MISP Training: Galaxies

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
Andras Iklody
Raphaël Vinot
TLP:WHITE

http://www.misp-project.org/
Twitter: *@MISPProject*

MISP Training Luxembourg
20170207

MISP Galaxies

- MISP started out as a platform for technical indicator sharing
- The need for a way to describe threat actors, tools and other commonalities became more and more pressing
- **Taxonomies quickly became essential for classifying events**
- The weakness of the tagging aproach is that it's not very descriptive
- We needed a way to attach **more complex structures to data**
- Also, with the different naming conventions for the same "thing" attribution was a mess
- This is where the Galaxy concept came in

Solution

- Pre-crafted galaxy "clusters" via GitHub project
- Attach them to an event (or soon attribute)
- The main design principle was that these higher level informations are meant for human consumption
- This means flexibility - key value pairs, describe them dynamically
- Technical indicators remain strongly typed and validated, galaxies are loose key value lists

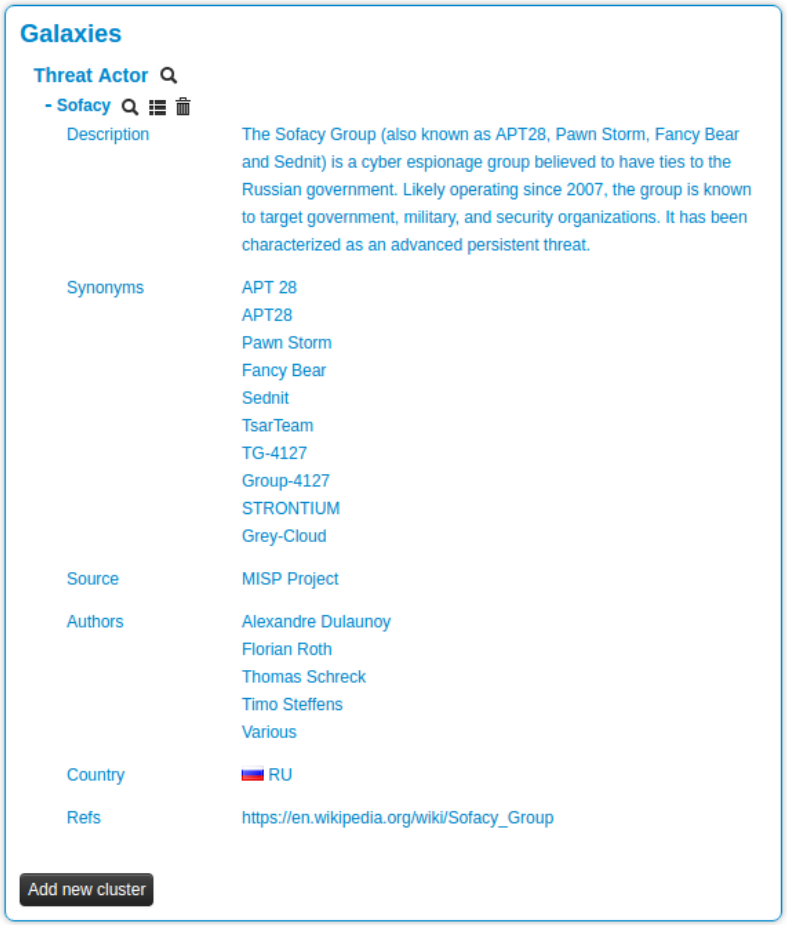
The galaxy object stack

- **Galaxy**: The type of data described (Threat actor, Tool, ...)
- **Cluster**: An individual instance of the galaxy (Sofacy, Turla, ...)
- **Element**: Key value pairs describing the cluster (Country: RU, Synonym: APT28, Fancy Bear)
- **Reference**: Referenced galaxy cluster (Such as a threat actor using a specific tool)

Existing clusters

- **Exploit-Kit**: An enumeration of known exploitation kits used by adversaries
- **Microsoft activity group**: Threat actors as defined by Microsoft
- **Preventive measure**: Potential preventive measures against threats
- **Ransomware**: List of known ransomwares
- **TDS**: Traffic Direction System used by adversaries
- **Threat-Actor**: Adversary groups - Known or estimated adversary groups
- **Tool**: Tools used by adversaries (from Malware to common tools)

What a cluster looks like

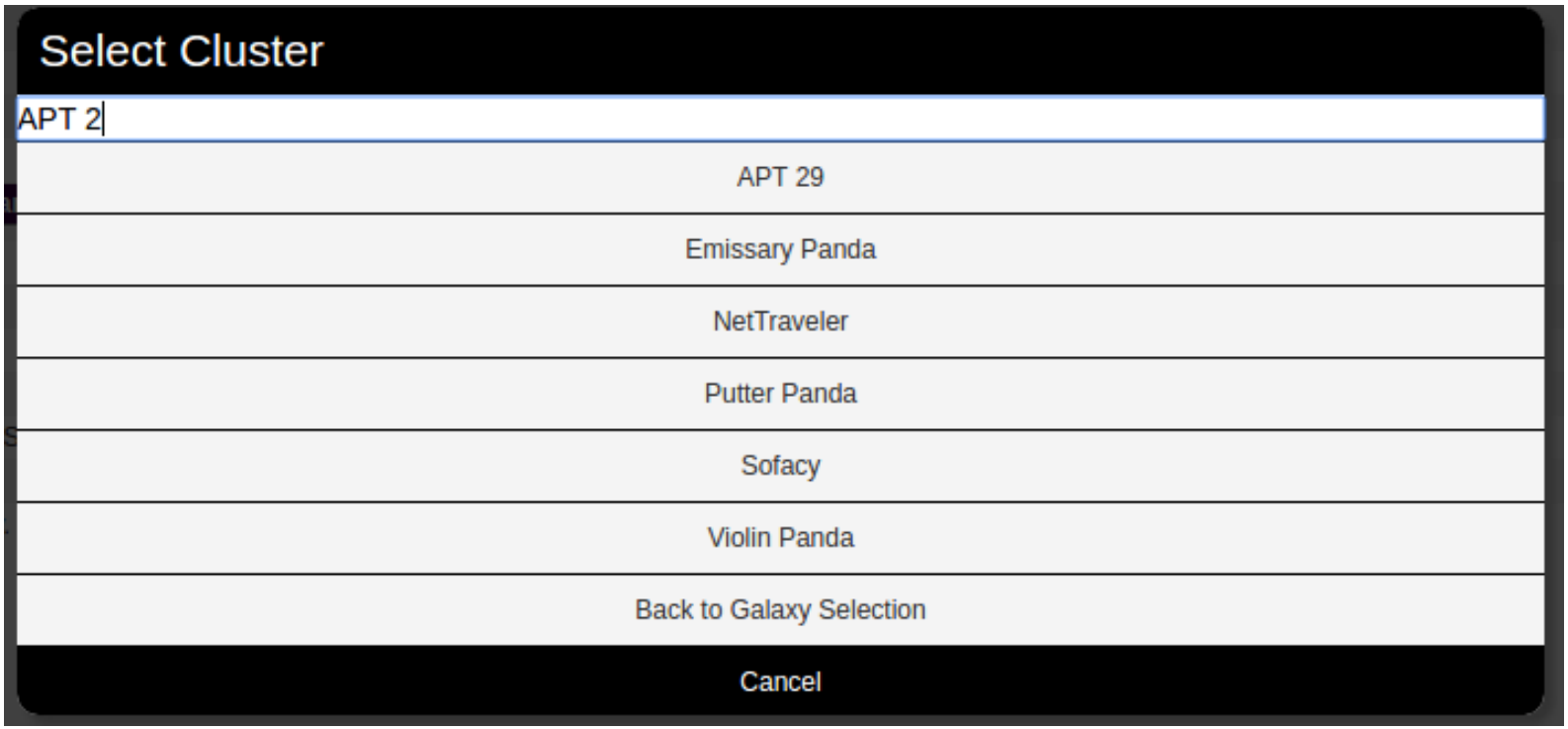


Attaching clusters to events

- Internally simply using a taxonomy-like tag to attach them to events
- Example: misp-galaxy:threat-actor="Sofacy"
- **Synchronisation works out of the box** with older instances too. They will simply see the tags until they upgrade.
- Currently, as mentioned we rely on the community's contribution of galaxies

Attaching clusters

- Use a searchable synonym database to find what you're after



Creating your own clusters

- Creating galaxy clusters has to be straight forward to get the community to contribute
- Building on the prior success of the taxonomies and warninglists
- Simple JSON format in similar fashion
- Just drop the JSON in the proper directory and let MISP ingest it
- We always look forward to contributions to our galaxies repository

Galaxy JSON

- If you want to create a completely new galaxy instead of enriching an existing one

```
{
    "name" : "Threat Actor",
    "type" : "threat-actor",
    "description": "Threat actors are characteristics of
        malicious actors (or adversaries) representing a cyber
        attack threat including presumed intent and
        historically observed behaviour.",
    "version": 1,
    "uuid": "698774c7-8022-42c4-917f-8d6e4f06ada3"
}
```

Cluster JSON

- Clusters contain the meat of the data
- Skeleton structure as follows

```
{
  "values": [
    {
      "meta": {},
      "description": "",
      "value": "",
      "related_clusters": [{}],
    }
  ]
}
```

Cluster JSON value example

```
1     {
2       "meta": {
3         "synonyms": [
4             "APT 28", "APT28", "Pawn Storm", "Fancy Bear",
5             "Sednit", "TsarTeam", "TG-4127", "Group-4127",
6             "STRONTIUM", "Grey-Cloud"
7         ],
8         "country": "RU",
9         "refs": [
10          "https://en.wikipedia.org/wiki/Sofacy_Group"
11        ]
12      },
13      "description": "The Sofacy Group (also known as APT28,
14          Pawn Storm, Fancy Bear and Sednit) is a cyber
15          espionage group believed to have ties to the
16          Russian government. Likely operating since 2007,
17          the group is known to target government, military,
18          and security organizations. It has been
19          characterized as an advanced persistent threat.",
20      "value": "Sofacy"
21    },
```

Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
- `https://github.com/MISP/` - `http://www.misp-project.org/`
- We welcome any contributions to the project, be it pull requests, ideas, github issues,...