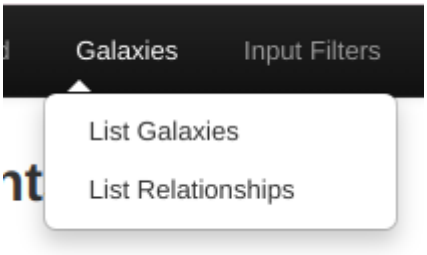
GALAXIES

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 ögeden oluşabilir. Ögeler, *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.

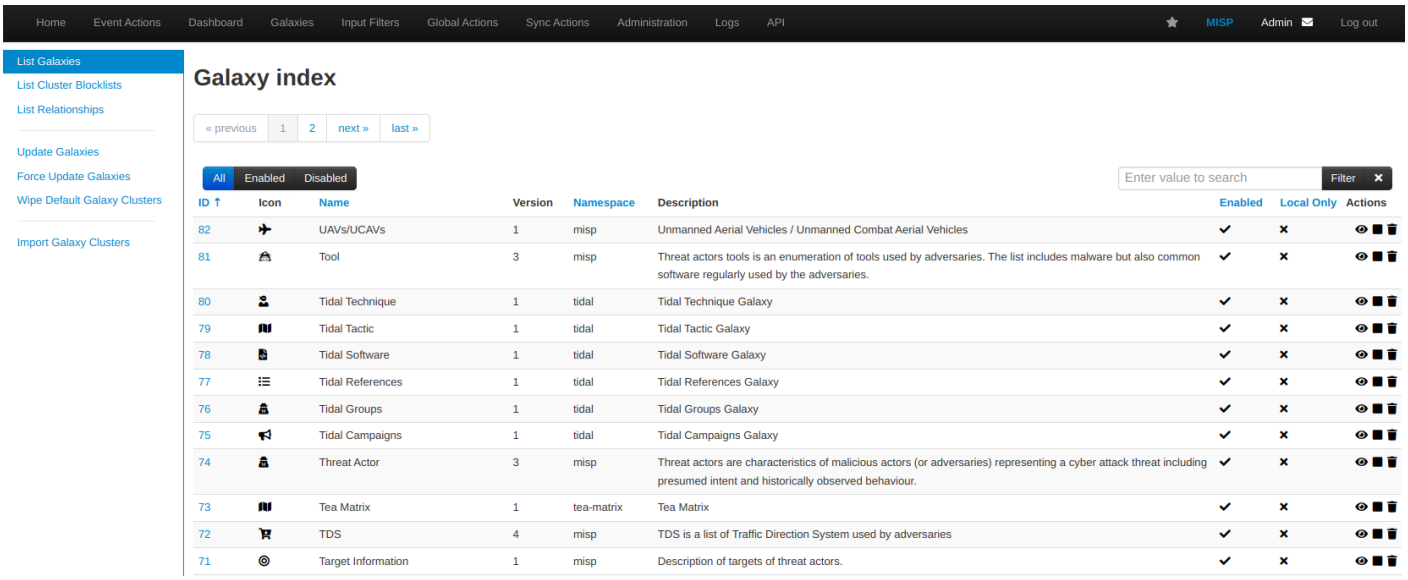
MISP *galaxy* varsayılan sözcük dağarcıkları bulunmaktadır, ancak bunlar istenildiği gibi üzerine yazılabilir, değiştirilebilir veya güncellenebilir. Sözcük dağarcıkları, mevcut standartlardan (STIX, Veris, ATT&CK, MISP vb.) veya yalnızca kuruluşlar için kullanılan özel standartlardan gelir.

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.



- **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