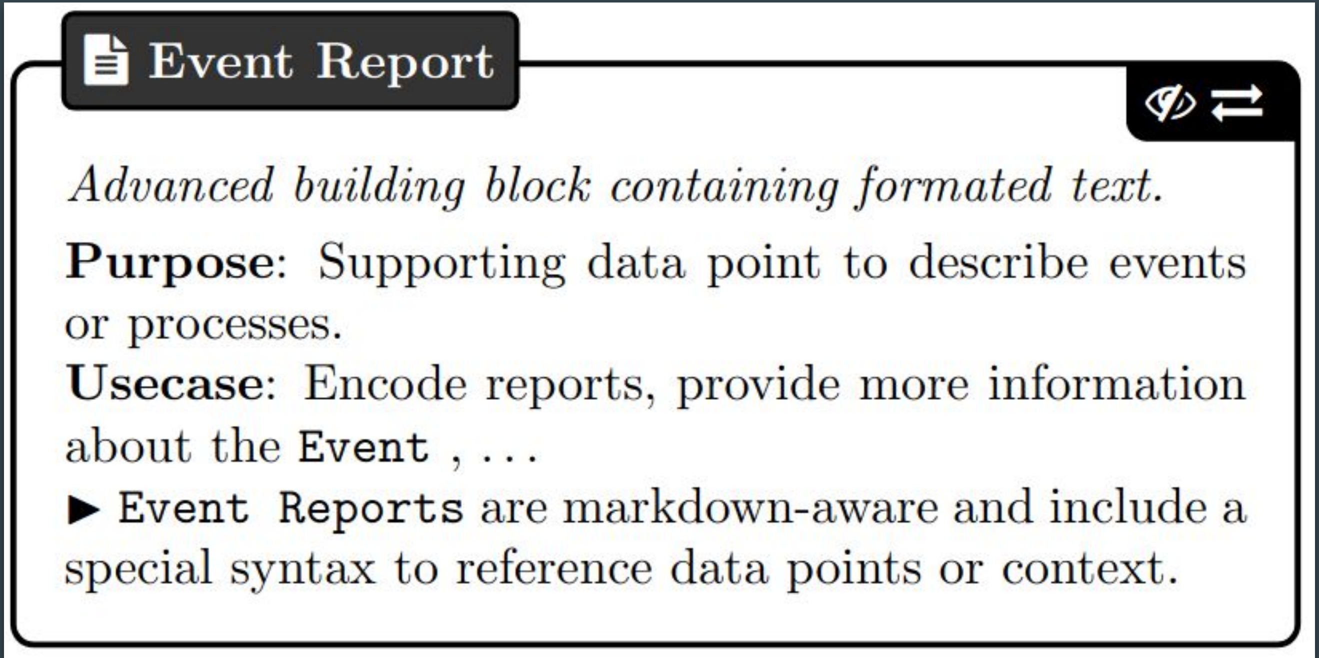
Purpose: Group datapoints and context together. Acting as an envelop, it allows setting distribution and sharing rules for itself and its children.

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.



MISP Event Report



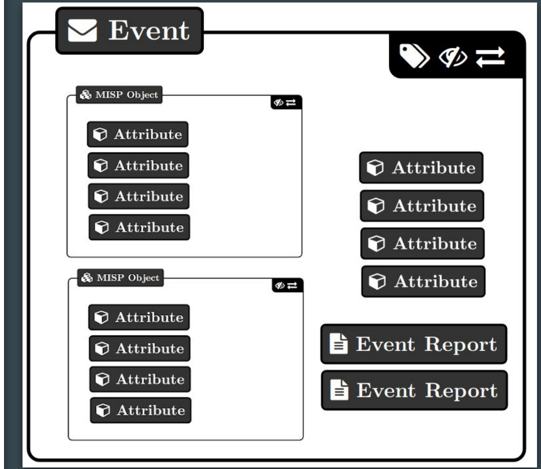
Event Report

Advanced building block containing formated text.

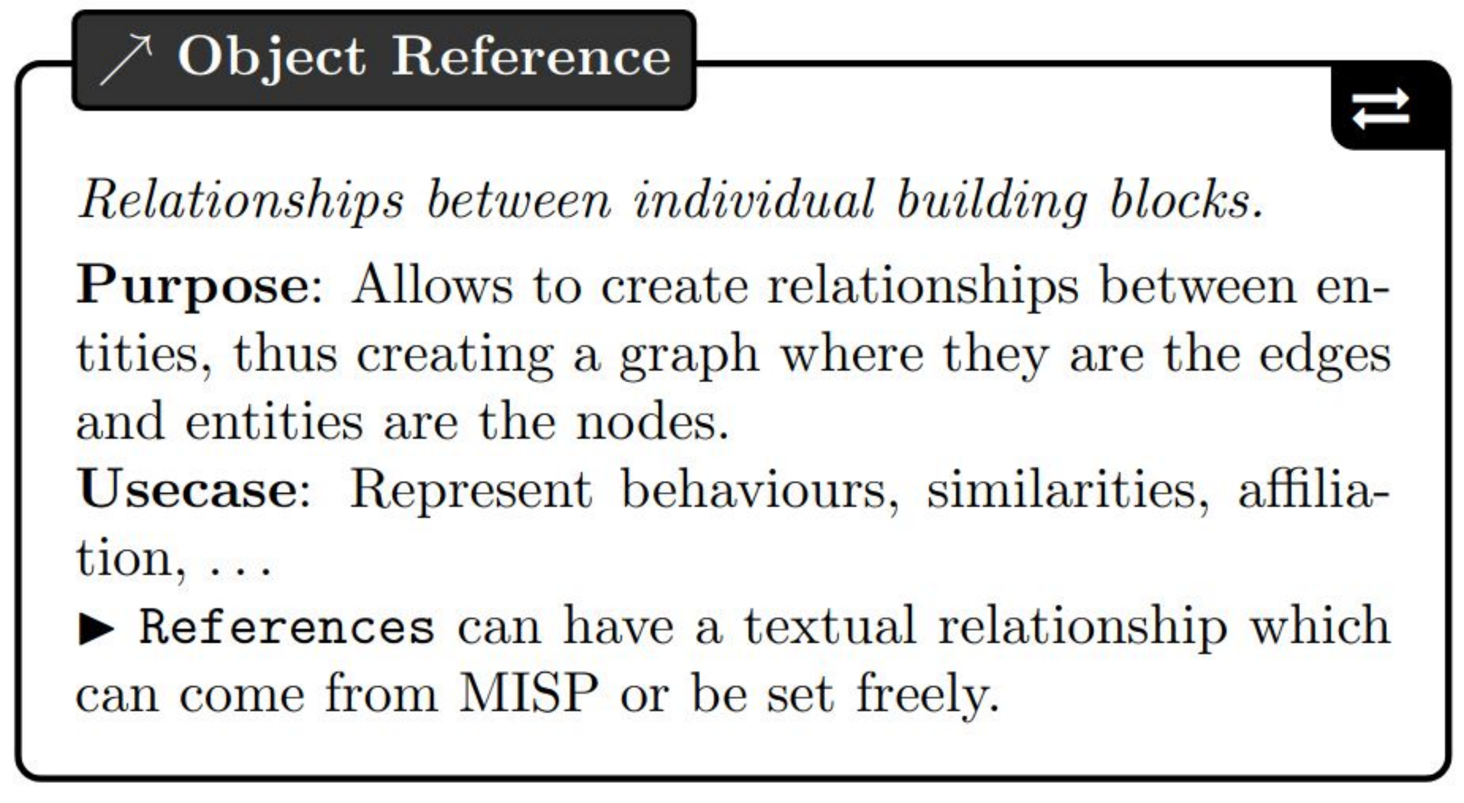
Purpose: Supporting data point to describe events or processes.

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.



Object Reference



↗ Object Reference ⇄

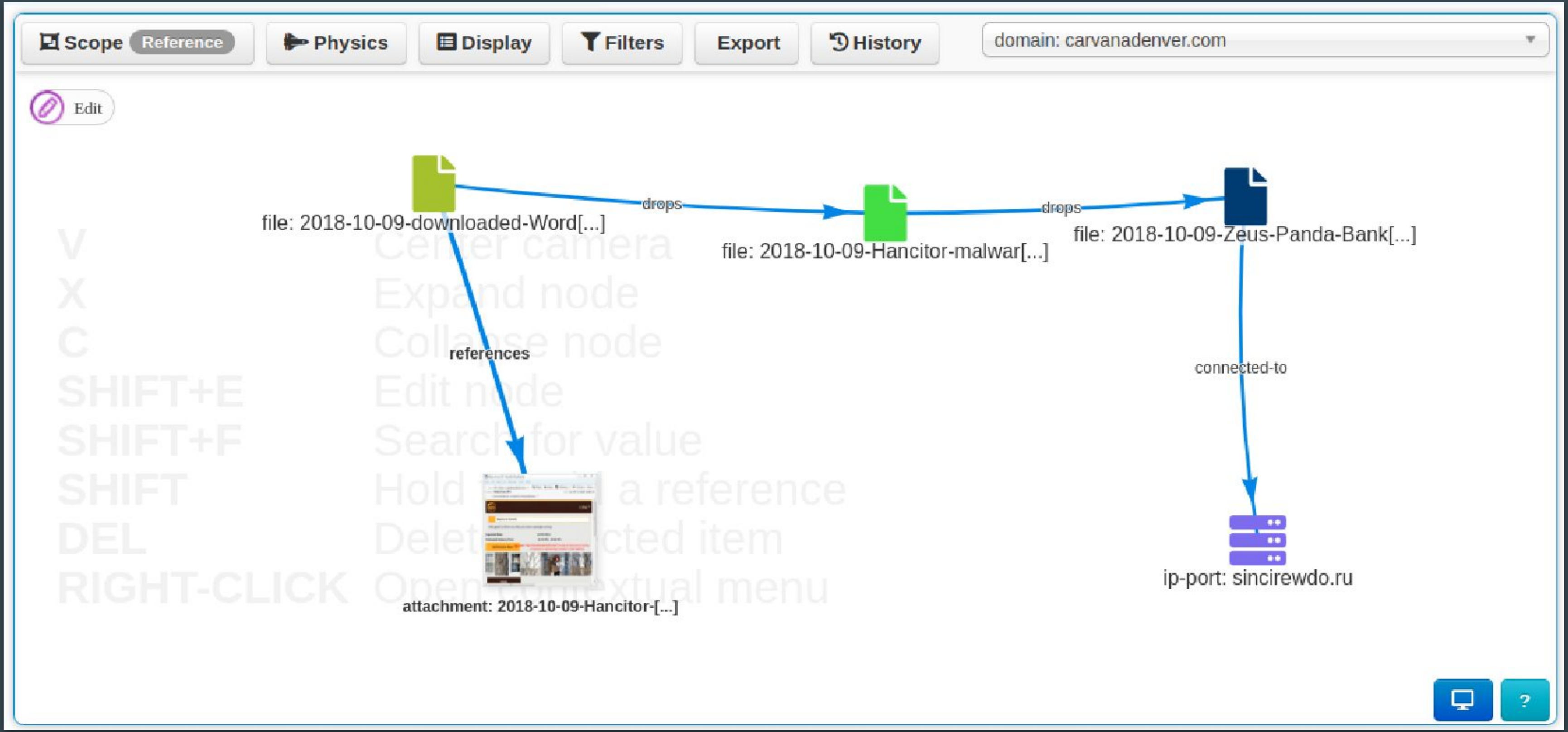
Relationships between individual building blocks.

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, …

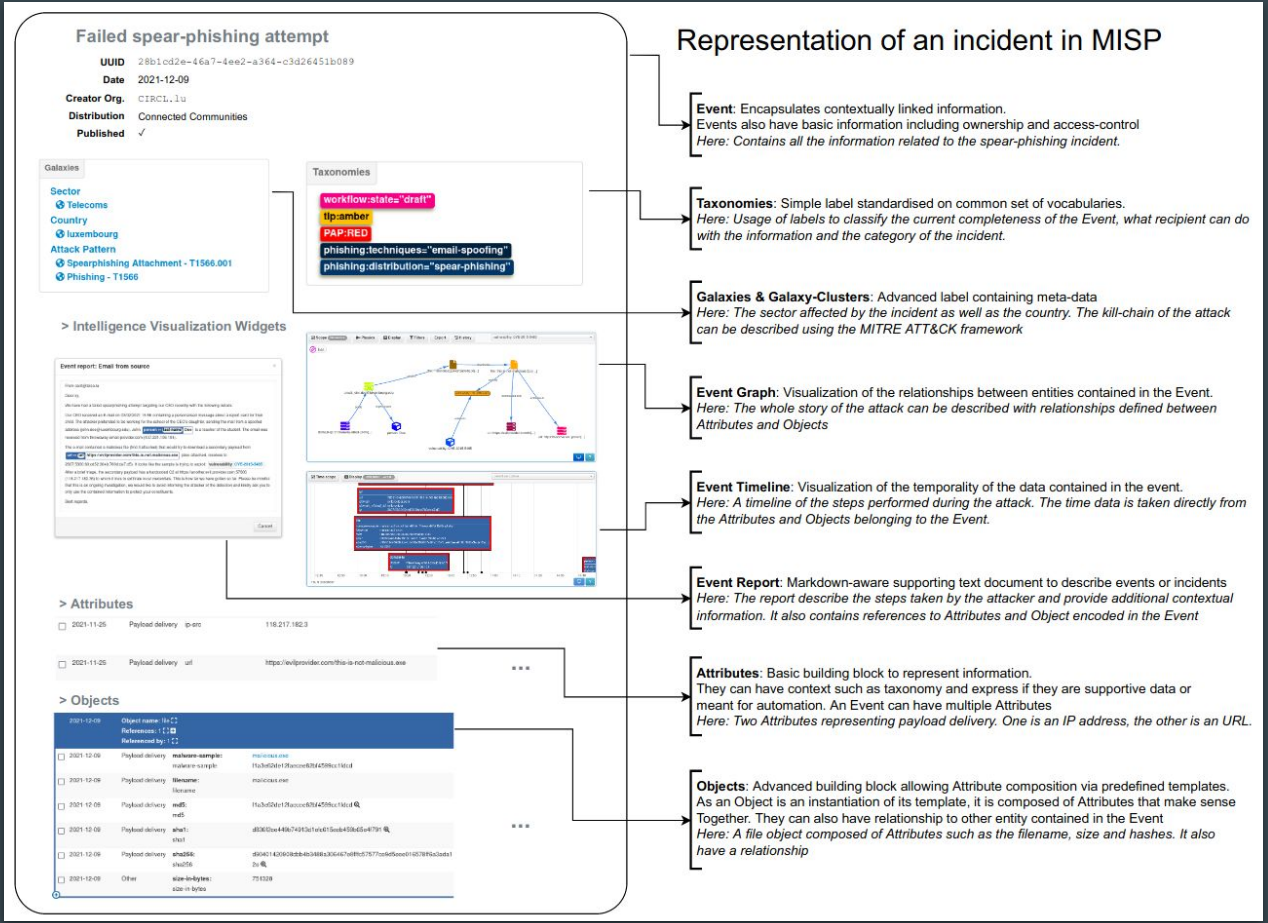
▶ `References` can have a textual relationship which can come from MISP or be set freely.

Object References


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 to add a reference
DEL	Delete selected item
RIGHT-CLICK	Open contextual menu

Anatomy of an Event



Failed spear-phishing attempt

UUID	28b1cd2e-46a7-4ee2-a364-c3d26451b089
Date	2021-12-09
Creator Org.	CIRCL.lu
Distribution	Connected Communities
Published	✓

Galaxies

- Sector
  - Telecoms
- Country
  - luxembourg
- Attack Pattern
  - Spearphishing Attachment - T1566.001
  - Phishing - T1566

Taxonomies

- workflow:state="draft"
- tlp:amber
- PAP:RED
- phishing:techniques="email-spoofing"
- phishing:distribution="spear-phishing"

> Intelligence Visualization Widgets

Event report: Email from source

[illegible]

Best regards.

Cancel

> Attributes

□	2021-11-25	Payload delivery	ip-src	118.217.182.3
□	2021-11-25	Payload delivery	url	https://evilprovider.com/this-is-not-malicious.exe

...

> Objects

	2021-12-09	Object name: file References: 1 Referenced by: 1		
□	2021-12-09	Payload delivery	malware-sample: malware-sample	malicous.exe f1a3e62de12faccee82bf4589cc1dcd
□	2021-12-09	Payload delivery	filename: filename	malicous.exe
□	2021-12-09	Payload delivery	md5: md5	f1a3e62de12faccee82bf4589cc1dcd
□	2021-12-09	Payload delivery	sha1: sha1	d8302ee449b74913d1a1c615ecb459b65e4f791
□	2021-12-09	Payload delivery	sha256: sha256	d90401420908dbb4b3488a306467a8ffc57577ce9d5eee016578f6a3ada12e
□	2021-12-09	Other	size-in-bytes: size-in-bytes	751328

...

Representation of an incident in MISP

Event: Encapsulates contextually linked information.
Events also have basic information including ownership and access-control
Here: Contains all the information related to the spear-phishing incident.

Taxonomies: Simple label standardised on common set of vocabularies.
Here: Usage of labels to classify the current completeness of the Event, what recipient can do with the information and the category of the incident.

Galaxies & Galaxy-Clusters: Advanced label containing meta-data
Here: The sector affected by the incident as well as the country. The kill-chain of the attack can be described using the MITRE ATT&CK framework

Event Graph: Visualization of the relationships between entities contained in the Event.
Here: The whole story of the attack can be described with relationships defined between Attributes and Objects

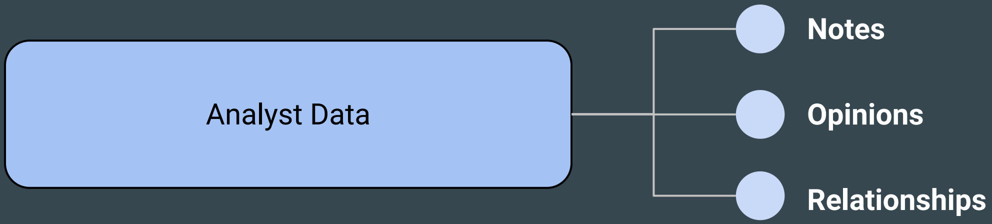
Event Timeline: Visualization of the temporality of the data contained in the event.
Here: A timeline of the steps performed during the attack. The time data is taken directly from the Attributes and Objects belonging to the Event.

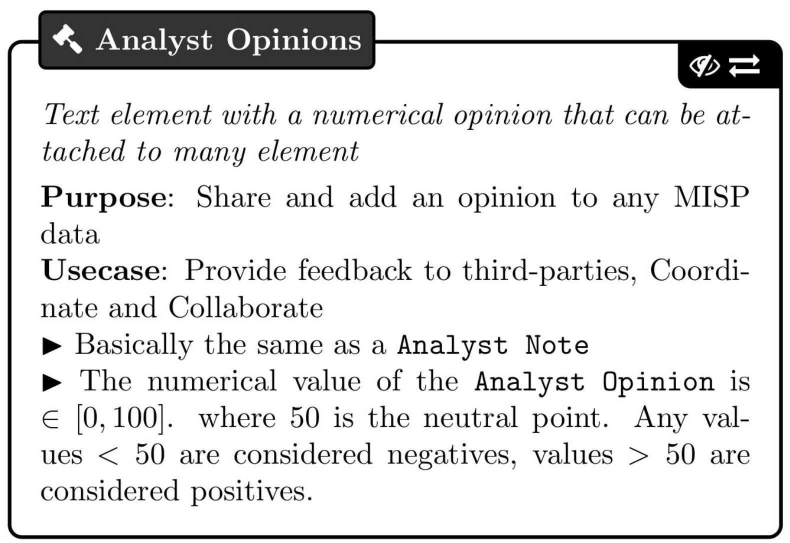
Event Report: Markdown-aware supporting text document to describe events or incidents
Here: The report describe the steps taken by the attacker and provide additional contextual information. It also contains references to Attributes and Object encoded in the Event

Attributes: Basic building block to represent information.
They can have context such as taxonomy and express if they are supportive data or meant for automation. An Event can have multiple Attributes
Here: Two Attributes representing payload delivery. One is an IP address, the other is an URL.

Objects: Advanced building block allowing Attribute composition via predefined templates.
As an Object is an instantiation of its template, it is composed of Attributes that make sense Together. They can also have relationship to other entity contained in the Event
Here: A file object composed of Attributes such as the filename, size and hashes. It also have a relationship

Analyst Data





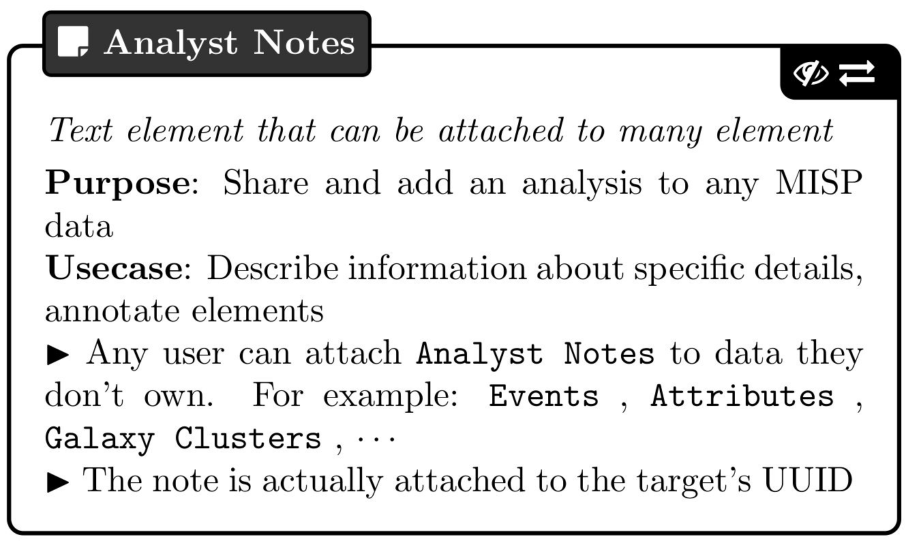
Analyst Opinions

Text element with a numerical opinion that can be attached to many element

Purpose: Share and add an opinion to any MISP data

Usecase: Provide feedback to third-parties, Coordinate and Collaborate

- ▶ Basically the same as a `Analyst Note`
- ▶ The numerical value of the `Analyst Opinion` is $\in [0, 100]$. where 50 is the neutral point. Any values < 50 are considered negatives, values > 50 are considered positives.



Analyst Notes

Text element that can be attached to many element

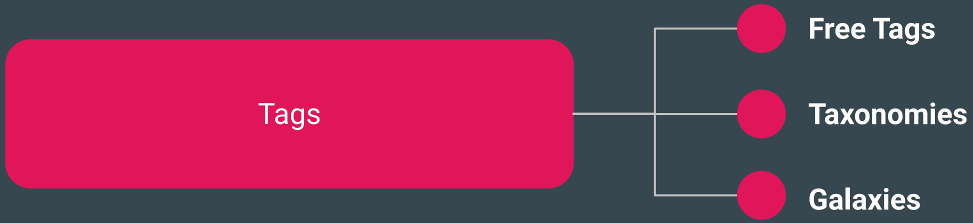
Purpose: Share and add an analysis to any MISP data

Usecase: Describe information about specific details, annotate elements

- ▶ Any user can attach `Analyst Notes` to data they don't own. For example: `Events` , `Attributes` , `Galaxy Clusters` , $\cdots$
- ▶ The note is actually attached to the target's UUID

Context Layer

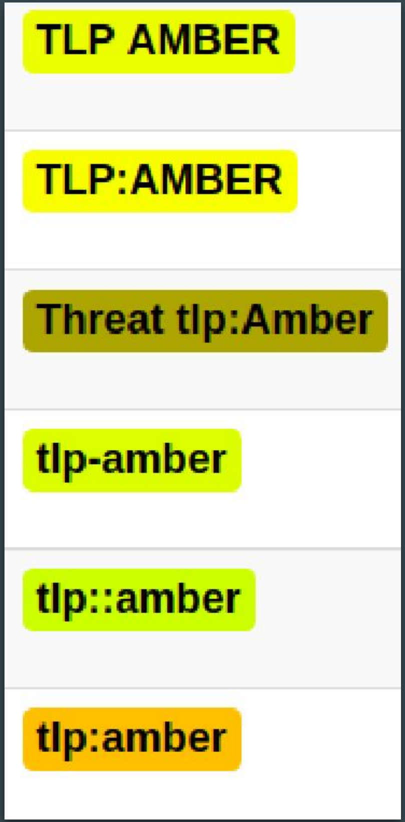
Tags



- **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

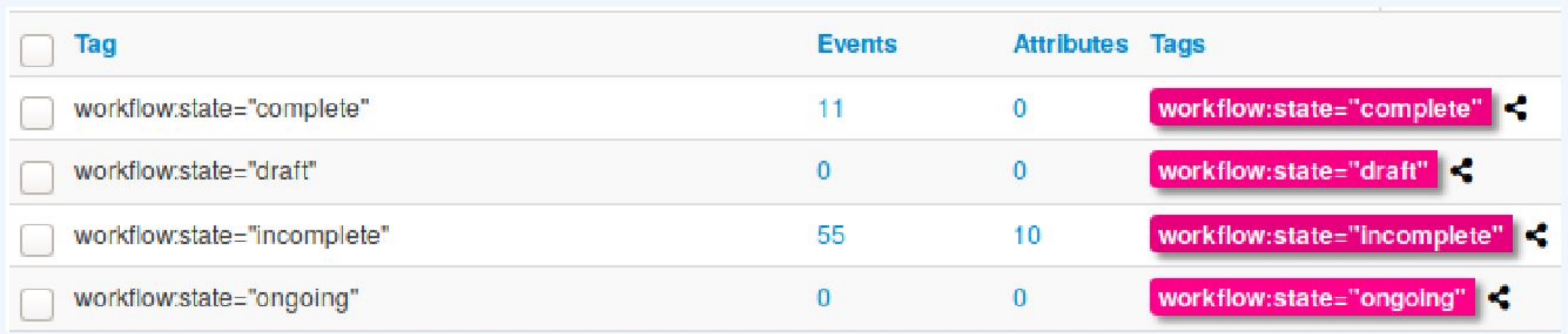
tlp-amber

tlp::amber

tlp:amber

Taxonomies

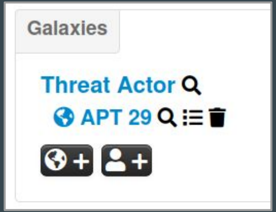
- Simple label standardised on common set of vocabularies
- Efficient classification globally understood
- Ease consumption and automation

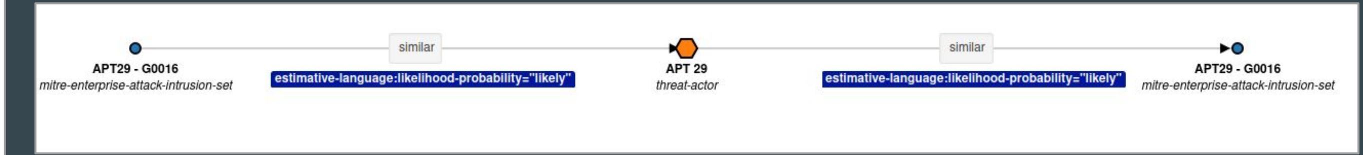


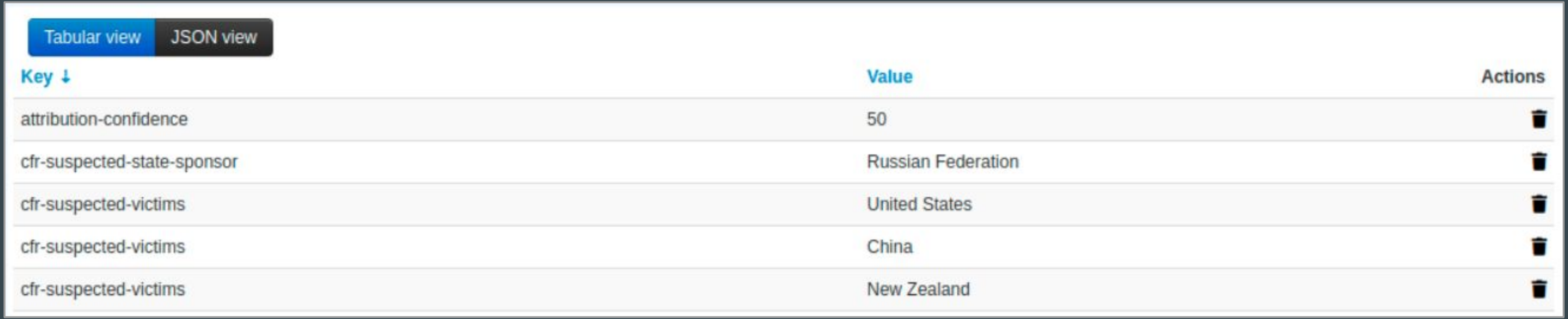
☐	Tag	Events	Attributes	Tags
☐	workflow:state="complete"	11	0	workflow:state="complete"
☐	workflow:state="draft"	0	0	workflow:state="draft"
☐	workflow:state="incomplete"	55	10	workflow:state="incomplete"
☐	workflow:state="ongoing"	0	0	workflow:state="ongoing"

Galaxies

- Normalized classification boosted by meta-data
- Enable description of complex high-level information
- Used internally to represent the MITRE ATT&CK Framework




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

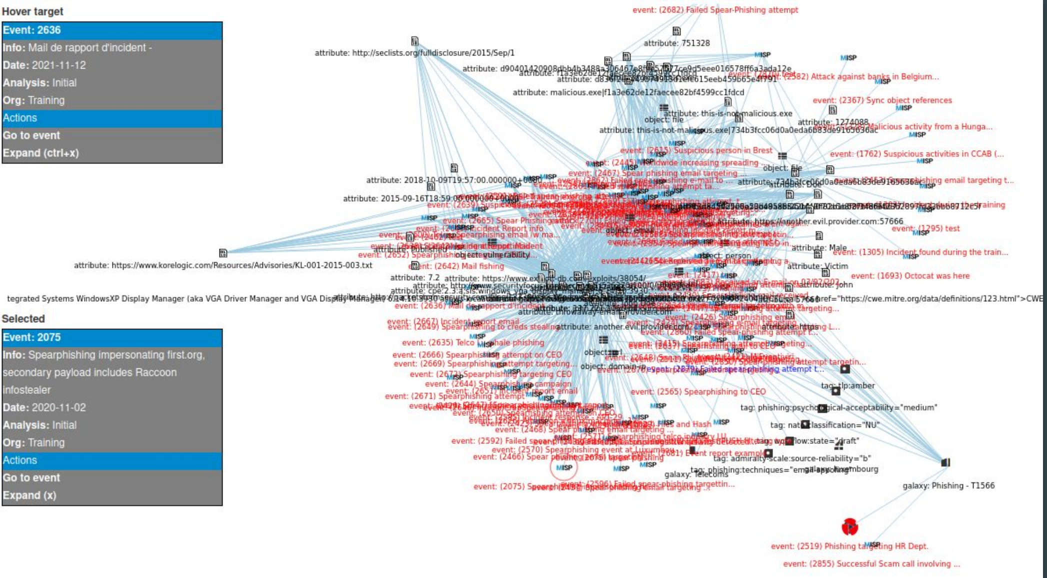


Key ↓	Value	Actions
attribution-confidence	50	🗑
cfr-suspected-state-sponsor	Russian Federation	🗑
cfr-suspected-victims	United States	🗑
cfr-suspected-victims	China	🗑
cfr-suspected-victims	New Zealand	🗑

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

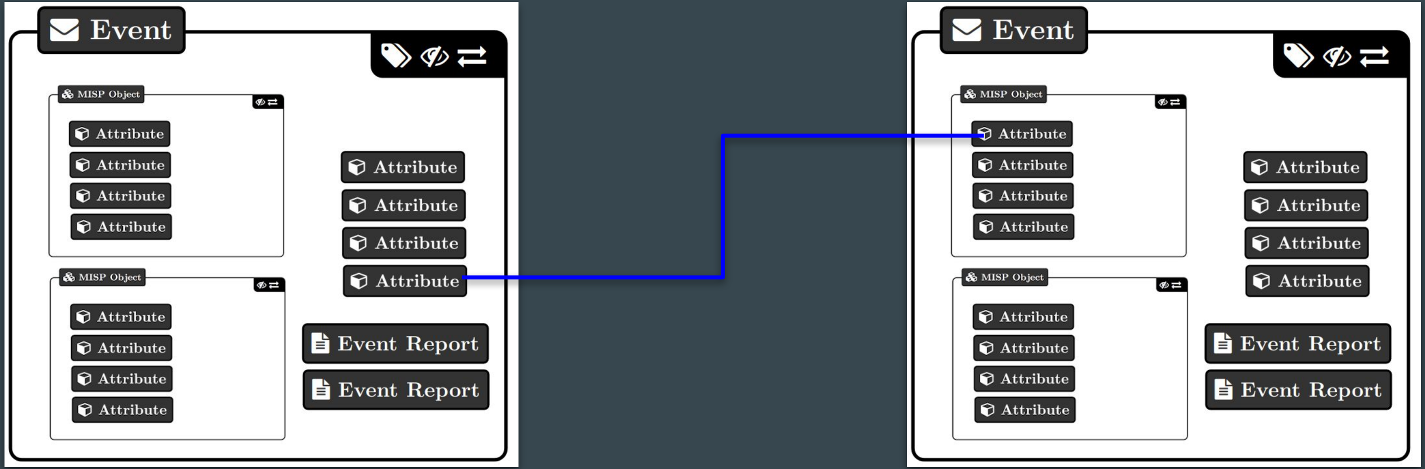
Actions

Go to event

Expand (x)

event: (2682) Failed Spear-Phishing attempt
attribute: 751328
attribute: http://seclists.org/fulldisclosure/2015/Sep/1
attribute: malicious.exe|f1a3e62de12faecee82bf4599cc1fdcd
event: (2367) Sync object references
attribute: this-is-not-malicious.exe
attribute: 1274088
event: (1762) Suspicious activities in CCAB (...
attribute: 2018-10-09T19:57:00.000000+0000
attribute: 2015-09-16T18:59:00.000000+0000
attribute: https://another.evil.provider.com:57666
event: (1295) test
attribute: Male
event: (1305) Incident found during the train...
attribute: https://www.korelogic.com/Resources/Advisories/KL-001-2015-003.txt
event: (2642) Mail fishing
attribute: Victim
event: (1693) Octocat was here
attribute: 7.2
attribute: John
tegrated Systems WindowsXP Display Manager (aka VGA Driver Manager and VGA Display Manager)
event: (2635) Telco whale phishing
event: (2666) Spearphishing attempt on CEO
event: (2565) Spearphishing to CEO
tag: tlp:amber
tag: phishing:psychological-acceptability="medium"
tag: workflow:state="draft"
tag: admiralty-scale:source-reliability="b"
galaxy: Telecoms
galaxy: Phishing - T1566
event: (2075) Spearphishing
event: (2519) Phishing targeting HR Dept.
event: (2855) Successful Scam call involving ...

Correlation in MISP



01 String Value

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

02 CDIR Block

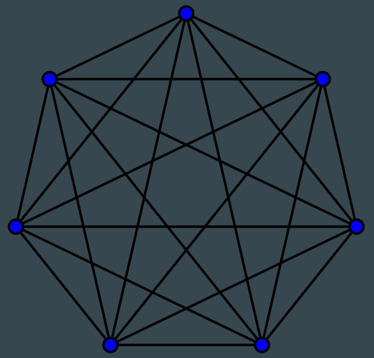
- If an IP is contained in the CIDR block
- 1.1.1.0/24 <-> 1.1.1.128

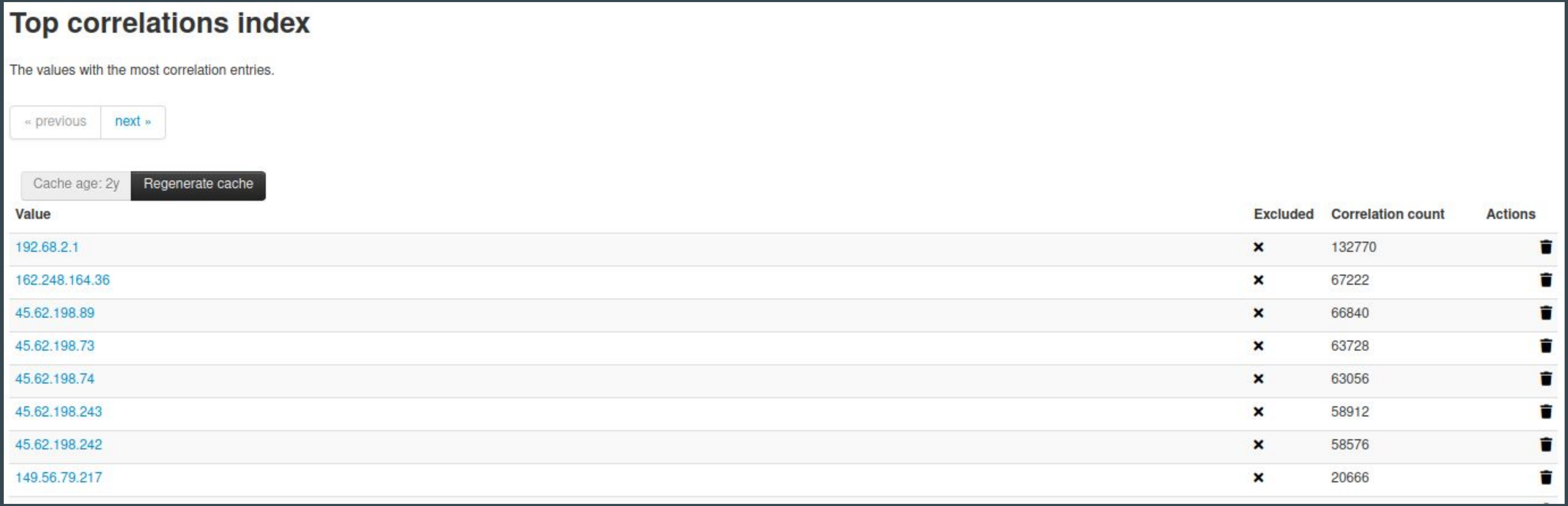
03 SSDEEP Hash

- 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.

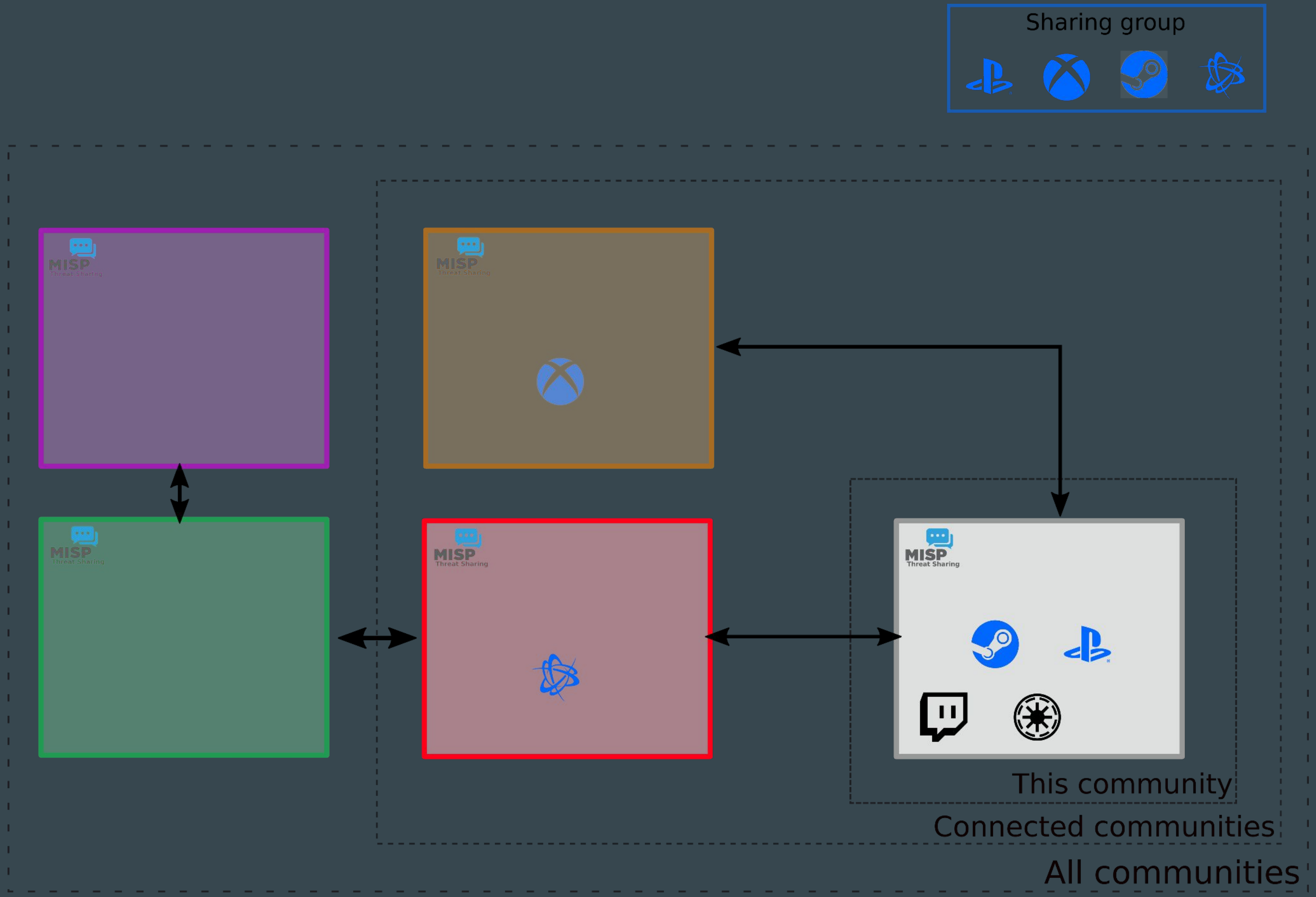
Value	Excluded	Correlation count	Actions
192.68.2.1	✗	132770	🗑
162.248.164.36	✗	67222	🗑
45.62.198.89	✗	66840	🗑
45.62.198.73	✗	63728	🗑
45.62.198.74	✗	63056	🗑
45.62.198.243	✗	58912	🗑
45.62.198.242	✗	58576	🗑
149.56.79.217	✗	20666	🗑

Distribution levels

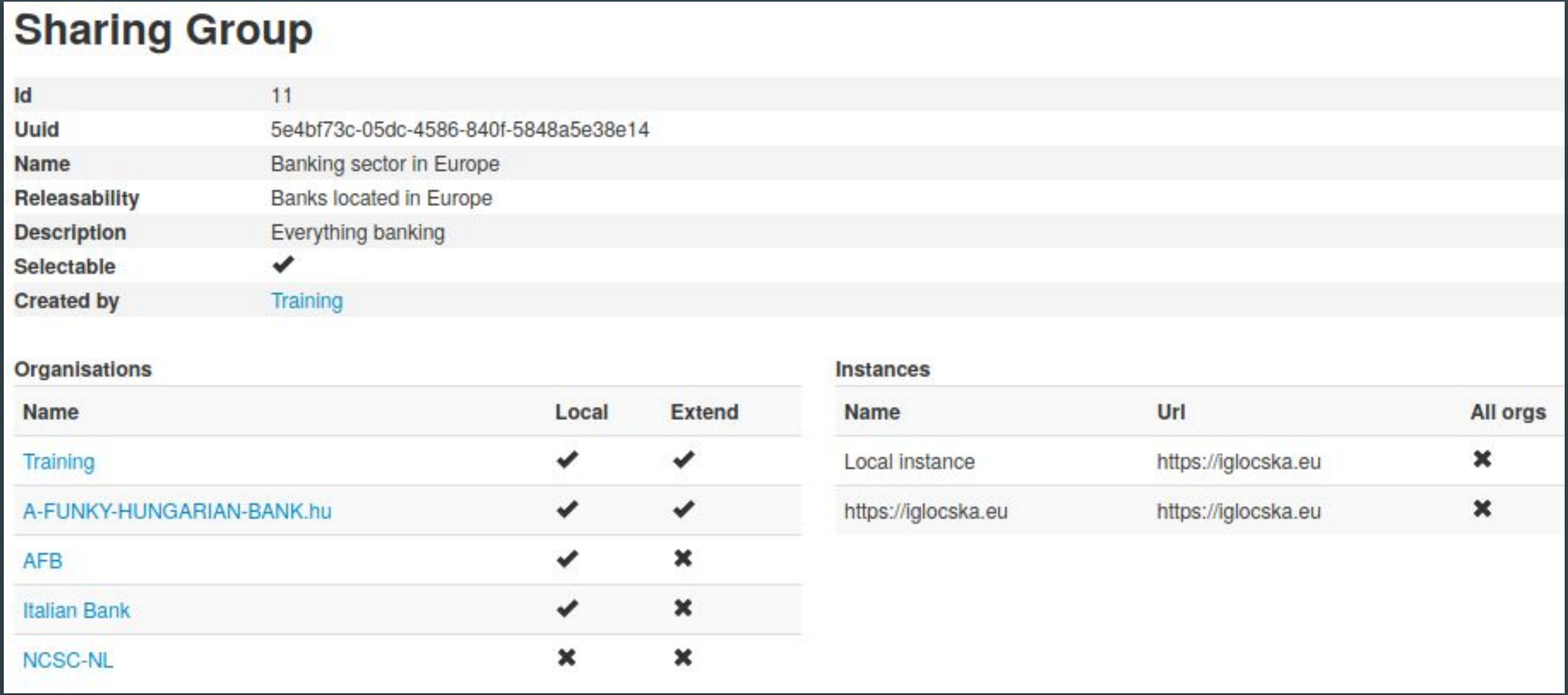
Distribution levels

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

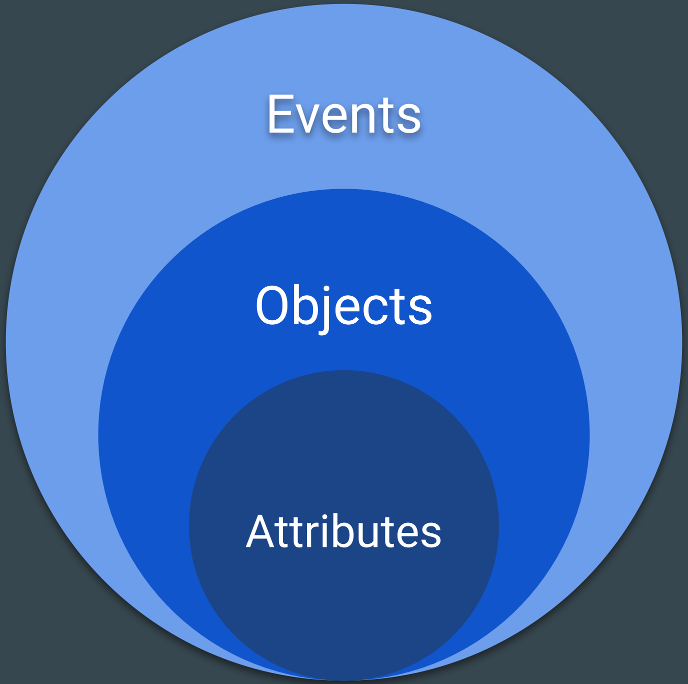
Name	Local	Extend
Training	✔	✔
A-FUNKY-HUNGARIAN-BANK.hu	✔	✔
AFB	✔	✖
Italian Bank	✔	✖
NCSC-NL	✖	✖

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