MISP - GALAXY 2.0

METHOD FOR SHARING THREAT INTELLIGENCE

TEAM CIRCL

INFO@CIRCL.LU

JULY 8, 2024



MISP - Galaxy 2.0



Threat Sharing

OUTLINE OF THE PRESENTATION

MISP - Galaxy 2.0

08

2024-07

└─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

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

MISP - Galaxy 2.0 6 7 7 8 MISP Galaxy 2.0 MISP GALAXY 2.0

salaxy 2.0 introduces various new features for Galaxies and their latters allowing. © Creation of castem Clasters ■ Connection of Clasters ■ Spectroelization to connected instances. ■ Synchroelization to connected instances.

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 CLUSTERS

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
- https://github.com/MISP/misp-galaxy

MISP - Galaxy 2.0

ω

6

2024-

—Default Galaxy clusters

DEFAULT GALAXY CLUSTER

Default Galaxy cluster

- Coming from the misp-galaxy repository¹
 Cannot be edited
- Only way to provide modification is to modify the stored it or to open a mill request
- Are not synchronized
- Restrictions propagate to their children (Galaxy cluster

Custom Galaxy cluster

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

MISP GALAXY 2.0 - COMPARISON WITH PRIOR VERSION

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

MISP Galaxy 2.0 - Comparison with prior version

MISP - Galaxy 2.0

80

2024-07

- Clusters and Relations can be edited. New Clusters fields Maintena Statistics (Statistics) (St
- org_id, orgc_id
- locked, published, deleted
 default
- Clusters coming from the misp-galaxies repository as marked as default
- Not synchronized Same purpose as Event's locked f
- extends_uuid
 Point to the Cluster that has been forked
- Point to the Cluster that has been forked
 extends_version
 Keep track of the Cluster version that has been for

MISP GALAXY 2.0 - OTHERS CHANGES

MISP - Galaxy 2.0

2024-07

└─MISP Galaxy 2.0 - Others changes

Role perm_galaxy_editor # Relations also have a distribution and can have Togs # Synchronization servers have 2 new flags > pull.galaxy_clusters > punh_galaxy_clusters Clusters blocklist

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 blocklist

FEATURES IN DEPTH: CRUD

Features in depth: CRUD

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"
- sing-play miter atlast-patient "suggifte dit) det dage skonded

Standard CRUD

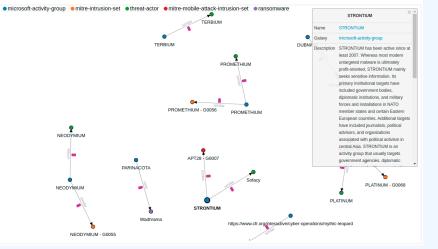
- Soft and Hard deletion
- Publishing
- Update forked cluster to keep it synchronized with its parent
- ACL on the *Cluster* itself, not on its tag
 - misp-galaxy:galaxy-type="cluster UUID"
 - misp-galaxy:mitre-attack-pattern="e4932f21-4867-4de6-849a-1b11e48e2682"



FEATURES IN DEPTH: VISUALIZATION

Tree and network views for Relations between Clusters

Microsoft Activity Group actor galaxy cluster relationships



MISP - Galaxy 2.0

07-08

2024-

└─Features in depth: Visualization



FEATURES IN DEPTH: VISUALIZATION

Tree and network views for Relations between Clusters

Source UUID	Relationship type	Target UL	IID		Distribution		
8ed81090-f098-4878-b87e-2d801	dropped	~		Picker	All communities	~	
ags							
	Picker						
+ Add relationship							
					similar		►• Ramnit
				estim	ative-language:likelihood-pr	obability="likely"	banker
Ramnit	similar tive-language:likelihood-prob	ability="likely"	Ramnit				
banker	uve-language.likelihoou-prob	ability= likely	botnet				
					similar		▶0
				estim	ative-language:likelihood-pr	obability="likely"	Ramnit malpedia
					9		

MISP - Galaxy 2.0

80

2024-07

└─Features in depth: Visualization



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

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

²Will be included in next release

MISP - Galaxy 2.0 08 2024-07 -Galaxy cluster elements

Hasn't been touched: Stil	l a key-value stored. But	new feature		
have been added ²				
Tabular view				
Allows you to browse	cluster elements like be	efore		
	cluster elements like be	efore		
Allows you to browse				
Allows you to browse	-			
Allows you to browse	2010/100400			
	2010/100400			
	Ver 20-0-(Thinks) uncern Un			
Allows you to browse In allows you to browse In allows In allows In allowse In allow	tas 20-julijiteks usuum Ma Ad			

MISP - Galaxy 2.0

08

2024-07

Galaxy cluster elements

AXY CLUSTER ELEMENTS

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

GALAXY CLUSTER ELEMENTS

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

Tabular view JSON view + Add JSON as cluster's elements	
{	
"created": [
"2018-10-01T00:00:00Z"	
1.	
"definition": {	
"access_privilege": [
(
"privilege_action": [
"CISAUSES"	
l.	
"privilege_scope": {	
"permitted_nationalities": [
[
"USA"	
].	

MISP - Galaxy 2.0 6 전 - 전 - 전 - Synchror

-Synchronization in depth

- 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 oush

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