

# AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

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

MISP PROJECT



2024-04-15

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

2024-04-15

## 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, ...

2024-04-15

## 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

2024-04-15

An Introduction to Cybersecurity Information  
Sharing

└─ Data sharing in MISP

DATA SHARING IN MISP

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-5848a5e38e14				
Name	Banking sector in Europe				
Releasability	Banks located in Europe				
Description	Everything banking				
Selectable	<input checked="" type="checkbox"/>				
Created by	Training				
Organisations		Instances			
Name	Local	Extend	Name	Url	All orgs
Training	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Local Instance	https://glocoska.eu	<input checked="" type="checkbox"/>
A-FUNKY-HUNGARIAN-BANK.hu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	https://glocoska.eu	https://glocoska.eu	<input checked="" type="checkbox"/>
AFB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Italian Bank	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
NCSC-NL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

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

└ Data sharing in MISP

└ Sharing in MISP: Distribution

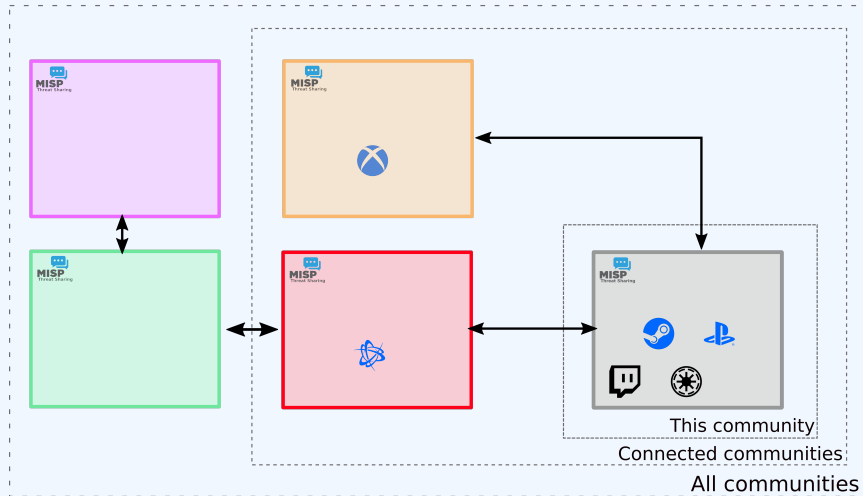
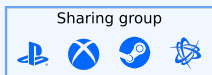
MISP offers granular distribution settings:

- 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

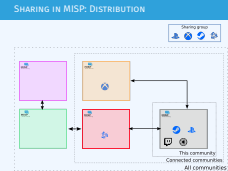


2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Data sharing in MISP

└ Sharing in MISP: Distribution



# DATA LAYER

2024-04-15

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*

2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ 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



**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	<span>ip:white</span> <span>osint:source-type="automatic-collection"</span> <span>circl:incident-classification="malware"</span> <span>adversary:infrastructure-action="take-down"</span>
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

2024-04-15

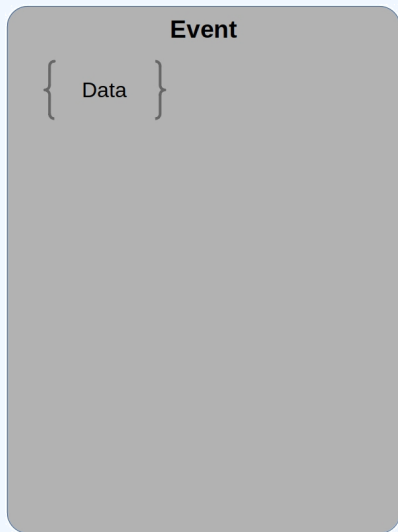
## An Introduction to Cybersecurity Information Sharing

└ Data layer

└ 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 / ...





2024-04-15

An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Base



```
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 }
```

**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	
2016-02-23		Network activity	domain	google.com		25	No	Inherit	
2016-02-23		Network activity	domain	circl.lu			No	Inherit	
2016-02-23		Network activity	ip-src	23.100.122.175	Derived from microsoft.com via the dns enrichment module.		No	Inherit	

2024-04-15

## An Introduction to Cybersecurity Information Sharing

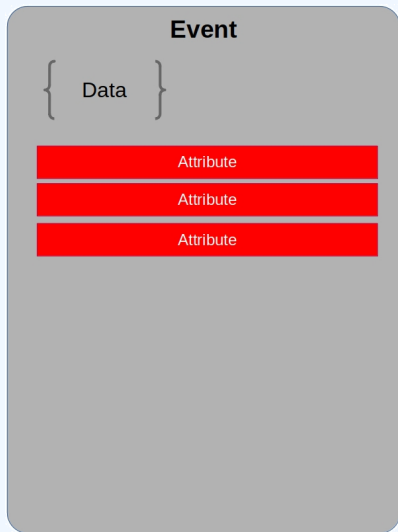
- Data layer

- 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, ...



2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Raw data



```
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

└ 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	<b>filename:</b> filename	putty.exe
2018-03-27	Other	<b>size-in-bytes:</b> size-in-bytes	774200
2018-03-27	Other	<b>entropy:</b> float	6.7264597226
2018-03-27	Payload delivery	<b>md5:</b> md5	b6c12d88eeb910784d75a5e4df954001
2018-03-27	Payload delivery	<b>sha1:</b> sha1	5ef9515e8fd92a254dd2dcdd9c4b50afa8007b8f
2018-03-27	Payload delivery	<b>sha256:</b> sha256	81de431987304676134138705fc1c21188ad7f27edf6b77a6551aa693194485e
2018-03-27	Payload delivery	<b>sha512:</b> sha512	e174ecf4fffb36d30c2cc66b37f82877d421244c924d5c9f39f2e0f37d85332b7d107d5ac5bd19cb7ffdcdbdd8b506d488faa30664ef610f62f3970c163cca76
2018-03-27	Payload delivery	<b>malware-sample:</b>	putty.exe

2024-04-15

## An Introduction to Cybersecurity Information Sharing

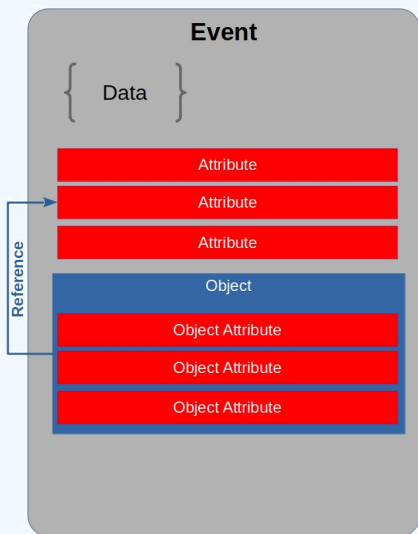
└ Data layer

└ 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, ...



# DATA LAYER: EVENT BUILDING BLOCKS - DATA COMPOSITION



2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Data





```
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

└ Data layer: MISP Objects

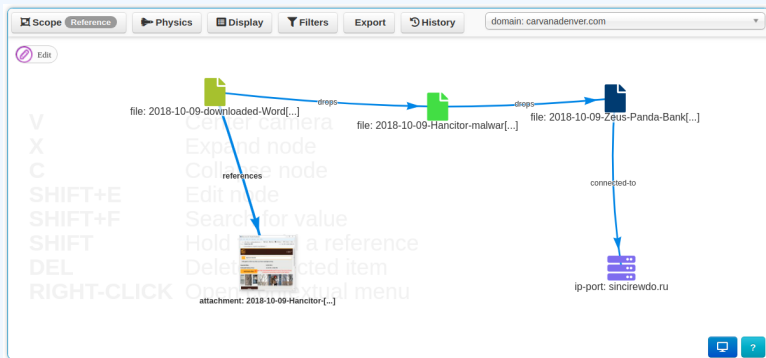
```
1 {  
2   "name": "elf-section",  
3   "meta-category": "file",  
4   "description": "Object describing a sect...",  
5   "template_uuid": "ca271f32-1234-4e87-b240-6b6e882de5de",  
6   "template_version": "4",  
7   "uuid": "ab5f0c85-5623-424c-bc03-d79841700d74",  
8   "timestamp": "1550655984",  
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, ...



2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Data layer

└ 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, ...

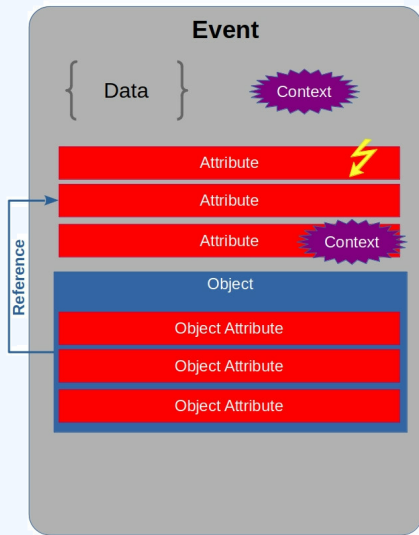


└ Data layer

└ 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": "ab5f0c85-5623-424c-bc03-d79841700d74",
7   "referenced_type": "1",
8   "relationship_type": "included-in",
9   "comment": "Section 0 of ELF"
10 }
```

```
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": "ab5f0c85-5623-424c-bc03-d79841700d74",
7   "referenced_type": "1",
8   "relationship_type": "included-in",
9   "comment": "Section 0 of ELF"
10 }
```



2024-04-15

## 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 <b>Sightings</b> CIRCL: 2 (2017-03-19 16:17:59)
<input checked="" type="checkbox"/>	No (2/0/0)
<input checked="" type="checkbox"/>	No Inherit (0/0/0)

```
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 }
```

2024-04-15

## 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, ...

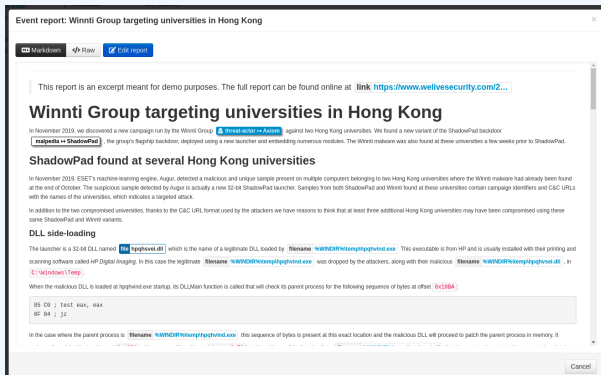
```
1 {  
2   "org_id": "1",  
3   "date_sighting": "1573722432",  
4   "uuid": "5dcd1940-5de8-4462-93dd-12a2a5e38e14",  
5   "source": "",  
6   "type": "o",  
7   "attribute_uuid": "5da97b59-9650-4be2-9443-2194a5e38e14"  
8 }
```

# 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, ...



2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event reports

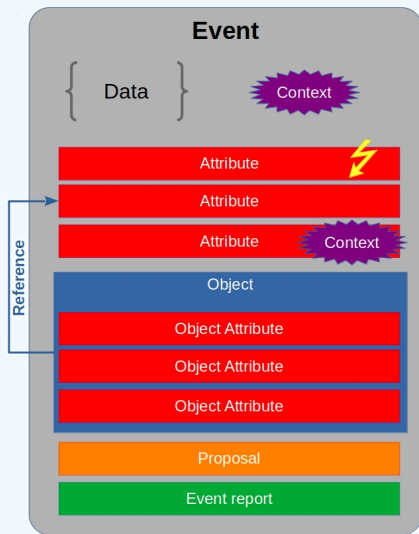
Event reports are supporting data for analysis to describe events, processes, ect

**Purpose:** Supporting data point to describe events or processes

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



# DATA LAYER: EVENT BUILDING BLOCKS - COLLABORATION & INTELLIGENCE



2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks -



```
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": "0",  
8   "timestamp": "1607362986"  
9 }
```

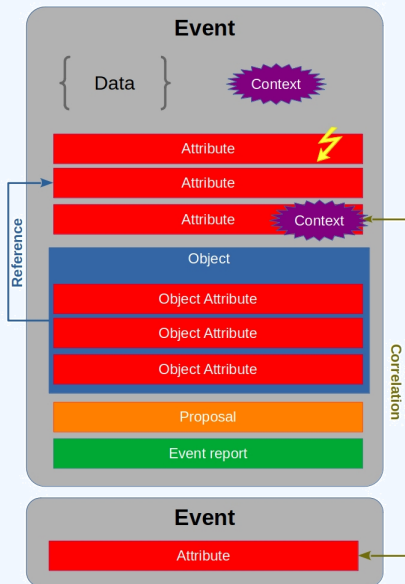
└ Data layer

└ 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": "0",  
8   "timestamp": "1607362986"  
9 }
```



# DATA LAYER: EVENT BUILDING BLOCKS - FULL

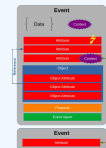


2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Data layer

└ Data layer: Event building blocks - Full



2024-04-15

An Introduction to Cybersecurity Information  
Sharing

└ Context layer

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 }
```

└ Context layer

└ Context layer: Tags

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 }
```

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

└ 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, ...

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" ↗

```
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 }
```

└ Context layer

└ Context layer: Taxonomies

```
1
2
3 "Taxonomy": {
4   "namespace": "admiralty-scale",
5   "description": "The Admiralty Scale or Ranking (also called
6     the NATO System)...",
7   "version": "6",
8   "exclusive": false,
9 }
10
11 "entries": [
12   {
13     "tag": "admiralty-scale:information-credibility=\"1\"",
14     "expanded": "Information Credibility: Confirmed by other
15       sources",
16     "numerical_value": 100,
17     "exclusive_predicate": true,
18   },
19   ...
20 ]
```

## 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 →](#)

[All](#) [Default](#) [Custom](#) [0](#) [My Clusters](#) [Deleted](#) [View Fork Tree](#) [View Galaxy Relationships](#)

 [Filter](#)| 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 | ✓ |  | 0 | 0 0 0 | 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 | [+](#) [-](#) [↻](#) [🗑️](#) |

2024-04-15

# An Introduction to Cybersecurity Information Sharing

- Context layer

- Context layer: Galaxies

### Collections of galaxy clusters

The screenshot shows a web interface for a 'Threat Actor galaxy'. It features a search bar at the top with the text 'apt29'. Below the search bar, there is a table listing threat actors. The first entry is 'APT 29' with a value of 'APT 29' and a description that matches the text in the main slide. The interface includes various navigation and filtering options.



# 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	7cdfb317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulauroy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	<a href="#">↗</a>
Creator Organisation	<a href="#">↗</a>
Connector tag	misp-galaxy-threat-actor="APT 29"
Events	0
Forked From	
Forked By	

2024-04-15

## An Introduction to Cybersecurity Information Sharing

└ Context layer

└ 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	7cdfb317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulauroy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	<a href="#">↗</a>
Creator Organisation	<a href="#">↗</a>
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 ↓		
attribution-confidence	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

```
{
  "attribution-confidence": [
    "50"
  ],
  "cfr-suspected-state-sponsor": [
    "Russian Federation"
  ],
  "cfr-suspected-victims": [
    "United States",
    "China",
    "New Zealand",
    "Ukraine"
  ]
}
```

2024-04-15

# An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Context layer: Galaxy clusters



```
1 {
2   "uuid": "5eda0a53-1d98-4d01-ae06-40da0a00020f",
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": "5eda0117-1e14-4b0a-9e26-34aff331dc3b",
15  "extends_version": "1591345431",
16  "GalaxyElement": [...],
17  "GalaxyClusterRelation": [...]
```

└ Context layer

└ Context layer: Galaxy clusters

```
1 {
2   "uuid": "5eda0a53-1d98-4d01-ae06-40da0a00020f",
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": "5eda0117-1e14-4b0a-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	
Spearpishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securty Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol	
Spearpishing 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	Rookit	Bash History	Process Discovery	Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol	
Replication Through Removable Media	Regovcs/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	
Spearpishing 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 Doppelgänger	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	

2024-04-15

## 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**

```
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": "c1dco3b2-89b3-42a5-9d41-782ef726435a",
19  "version": 1
}
```

## An Introduction to Cybersecurity Information Sharing

└ Context layer

└ Galaxy JSON matrix-like

2024-04-15

```
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": "c1dco3b2-89b3-42a5-9d41-782ef726435a",
19 "version": 1
}
```

```
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 }
```

└ Context layer

└ Cluster JSON matrix-like

```
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 }
```

- 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      "estimative-language:likelihood-probability=\"likely\"  
6    ],  
7    "type": "similar"  
8  }  
9  ],  
10 "uuid": "oca45163-e223-4167-b1af-f088ed14a93d",  
11 "value": "Putter Panda"
```

└ 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      "estimative-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

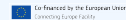
2024-04-15

## 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