

MISP - GALAXY 2.0

METHOD FOR SHARING THREAT INTELLIGENCE

TEAM CIRCL

INFO@CIRCL.LU

OCTOBER 2, 2024



MISP
Threat Sharing

OUTLINE OF THE PRESENTATION

- Present the features available for Sharing *galaxy clusters*
- Look at the internals of what changed in the datamodel and MISP's behaviors

Galaxy 2.0 introduces various new features for *Galaxies* and their *Clusters* allowing:

- Creation of **custom** *Clusters*
- **ACL** on *Clusters*
- **Connection** of *Clusters* via *Relations*
- **Synchronization** to connected instances.
- **Visualization** of forks and relationships

Default *Galaxy cluster*

- Coming from the `misp-galaxy` repository¹
- Cannot be edited
 - ▶ Only way to provide modification is to modify the stored JSON or to open a pull request
 - ▶ Are not synchronized
 - ▶ Source of trust
- Restrictions propagate to their children (Galaxy cluster elements, Cluster relationships)

Custom *Galaxy cluster*

- Can be created via the UI or API
- Belongs to an organisation
 - ▶ Fully editable
 - ▶ Are synchronized

¹<https://github.com/MISP/misp-galaxy>

Clusters and *Relations* can be edited.

■ New *Clusters* fields

- ▶ `distribution`, `sharing_group_id`
- ▶ `org_id`, `orgc_id`
- ▶ `locked`, `published`, `deleted`
- ▶ `default`
 - *Clusters* coming from the `misp-galaxies` repository are marked as `default`
 - Not synchronized
 - Same purpose as *Event's* `locked` field
- ▶ `extends_uuid`
 - Point to the *Cluster* that has been forked
- ▶ `extends_version`
 - Keep track of the *Cluster* version that has been forked

- *Role perm_galaxy_editor*
- Relations also have a distribution and can have *Tags*
- Synchronization servers have 2 new flags
 - ▶ *pull_galaxy_clusters*
 - ▶ *push_galaxy_clusters*
- Clusters blacklist

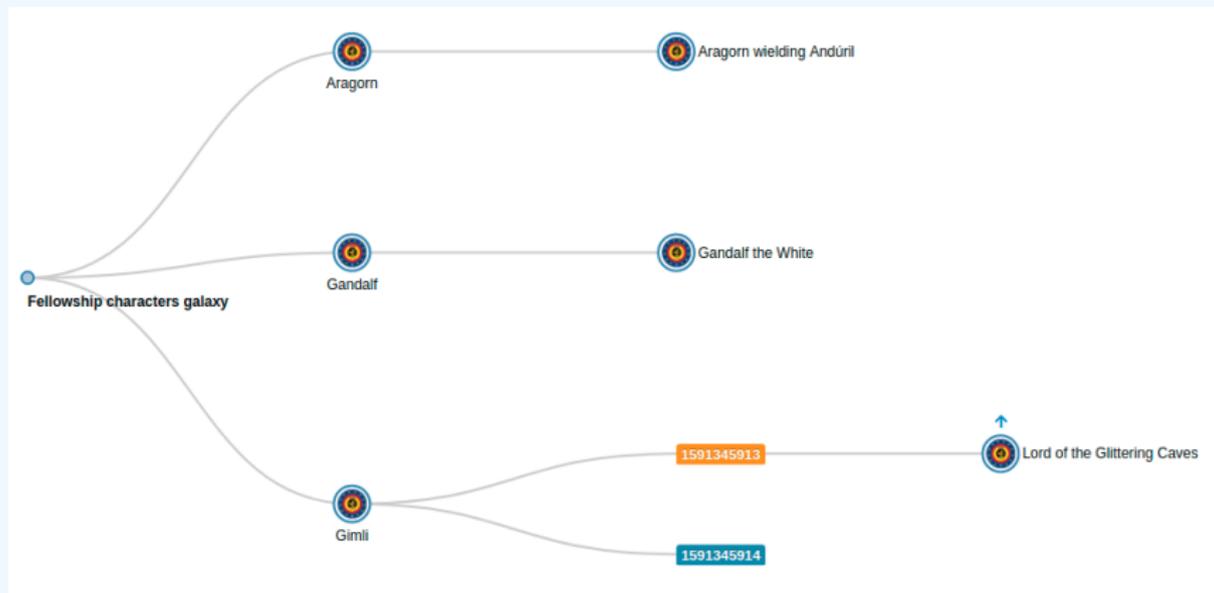
- Standard CRUD
- Soft and Hard deletion
- Publishing
- Update forked cluster to keep it synchronized with its parent
- ACL on the *Cluster* itself, not on its tag
 - ▶ `misp-galaxy:galaxy-type="cluster UUID"`
 - ▶ `misp-galaxy:mitre-attack-pattern="e4932f21-4867-4de6-849a-1b11e48e2682"`

FEATURES IN DEPTH: VISUALIZATION

Advertising

- └─ Online Advertising
- └─ Postal Advertising

Tree view of forked Clusters



FEATURES IN DEPTH: VISUALIZATION

Tree and network views for Relations between Clusters

Microsoft Activity Group actor galaxy cluster relationships

● microsoft-activity-group ● mitre-intrusion-set ● threat-actor ● mitre-mobile-attack-intrusion-set ● ransomware



STRONTIUM

Name	STRONTIUM
Galaxy	microsoft-activity-group
Description	STRONTIUM has been active since at least 2007. Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information. Its primary institutional targets have included government bodies, diplomatic institutions, and military forces and installations in NATO member states and certain Eastern European countries. Additional targets have included journalists, political advisors, and organizations associated with political activism in central Asia. STRONTIUM is an activity group that usually targets government agencies, diplomatic

FEATURES IN DEPTH: VISUALIZATION

Tree and network views for Relations between Clusters

Source UUID: Relationship type: Target UUID: Distribution:

Tags:

```
graph LR; RB1[Ramnit banker] --- similar1[similar] --- RB2[Ramnit banker]; RB1 --- similar2[similar] --- RB3[Ramnit banker]; RB1 --- similar3[similar] --- RM[Ramnit malpedia]; RB1 --- similar4[similar] --- RB5[Ramnit botnet]; RB2 --- similar5[similar] --- RB3; RB3 --- similar6[similar] --- RB5; RB5 --- similar7[similar] --- RB6[Ramnit banker]; RB5 --- similar8[similar] --- RB7[Ramnit botnet]; RB5 --- similar9[similar] --- RB8[Ramnit malpedia]; RB6 --- similar10[similar] --- RB7; RB7 --- similar11[similar] --- RB8;
```

The diagram illustrates a network of relationships between clusters. A central node, 'Ramnit botnet', is connected to three other nodes: 'Ramnit banker', 'Ramnit banker', and 'Ramnit malpedia'. All relationships are labeled 'similar' and have a tag 'estimative-language:likelihood-probability:~"likely"'. The nodes are represented by colored circles: orange for 'Ramnit banker', green for 'Ramnit botnet', and blue for 'Ramnit malpedia'. The relationships are represented by lines connecting the nodes, with labels 'similar' and tags 'estimative-language:likelihood-probability:~"likely"'.

GALAXY CLUSTER ELEMENTS

Hasn't been touched: Still a key-value stored. But new feature have been added²

Tabular view

- Allows you to browse **cluster elements** like before

« previous 1 2 3 next » last »

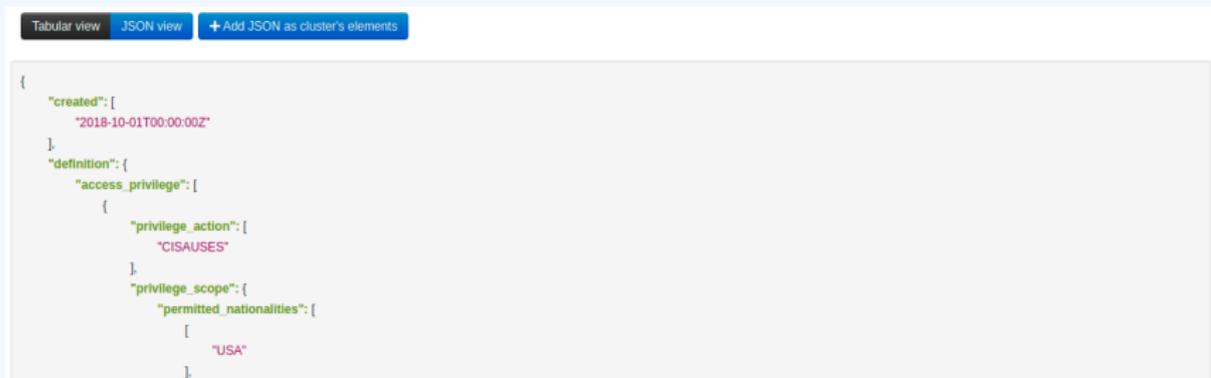
Tabular view JSON view

Key ↓	Value	Actions
created	2018-10-01T00:00:00Z	
definition.access_privilege.0.privilege_action	CISAUSES	
definition.access_privilege.0.privilege_scope.permitted_nationalities.0	USA	
definition.access_privilege.0.privilege_scope.permitted_nationalities.1	AUS	
definition.access_privilege.0.privilege_scope.permitted_nationalities.2	CAN	
definition.access_privilege.0.privilege_scope.permitted_nationalities.3	GBR	
definition.access_privilege.0.privilege_scope.permitted_nationalities.4	NZL	

²Will be included in next release

JSON view

- Allows you to visualisation **cluster element** in a JSON structure
- Allows you to convert any JSON into **cluster elements** enabling searches and correlations



```
{
  "created": [
    "2018-10-01T00:00:00Z"
  ],
  "definition": {
    "access_privilege": [
      {
        "privilege_action": [
          "CISAUSES"
        ],
        "privilege_scope": {
          "permitted_nationalities": [
            "USA"
          ]
        }
      }
    ]
  }
}
```

Has its own synchronization mechanism which can be enabled with the `pull_galaxy_cluster` and `push_galaxy_cluster` flags

- **Pull All:** Pull all remote Clusters (similar to event's pull all)
- **Pull Update:** Update local Clusters (similar to event's pull update)
- **Pull Relevant:** Pull missing Clusters based on local Tags
- **Push:** Triggered whenever a Cluster is published or via standard push