

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

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

MISP PROJECT



2022-09-13

An Introduction to Cybersecurity Information Sharing

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT
<https://www.misp-project.org/>

MISP PROJECT



- Data sharing in MISP
- Data models for the Data layer
- Data models for the Context layer

2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Content of the presentation

- Data sharing in MISP
- Data models for the Data layer
- Data models for the Context layer

■ Data layer

- ▶ The raw data itself as well as element to link them together
- ▶ Indicators, Observables and means to contextually link them
- ▶ MISP terminology: Event, Attributes, misp-objects, ...

■ Context layer

- ▶ As important as the data layer, allow triage, false-positive management, risk-assessment and prioritisation
- ▶ Latches on the data layer, usually referencing threat intelligence, concepts, knowledge base and vocabularies
- ▶ Tags, Taxonomies, Galaxies, ...

2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Layers of data model

- Data layer
 - ▶ The raw data itself as well as element to link them together
 - ▶ Indicators, Observables and means to contextually link them
 - ▶ MISP terminology: Event, Attributes, misp-objects, ...
- Context layer
 - ▶ As important as the data layer, allow triage, false-positive management, risk-assessment and prioritisation
 - ▶ Latches on the data layer, usually referencing threat intelligence, concepts, knowledge base and vocabularies
 - ▶ Tags, Taxonomies, Galaxies, ...

DATA SHARING IN MISP

2022-09-13

An Introduction to Cybersecurity Information
Sharing

└─ Data sharing in MISP

DATA SHARING IN MISP

SHARING IN MISP: DISTRIBUTION

MISP offers granular distribution settings:

- Organisation only
- This community
- Connected communities
- All communities
- Distribution lists - aka **Sharing groups**

Sharing Group

| | |
|---------------|-------------------------------------|
| Id | 11 |
| Uuid | 5e4b73c-05dc-4586-840f-5848a5c38e14 |
| 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://lgloscka.eu | ✗ |
| https://lgloscka.eu | https://lgloscka.eu | ✗ |

At multiple levels: **Events, Attributes, Objects** (and their **Attributes**) and **Galaxy-clusters**

An Introduction to Cybersecurity Information Sharing

└ Data sharing in MISP

└ Sharing in MISP: Distribution

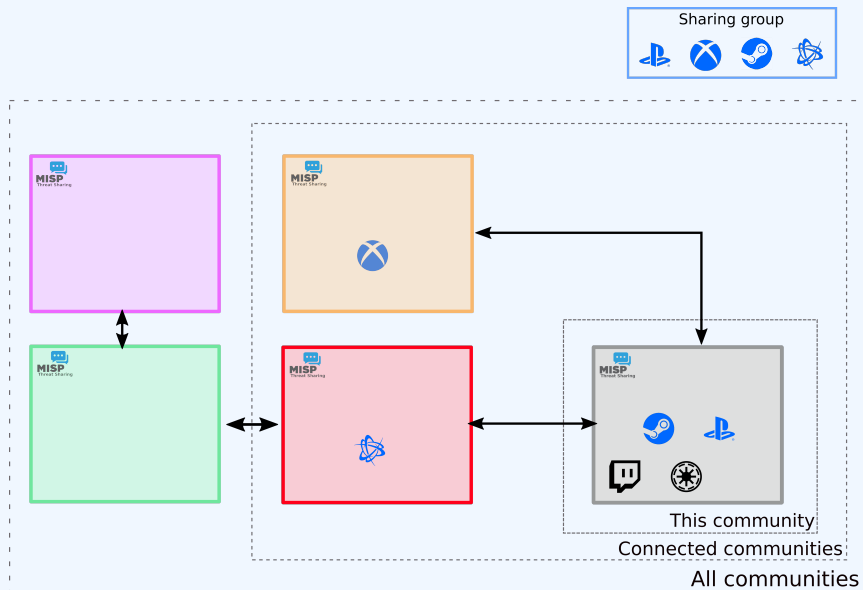
MISP offers granular distribution settings:

- Organisation only
- This community
- Connected communities
- All communities
- Distribution lists - aka **Sharing groups**



At multiple levels: **Events, Attributes, Objects** (and their **Attributes**) and **Galaxy-clusters**

SHARING IN MISP: DISTRIBUTION

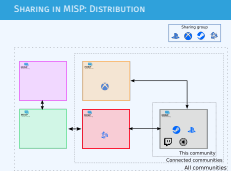


2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Data sharing in MISP

└ Sharing in MISP: Distribution



DATA LAYER

2022-09-13

An Introduction to Cybersecurity Information
Sharing

└ Data layer

DATA LAYER

■ Data layer

- ▶ **Events** are encapsulations for contextually linked information
- ▶ **Attributes** are individual data points, which can be indicators or supporting data.
- ▶ **Objects** are custom templated Attribute compositions
- ▶ **Object references** are the relationships between individual building blocks
- ▶ **Shadow Attributes/Proposal** are suggestions made by users to modify an existing *attribute*
- ▶ **Sightings** are a means to convey that a data point has been seen
- ▶ **Event reports** are supporting materials for analysts to describe *events, processes, etc*

└ Data layer

└ Data layer: Naming conventions

- Data layer
 - ▶ Events are encapsulations for contextually linked information
 - ▶ Attributes are individual data points, which can be indicators or supporting data.
 - ▶ Objects are custom templated Attribute compositions
 - ▶ Object references are the relationships between individual building blocks
 - ▶ Shadow Attributes/Proposal are suggestions made by users to modify an existing attribute
 - ▶ Sightings are a means to convey that a data point has been seen
 - ▶ Event reports are supporting materials for analysts to describe events, processes, etc















DATA LAYER: EVENTS

Events are 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 / ...

IoT malware - Gafgyt.Gen28 (active) - 20190220 - 20190222

| | |
|-----------------------|--|
| Event ID | 178 |
| UUID | 5c6d21e5-bb60-47b7-b892-42e6950d2111  |
| Creator org | CIRCL |
| Owner org | Training |
| Creator user | andras.klody@circl.lu |
| Tags |  tip:white  osint:source-type="automatic-collection"  circl:incident-classification="malware"   adversary:infrastructure-action="take-down"    |
| Date | 2019-02-20 |
| Threat Level |  Low |
| Analysis | Completed |
| Distribution | All communities   |
| Info | IoT malware - Gafgyt.Gen28 (active) - 20190220 - 20190222 |
| Published | Yes (2020-11-28 07:53:39) |
| #Attributes | 2601 (296 Objects) |
| First recorded change | 2019-02-20 09:46:24 |
| Last change | 2020-10-10 07:36:28 |
| Modification map |  |
| Sightings | 0 (0) - restricted to own organisation only  |

An Introduction to Cybersecurity Information Sharing

└ Data layer

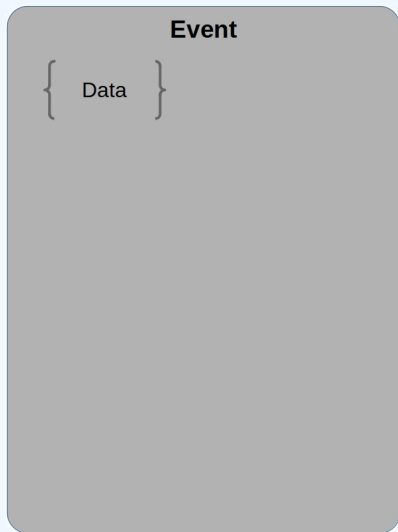
└ Data layer: Events

2022-09-13

Events are 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 / ...



| | |
|---|--|
| IoT malware - Gafgyt.Gen28 (active) - 20190220 - 20190222 | |
| Event ID | 178 |
| UUID | 5c6d21e5-bb60-47b7-b892-42e6950d2111 |
| Creator org | CIRCL |
| Owner org | Training |
| Creator user | andras.klody@circl.lu |
| Tags | tip:white osint:source-type="automatic-collection" circl:incident-classification="malware" adversary:infrastructure-action="take-down" |
| Date | 2019-02-20 |
| Threat Level | Low |
| Analysis | Completed |
| Distribution | All communities |
| Info | IoT malware - Gafgyt.Gen28 (active) - 20190220 - 20190222 |
| Published | Yes (2020-11-28 07:53:39) |
| #Attributes | 2601 (296 Objects) |
| First recorded change | 2019-02-20 09:46:24 |
| Last change | 2020-10-10 07:36:28 |
| Modification map | |
| Sightings | 0 (0) - restricted to own organisation only |



```
1 {  
2   "date": "2019-02-20",  
3   "info": "IoT malware - Gafgyt.Gen28 (active)",  
4   "uuid": "5c6d21e5-bb60-47b7-b892-42e6950d2111",  
5   "analysis": "2",  
6   "timestamp": "1602315388",  
7   "distribution": "3",  
8   "sharing_group_id": "0",  
9   "threat_level_id": "3",  
10  "extends_uuid": "",  
11  "Attribute": [...],  
12  "Object": [...],  
13  "EventReport": [...],  
14  "Tag": [...],  
15  "Galaxy": [...]  
16 }
```

└ Data layer

└ Data layer: Events

```
1 {  
2   "date": "2019-02-20",  
3   "info": "IoT malware - Gafgyt.Gen28 (active)",  
4   "uuid": "5c6d21e5-bb60-47b7-b892-42e6950d2111",  
5   "analysis": "2",  
6   "timestamp": "1602315388",  
7   "distribution": "3",  
8   "sharing_group_id": "0",  
9   "threat_level_id": "3",  
10  "extends_uuid": "",  
11  "Attribute": [...],  
12  "Object": [...],  
13  "EventReport": [...],  
14  "Tag": [...],  
15  "Galaxy": [...]  
16 }
```

DATA LAYER: ATTRIBUTES

Attributes are individual data points, indicators or supporting data

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

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

« previous

next »

view all

+

Filters:

All

File

Network

Financial

Proposal

Correlation

| Date | Org | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|------------|-----|------------------|--------|----------------|---|----------------|-----|--------------|--|
| 2016-02-23 | | Network activity | domain | microsoft.com | | | No | Inherit | <div><div></div><div></div><div></div></div> |
| 2016-02-23 | | Network activity | domain | google.com | | 25 | No | Inherit | <div><div></div><div></div><div></div></div> |
| 2016-02-23 | | Network activity | domain | circl.lu | | | No | Inherit | <div><div></div><div></div><div></div></div> |
| 2016-02-23 | | Network activity | ip-src | 23.100.122.175 | Derived from microsoft.com via the dns enrichment module. | | No | Inherit | <div><div></div><div></div><div></div></div> |

2022-09-13

An Introduction to Cybersecurity Information Sharing

- Data layer












- Data layer: Attributes

Data Layer: Attributes

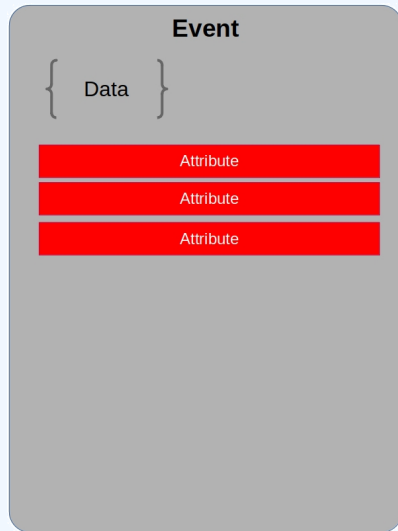
Attributes are individual data points, indicators or supporting data

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

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

| ID | Category | Type | Value | Comment | Related Events | IDS | Distribution | Actions |
|----|------------------|--------|----------------|---|----------------|-----|--------------|---|
| 1 | Network activity | domain | microsoft.com | | | No | Inherit |    |
| 2 | Network activity | domain | google.com | | 25 | No | Inherit |    |
| 3 | Network activity | domain | circl.lu | | | No | Inherit |    |
| 4 | Network activity | ip-src | 23.100.122.175 | Derived from microsoft.com via the dns enrichment module. | | No | Inherit |   |

DATA LAYER: EVENT BUILDING BLOCKS - RAW DATA



2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Raw data



DATA LAYER: ATTRIBUTES

```
1 {  
2   "type": "url",  
3   "category": "Network activity",  
4   "to_ids": true,  
5   "uuid": "5c6d24bd-d094-4dd6-a1b6-4fa3950d2111",  
6   "event_id": "178",  
7   "distribution": "5",  
8   "sharing_group_id": "0",  
9   "timestamp": "1550656701",  
10  "comment": "Delivery point for the malware",  
11  "object_id": "0",  
12  "object_relation": null,  
13  "first_seen": null,  
14  "last_seen": null,  
15  "value": "ftp://185.135.80.163/",  
16  "Tag": [...]  
17  "Galaxy": [...]  
18 }
```

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Attributes

```
1 {  
2   "type": "url",  
3   "category": "Network activity",  
4   "to_ids": true,  
5   "uuid": "5c6d24bd-d094-4dd6-a1b6-4fa3950d2111",  
6   "event_id": "178",  
7   "distribution": "5",  
8   "sharing_group_id": "0",  
9   "timestamp": "1550656701",  
10  "comment": "Delivery point for the malware",  
11  "object_id": "0",  
12  "object_relation": null,  
13  "first_seen": null,  
14  "last_seen": null,  
15  "value": "ftp://185.135.80.163/",  
16  "Tag": [...]  
17  "Galaxy": [...]  
18 }
```

DATA LAYER: MISP OBJECTS

Objects are custom templated Attribute compositions

Purpose: Groups Attributes that are intrinsically linked together

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

| | | |
|------------|------------------|---|
| 2018-03-27 | Name: file ✓ | References: 1 ✓ + |
| 2018-03-27 | Payload delivery | filename: putty.exe + |
| 2018-03-27 | Other | size-in-bytes: 774200 + |
| 2018-03-27 | Other | entropy: 6.7264597226 float + |
| 2018-03-27 | Payload delivery | md5: b6c12d88eeb910784d75a5e4df954001 md5 + |
| 2018-03-27 | Payload delivery | sha1: 5ef9515e8fd92a254dd2dcdd9c4b50afa8007b8f sha1 + |
| 2018-03-27 | Payload delivery | sha256: 81de431987304676134138705fc1c21188ad7f27edf6b77a6551aa693194485e sha256 + |
| 2018-03-27 | Payload delivery | sha512: e174ecf4fffb36d30c2cc66b37f82877d421244c924d5c9f39f2e0f37d85332b7d107d5ac5bd19cb7ffdcdbdd8b506d488faa30664ef610f62f3970c163cca76 sha512 + |
| 2018-03-27 | Payload delivery | malware-sample: putty.exe + |

2022-09-13

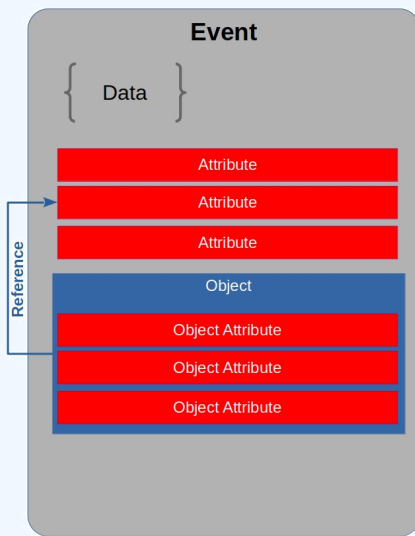
An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: MISP Objects



DATA LAYER: EVENT BUILDING BLOCKS - DATA COMPOSITION



2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Data

...



DATA LAYER: MISP OBJECTS

```
1 {  
2   "name": "elf-section",  
3   "meta-category": "file",  
4   "description": "Object describing a sect...",  
5   "template_uuid": "ca271f32-1234-4e87-b240-6b6e882de5de",  
6   "template_version": "4",  
7   "uuid": "ab5f0c85-5623-424c-bc03-d79841700d74",  
8   "timestamp": "1550655984",  
9   "distribution": "5",  
10  "sharing_group_id": "0",  
11  "comment": "",  
12  "first_seen": null,  
13  "last_seen": null,  
14  "ObjectReference": [],  
15  "Attribute": [...]  
16 }
```

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: MISP Objects

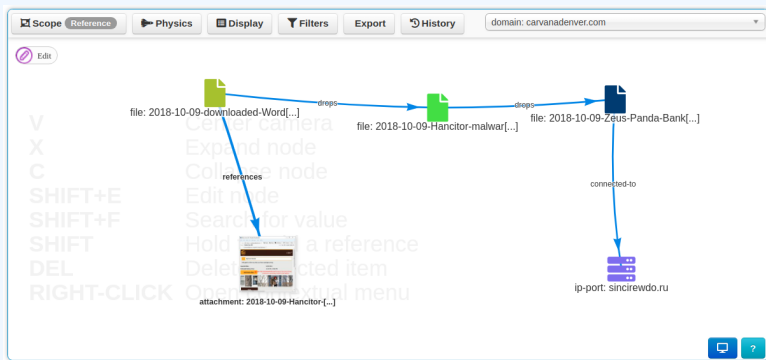
```
1 {  
2   "name": "elf-section",  
3   "meta-category": "file",  
4   "description": "Object describing a sect...",  
5   "template_uuid": "ca271f32-1234-4e87-b240-6b6e882de5de",  
6   "template_version": "4",  
7   "uuid": "ab5f0c85-5623-424c-bc03-d79841700d74",  
8   "timestamp": "1550655984",  
9   "distribution": "5",  
10  "sharing_group_id": "0",  
11  "comment": "",  
12  "first_seen": null,  
13  "last_seen": null,  
14  "ObjectReference": [],  
15  "Attribute": [...]  
16 }
```

DATA LAYER: OBJECT REFERENCES

Object references are the 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, ...

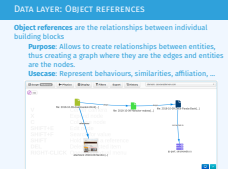


2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Object references



DATA LAYER: OBJECT REFERENCES

```
1 {  
2   "uuid": "5c6d21f9-0384-4bd2-b256-40de950d2111",  
3   "timestamp": "1602318569",  
4   "object_id": "1024",  
5   "source_uuid": "23275e05-c202-460e-aadf-819c417fb326",  
6   "referenced_uuid": "ab5foc85-5623-424c-bc03-d79841700d74",  
7   "referenced_type": "1",  
8   "relationship_type": "included-in",  
9   "comment": "Section 0 of ELF"  
10 }
```

2022-09-13

An Introduction to Cybersecurity Information Sharing

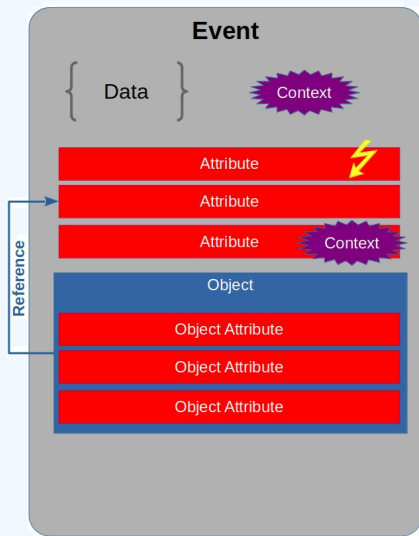
└ Data layer

└ Data layer: Object references

DATA LAYER: OBJECT REFERENCES

```
1 {  
2   "uuid": "5c6d21f9-0384-4bd2-b256-40de950d2111",  
3   "timestamp": "1602318569",  
4   "object_id": "1024",  
5   "source_uuid": "23275e05-c202-460e-aadf-819c417fb326",  
6   "referenced_uuid": "ab5foc85-5623-424c-bc03-d79841700d74",  
7   "referenced_type": "1",  
8   "relationship_type": "included-in",  
9   "comment": "Section 0 of ELF"  
10 }
```

DATA LAYER: EVENT BUILDING BLOCKS - CONTEXT



2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Context



DATA LAYER: SIGHTINGS

Sightings are a means to convey that a data point has been seen

Purpose: Allows to add temporality to the data.

Usecase: Record activity or occurrence, perform IoC expiration, ...

| Events | | | | |
|-------------------------------------|----|---------|--|--|
| <input checked="" type="checkbox"/> | No | | | |
| <input checked="" type="checkbox"/> | No | Inherit | | |
| <input checked="" type="checkbox"/> | No | Inherit | | |

```
1 {
2   "org_id": "1",
3   "date_sighting": "1573722432",
4   "uuid": "5dcd1940-5de8-4462-93dd-12a2a5e38e14",
5   "source": "",
6   "type": "o",
7   "attribute_uuid": "5da97b59-9650-4be2-9443-2194a5e38e14"
8 }
```

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Sightings

DATA LAYER: SIGHTINGS

Sightings are a means to convey that a data point has been seen

Purpose: Allows to add temporality to the data.

Usecase: Record activity or occurrence, perform IoC expiration, ...



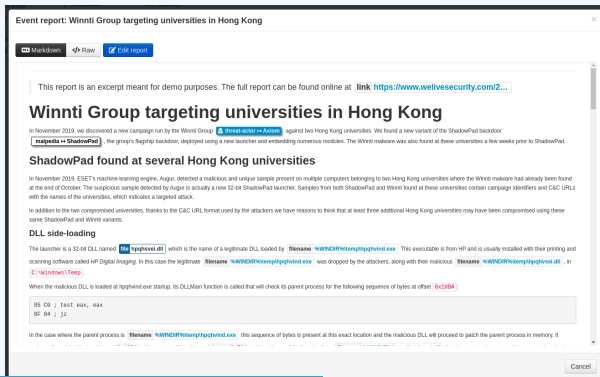
```
1 {
2   "org_id": "1",
3   "date_sighting": "1573722432",
4   "uuid": "5dcd1940-5de8-4462-93dd-12a2a5e38e14",
5   "source": "",
6   "type": "o",
7   "attribute_uuid": "5da97b59-9650-4be2-9443-2194a5e38e14"
8 }
```

DATA LAYER: EVENT REPORTS

Event reports are supporting data for analysis to describe **events, processes, ect**

Purpose: Supporting data point to describe events or processes

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



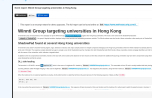
An Introduction to Cybersecurity Information Sharing

└ Data layer

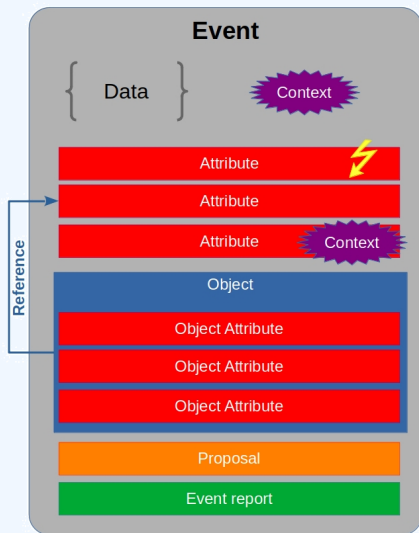
└ Data layer: Event reports

2022-09-13

Event reports are supporting data for analysis to describe events, processes, ect
Purpose: Supporting data point to describe events or processes
Usecase: Encode reports, provide more information about the Event, ...



DATA LAYER: EVENT BUILDING BLOCKS - COLLABORATION & INTELLIGENCE



2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks -



DATA LAYER: EVENT REPORTS

```
1 {  
2   "uuid": "076e240b-5a76-4a8b-9eab-cfff551993dd",  
3   "event_id": "2127",  
4   "name": "Event report (1607362986)",  
5   "content": "...",  
6   "distribution": "5",  
7   "sharing_group_id": "o",  
8   "timestamp": "1607362986"  
9 }
```

2022-09-13

An Introduction to Cybersecurity Information Sharing

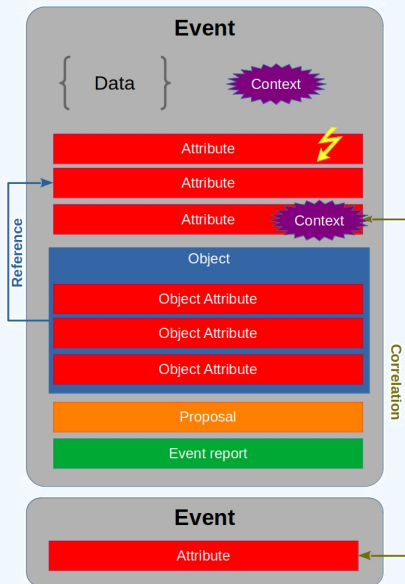
└ Data layer

└ Data layer: Event reports

DATA LAYER: EVENT REPORTS

```
1 {  
2   "uuid": "076e240b-5a76-4a8b-9eab-cfff551993dd",  
3   "event_id": "2127",  
4   "name": "Event report (1607362986)",  
5   "content": "...",  
6   "distribution": "5",  
7   "sharing_group_id": "o",  
8   "timestamp": "1607362986"  
9 }
```


DATA LAYER: EVENT BUILDING BLOCKS - FULL



2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Full



CONTEXT LAYER

2022-09-13

An Introduction to Cybersecurity Information
Sharing
└ Context layer

CONTEXT LAYER

■ Context layer

- ▶ **Tags** are free-text labels attached to events/attributes and can come from **Taxonomies**
 - Android Malware, C2, ...
- ▶ **Taxonomies** are a set of common classification allowing to express the same vocabulary among a distributed set of users and organisations
 - tlp:green,false-positive:risk="high",
admiralty-scale:information-credibility="2"

└ Context layer

└ Context layer: Naming conventions

- Context layer
 - ▶ **Tags** are free-text labels attached to events/attributes and can come from **Taxonomies**
 - Android Malware, C2, ...
 - ▶ **Taxonomies** are a set of common classification allowing to express the same vocabulary among a distributed set of users and organisations
 - tlp:green,false-positive:risk="high",
admiralty-scale:information-credibility="2"

■ Context layer

- ▶ **Galaxies** are container composed of **Galaxy-clusters** that belongs to the same family
 - Similar to what **Events** are to **Attributes**
 - Country, Threat actors, Botnet, ...
- ▶ **Galaxy-clusters** are knowledge base items coming from **Galaxies**.
 - Basically a taxonomy with additional meta-information
 - `misp-galaxy:threat-actor="APT_29"`,
`misp-galaxy:country="luxembourg"`

└ Context layer

└ Context layer: Naming conventions

- Context layer
 - ▶ **Galaxies** are container composed of **Galaxy-clusters** that belongs to the same family
 - Similar to what **Events** are to **Attributes**
 - Country, Threat actors, Botnet, ...
 - ▶ **Galaxy-clusters** are knowledge base items coming from **Galaxies**.
 - Basically a taxonomy with additional meta-information
 - `misp-galaxy:threat-actor="APT_29"`,
`misp-galaxy:country="luxembourg"`

CONTEXT LAYER: TAGS

Simple free-text labels

TLP AMBER

TLP:AMBER

Threat tlp:Amber

tlp-amber

tlp::amber

tlp:amber

```
1 {  
2   "name": "Android malware",  
3   "colour": "#22681c",  
4   "exportable": true,  
5   "numerical_value": null,  
6 }
```

An Introduction to Cybersecurity Information Sharing

- Context layer

- Context layer: Tags

2022-09-13



CONTEXT LAYER: TAXONOMIES

Simple label standardised on common set of vocabularies

Purpose: Enable efficient classification globally understood, easing consumption and automation.

Usecase: Provide classification such as: TLP, Confidence, Source, Workflows, Event type, ...

| <input type="checkbox"/> Tag | Events | Attributes | Tags |
|--|--------|------------|-------------------------------|
| <input type="checkbox"/> workflow:state="complete" | 11 | 0 | workflow:state="complete" < |
| <input type="checkbox"/> workflow:state="draft" | 0 | 0 | workflow:state="draft" < |
| <input type="checkbox"/> workflow:state="incomplete" | 55 | 10 | workflow:state="incomplete" < |
| <input type="checkbox"/> workflow:state="ongoing" | 0 | 0 | workflow:state="ongoing" < |

2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Context layer: Taxonomies

CONTEXT LAYER: TAXONOMIES

Simple label standardised on common set of vocabularies

Purpose: Enable efficient classification globally understood, easing consumption and automation.

Usecase: Provide classification such as: TLP, Confidence, Source, Workflows, Event type, ...

| <input type="checkbox"/> Tag | Events | Attributes | Tags |
|--|--------|------------|-------------------------------|
| <input type="checkbox"/> workflow:state="complete" | 11 | 0 | workflow:state="complete" < |
| <input type="checkbox"/> workflow:state="draft" | 0 | 0 | workflow:state="draft" < |
| <input type="checkbox"/> workflow:state="incomplete" | 55 | 10 | workflow:state="incomplete" < |
| <input type="checkbox"/> workflow:state="ongoing" | 0 | 0 | workflow:state="ongoing" < |

CONTEXT LAYER: TAXONOMIES

```
1 {  
2   "Taxonomy": {  
3     "namespace": "admiralty-scale",  
4     "description": "The Admiralty Scale or Ranking (also called  
5       the NATO System)...",  
6     "version": "6",  
7     "exclusive": false,  
8   },  
9   "entries": [  
10    {  
11      "tag": "admiralty-scale:information-credibility=\"1\"",  
12      "expanded": "Information Credibility: Confirmed by other  
13        sources",  
14      "numerical_value": 100,  
15      "exclusive_predicate": true,  
16    },  
17    ...  
18  ]  
19 }
```

2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Context layer: Taxonomies

CONTEXT LAYER: TAXONOMIES

```
1 "Taxonomy": {  
2   "namespace": "admiralty-scale",  
3   "description": "The Admiralty Scale or Ranking (also called  
4     the NATO System)...",  
5   "version": "6",  
6   "exclusive": false,  
7 }  
8 "entries": [  
9   {  
10    "tag": "admiralty-scale:information-credibility=\"1\"",  
11    "expanded": "Information Credibility: Confirmed by other  
12      sources",  
13    "numerical_value": 100,  
14    "exclusive_predicate": true,  
15  },  
16  ...  
17 ]
```

Collections of galaxy clusters

Threat Actor galaxy

Galaxy ID

8

Name

Threat Actor

Namespace

misp

UUID

698774c7-8022-42c4-917f-8d6e4f06ada3

Description

Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.

Version

3

= previous

next =

AllDefaultCustom0My ClustersDeletedView Fork TreeView Galaxy Relationships

apt29Filter

| ID | Published | Value | Synonyms | Owner Org | Creator Org | Default | Activity | #Events | #Relations | Description | Distribution | Actions |
|------|-----------|--------|---|-----------|-------------|---------|-------------|---------|------------|---|-----------------|-------------|
| 7059 | N/A | APT 29 | Dukes, Group 100, Cozy Duke, CozyDuke, EuroAPT, CozyBear, CozyCar, Cozer, Office Markov | MISP | MISP | ✓ | <div></div> | 0 | 000 | A 2015 report by F-Secure describe APT29 as: 'The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making. The Dukes show unusual confidence in their ability to continue successfully compromising their | All communities | <div></div> |

2022-09-13

An Introduction to Cybersecurity Information Sharing

- Context layer
 - Context layer: Galaxies



CONTEXT LAYER: GALAXY CLUSTERS

Knowledge base items including a description, links, synonyms, meta-information and relationships

Purpose: Enable description of complex high-level information for classification

Usecase: Extensively describe elements such as threat actors, countries, technique used, ...

Threat Actor :: APT 29

| | |
|----------------------|---|
| Cluster ID | 2805 |
| Name | APT 29 |
| Parent Galaxy | Threat Actor |
| Description | A 2015 report by F-Secure describe APT29 as: "The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation..." |
| Published | No |
| Default | Yes |
| Version | 190 |
| UUID | b2056ff0-00b9-482e-b11c-c771daa5f28a |
| Collection UUID | 7cdf1317-a673-4474-84ec-4f1754947823 |
| Source | MISP Project |
| Authors | Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various |
| Distribution | All communities |
| Owner Organisation | MISP |
| Creator Organisation | MISP |
| Connector tag | misp-galaxy-threat-actor="APT 29" |
| Events | 0 |
| Forked From | |
| Forked By | |

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Context layer: Galaxy clusters

2022-09-13

Knowledge base items including a description, links, synonyms, meta-information and relationships

Purpose: Enable description of complex high-level information for classification

Usecase: Extensively describe elements such as threat actors, countries, technique used, ...

| | |
|------------------------|---|
| Threat Actor :: APT 29 | |
| Cluster ID | 2805 |
| Name | APT 29 |
| Parent Galaxy | Threat Actor |
| Description | A 2015 report by F-Secure describe APT29 as: "The Dukes are a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation..." |
| Published | No |
| Default | Yes |
| Version | 190 |
| UUID | b2056ff0-00b9-482e-b11c-c771daa5f28a |
| Collection UUID | 7cdf1317-a673-4474-84ec-4f1754947823 |
| Source | MISP Project |
| Authors | Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various |
| Distribution | All communities |
| Owner Organisation | MISP |
| Creator Organisation | MISP |
| Connector tag | misp-galaxy-threat-actor="APT 29" |
| Events | 0 |
| Forked From | |
| Forked By | |

CONTEXT LAYER: GALAXY CLUSTERS

Galaxy cluster elements: Tabular view

Tabular view

JSON view

| 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 | |

Galaxy cluster elements: JSON view

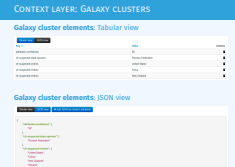
| Tabular view | JSON view | + Add JSON as cluster's elements |
|---|-----------|----------------------------------|
| <pre>{ "attribution-confidence": ["50"], "cfr-suspected-state-sponsor": ["Russian Federation"], "cfr-suspected-victims": ["United States", "China", "New Zealand", "Ukraine"] }</pre> | | |

An Introduction to Cybersecurity Information Sharing

Context layer

Context layer: Galaxy clusters

2022-09-13



CONTEXT LAYER: GALAXY CLUSTERS

```
1 {  
2   "uuid": "5edaoa53-1d98-4d01-ae06-4odaoa0002of",  
3   "type": "fellowship-characters",  
4   "value": "Aragorn wielding Anduril",  
5   "tag_name": "misp-galaxy:fellowship-characters=\"c3fe907a-6a36  
6     -4cd1-9456-dcdf35c3f907\"",  
7   "description": "The Aragorn character wielding Anduril",  
8   "source": "Middle-earth universe by J. R. R. Tolkien",  
9   "authors": null,  
10  "version": "1591347795",  
11  "distribution": "o",  
12  "sharing_group_id": null,  
13  "default": false,  
14  "extends_uuid": "5edao117-1e14-4boa-9e26-34aff331dc3b",  
15  "extends_version": "1591345431",  
16  "GalaxyElement": [...],  
17  "GalaxyClusterRelation": [...]
```

2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Context layer: Galaxy clusters

CONTEXT LAYER: GALAXY CLUSTERS

```
1 {  
2   "uuid": "5edaoa53-1d98-4d01-ae06-4odaoa0002of",  
3   "type": "fellowship-characters",  
4   "value": "Aragorn wielding Anduril",  
5   "tag_name": "misp-galaxy:fellowship-characters=\"c3fe907a-6a36  
6     -4cd1-9456-dcdf35c3f907\"",  
7   "description": "The Aragorn character wielding Anduril",  
8   "source": "Middle-earth universe by J. R. R. Tolkien",  
9   "authors": null,  
10  "version": "1591347795",  
11  "distribution": "o",  
12  "sharing_group_id": null,  
13  "default": false,  
14  "extends_uuid": "5edao117-1e14-4boa-9e26-34aff331dc3b",  
15  "extends_version": "1591345431",  
16  "GalaxyElement": [...],  
17  "GalaxyClusterRelation": [...]
```

CONTEXT LAYER: GALAXIES & GALAXY CLUSTERS

- MISP integrates MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and similar **Galaxy Matrix**
- MISP terminology of these matrixes: **Galaxy Matrix**

| Pre Attack - Attack Pattern | Enterprise Attack - Attack Pattern | Mobile Attack - Attack Pattern | | | | | | | | |
|-------------------------------------|------------------------------------|---|----------------------------------|----------------------------------|--|--|------------------------------------|------------------------------------|---|---------------------------------------|
| Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Exfiltration | Command and control |
| Spearphishing Attachment | Scripting | Screensaver | File System Permissions Weakness | Process Hollowing | Securityd Memory | Password Policy Discovery | AppleScript | Data from Information Repositories | Exfiltration Over Alternative Protocol | Standard Application Layer Protocol |
| Spearphishing via Service | Command-Line Interface | Login Item | AppCert DLLs | Code Signing | Input Capture | System Network Configuration Discovery | Distributed Component Object Model | Data from Removable Media | Exfiltration Over Command and Control Channel | Communication Through Removable Media |
| Trusted Relationship | User Execution | Trap | Application Shimming | Rootkit | Bash History | Process Discovery | Pass the Hash | Man in the Browser | Data Compressed | Custom Command and Control Protocol |
| Replication Through Removable Media | Regsvcs/Regasm | System Firmware | Scheduled Task | NTFS File Attributes | Exploitation for Credential Access | Network Share Discovery | Exploitation of Remote Services | Data Staged | Automated Exfiltration | Multi-Stage Channels |
| Exploit Public-Facing Application | Trusted Developer Utilities | Registry Run Keys / Start Folder | Startup Items | Exploitation for Defense Evasion | Private Keys | Peripheral Device Discovery | Remote Desktop Protocol | Screen Capture | Scheduled Transfer | Remote Access Tools |
| Spearphishing Link | Windows Management Instrumentation | LC_LOAD_DYLIB Addition | New Service | Network Share Connection Removal | Brute Force | Account Discovery | Pass the Ticket | Email Collection | Data Encrypted | Uncommonly Used Port |
| Valid Accounts | Service Execution | LSASS Driver | Sudo Caching | Process Doppelganging | Password Filter DLL | System Information Discovery | Windows Remote Management | Clipboard Data | Exfiltration Over Other Network Medium | Multilayer Encryption |
| Supply Chain Compromise | CMSTP | Rccommon | Process Injection | Disabling Security Tools | Two-Factor Authentication Interception | System Network Connections Discovery | Windows Admin Shares | Video Capture | Exfiltration Over Physical Medium | Domain Fronting |
| Drive-by Compromise | Control Panel Items | Authentication Package | Bypass User Account Control | Timestamp | LLMNR/NBT-NS Poisoning | Network Service Scanning | Remote Services | Audio Capture | Data Transfer Size Limits | Data Obfuscation |
| Hardware Additions | Dynamic Data Exchange | Component Firmware | Extra Window Memory Injection | Modify Registry | Credentials in Files | File and Directory Discovery | Taint Shared Content | Data from Network Shared Drive | | Connection Proxy |
| | Source | Windows Management Instrumentation Event Subscription | Setuid and Setgid | Indicator Removal from Tools | Forced Authentication | Security Software Discovery | Application Deployment Software | Data from Local System | | Commonly Used Port |
| | Space after Filename | Change Default File | Launch Daemon | Hidden Window | Keychain | System Service Discovery | Third-party Software | Automated Collection | | Data Encoding |

An Introduction to Cybersecurity Information Sharing

Context layer

Context layer: Galaxies & Galaxy clusters

- MISP integrates MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and similar **Galaxy Matrix**
- MISP terminology of these matrixes: **Galaxy Matrix**

| Pre Attack - Attack Pattern | Enterprise Attack - Attack Pattern | Mobile Attack - Attack Pattern | | | | | | | | |
|-------------------------------------|------------------------------------|---|----------------------------------|----------------------------------|--|--|------------------------------------|------------------------------------|---|---------------------------------------|
| Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Exfiltration | Command and control |
| Spearphishing Attachment | Scripting | Screensaver | File System Permissions Weakness | Process Hollowing | Securityd Memory | Password Policy Discovery | AppleScript | Data from Information Repositories | Exfiltration Over Alternative Protocol | Standard Application Layer Protocol |
| Spearphishing via Service | Command-Line Interface | Login Item | AppCert DLLs | Code Signing | Input Capture | System Network Configuration Discovery | Distributed Component Object Model | Data from Removable Media | Exfiltration Over Command and Control Channel | Communication Through Removable Media |
| Trusted Relationship | User Execution | Trap | Application Shimming | Rootkit | Bash History | Process Discovery | Pass the Hash | Man in the Browser | Data Compressed | Custom Command and Control Protocol |
| Replication Through Removable Media | Regsvcs/Regasm | System Firmware | Scheduled Task | NTFS File Attributes | Exploitation for Credential Access | Network Share Discovery | Exploitation of Remote Services | Data Staged | Automated Exfiltration | Multi-Stage Channels |
| Exploit Public-Facing Application | Trusted Developer Utilities | Registry Run Keys / Start Folder | Startup Items | Exploitation for Defense Evasion | Private Keys | Peripheral Device Discovery | Remote Desktop Protocol | Screen Capture | Scheduled Transfer | Remote Access Tools |
| Spearphishing Link | Windows Management Instrumentation | LC_LOAD_DYLIB Addition | New Service | Network Share Connection Removal | Brute Force | Account Discovery | Pass the Ticket | Email Collection | Data Encrypted | Uncommonly Used Port |
| Valid Accounts | Service Execution | LSASS Driver | Sudo Caching | Process Doppelganging | Password Filter DLL | System Information Discovery | Windows Remote Management | Clipboard Data | Exfiltration Over Other Network Medium | Multilayer Encryption |
| Supply Chain Compromise | CMSTP | Rccommon | Process Injection | Disabling Security Tools | Two-Factor Authentication Interception | System Network Connections Discovery | Windows Admin Shares | Video Capture | Exfiltration Over Physical Medium | Domain Fronting |
| Drive-by Compromise | Control Panel Items | Authentication Package | Bypass User Account Control | Timestamp | LLMNR/NBT-NS Poisoning | Network Service Scanning | Remote Services | Audio Capture | Data Transfer Size Limits | Data Obfuscation |
| Hardware Additions | Dynamic Data Exchange | Component Firmware | Extra Window Memory Injection | Modify Registry | Credentials in Files | File and Directory Discovery | Taint Shared Content | Data from Network Shared Drive | | Connection Proxy |
| | Source | Windows Management Instrumentation Event Subscription | Setuid and Setgid | Indicator Removal from Tools | Forced Authentication | Security Software Discovery | Application Deployment Software | Data from Local System | | Commonly Used Port |
| | Space after Filename | Change Default File | Launch Daemon | Hidden Window | Keychain | System Service Discovery | Third-party Software | Automated Collection | | Data Encoding |

```

1 {
2   "description": "Universal Development and Security Guidelines as
3     Applicable to Election Technology.",
4   "icon": "map",
5   "kill_chain_order": {           \\Tab in the matrix
6     "example-of-threats": [       \\Column in the matrix
7       "setup | party/candidate-registration",
8       "setup | electoral-rolls",
9       "campaign | campaign-IT",
10      "all-phases | government-IT",
11      "voting | election-technology",
12      "campaign/public-communication | media/press"
13    ]
14  },
15  "name": "Election guidelines",
16  "namespace": "misp",
17  "type": "guidelines",
18  "uuid": "c1dc03b2-89b3-42a5-9d41-782ef726435a",
19  "version": 1
20 }
```

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Galaxy JSON matrix-like

```

1 {
2   "description": "Universal Development and Security Guidelines as
3     Applicable to Election Technology.",
4   "icon": "map",
5   "kill_chain_order": {           \\Tab in the matrix
6     "example-of-threats": [       \\Column in the matrix
7       "setup | party/candidate-registration",
8       "setup | electoral-rolls",
9       "campaign | campaign-IT",
10      "all-phases | government-IT",
11      "voting | election-technology",
12      "campaign/public-communication | media/press"
13    ]
14  },
15  "name": "Election guidelines",
16  "namespace": "misp",
17  "type": "guidelines",
18  "uuid": "c1dc03b2-89b3-42a5-9d41-782ef726435a",
19  "version": 1
20 }
```

CLUSTER JSON MATRIX-LIKE

```
1 {
2   "description": "DoS or overload of party/campaign
3     registration, causing them to miss the deadline",
4   "meta": {
5     "date": "March 2018.",
6     "kill_chain": [ \\Define in which column the cluster should be placed
7       "example-of-threats:setup | party/candidate-registration"
8     ],
9     "refs": [
10      "https://www.ria.ee/sites/default/files/content-editors/
11        kuberturve/cyber_security_of_election_technology.pdf"
12    ]
13  },
14  "uuid": "154c6186-a007-4460-a029-ea23163448fe",
15  "value": "DoS or overload of party/campaign registration,
16    causing them to miss the deadline"
17 }
```

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Cluster JSON matrix-like

2022-09-13

```
1 "description": "DoS or overload of party/campaign
2   registration, causing them to miss the deadline",
3 "meta": {
4   "date": "March 2018.",
5   "kill_chain": [ \\Define in which column the cluster should be placed
6     "example-of-threats:setup | party/candidate-registration"
7   ],
8   "refs": [
9     "https://www.ria.ee/sites/default/files/content-editors/
10       kuberturve/cyber_security_of_election_technology.pdf"
11   ]
12 },
13 "uuid": "154c6186-a007-4460-a029-ea23163448fe",
14 "value": "DoS or overload of party/campaign registration,
15   causing them to miss the deadline"
16 }
```

EXPRESSING RELATION BETWEEN CLUSTERS

- Cluster can be related to one or more clusters using default relationships from MISP objects and a list of tags to classify the relation.

```
1      "related": [  
2      {  
3        "dest-uuid": "5ce5392a-3a6c-4e07-9df3-9b6a9159ac45",  
4        "tags": [  
5          "estimates-language:likelihood-probability=\"likely\"",  
6        ],  
7        "type": "similar"  
8      }  
9    ],  
10    "uuid": "oca45163-e223-4167-b1af-f088ed14a93d",  
11    "value": "Putter Panda"
```

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Expressing relation between clusters

- Cluster can be related to one or more clusters using default relationships from MISP objects and a list of tags to classify the relation.

```
1      "related": [  
2      {  
3        "dest-uuid": "5ce5392a-3a6c-4e07-9df3-9b6a9159ac45",  
4        "tags": [  
5          "estimates-language:likelihood-probability=\"likely\"",  
6        ],  
7        "type": "similar"  
8      }  
9    ],  
10    "uuid": "oca45163-e223-4167-b1af-f088ed14a93d",  
11    "value": "Putter Panda"
```

■ Supported by the grant 2018-LU-IA-0148



Co-financed by the European Union
Connecting Europe Facility

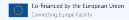
2022-09-13

An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Acknowledgements

■ Supported by the grant 2018-LU-IA-0148



Co-financed by the European Union
Connecting Europe Facility