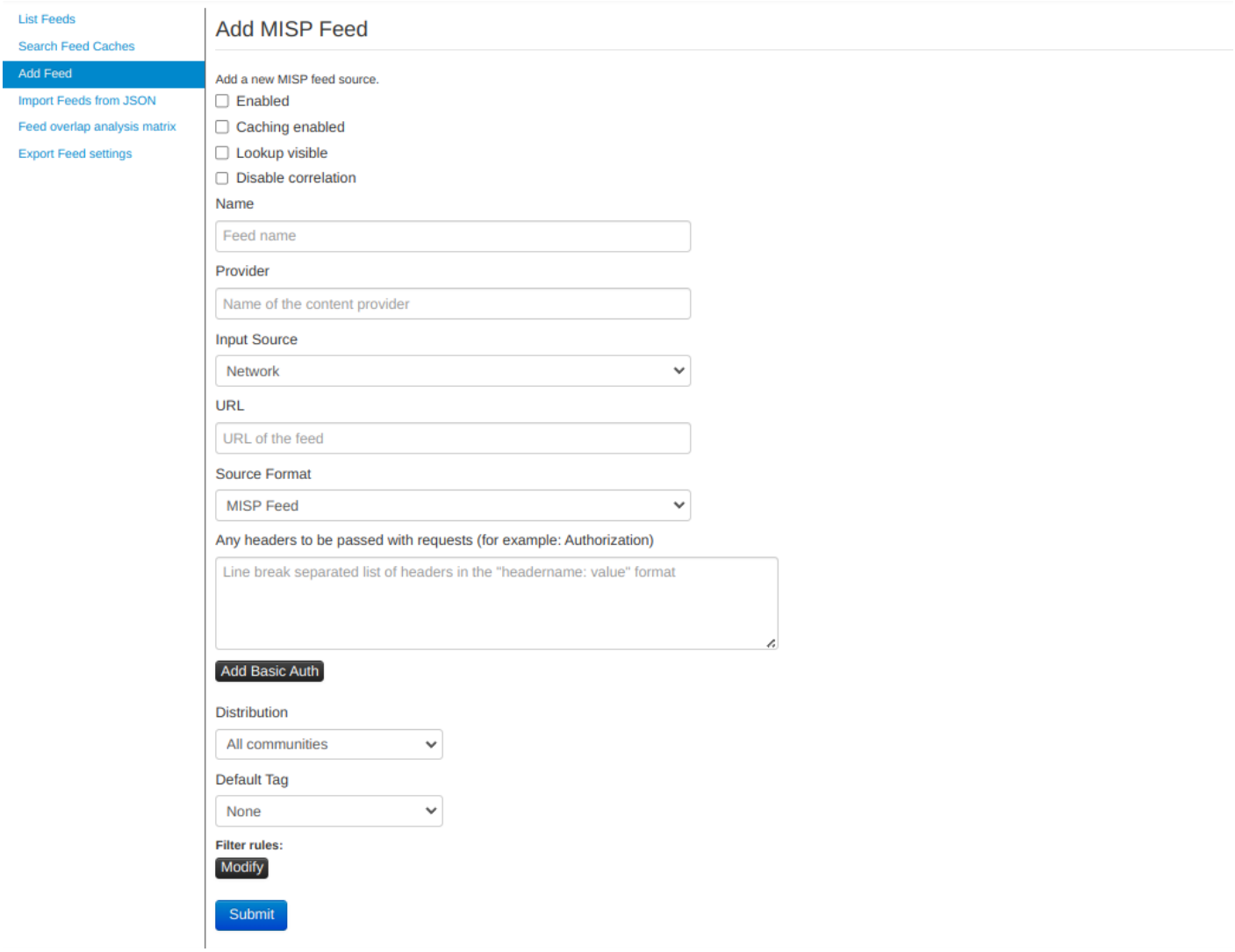
Feed

MISP Feed'ler, düzenli aralıklarla MISP'e otomatik olarak aktarılabilen göstergeler içeren uzak veya yerel kaynaklardır. Bu CTI (Siber Tehdit İstihbaratı) feed'leri, verilerini MISP, CSV veya serbest metin formatlarında sunabilir aynı zamanda uzak veya yerel bir URL sorgulanarak içe aktarılabilir.

- Sync Actions -> Feeds menüsü içinde bulunan "add feed" alanı aşağıda gösterildiği gibidir;



1. **Enabled:** Bu özellik, *feed*'in etkinleştirilip etkinleştirilmeyeceğini belirtir. Etkinleştirildiğinde, *feed* düzenli olarak sorgulanır ve güncellenir.
2. **Caching enabled:** Bu seçenek, *feed*'den alınan verilerin önbelleğe alınıp alınmayacağını belirtir. Önbelleğe alma, aynı verilerin tekrar tekrar sorgulanmasını önleyerek performansı artırabilir.

3. **Lookup visible:** Bu seçenek, *feed*'den alınan verilerin aramalarda görünüp görünmeyeceğini belirtir. Aramalarda görünmesi, kullanıcıların *feed*'den alınan verilere kolayca erişmesine olanak tanır.
4. **Disable correlation:** Bu seçenek, *feed*'den alınan verilerin MISP içindeki diğer verilerle ilişkilendirilip ilişkilendirilmeyeceğini belirtir.
5. **Name:** *Feed*'in genel adını belirtir. Bu ifade, *feed*'i tanımlamak için genel ad olarak kullanılacaktır.
6. **Provider:** Bu alan, *feed*'in sağlayıcısının adını belirtir.
7. **Input Source:** Bu alan, *feed*'in kaynağını belirtir. *Feed*'in nereden alındığını gösterir.
8. **URL:** *Feed*'in URL'sini belirtir. Bu sayede, MISP düzenli olarak *feed*'i sorgular ve güncel verileri alması için kullanılır.
9. **Source Format:** Bu alan, *feed*'in hangi formatta olduğunu belirtir. MISP *feed* seçeneği, *feed*'in MISP formatında olduğunu belirtir.
10. **Any headers to be passed with requests:** Bu alan, isteklerle birlikte iletilmesi gereken herhangi bir başlık bilgisini belirtir. Örneğin, yetkilendirme bilgilerini içerebilir.
11. **Distribution:** *Feed*'den alınan verilerin hangi dağıtım seviyesine sahip olacağını belirtir. Distribution, hangi kullanıcılar veya organizasyonlarla paylaşılacağını belirler.
12. **Default Tag:** Varsayılan etiketi belirtir.
13. **Filter rules:** Bu alan, *feed*'den alınan verileri filtrelemek için kullanılır.

Feed eklemek ve Free-Text Import aracı arasındaki fark:

Free text import, genellikle metin tabanlı verilerin MISP'e manuel olarak eklenmesini veya yapıştırılmasını sağlar. Kullanıcıların çeşitli kaynaklardan aldıkları tehdit bilgilerini hızlıca MISP'e aktarmasına olanak tanır.

Öte yandan, feed eklemek, belirli bir format veya protokol kullanılarak otomatik olarak güncellenen ve sürekli olarak beslenen tehdit bilgisi kaynaklarıdır. Bu kaynaklar, genellikle IOC'ler, zararlı URL'ler, kötü amaçlı dosya hash'leri gibi tehdit belirteçlerini içerir. MISP, bu feed'leri kullanarak otomatik olarak güncellenen tehdit bilgilerini alabilir ve MISP ortamında kullanıcıların erişimine sunabilir.

Bu nedenle, free text import daha manuel ve kullanıcı tarafından yönetilen bir süreci ifade ederken, feed eklemek daha otomatik ve sistem tarafından yönetilen bir süreci ifade eder. Her ikisi de tehdit istihbaratı toplamak ve analiz etmek için farklı yöntemler sunar.

Revision #4
Created 7 April 2024 19:32:02 by İlayda Durlanık
Updated 8 April 2024 19:37:36 by İlayda Durlanık