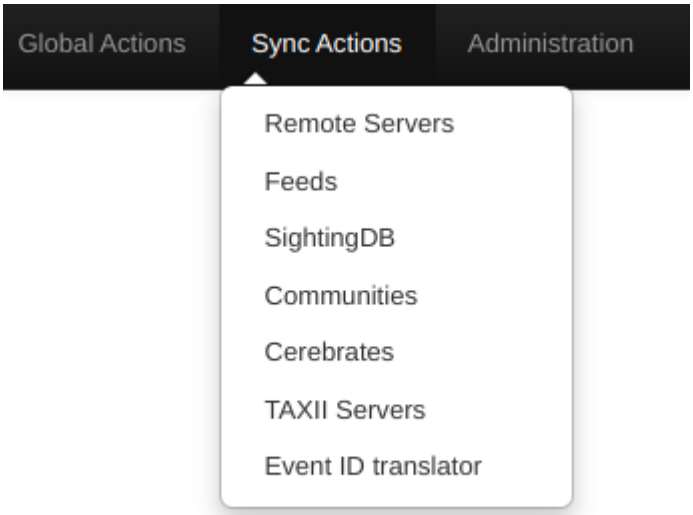
SYNC ACTIONS

Tehdit bilgilerinin diğer güvenlik sistemleri veya hizmetlerle otomatik olarak paylaşılmasını ve senkronize edilmesini sağlar. Bu sayede, bir tehdit bilgisinin MISP'te paylaşılmasıyla birlikte, ilgili güvenlik araçları ve sistemler de bu bilgiye otomatik olarak erişebilir ve buna göre aksiyon alabilir.

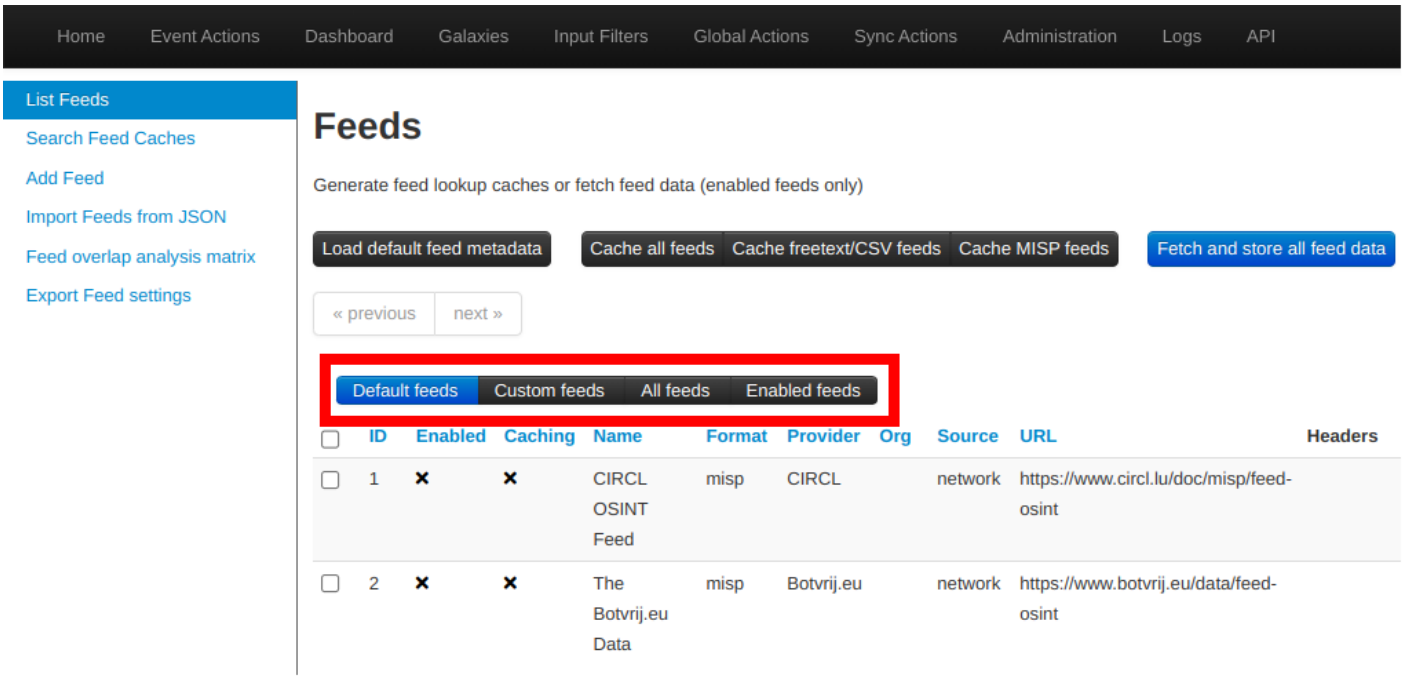
Örneğin, bir güvenlik tehdidi MISP üzerinde tespit edildiğinde, MISP Sync Actions aracılığıyla bu bilgi bir SIEM (Security Information and Event Management) sistemi ile senkronize edilerek, SIEM sistemi o tehdide karşı otomatik olarak koruma politikalarını güncelleyebilir veya alarm üretebilir.



- **Remote Servers:** Uzak sunuculara erişim sağlayarak, farklı MISP örnekleri arasında veri alışverişi yapılmasını sağlar.

- **Feeds:** Feedler, düzenli aralıklarla MISP'e otomatik olarak alınabilen göstergeleri içeren uzak veya yerel kaynaklardır. Feedler, MISP formatında, CSV formatında veya serbest metin formatında yapılandırılabilir.

List Feeds kategorisi altında, feed oluşturmak için kullanılan "Load default feed metadata", "Caching Feeds" ve "Fetching feeds" butonları yer almaktadır.



Default Feeds: Kullanıcılara bir dizi açık kaynaklı feed sağlar. Bu feedler, güncel tehdit bilgilerini içeren ve MISP platformuna otomatik olarak yüklenebilen kaynaklardır.

Feed tanımlarını, Feeds sayfasındaki **"Load default feed metadata"** butonu kullanılarak kolayca yüklenebilir. Bu özellik, "app/files/feed-metadata/defaults.json" dosyasındaki girişleri veritabanına içe aktararak yeni feedler oluşturur.

"Feed"lerin mevcut "feed"lerle çakışmasını önlemek için, feed URL'sini kullanarak yinelenenleri kontrol eder. Eğer aynı URL'ye sahip bir feed zaten veritabanında varsa, bu giriş içe aktarılmaz. Böylece, kullanıcıların yerel değişiklikleri (ad, dağıtım veya etkin durum gibi) korunur ve üzerine yazılması önlenir.

Bu sayede, güncel feed tanımları MISP örneğine hızlıca entegre edilebilir ve mevcut "feed"ler korunabilir.

Caching Feeds: Kullanıcıların belirli veri "feed"lerinden gelen bilgileri önbelleğe almasını sağlar. Bu sayede, kullanıcılar sık sık eriştiği veya talep ettiği verilere daha hızlı bir şekilde erişilebilir hale gelir.

Bir feed içeriğini önbelleğe almak, bu verileri sunucuda depolamak ve bir sonraki erişimde daha hızlı erişilebilir hale getirmek anlamına gelir. Veri alışverişi süreçlerini hızlandırır ve kullanıcı deneyimini iyileştirir.

Fetching Feeds: Veri kaynaklarından (feedlerden) güncel bilgilerin alınması işlemidir. Bu işlem, kullanıcıların güncel tehdit bilgilerini veya diğer güvenlik verilerini MISP örneğine aktarmasını sağlar.

"Fetching feeds" işlemi genellikle düzenli aralıklarla otomatik olarak gerçekleştirilir.

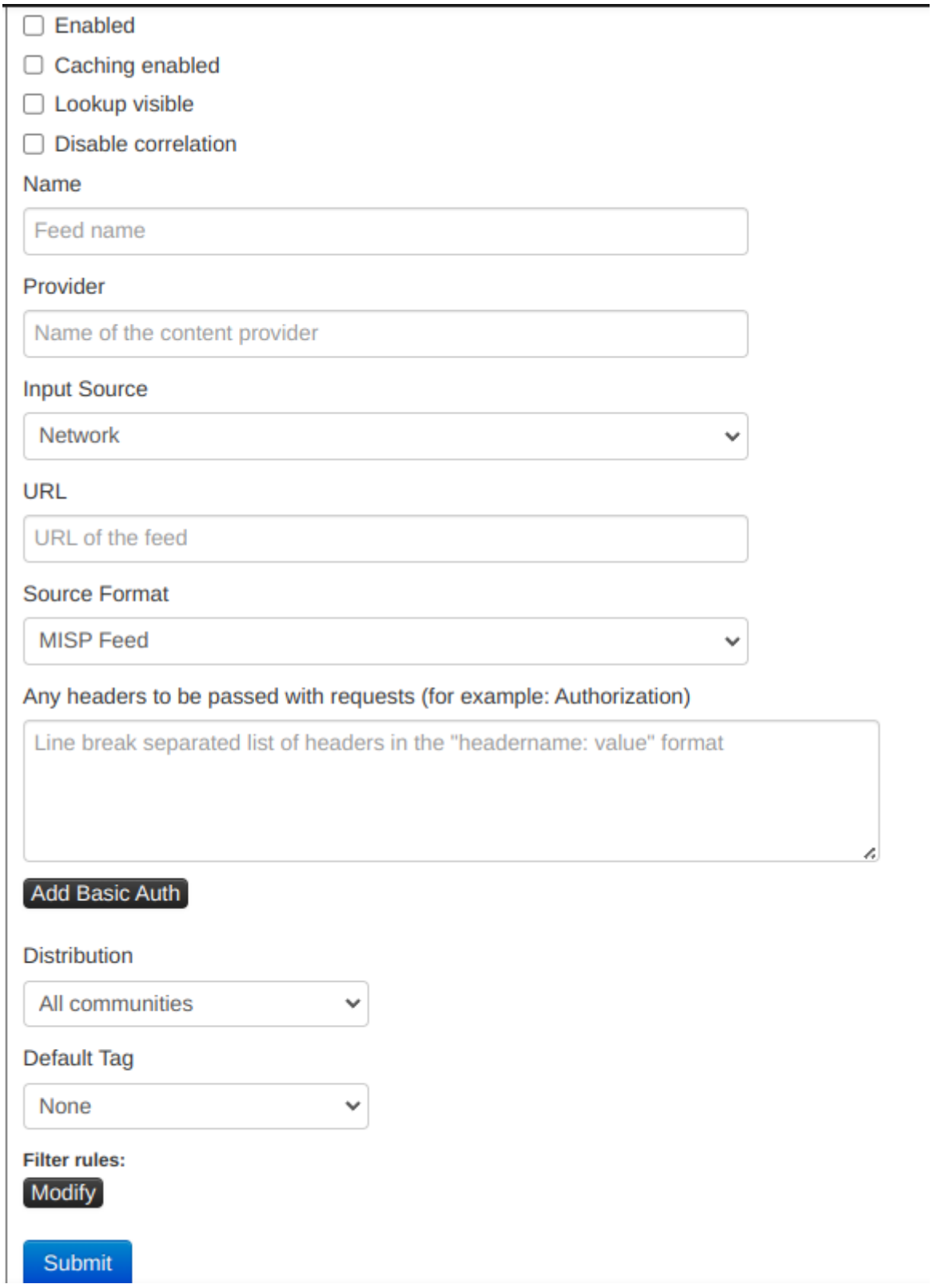
Belirli aralıklarla otomatik güncelleme yapmak için, MISP platformunda genellikle bir zamanlama ayarı bulunur. Bu ayar, ne sıklıkla "feed"lerin güncelleneceğini belirlemek için kullanılır. Ayarlar, genellikle MISP'in yönetim arayüzünde veya yapılandırma dosyalarında yapılır.

MISP'in yapılandırma dosyalarında (örneğin config.php) "Feeds_auto_update" veya benzeri bir parametre bulunabilir. Bu parametre, "feed"lerin ne sıklıkla güncelleneceğini belirler ve genellikle saniye cinsinden bir değerdir.

Kullanıcılar ayrıca, ihtiyaç duydukları zaman manuel olarak da feedleri alabilirler.

FEED EKLEME:

Yeni bir feed eklemek için yan menüdeki "Add Feed" seçeneği seçilir.



Enabled: Feed aktif mi, değil mi? Eğer bu alan aktifse, o feedin düzenli olarak güncellendiği ve içeriğinin kullanıcılara ulaştırıldığı anlamına gelir. Eğer bu alan aktif değilse, feedin güncellenmediği veya geçici bir süre için devre dışı bırakıldığı anlamına gelir.

Caching enabled: Feed verilerinin önbelleğe alınıp alınmayacağını belirtir.

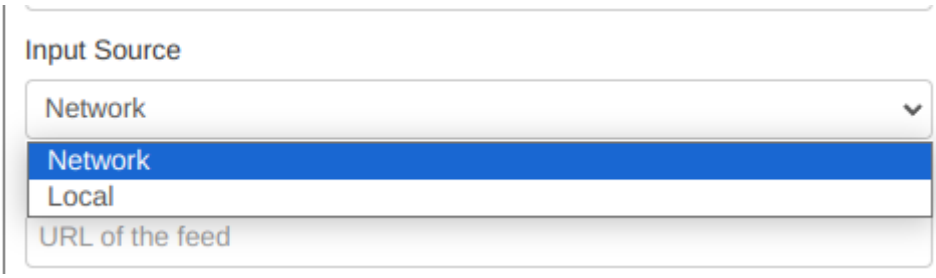
Lookup visible: İşaretlenmediğinde, korelasyonlar sadece sizin için görünür; işaretlendiğinde ise, korelasyonlar diğer kullanıcılar tarafından da görünür.

Disable correlation: İşaretlendiğinde, Feed'den gelen tüm olaylar için korelasyonlar devre dışı bırakılır.

Name: Feed'i tanımlamak için ad; benzersiz olması gerekmez.

Provider: İçerik sağlayıcısının adıdır.

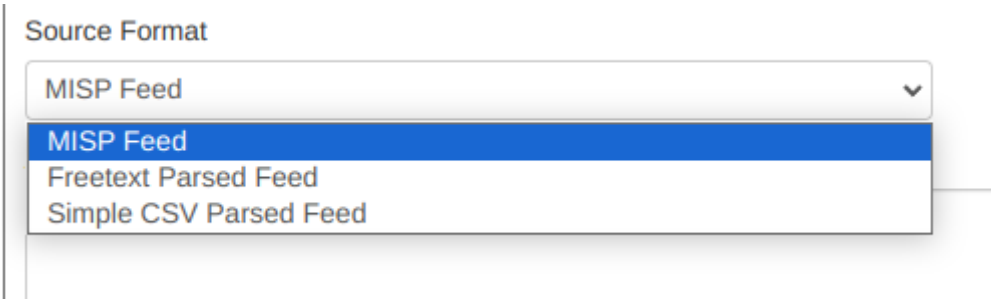
Input Source: Giriş kaynağı belirlenir. İki seçenek vardır:



- **Network:** Verinin platform dışında bir ağ kaynağından geldiğini belirtir. Örneğin, bir web sitesi, bir uzak sunucu veya bir bulut hizmeti gibi dış kaynaklar, ağ üzerinden veri sağlar.
- **Local:** Verinin yerel bir kaynaktan geldiğini belirtir. Yerel kaynaklar, kullanıcının kendi cihazında veya ağında barındırılan sunucular gibi doğrudan erişilebilen kaynaklar olabilir. Bu durumda, kullanıcı veriyi kendi kontrolü altındaki bir yerden alır.
  - **Not:** Bu durumda, "Remove input after ingestion(Girişten sonra kaldır)" adında yeni bir onay kutusu görünür. İşaretlenirse, kaynak kullanımdan sonra silinir.

URL: "Feed"in internet üzerindeki adresini veya yerel dosyanın yolunu belirtir.

Source Format: 3 farklı kaynak formatı vardır. Kaynak formatına göre feed ekleme alanları değişiklik gösterebilir.

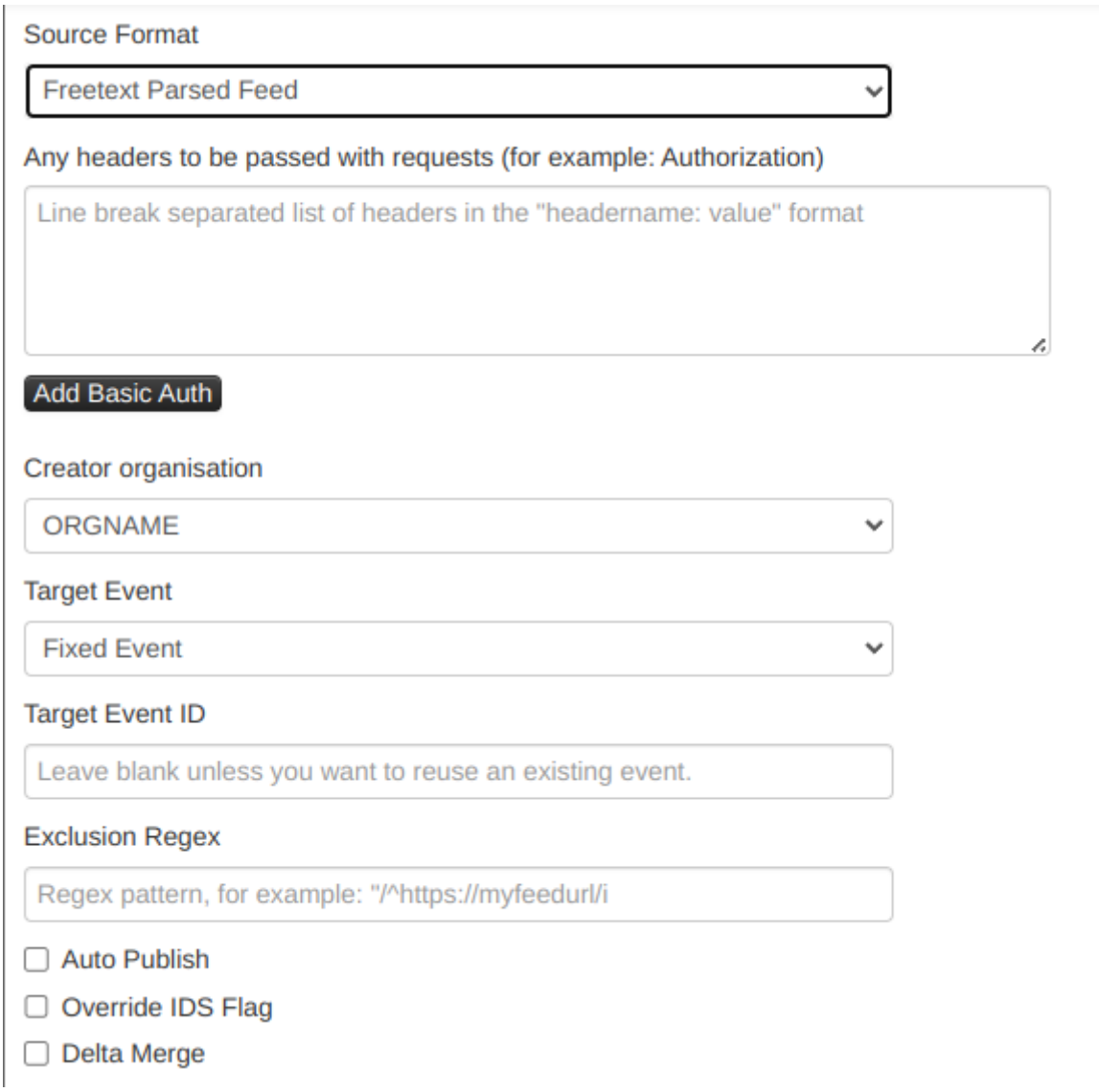


MISP Feed: Kaynak, MISP "Event"leri gibi JSON biçimli dosyaların bir listesine işaret eder.

Örneğin: https://www.circl.lu/doc/misp/feed-osint

Freetext Parsed Feed: Metin tabanlı içeriklerin yapılandırılmış bir formatta eklenmesini sağlar.

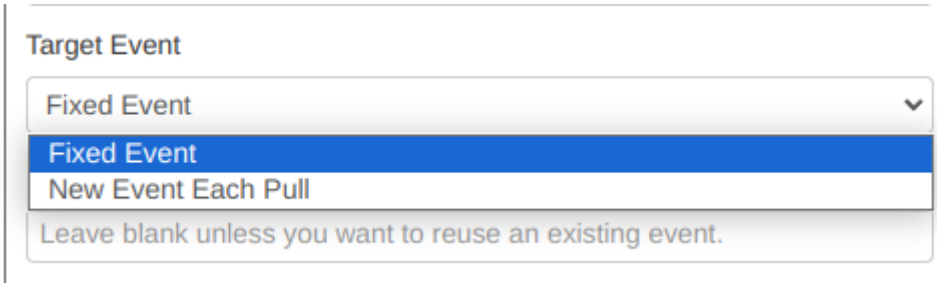
NOT: Freetext Parsed Feed seçeneği seçildiği takdirde yeni alanlar açılacaktır.



Creator organisation: "Feed"den oluşturulan Event için oluşturucu organizasyonu(orgc_id) temsil eder. List Feeds ekranındaki Org sütununda görünür.

Target Event: "Feed"den verileri tutacak Event türüdür.

- "New Event Each Pull" (feed çekildiğinde her seferinde yeni bir "Event" oluşturulur)
- "Fixed Event" (bir sonraki alanda yapılacak seçimlere göre yeni verilerle güncellenecek benzersiz bir Event)



Target Event ID: Verinin ekleneceği "Event"in kimliğidir. Eğer belirtilmemişse, alan ilk kez feed alındığında ayarlanır.

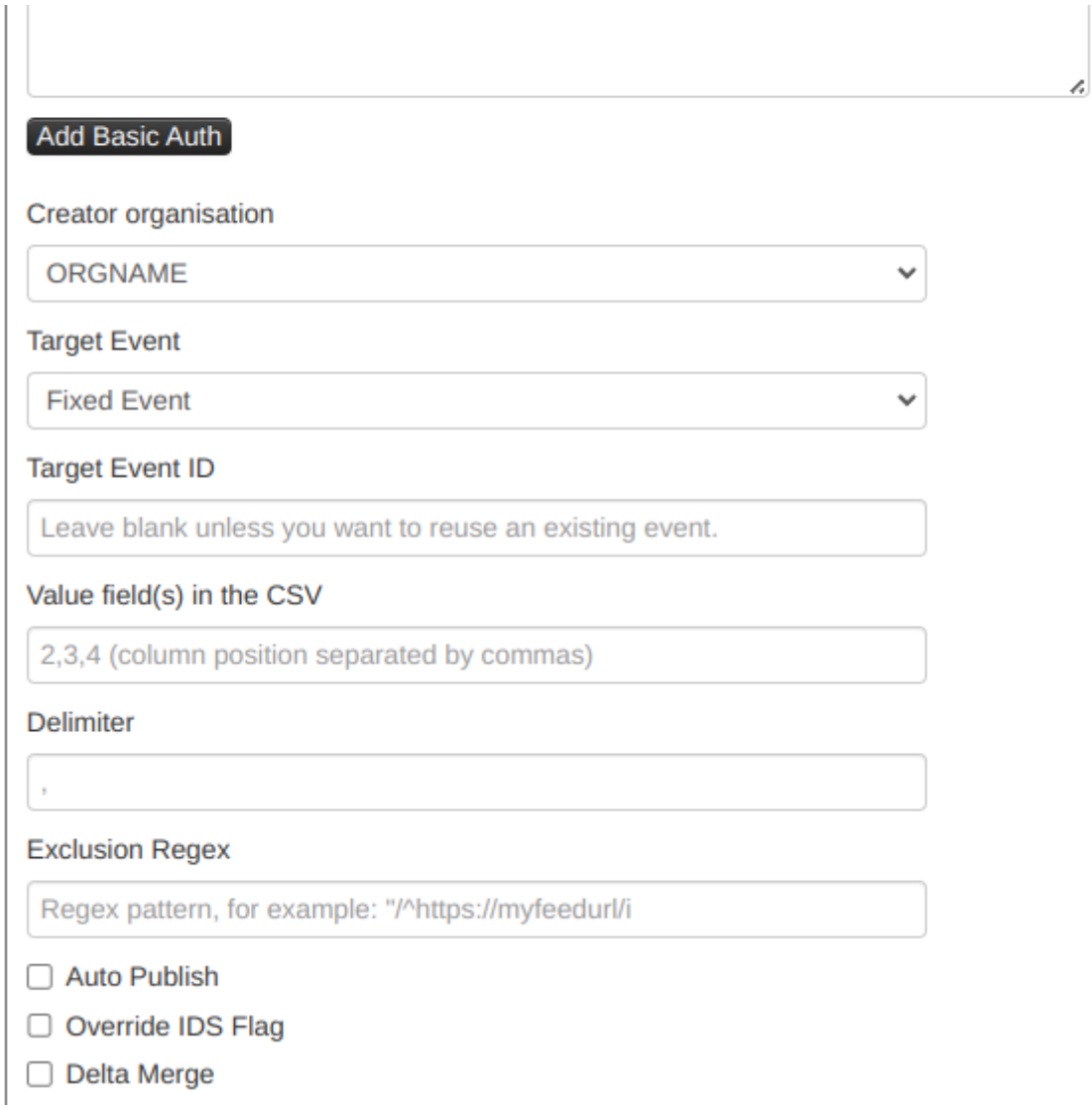
Exclusion Regex: Atlanması gereken IoC'leri tespit etmek için bir regex deseni eklenebilir. Örneğin, gerçek raporun / "feed"in herhangi bir referansını hariç tutmak için kullanışlı olabilir.

Auto Publish: İşaretlendiğinde, "feed"den oluşturulan "Event" otomatik olarak yayımlanır.

Override IDS Flag: İşaretlendiğinde, IDS bayrağı false olarak ayarlanır.

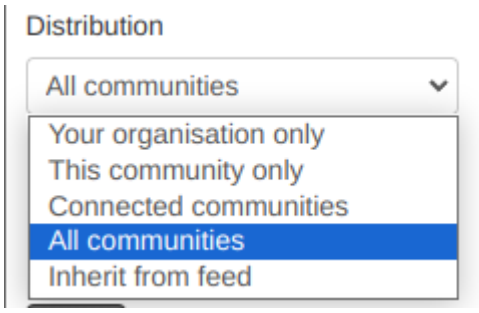
Delta Merge: İşaretlendiğinde, yalnızca en son alınan "feed"den özellikler saklanır, eski olanlar (geçici olarak) silinir.

Simple CSV Parsed Feed: CSV formatındaki verilerin MISP platformuna aktarılması için kullanılan bir feed türüdür. Bu seçenekte, "Freetext parsed Feed" seçeneğinde eklenen alanlara kıyasla 2 farklı alan daha eklenmektedir.



> **Values field(s) in the CSV:** Hangi alanların MISP özelliklerine dönüştürüleceğini belirler. Sütun pozisyonları virgülle ayrılarak belirtilebilir.
>
> **Delimeter:** Alan ayırıcısı belirlenir; varsayılan alan ayırıcısı virgüldür ",".

Dağıtım: Feed'den oluşturulan "Event"e ayarlanacak dağıtım seçeneği belirlenir. 5 farklı seçenek sunulmaktadır.



Default Tag: Oluşturulan "Event"lere bir varsayılan etiket eklenebilir.

Filter Rules: Hangi "Event"lerin ya da kuruluşların izin verildiği veya engellendiği tanımlanabilir.

- **SightingDB:** Gözlemlerle ilgili verilere erişim sağlanır ve MISP platformunda gözlemlenen tehditler hakkında daha fazla bilgi edinilebilir.
- **Communities:** MISP topluluğuna erişim sağlayarak, farklı kullanıcılar ve kuruluşlarla veri paylaşımı ve işbirliği yapılmasını sağlar.
- **Cerebrates:** Yapay Zeka servislerine erişim sağlayarak, farklı yapay zeka sağlayıcılarından gelen tehdit istihbaratı verilerine erişilmesini sağlar.
- **TAXII Servers:** TAXII protokolü üzerinden çalışan sunuculara erişim sağlayarak MISP örneğine farklı kaynaklardan veri alışverişi yapılmasını sağlar.
- **Event ID translator:** Farklı olay kimlik formatları arasında dönüşüm yapılmasını sağlayarak MISP örneğini "Event"lerin tutarlı bir şekilde işlenmesini ve yönetilmesini sağlar.

Revision #7
Created 8 April 2024 21:17:57 by İlayda Durlanık
Updated 9 April 2024 21:38:55 by İlayda Durlanık