

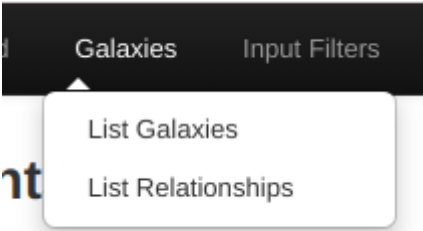
GALAXIES

MISP'teki *Galaxy*, MISP *Event*'lerine veya özelliklerine (attribute) eklenen bir obje olan kümelere (cluster) bağlı büyük bir nesneyi ifade etmek için kullanılan bir yöntemdir. Bir küme, bir veya daha fazla öğeden oluşabilir. Öğeler, *key-value* çiftleri olarak ifade edilir. Bir "Galaxy" genellikle birbirleriyle ilişkili tehdit verilerini gruplamak için kullanılan bir yapı veya kategoridir. Örneğin, bir tehdit aktörünün kullandığı zararlı yazılımlar, saldırı teknikleri, hedef sektörler veya saldırı vektörleri gibi konseptleri gruplamak için kullanılabilir.

MISP *galaxy* varsayılan sözcük dağarcıkları bulunmaktadır, ancak bunlar istenildiği gibi üzerine yazılabilir, değiştirilebilir veya güncellenebilir. Sözcük dağarcıkları, mevcut standartlardan (STIX, Veris, ATT&CK, MISP vb.) veya yalnızca kuruluşlar için kullanılan özel standartlardan gelir.

Mevcut kümeler ve sözcük dağarcıkları doğrudan veya bir şablon olarak kullanılabilir. Amaç, analize başlayan organizasyonlar için ortak bir küme setine sahip olmaktır, ancak bu set yerel bilgilere (paylaşılmayan) veya ek bilgilere (paylaşılabilir) genişletilebilir.

Galaxies menüsü içinde List Galaxies ve List Relationship kategorileri bulunmaktadır.



- **List Galaxies:** Sunucuda bulunan tüm galaksileri içeren bir liste görünecektir.

Home	Event Actions	Dashboard	Galaxies	Input Filters	Global Actions	Sync Actions	Administration	Logs	API	★	MISP	Admin	✉	Log out
List Galaxies	List Cluster Blocklists	List Relationships	Update Galaxies	Force Update Galaxies	Wipe Default Galaxy Clusters	Import Galaxy Clusters								
Galaxy index														
« previous 1 2 next » last »														
All	Enabled	Disabled	Enter value to search Filter x											
ID	Icon	Name	Version	Namespace	Description	Enabled	Local Only	Actions						
82	✈️	UAVs/UCAVs	1	misp	Unmanned Aerial Vehicles / Unmanned Combat Aerial Vehicles	✓	✗	🔍 📄 🗑️						
81	🔧	Tool	3	misp	Threat actors tools is an enumeration of tools used by adversaries. The list includes malware but also common software regularly used by the adversaries.	✓	✗	🔍 📄 🗑️						
80	👤	Tidal Technique	1	tidal	Tidal Technique Galaxy	✓	✗	🔍 📄 🗑️						
79	👤	Tidal Tactic	1	tidal	Tidal Tactic Galaxy	✓	✗	🔍 📄 🗑️						
78	👤	Tidal Software	1	tidal	Tidal Software Galaxy	✓	✗	🔍 📄 🗑️						
77	👤	Tidal References	1	tidal	Tidal References Galaxy	✓	✗	🔍 📄 🗑️						
76	👤	Tidal Groups	1	tidal	Tidal Groups Galaxy	✓	✗	🔍 📄 🗑️						
75	👤	Tidal Campaigns	1	tidal	Tidal Campaigns Galaxy	✓	✗	🔍 📄 🗑️						
74	👤	Threat Actor	3	misp	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.	✓	✗	🔍 📄 🗑️						
73	👤	Tea Matrix	1	tea-matrix	Tea Matrix	✓	✗	🔍 📄 🗑️						
72	👤	TDS	4	misp	TDS is a list of Traffic Direction System used by adversaries	✓	✗	🔍 📄 🗑️						
71	👤	Target Information	1	misp	Description of targets of threat actors.	✓	✗	🔍 📄 🗑️						

- **List Relationships:** Bu kategori; tehdit aktörleri, zararlı yazılımlar, saldırı teknikleri ve diğer tehdit unsurları arasındaki ilişkileri belirlemek ve görselleştirmek için kullanılır. Kullanıcılar, bu ilişkileri analiz ederek tehditlerin karmaşıklığını anlayabilir ve savunma stratejilerini buna göre ayarlayabilirler. Bu kategori, tehdit istihbaratını daha iyi anlamak ve siber güvenlik önlemlerini geliştirmek için bir araç sağlar.

Galaxy Repository Ekleme:

- GitHub'da MISP-Galaxy deposunu kendi hesabınıza çoğaltın.
- Ardından MISP kurulumunuzdaki "misp-galaxy" dizinini güncelleyin.

```
cd /var/www/MISP/app/files/  
sudo rm -rf misp-galaxy  
  
sudo -u www-data git clone https://github.com/SteveClement/misp-galaxy.git
```

Revision #4

Created 8 April 2024 12:36:39 by İlayda Durlanık

Updated 8 April 2024 20:03:46 by İlayda Durlanık