An Introduction to Cybersecurity Information Sharing

MISP - Threat Sharing

CIRCL / Team MISP Project

MISP Project
https://www.misp-project.org/

13th ENISA-EC3 Workshop

MISP Threat Sharing

An Introduction to Cybersecurity Information Sharing
MISP - Threat Sharing
CIRCL / Team MISP Project
MISP Project
https://www.misp-project.org/
13th ENISA-EC3 Workshop
MISP Threat Sharing

Content of the presentation

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

Content of the presentation
Data sharing in MISP
Data models for the Data layer
Data models for the Context layer

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, ...

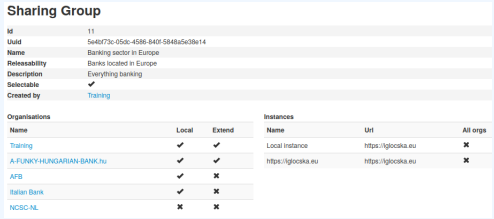
Layers of data model
- Data layer
  - The raw data itself as well as element to link them together
  - Indicators, Observables and means to contextually link them
  - MISP terminology: Event, Attributes, misp-objects, ...
- Context layer
  - As important as the data layer, allow triage, false-positive 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

Sharing in MISP: Distribution

MISP offers granulars distribution settings:

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



Sharing Group

Id	11
Uuid	5e46f73c-05d0-45f6-840f-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

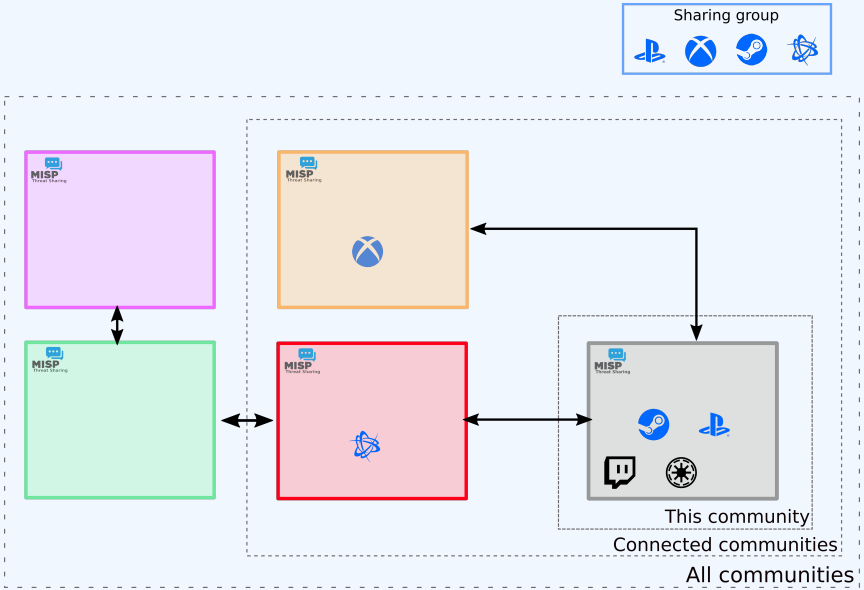
Name	Url	All orgs
Local instance	https://igloocska.eu	✖
https://igloocska.eu	https://igloocska.eu	✖

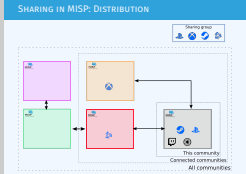
At multiple levels: **Events**, **Attributes**, **Objects** (and their **Attributes**) and **Galaxy-clusters**

Sharing in MISP: Distribution
MISP offers granulars 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





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: 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

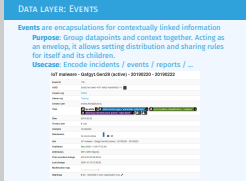
Events are encapsulations for contextually linked information

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

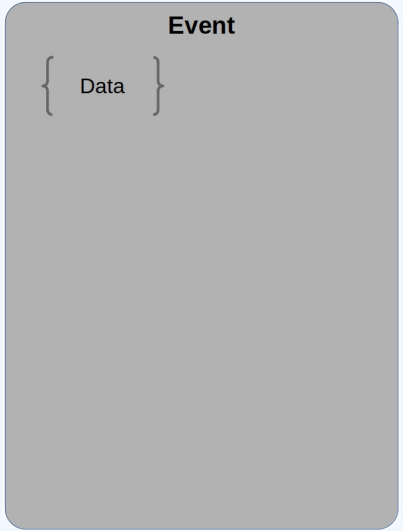
Usecase: Encode incidents / events / reports / ...

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.iklody@circl.lu
Tags	tlp:white x osint:source-type="automatic-collection" x circl:incident-classification="malware" x adversary:infrastructure-action="take-down" x
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.



Data layer: Event building blocks - Base



Data layer: Event building blocks - Base

Data layer: Events

```
{
    "date": "2019-02-20",
    "info": "IoT malware - Gafgyt.Gen28 (active)",
    "uuid": "5c6d21e5-bb60-47b7-b892-42e6950d2111",
    "analysis": "2",
    "timestamp": "1602315388",
    "distribution": "3",
    "sharing_group_id": "0",
    "threat_level_id": "3",
    "extends_uuid": "",
    "Attribute": [...],
    "Object": [...],
    "EventReport": [...],
    "Tag": [...],
    "Galaxy": [...]
}
```

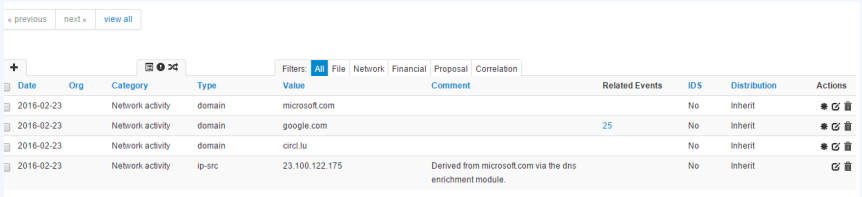

Data layer: Events

Data layer: Attributes

Attributes are individual data points, indicators or supporting data

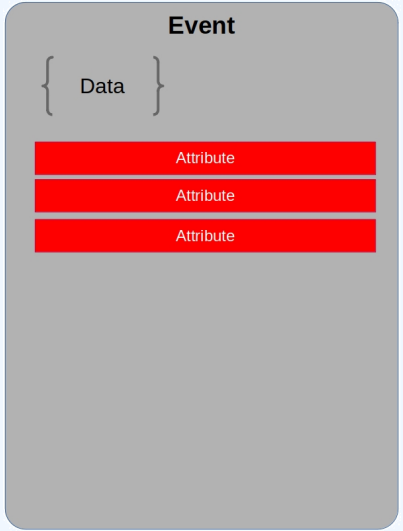
Purpose: Individual data point. Can be an indicator or supporting data.

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



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, ...

Data layer: Event building blocks - Raw data



Data layer: Event building blocks - Raw data

Data layer: Attributes

```
{
    "type": "url",
    "category": "Network activity",
    "to_ids": true,
    "uuid": "5c6d24bd-d094-4dd6-a1b6-4fa3950d2111",
    "event_id": "178",
    "distribution": "5",
    "sharing_group_id": "0",
    "timestamp": "1550656701",
    "comment": "Delivery point for the malware",
    "object_id": "0",
    "object_relation": null,
    "first_seen": null,
    "last_seen": null,
    "value": "ftp://185.135.80.163/",
    "Tag": [...]
    "Galaxy": [...]
}
```


Data layer: Attributes

{
"type": "url",
"category": "Network activity",
"to_ids": true,
"uuid": "5c6d24bd-d094-4dd6-a1b6-4fa3950d2111",
"event_id": "178",
"distribution": "5",
"sharing_group_id": "0",
"timestamp": "1550656701",
"comment": "Delivery point for the malware",
"object_id": "0",
"object_relation": null,
"first_seen": null,
"last_seen": null,
"value": "ftp://185.135.80.163/",
"Tag": [...]
"Galaxy": [...]
}

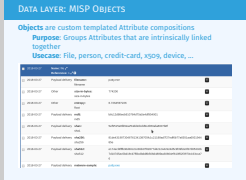
Data layer: MISP Objects

Objects are custom templated Attribute compositions

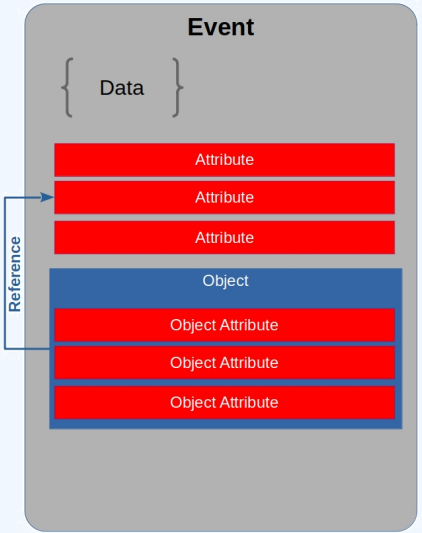
Purpose: Groups Attributes that are intrinsically linked together

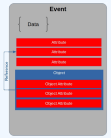
Usecase: File, person, credit-card, x509, device, ...

2018-03-27	**Name:** file **References:** 1			
2018-03-27	Payload delivery	**filename:** filename	putty.exe	+
2018-03-27	Other	**size-in-bytes:** size-in-bytes	774200	+
2018-03-27	Other	**entropy:** float	6.7264597226	+
2018-03-27	Payload delivery	**md5:** md5	b6c12d88eeb910784d75a5e4df954001	+
2018-03-27	Payload delivery	**sha1:** sha1	5ef9515e8fd92a254dd2dcdd9c4b50afa8007b8f	+
2018-03-27	Payload delivery	**sha256:** sha256	81de4319873046761341387 05fc1c21188ad7f27edf6b77a6551aa693194485e	+
2018-03-27	Payload delivery	**sha512:** sha512	e174ecf4fffb36d30c2cc66b37f82877d421244c924d5c9f39f2e0f37d85332b7d107d5ac5bd19cb7ffdcdbdd8b506d488faa30664ef610f62f3970c163cca76	+
2018-03-27	Payload delivery	**malware-sample:**	putty.exe	+



Data layer: Event building blocks - Data composition





Data layer: MISP Objects

```
{
    "name": "elf-section",
    "meta-category": "file",
    "description": "Object describing a sect...",
    "template_uuid": "ca271f32-1234-4e87-b240-6b6e882de5de",
    "template_version": "4",
    "uuid": "ab5f0c85-5623-424c-bc03-d79841700d74",
    "timestamp": "1550655984",
    "distribution": "5",
    "sharing_group_id": "0",
    "comment": "",
    "first_seen": null,
    "last_seen": null,
    "ObjectReference": [],
    "Attribute": [...]
}
```


Data layer: MISP Objects

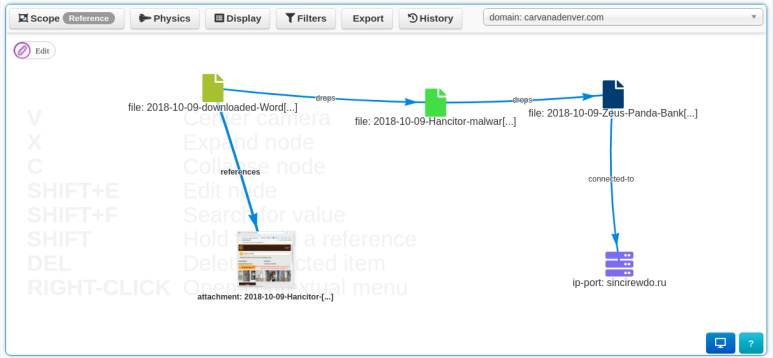
{
"name": "elf-section",
"meta-category": "file",
"description": "Object describing a sect...",
"template_uuid": "ca271f32-1234-4e87-b240-6b6e882de5de",
"template_version": "4",
"uuid": "ab5f0c85-5623-424c-bc03-d79841700d74",
"timestamp": "1550655984",
"distribution": "5",
"sharing_group_id": "0",
"comment": "",
"first_seen": null,
"last_seen": null,
"ObjectReference": [],
"Attribute": [...]
}

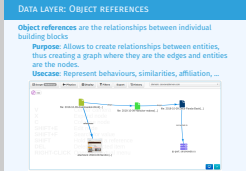
Data layer: Object references

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, ...

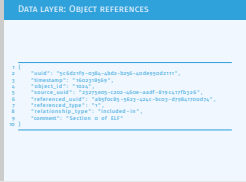




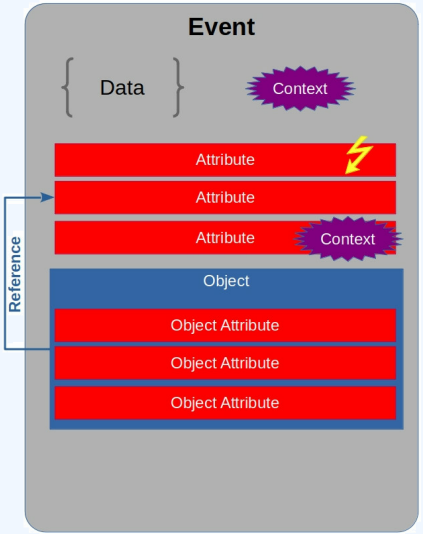
Data layer: Object references

```
{
    "uuid": "5c6d21f9-0384-4bd2-b256-40de950d2111",
    "timestamp": "1602318569",
    "object_id": "1024",
    "source_uuid": "23275e05-c202-460e-aadf-819c417fb326",
    "referenced_uuid": "ab5f0c85-5623-424c-bc03-d79841700d74",
    "referenced_type": "1",
    "relationship_type": "included-in",
    "comment": "Section 0 of ELF"
}
```


Data layer: Object references



Data layer: Event building blocks - Context



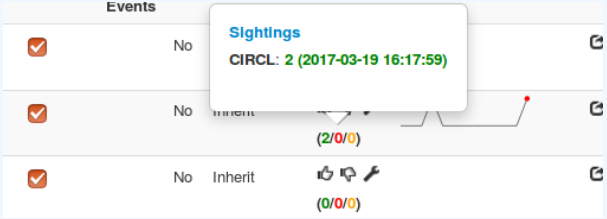
Data layer: Event building blocks - Context

Data layer: Sightings

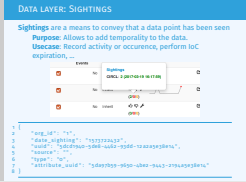
Sightings are a means to convey that a data point has been seen

Purpose: Allows to add temporality to the data.

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



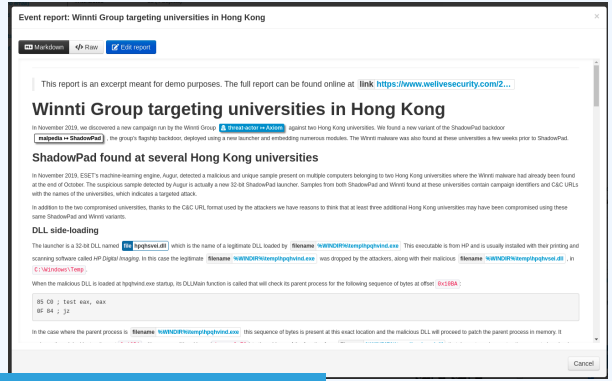

```
{
    "org_id": "1",
    "date_sighting": "1573722432",
    "uuid": "5dcd1940-5de8-4462-93dd-12a2a5e38e14",
    "source": "",
    "type": "0",
    "attribute_uuid": "5da97b59-9650-4be2-9443-2194a5e38e14"
}
```

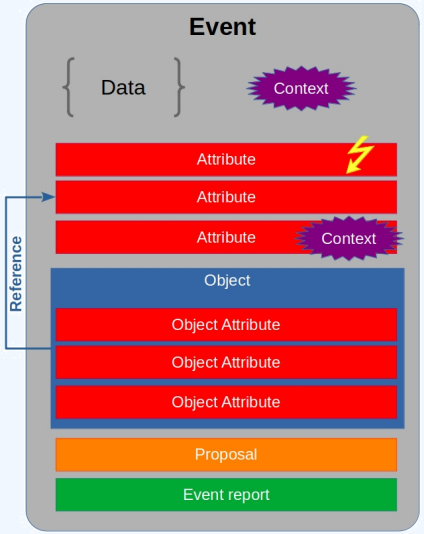
Data layer: Event reports

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



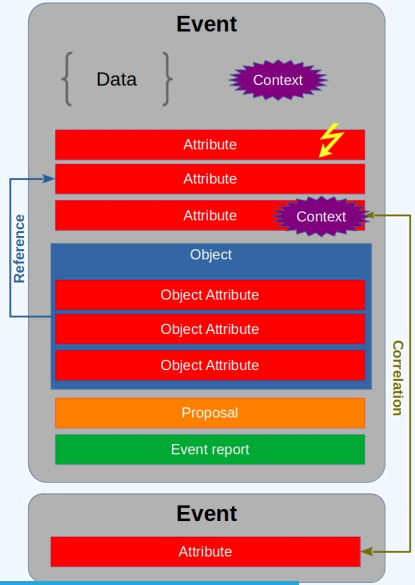
Data layer: Event reports

```
{
    "uuid": "076e240b-5a76-4a8b-9eab-cfff551993dd",
    "event_id": "2127",
    "name": "Event report (1607362986)",
    "content": "...",
    "distribution": "5",
    "sharing_group_id": "0",
    "timestamp": "1607362986"
}
```


Data layer: Event reports

{
"uuid": "076e240b-5a76-4a8b-9eab-cfff551993dd",
"event_id": "2127",
"name": "Event report (1607362986)",
"content": "...",
"distribution": "5",
"sharing_group_id": "0",
"timestamp": "1607362986"
}

Data layer: Event building blocks - Full

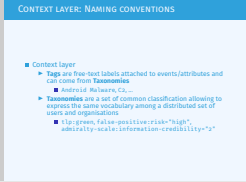


Data layer: Event building blocks - Full

Context layer

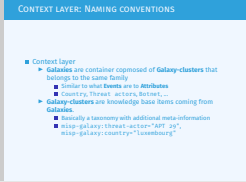
Context layer: Naming conventions

- 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: Naming conventions

- Context layer
  - **Galaxies** are container copmosed 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

```
{
    "name": "Android malware",
    "colour": "#22681c",
    "exportable": true,
    "numerical_value": null,
}
```

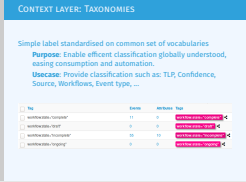

Context layer: Taxonomies

Simple label standardised on common set of vocabularies

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

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

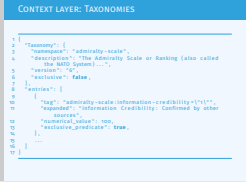
Tag	Events	Attributes	Tags
workflow:state="complete"	11	0	workflow:state="complete"
workflow:state="draft"	0	0	workflow:state="draft"
workflow:state="incomplete"	55	10	workflow:state="incomplete"
workflow:state="ongoing"	0	0	workflow:state="ongoing"



Context layer: Taxonomies

```
{
  "Taxonomy": {
    "namespace": "admiralty-scale",
    "description": "The Admiralty Scale or Ranking (also called
        the NATO System)...",
    "version": "6",
    "exclusive": false,
  },
  "entries": [
    {
      "tag": "admiralty-scale:information-credibility=\"1\"",
      "expanded": "Information Credibility: Confirmed by other
          sources",
      "numerical_value": 100,
      "exclusive_predicate": true,
    },
    ...
  ]
}
```


Context layer: Taxonomies



Context layer: Galaxies

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

apt29 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,	MISP	MISP	✔		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	All communities	

Context layer: Galaxy clusters

Kownledge 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	7cdff317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	
Creator Organisation	
Connector tag	misp-galaxy:threat-actor="APT 29"
Events	0
Forked From	
Forked By	

Context layer: Galaxy clusters
Kownledge 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, ...

Context layer: Galaxy clusters

Galaxy cluster elements: Tabular view

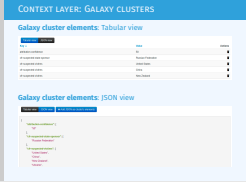
Tabular view | JSON view

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


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

Context layer: Galaxy clusters

```
{
    "uuid": "5eda0a53-1d98-4d01-ae06-40da0a00020f",
    "type": "fellowship-characters",
    "value": "Aragorn wielding Anduril",
    "tag_name": "misp-galaxy:fellowship-characters=\"c3fe907a-6a36
        -4cd1-9456-dcdf35c3f907\"",
    "description": "The Aragorn character wielding Anduril",
    "source": "Middle-earth universe by J. R. R. Tolkien",
    "authors": null,
    "version": "1591347795",
    "distribution": "0",
    "sharing_group_id": null,
    "default": false,
    "extends_uuid": "5eda0117-1e14-4b0a-9e26-34aff331dc3b",
    "extends_version": "1591345431",
    "GalaxyElement": [...],
    "GalaxyClusterRelation": [...]
}
```


Context layer: Galaxy clusters

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 Doppelgänging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption
Supply Chain Compromise	CMSTP	Rc.common	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	Timestomp	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

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

Galaxy JSON matrix-like

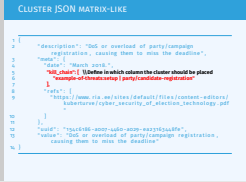
```
{
  "description": "Universal Development and Security Guidelines as
       Applicable to Election Technology.",
  "icon": "map",
  "kill_chain_order": {                    \\Tab in the matrix
      "example-of-threats": [              \\Column in the matrix
      "setup | party/candidate-registration",
      "setup | electoral-rolls",
      "campaign | campaign-IT",
      "all-phases | governement-IT",
      "voting | election-technology",
      "campaign/public-communication | media/press"
    ]
  },
  "name": "Election guidelines",
  "namespace": "misp",
  "type": "guidelines",
  "uuid": "c1dc03b2-89b3-42a5-9d41-782ef726435a",
  "version": 1
}
```


Galaxy JSON matrix-like

Cluster JSON matrix-like

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


Cluster JSON matrix-like



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.

```
      "related": [
      {
        "dest-uuid": "5ce5392a-3a6c-4e07-9df3-9b6a9159ac45",
        "tags": [
          "estimative-language:likelihood-probability=\"likely\"
              "
        ],
        "type": "similar"
      }
    ],
    "uuid": "0ca45163-e223-4167-b1af-f088ed14a93d",
    "value": "Putter Panda"
```


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.

Acknowledgements

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

Co-financed by the European Union
Connecting Europe Facility

Acknowledgements
Supported by the grant 2018-LU-IA-0148
Co-financed by the European Union
Connecting Europe Facility