

AN INTRODUCTION TO CYBERSECURITY INFORMATION SHARING

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

MISP PROJECT

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

[FIRST.ORG](https://first.org/)/AFRICA CERT



MISP
Threat 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, ...

DATA SHARING IN MISP

SHARING IN MISP: DISTRIBUTION

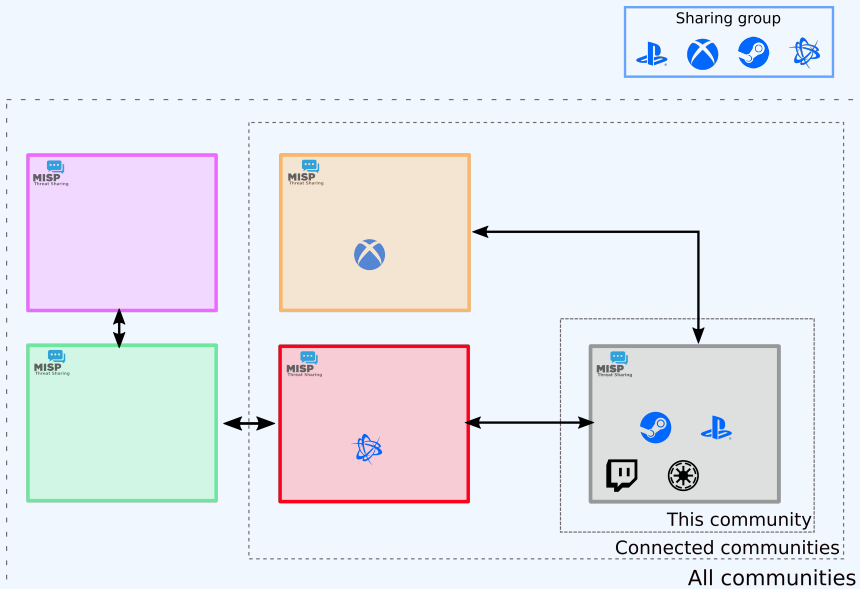
MISP offers granular distribution settings:

- 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				Instances		
Name	Local	Extend		Name	Url	All orgs
Training	✓	✓		Local Instance	https://lgloska.eu	✗
A-FUNKY-HUNGARIAN-BANK.hu	✓	✓		https://lgloska.eu	https://lgloska.eu	✗
AFB	✓	✗				
Italian Bank	✓	✗				
NCSC-NL	✗	✗				

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

SHARING IN MISP: DISTRIBUTION



DATA LAYER


















■ Data layer

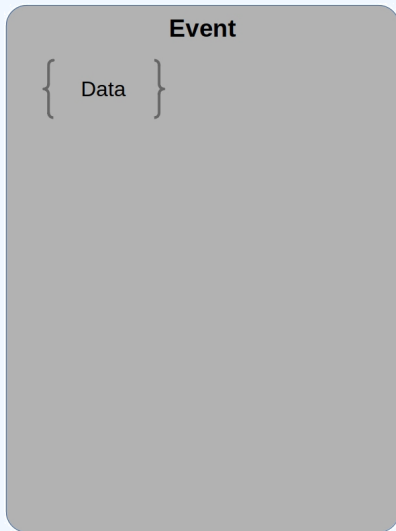
- ▶ **Events** are encapsulations for contextually linked information
- ▶ **Attributes** are individual data points, which can be indicators or supporting data.
- ▶ **Objects** are custom templated Attribute compositions
- ▶ **Object references** are the relationships between individual building blocks
- ▶ **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: EVENTS

Events are encapsulations for contextually linked information

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

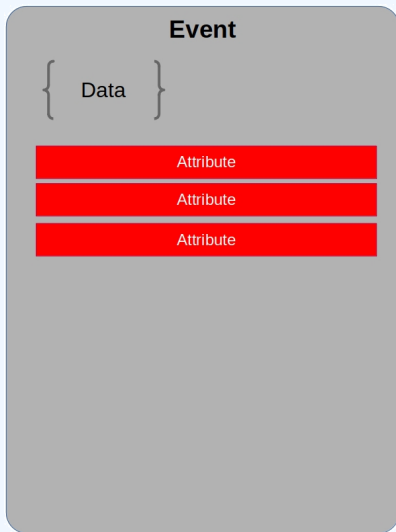
Event ID	178
UUID	5c6d21e5-bb60-47b7-b892-42e6950d2111 
Creator org	CIRCL
Owner org	Training
Creator user	andras.iklody@circl.lu
Tags	 ttp:white   osInt:source-type="automatic-collection"   circl:incident-classification="malware"   adversary:infrastructure-action="take-down"    
Date	2019-02-20
Threat 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. 



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: EVENT BUILDING BLOCKS - RAW DATA














DATA LAYER: ATTRIBUTES

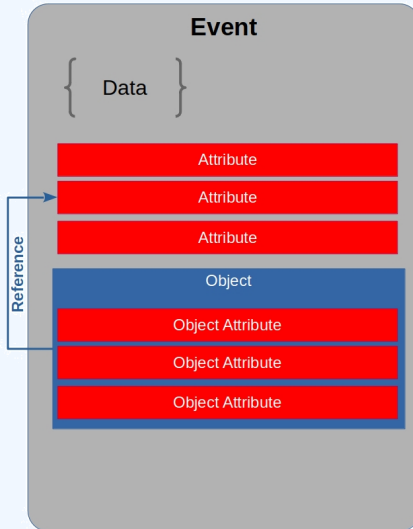
```
1 {  
2     "type": "url",  
3     "category": "Network activity",  
4     "to_ids": true,  
5     "uuid": "5c6d24bd-d094-4dd6-a1b6-4fa3950d2111",  
6     "event_id": "178",  
7     "distribution": "5",  
8     "sharing_group_id": "o",  
9     "timestamp": "1550656701",  
10    "comment": "Delivery point for the malware",  
11    "object_id": "o",  
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

■ 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	81de431987304676134138705fc1c21188ad7f2edf6b77a6551aa693194485e	
■ 2018-03-27	Payload delivery	sha512: sha512	e174ecf4fffb36d30c2cc66b37f82877d421244c924d5c9f39f2e0f37d85332b7d107d5ac5bd19cb7ffdcdbdd8b506d488faa30664ef610f62f3970c163cca76	
■ 2018-03-27	Payload delivery	malware-sample:	putty.exe	

DATA LAYER: EVENT BUILDING BLOCKS - DATA COMPOSITION

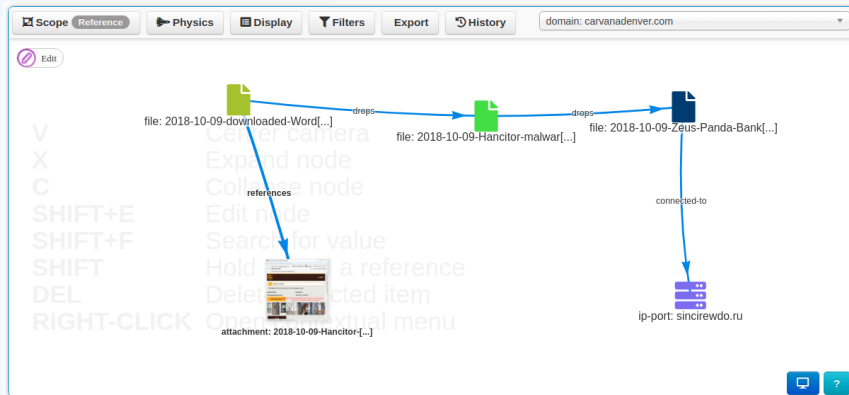


DATA LAYER: MISP OBJECTS

```
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": "ab5foc85-5623-424c-bco3-d798417ood74",  
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

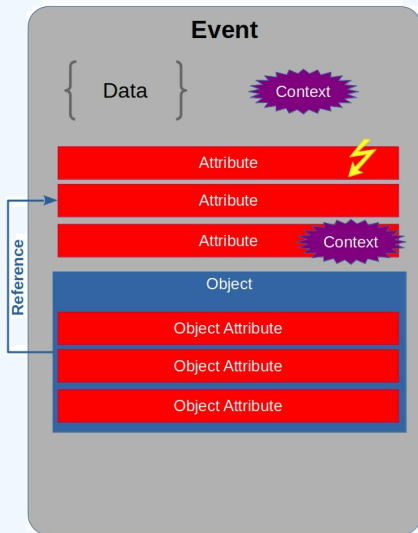
Object references are the relationships between individual building blocks



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 o of ELF"  
10 }
```

DATA LAYER: EVENT BUILDING BLOCKS - CONTEXT



DATA LAYER: SIGHTINGS

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

Events			
<input checked="" type="checkbox"/>	No		
<input checked="" type="checkbox"/>	No	Inherit	(2/0/0)
<input checked="" type="checkbox"/>	No	Inherit	(0/0/0)

Sightings

CIRCL: 2 (2017-03-19 16:17:59)

```
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

Event report: Winnti Group targeting universities in Hong Kong

Markdown Raw Edit report

This report is an excerpt meant for demo purposes. The full report can be found online at [link https://www.welivesecurity.com/2...](https://www.welivesecurity.com/2...)

Winnti Group targeting universities in Hong Kong

In November 2019, we discovered a new campaign run by the Winnti Group **threat-actor** **Axiom** against two Hong Kong universities. We found a new variant of the ShadowPad backdoor **malpedia** **ShadowPad**, the group's flagship backdoor, deployed using a new launcher and embedding numerous modules. The Winnti malware was also found at these universities a few weeks prior to ShadowPad.

ShadowPad found at several Hong Kong universities

In November 2019, ESET's machine-learning engine, Augur, detected a malicious and unique sample present on multiple computers belonging to two Hong Kong universities where the Winnti malware had already been found at the end of October. The suspicious sample detected by Augur is actually a new 32-bit ShadowPad launcher. Samples from both ShadowPad and Winnti found at these universities contain campaign identifiers and C&C URLs with the names of the universities, which indicates a targeted attack.

In addition to the two compromised universities, thanks to the C&C URL format used by the attackers we have reasons to think that at least three additional Hong Kong universities may have been compromised using these same ShadowPad and Winnti variants.

DLL side-loading

The launcher is a 32-bit DLL named `file hpqhsvel.dll` which is the name of a legitimate DLL loaded by `filename %WINDIR%temp\hpqhvind.exe`. This executable is from HP and is usually installed with their printing and scanning software called HP Digital imaging. In this case the legitimate `filename %WINDIR%temp\hpqhvind.exe` was dropped by the attackers, along with their malicious `filename %WINDIR%temp\hpqhsvel.dll`, in `C:\Windows\Temp`.

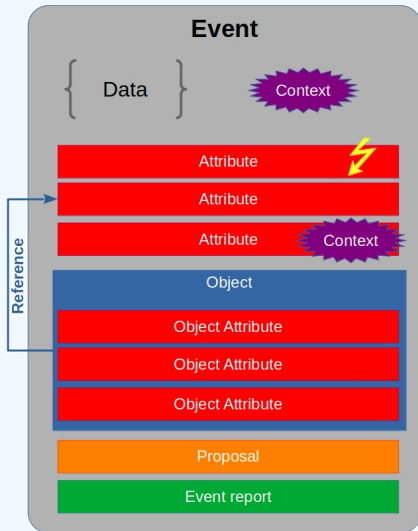
When the malicious DLL is loaded at hpqhvind.exe startup, its DLLMain function is called that will check its parent process for the following sequence of bytes at offset `0x108A`:

```
85 C0 ; test eax, eax
9F B4 ; jz
```

In the case where the parent process is `filename %WINDIR%temp\hpqhvind.exe` this sequence of bytes is present at this exact location and the malicious DLL will proceed to patch the parent process in memory. It

Cancel

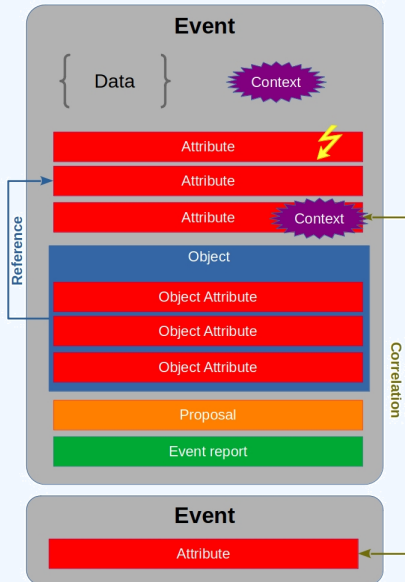
DATA LAYER: EVENT BUILDING BLOCKS - COLLABORATION & INTELLIGENCE



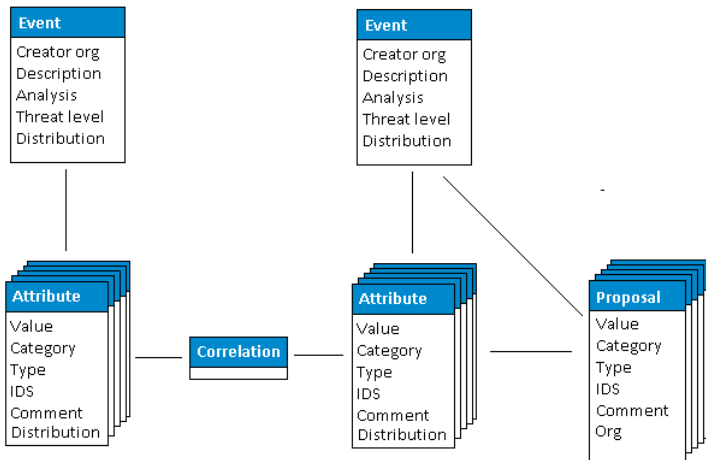
DATA LAYER: EVENT REPORTS

```
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



DATA LAYER: COMBINING THE DATA 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

- ▶ **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 }
```

Simple label standardised on common set of vocabularies

<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 }
```


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											
ID	Published	Value	Synonyms	Owner Org	Creator Org	Default	Activity	#Events	#Relations	Description	Distribution
7059	N/A	APT 29	Dukes, Group 100, Cozy Duke, EuroAPT, CozyBear, CozyCar, Cozer, Office Markose	MISP	MISP	✓	<div></div>	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

CONTEXT LAYER: GALAXY CLUSTERS

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

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	7cdf317-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>		

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": [...]  
18 }
```

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	Secured 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

GALAXY JSON MATRIX-LIKE

```
1 {
2   "description": "Universal Development and Security Guidelines as
   Applicable to Election Technology.",
3   "icon": "map",
4   "kill_chain_order": {           \\Tab in the matrix
5     "example-of-threats": [       \\Column in the matrix
6       "setup | party/candidate-registration",
7       "setup | electoral-rolls",
8       "campaign | campaign-IT",
9       "all-phases | governement-IT",
10      "voting | election-technology",
11      "campaign/public-communication | media/press"
12    ]
13  },
14  "name": "Election guidelines",
15  "namespace": "misp",
16  "type": "guidelines",
17  "uuid": "c1dco3b2-89b3-42a5-9d41-782ef726435a",
18  "version": 1
19 }
```

CLUSTER JSON MATRIX-LIKE

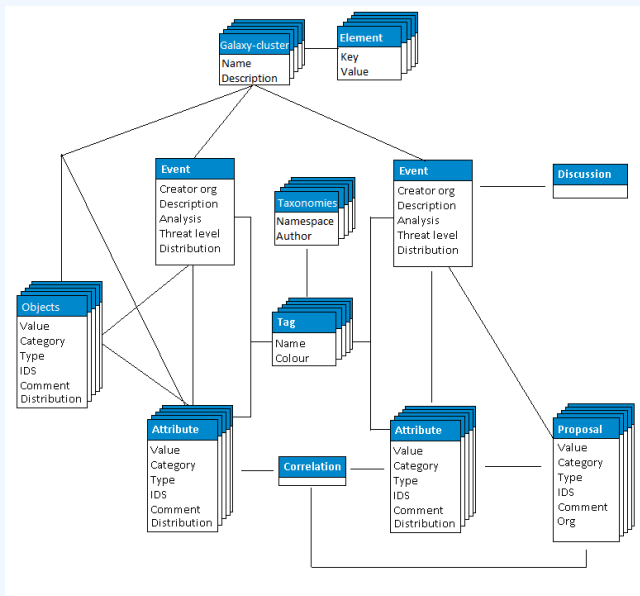
```
1 {
2     "description": "DoS or overload of party/campaign
3     registration , causing them to miss the deadline",
4     "meta": {
5         "date": "March 2018.",
6         "kill_chain": [ \\Define in which column the cluster should be placed
7             "example-of-threats:setup | party/candidate-registration"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

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"
```

BOTH LAYERS: COMBINING EVERYTHING



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



Co-financed by the European Union

Connecting Europe Facility