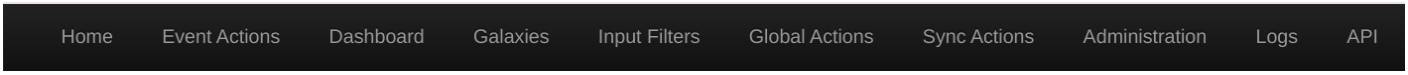
Kullanım Kılavuzu

MISP kullanım kılavuzu bölümü, MISP platformunun temel özelliklerini ve işlevlerini inceler. Temel kavramlar ve kullanım senaryoları bu bölümde ele alınır.

Temel Kavramlar

HOME



Üst bar, Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API alanlarından oluşmaktadır.

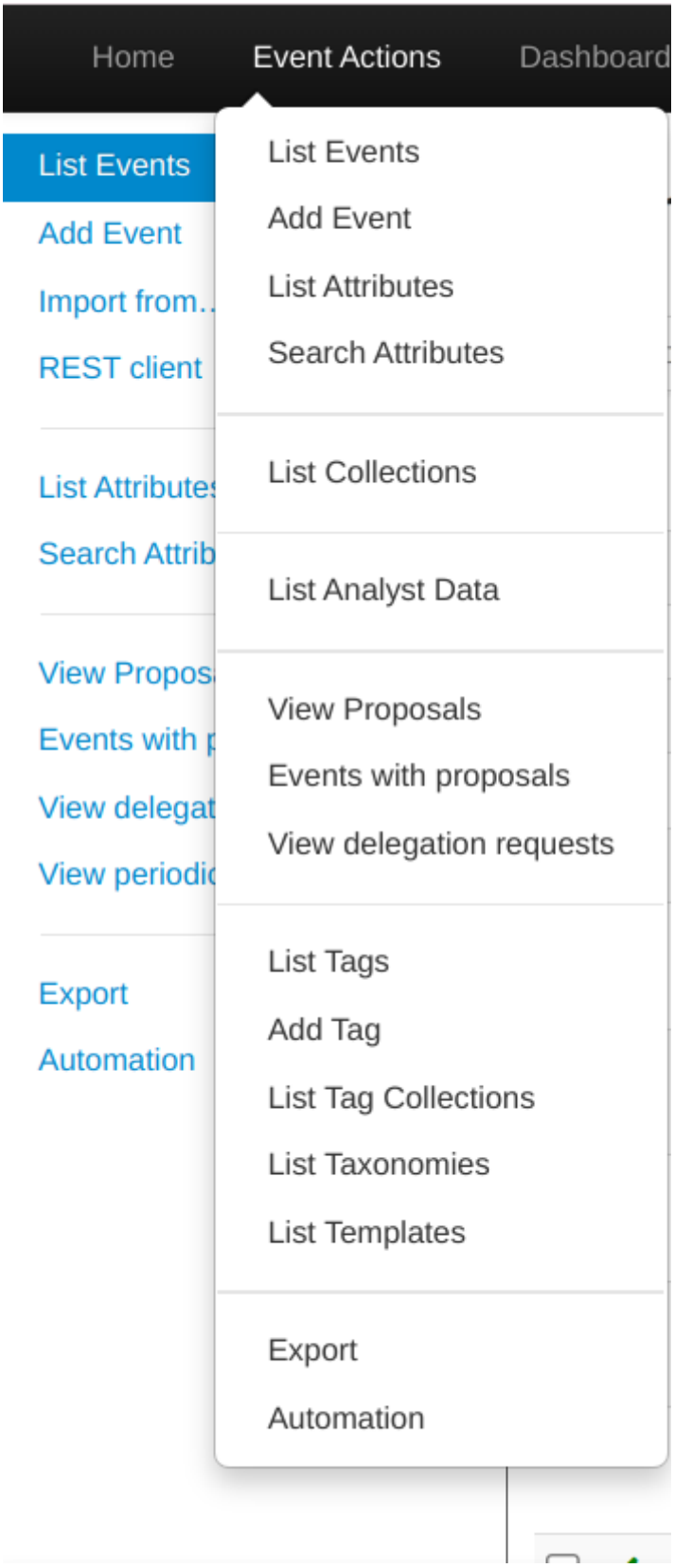
HOME

Bu buton, kullanıcıyı uygulamanın başlangıç ekranına geri götürür. Başlangıç ekranı, *Event* dizini sayfası veya kullanıcının özel ana sayfa olarak belirlediği sayfa olabilir, bu da kullanıcının üst çubuktaki yıldızı kullanarak belirlenir.

EVENT ACTIONS

MISP'e girilen tüm kötü amaçlı yazılım verileri, bir *Event* tarafından açıklanan bağlantılı özelliklerle tanımlanır. *Event Actions* menüsü, *Event*'*leri* ve bu *Event*'*lere* bağlı özelliklerin oluşturulması, düzenlenmesi, silinmesi, yayınlanması, aranması ve listelenmesi gibi işlevlere erişim sağlar. Bağlantılı özellikler, kötü amaçlı yazılımlar hakkında ek bilgiler içerir ve bu bilgiler *Event*'*lerle* ilişkilendirilir. Bu sayede, kullanıcılar kötü amaçlı yazılımlar hakkında daha detaylı bilgilere erişebilirler ve bu bilgileri etkili bir şekilde yönetebilirler.

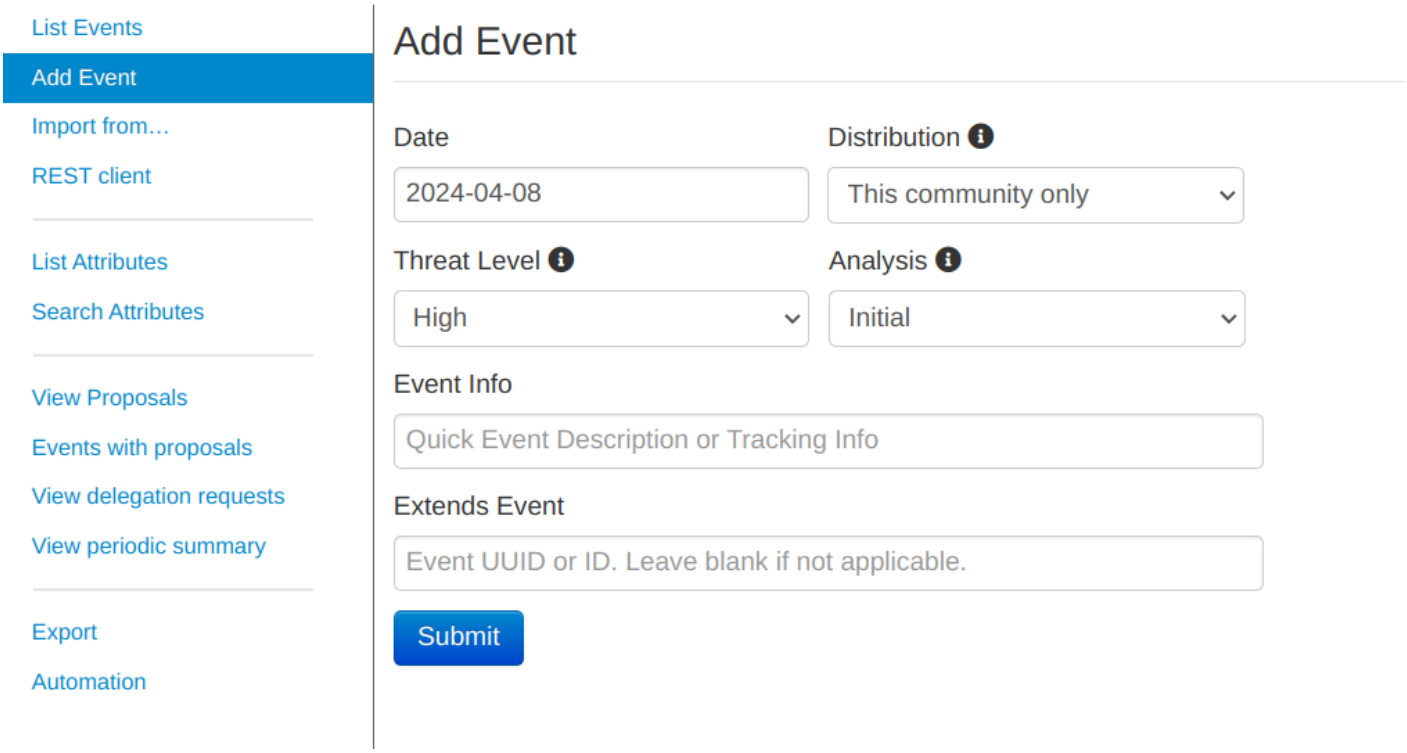
Event Action menüsü farklı kategoriler içerir ve her biri farklı işlevleri temsil eder:



- **List Events:** Sistemde özel olmayan veya kuruluşa ait olmayan tüm *Event'leri* listeleyerek, kullanıcılara bu *Event'leri* görüntüleme, düzenleme, silme, yayınlama veya inceleme olanağı sağlar.

Actions bölümü altında sırasıyla *Event'i* yayınlama, düzenleme, silme ve görüntüleme butonları yer almaktadır.

- **Add Event:** Kullanıcılara, bir *Event* oluşturma formunu doldurarak ve ardından bu *Event objesini* oluşturarak, yeni *Event'ler* oluşturma yetkisi verir.



Date: *Event'in* meydana geldiği tarih.

Distribution: *Event* yayımlandığında ve geri çekildiğinde kimlerin görebileceğini kontrol eder. Ayrıca, *Event'in* diğer sunucularla senkronize edilip edilmeyeceğini de belirler.

Your organization only: Sadece kendi kuruluşunuzun üyelerinin *Event'i* görmesine izin verir. Senkronizasyon yapılmaz.

This Community-only: MISP topluluğunuzun bir parçası olan kullanıcılar *Event'i* görebilir. Bağlı sunucular kısıtlanır.

Connected communities: MISP topluluğunun bir parçası olan kullanıcılar *Event'i* görebilir. Bağlı sunucuların üyeleri kısıtlanır.

All communities: *Event'i* tüm MISP topluluklarıyla paylaşır.

Sharing group: Belirlenen paylaşım grubuna *Event'i* paylaşır, yalnızca paylaşım grubunda tanımlanan kuruluşları içerir.

Threat Level: Bu alan, *Event'in* risk seviyesini gösterir. *Event'ler* üç farklı tehdit kategorisine (düşük, orta, yüksek) kategorize edilebilir.

Düşük: Genel kitlesel kötü amaçlı yazılım.

Orta: Gelişmiş Kalıcı Tehditler (APT)

Yüksek: Sofistike APT'ler ve 0-gün saldırıları.

Analysis: *Event* için mevcut analiz aşamasını gösterir.

Başlangıç: Analiz henüz başlıyor.

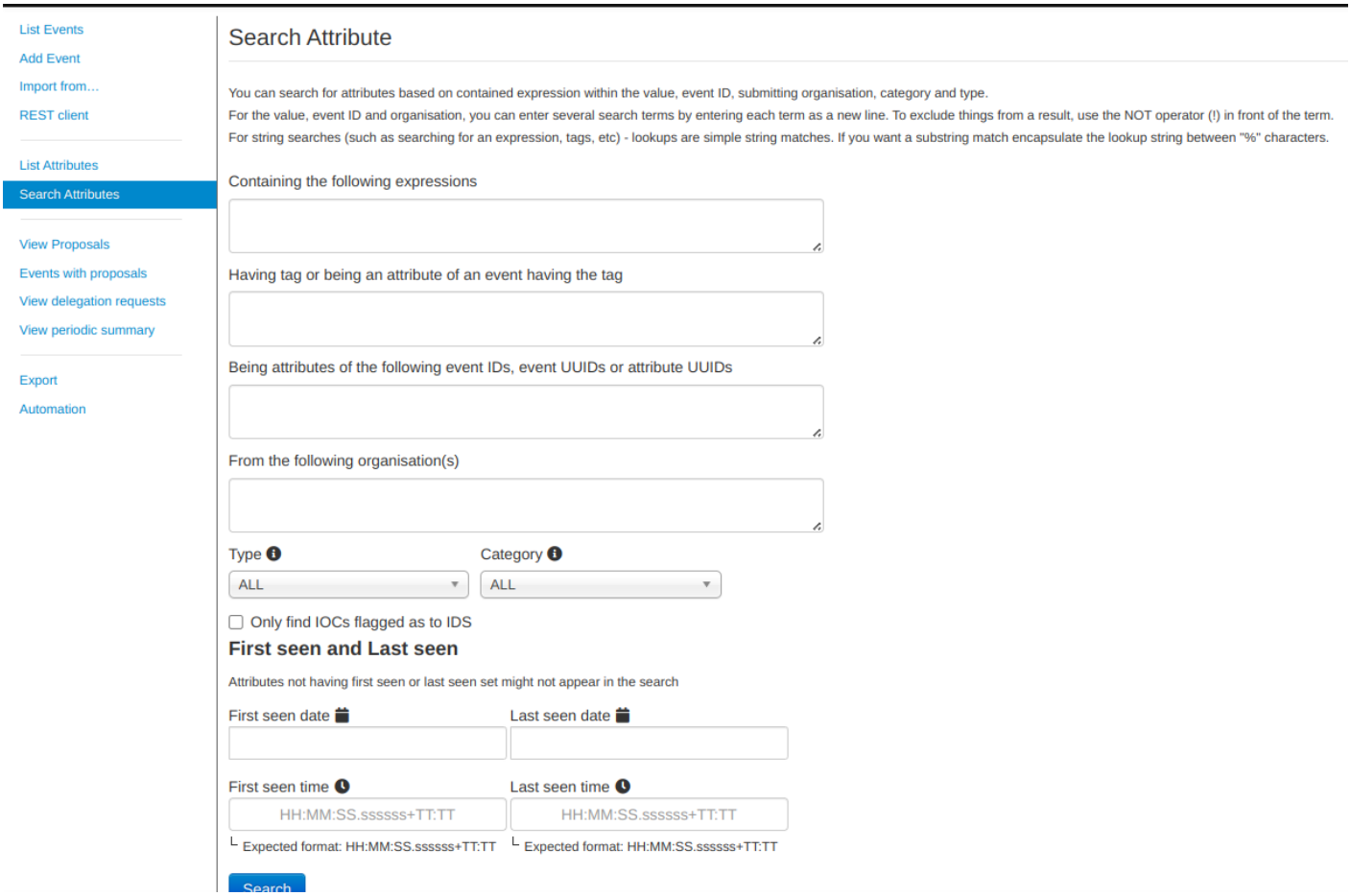
Devam eden: Analiz devam ediyor.

Tamamlandı: Analiz tamamlandı.

Event Info: *Event'in* kısa bir tanımının bulunduğu bilgi alanıdır.

Extends Event: Bir *Event'in* başka bir *Event'e* atıfta bulunmasını sağlar. Bir *Event'in* diğer bir *Event'le* olan ilişkisini belirtir.

- **List Attributes:** Sistemdeki özel olmayan veya kuruluşa ait olmayan tüm özellikleri listeler. Her bir özellik bu alanda değiştirilebilir, silinebilir veya görüntülenebilir.
- **Search Attributes:** Bu alanda filtrelenmiş bir özellik dizini görünümü için arama terimleri ayarlanabilir.



- **REST Client:** API'ye doğrudan bir Web Kullanıcı Arayüzü üzerinden çağrı yaparak, kullanıcıların API üzerinden otomatikleştirilmiş işlemleri gerçekleştirmelerine olanak tanır.
- **View Proposals:** Kullanıcının görebileceği tüm önerilerin bir listesini sunar.
- **Events with proposals:** Kullanıcının kuruluşu tarafından oluşturulan ve bekleyen önerileri içeren tüm Event'leri listeler.
- **List Tags:** Kullanıcıların oluşturduğu tüm *Tag'ları* listeleyerek, kullanıcılara *Tag'ları* inceleme ve yönetme olanağı sağlar.
- **Add Tag:** Kullanıcılara yeni bir *Tag* oluşturma yetkisi verir.
- **List Tag Collections:** Kullanıcıların oluşturduğu *Tag* koleksiyonlarını listeleyerek, kullanıcılara bir dizi *Tag'ı* tek bir eylemde bir *Event'e* veya özelliğe(attribute) atama olanağı sağlar.
- **List Taxonomies:** MISP örneğine yüklenmiş tüm taksonomileri listeleyerek, kullanıcılara taksonomileri inceleme ve yönetme olanağı sunar.

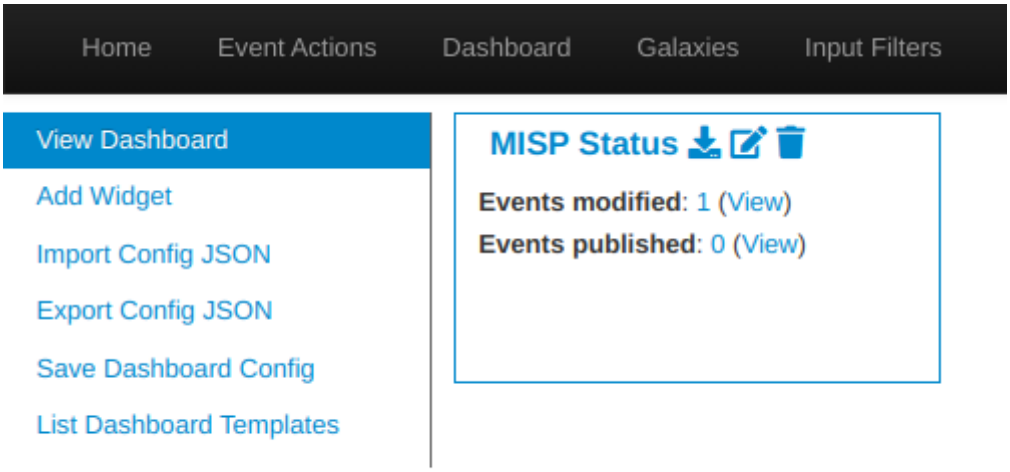
  MISP taxonomileri, tehditlerin ve diğer güvenlik olaylarının kategorize edilmesine ve sınıflandırılmasına olanak tanır. Ayrıca, MISP kullanıcılarının tehditlerle ilgili verileri daha tutarlı bir şekilde kaydetmelerine ve paylaşmalarına yardımcı olur.

- **List Templates:** Kullanıcıların oluşturduğu tüm Event templatelerini listeleyerek, kullanıcılara templateleri inceleme ve yönetme olanağı sağlar.
- **Add Template:** Kullanıcılara yeni bir template oluşturma yetkisi verir.
- **Export:** Erişilebilen verileri çeşitli formatlarda dışa aktarır.
- **Automation:** Kullanıcılar MISP ile entegre edilmiş sistemler arasında otomatik veri alışverişlerini ve işlemlerini yapılandırabilirler. Bu, güvenlik olaylarını otomatik olarak

paylaşma, veri senkronizasyonu, otomatik tehdit analizi ve diğer otomasyon görevlerini gerçekleştirme gibi işlemleri içerebilir.

DASHBOARD

Widget'ları kullanarak özel bir kontrol paneli oluşturulmasına olanak sağlar. Kullanıcılara MISP platformundaki güvenlik olaylarını ve tehditleri görsel olarak takip etme ve analiz etme imkanı sunar. Genellikle çeşitli grafikler, tablolar ve özet bilgiler bulunur. Kullanıcılar, *Dashboard*'da sunulan veriler aracılığıyla güncel tehdit durumunu anlayabilir, *Event*'*lerin* dağılımını görebilir ve analiz yapabilirler. Ayrıca, *Dashboar*d'da genellikle belirli *Event*'*ler* veya tehditler hakkında daha detaylı bilgiye erişmek için bağlantılar veya araçlar bulunabilir.



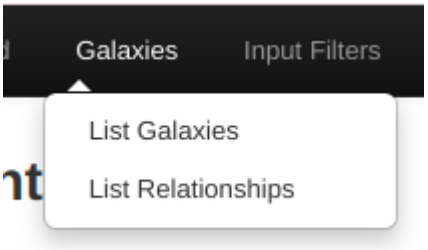
GALAXIES

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.

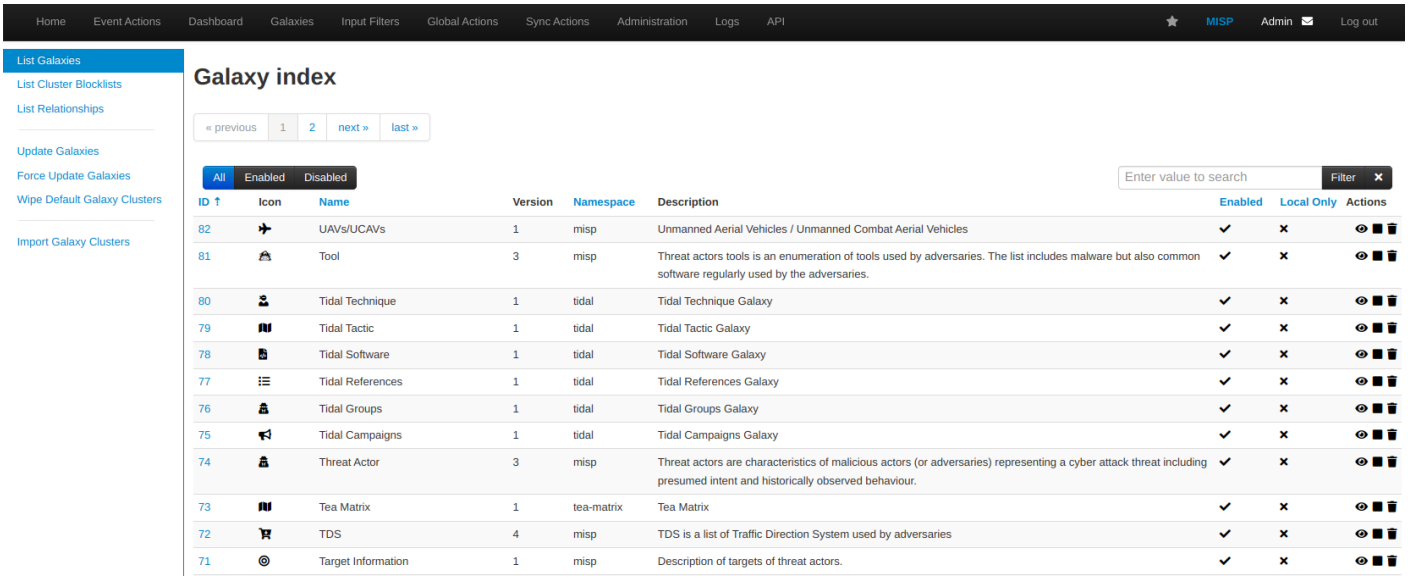
MISP *galaxy* varsayılan sözcük dağarcıkları bulunmaktadır, ancak bunlar istenildiği gibi üzerine yazılabilir, değiştirilebilir veya güncellenebilir. Sözcük dağarcıkları, mevcut standartlardan (STIX, Veris, ATT&CK, MISP vb.) veya yalnızca kuruluşlar için kullanılan özel standartlardan gelir.

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.

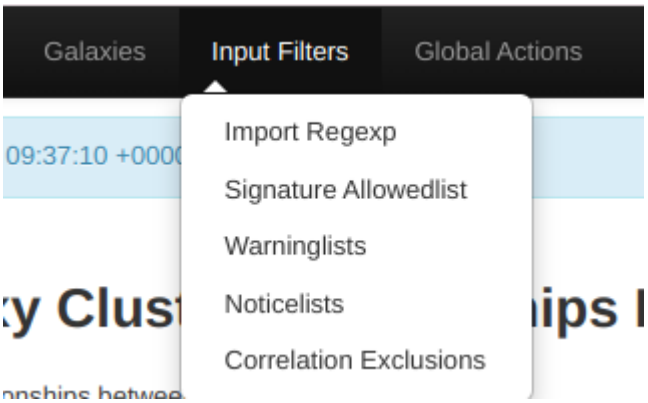
```
cd /var/www/MISP/app/files/
sudo rm -rf misp-galaxy


sudo -u www-data git clone https://github.com/SteveClement/misp-galaxy.git
```

INPUT FILTERS

Input Filters, MISP platformunda kullanıcıların veri girişlerini kontrol etmelerini sağlayan bir özelliktir.

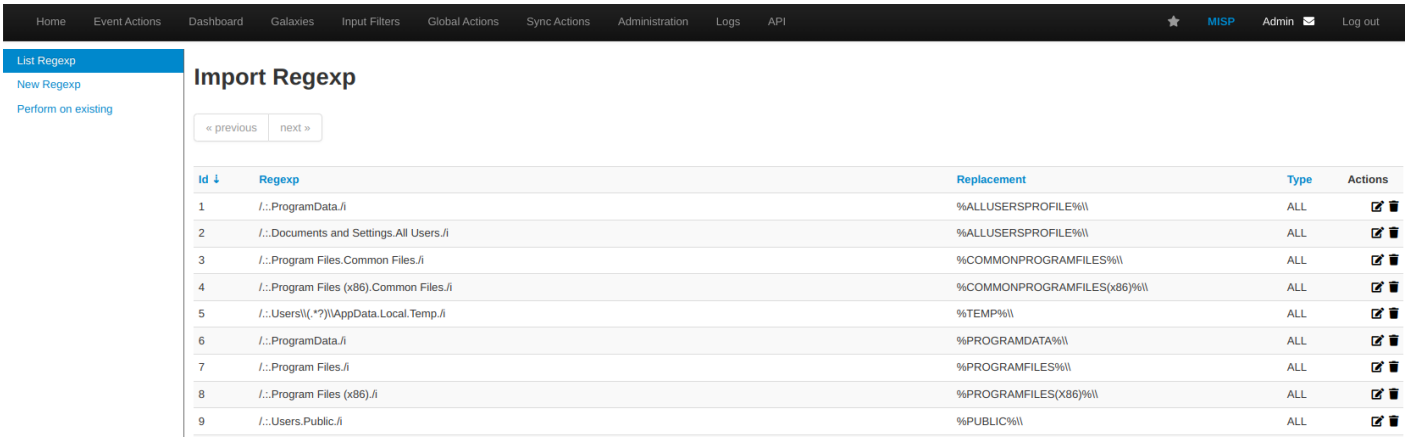
Bu filtreler, kullanıcıların veri girişini doğrulamak, belirli veri türlerini kabul etmek veya reddetmek, düzenli ifadeleri kullanarak veri biçimlerini kontrol etmek ve kötü amaçlı veya istenmeyen verileri engellemek gibi işlevlere sahiptir. Kullanıcılar, MISP giriş filtreleri aracılığıyla veri kalitesini artırabilir ve güvenliklerini sağlamlaştırabilir.

Ayrıca, belirli değerlerin dışa aktarılmasını engellemenin yanı sıra, belirli değerlerin engellenmesi de mümkündür. Kullanıcılar bu değiştirme ve engelleme kurallarını görüntüleyebilir, ancak bir yönetici bunları değiştirebilir. Bu sayede veri girişi ve işleme süreçleri daha güvenli ve kontrol edilebilir hale gelir.



- **Import Regexp:** Belirli türdeki verilerin içeri aktarılması sırasında uygulanacak düzenli ifadelerin tanımlanmasını sağlar.

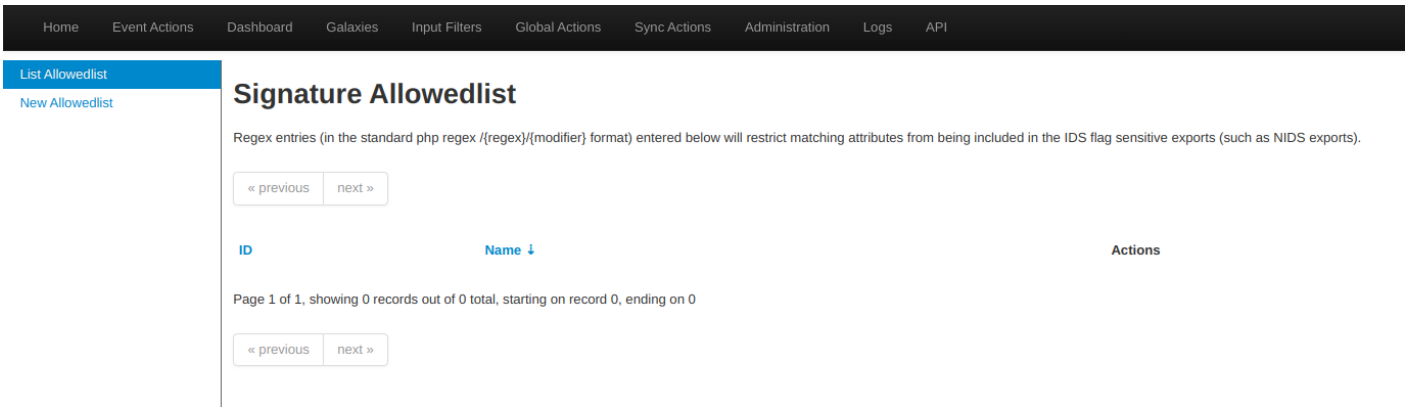
Bu alanda belirtilen düzenli ifadeler, içeri aktarılan verilerin belirli bir formata veya desene uyması gerektiğini belirtir. Örneğin, e-mail adresleri, URL'ler veya dosya adları gibi belirli veri türlerinin doğruluğunu kontrol etmek için kullanılabilirler. Bu şekilde, yanlış veya zararlı verilerin sisteme girmesi engellenir ve veri bütünlüğü sağlanır.



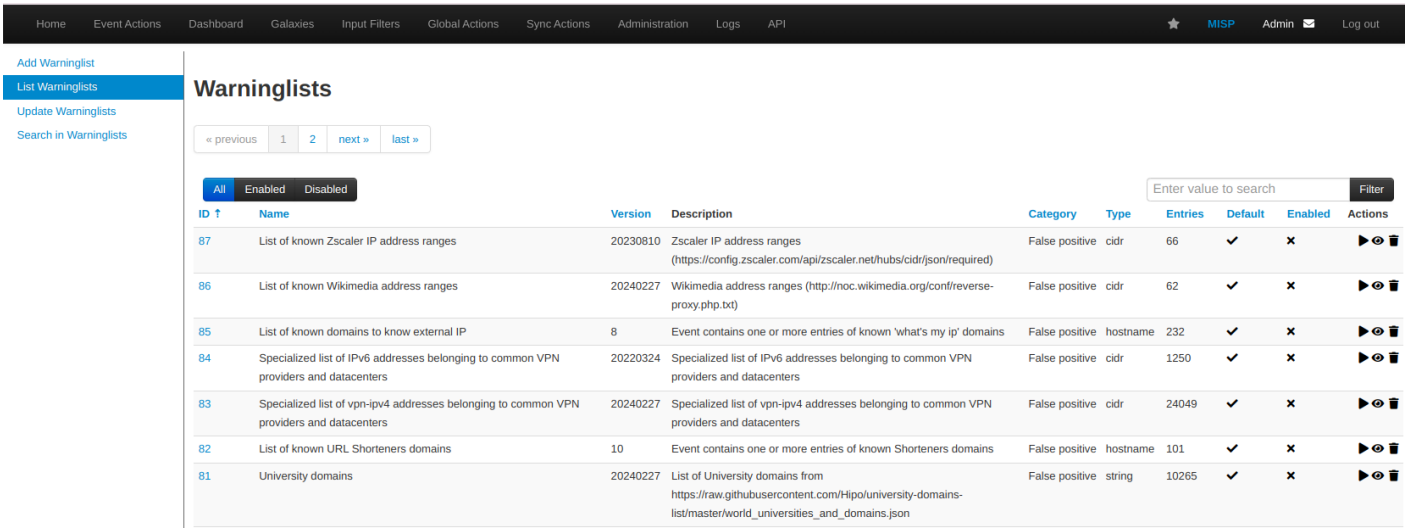
- **Signature Allowedlist:** İçeri aktarılan verilerin belirli imzaları veya desenleri içermesine izin verilen bir izin listesini tanımlar.

Bu alanda belirtilen imzalar veya desenler, verilerin içeri aktarılmasını engelleyen diğer filtrelerin aksine, içeri aktarılan verilerin içinde belirli imzaların bulunmasını gerektirir.

Örneğin, bir organizasyonun belirli bir veri türünü veya formatını kabul etmesi gerekiyorsa, bu alanda bu tür imzalar veya desenler tanımlanabilir. Bu şekilde, kabul edilmeyen veya istenmeyen verilerin içeri aktarılması önlenir ve sistemin belirli bir standarda veya gereksinime uygun olarak çalışması sağlanır.



- **Warninglists:** Potansiyel false-positive, errorlar veya yanlışlıklarla ilişkilendirilebilecek iyi bilinen göstergelerin listeleridir. Python dilinde, *warninglist*'lerle çalışmak için PyMISPWarningLists adında bir Python modülü bulunmaktadır.



- **False-Positive İkilemi:**

False-Positiveler, tehdit istihbaratı paylaşımında sıkça karşılaşılan bir problem olarak öne çıkar.

Genellikle durumlara ya da koşullara göre değişkenlik gösterebilir;

  - False-Positiveler, bilgi paylaşan kullanıcı topluluğuna göre değişkenlik gösterebilir.
  - Kuruluşlar,False-Positiveler konusunda kendi bakış açılarına sahip olabilirler.
- **Warninglist Kullanımı:**

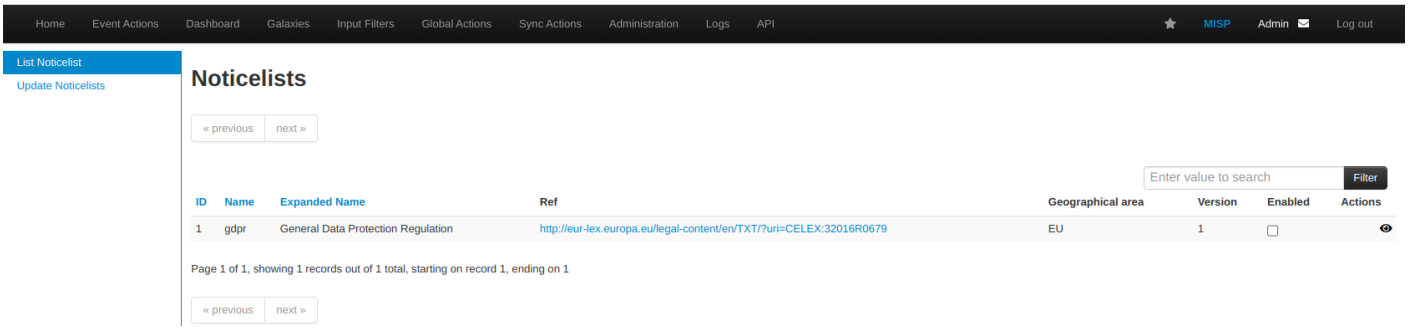
Varsayılan olarak, MISP, warninglist olarak adlandırılan belirli veri listelerindeki özelliklerin (attribute) sadece bir tür bayrağı belirli olduğunda eşleşmeleri tetikler. Ancak bu davranış, MISP'in yapılandırma ayarlarından biri olan "MISP.warning_for_all" parametresi "true" olarak ayarlandığında değiştirilebilir.

Özellikler, genellikle bir olayın veya tehdidin belirli bir yönünü tanımlamak için kullanılan veri parçalarıdır. Özellikler arasında IP adresleri, alan adları, dosya adları gibi bilgiler bulunabilir. MISP, bu özelliklerin, MISP'e özgü bir kimlik tespit sistemi (IDS) tarafından işaretlendiğinde, yani bir tehdit olarak algılandığında, *warninglist*'lerdeki verilerle eşleşip eşleşmediğini kontrol eder.

Bir özellik, *warninglist* adı verilen önceden tanımlanmış bir veri listesinde bir eşleşme bulursa, bu durum kullanıcıya bildirilir. Kullanıcı, bu bilgiyi olay ve özellik düzeyinde bir bilgi veya uyarı kutusu aracılığıyla görebilir. Kullanıcının potansiyel olarak tehlikeli olduğu düşünülen verilere dikkat etmesini ve gerekli önlemleri almasını sağlar.

- **Noticelists:** MISP Noticelists, belirli özelliklerin, kategorilerin veya nesnelerin kullanımının yasal, gizlilik, politika veya hatta teknik sonuçları hakkında MISP kullanıcılarını bilgilendirmek için kullanılan bildirim listeleridir.

Kullanıcının eylemlerinin olası sonuçları konusunda daha bilinçli olmasını sağlamak ve uyarı bildirimlerini tetiklemek için kullanılan basit bir JSON açıklamasıdır.



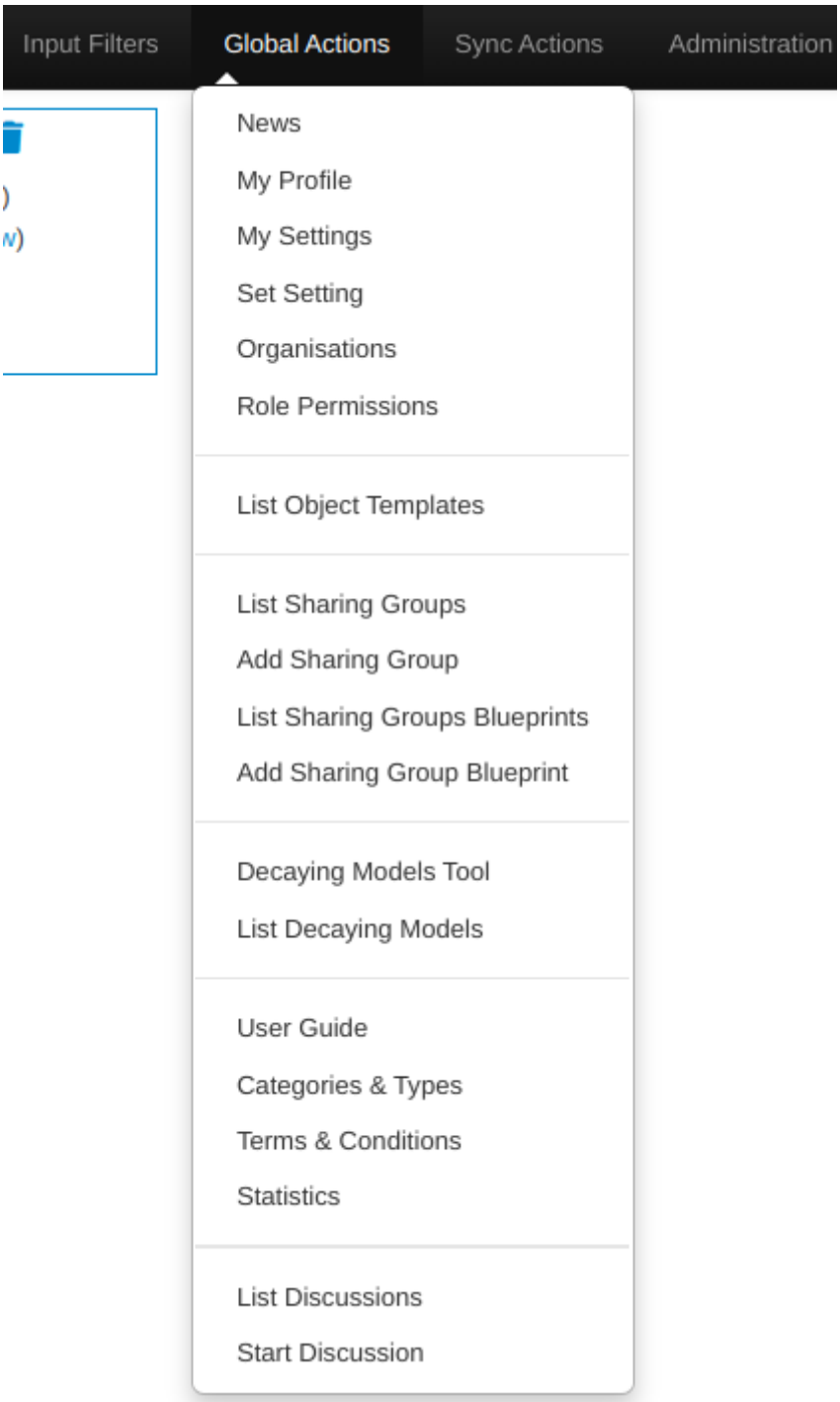
- **Correlation Exclusions:** Veri girişlerinin nasıl işleneceğini ve yorumlanacağını belirlemek için kullanılan bir özelliktir.

"Correlation Exclusions" ayarları, özellikle veri analizi ve tehdit istihbaratı paylaşımında kullanışlıdır. Örneğin, belirli bir olay veya tehdit örneğinin birbirleriyle ilişkilendirilmemesi gereken özellikleri veya nesneleri belirtmek için kullanılabilir. Böylece, "False-Positive"lerin ve yanlış sonuçların önlenmesine yardımcı olur ve analizin doğruluğunu artırır.

GLOBAL ACTIONS

Global Actions menüsü, MISP platformunda genel işlevlere erişimi sağlamaktır. Genellikle yönetici düzeyinde kullanıcılar için mevcuttur ve MISP sisteminin genel yapılandırma ve yönetimi ile ilgili işlemleri gerçekleştirmelerine olanak tanır.

Örneğin, bu menü aracılığıyla yeni kullanıcılar eklemek, API anahtarlarını yönetmek, güvenlik ayarlarını yapılandırmak, sistem güncellemelerini denetlemek veya genel MISP yapılandırmasını yönetmek gibi işlemler gerçekleştirilebilir. MISP platformunun yönetimi ve yapılandırılması için kritik bir araçtır.



ChatGPT

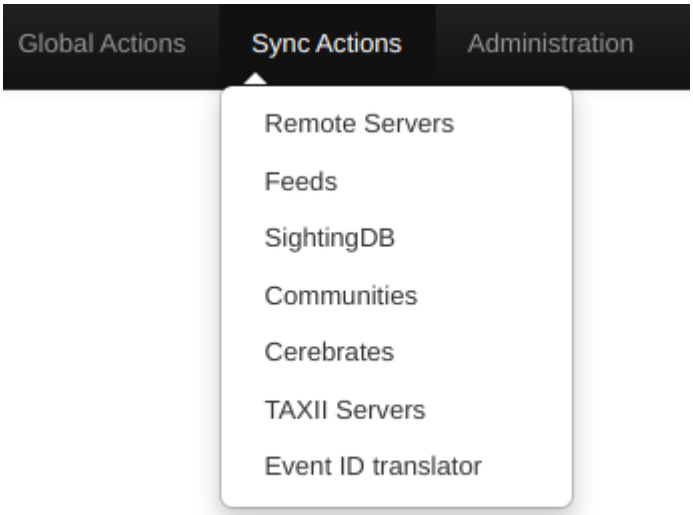
- **News:** MISP sistemiyle ilgili en son haberler okunabilir ve gerçekleşen güncellemeleri, yeni özellikleri veya önemli duyuruları içerir.
- **My Profile:** Kullanıcı hesabını yönetebilir ve kişisel bilgilerinin görüntülenmesini, güncellenmesini veya diğer kullanıcı ayarlarının yönetilmesini sağlar.
- **My Settings:** Kullanıcıya özgü ayarlar görüntülenebilir ve belirlenebilir. Hesap tercihlerini, bildirim ayarlarını veya diğer kullanıcı özelliklerini yapılandırmayı içerir.
- **Set Setting:** Tercihlerin özelleştirilmesini veya özel bildirim ayarlarının oluşturulmasını sağlar.
- **Organisations:** Farklı kuruluşların platforma bağlı olduğu bir listeyi içerir.

- **Role Permissions:** Farklı kullanıcı rollerinin ve bu rollerin sistemde hangi izinlere sahip olduğunun bir listesini içerir.
- **List Sharing Groups:** Mevcut Paylaşım Gruplarının listesi görüntülenebilir, bu gruplara erişiminiz varsa, gruplar aracılığıyla veri paylaşımını kolaylaştırabilirsiniz.
- **Add Sharing Group:** Yeni bir paylaşım grubu oluşturulabilir. Bu sayede, belirli kullanıcılar arasında veri paylaşımını daha organize bir şekilde düzenlemek için kullanılabilir.
- **Decaying Models Tool:** Belirli veri ögelerinin zaman içinde nasıl değişeceğini tanımlayan matematiksel modellerdir.
- **List Decaying Models:** Var olan modellerin görüntülenmesini, düzenlenmesini veya silinmesini içerir.
- **User Guide:** Kullanıcıların MISP platformunun nasıl kullanılacağına dair rehber bilgilere erişmelerini sağlar.
- **Categories & Types:** Belirli veri özelliklerinin hangi kategorilere ve türlere ait olduğunu açıklar.
- **Terms & Conditions:** Kullanıcıların platformu kullanırken dikkate almaları gereken hükümleri içerir.
- **Statistics:** Platformun kullanımı ve veri dağılımı hakkında genel bir görünüm sağlar.
- **List Discussions:** Yerel organizasyonlara bağlı kuruluşlar tarafından oluşturulan tartışma başlıklarının listesini gösterir. Kullanıcıların belirli konular hakkında tartışmaları ve bilgi paylaşımını kolaylaştırır.
- **Start Discussion:** Kullanıcıların belirli konular hakkında yeni tartışma başlıkları başlatmasını sağlar.

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.

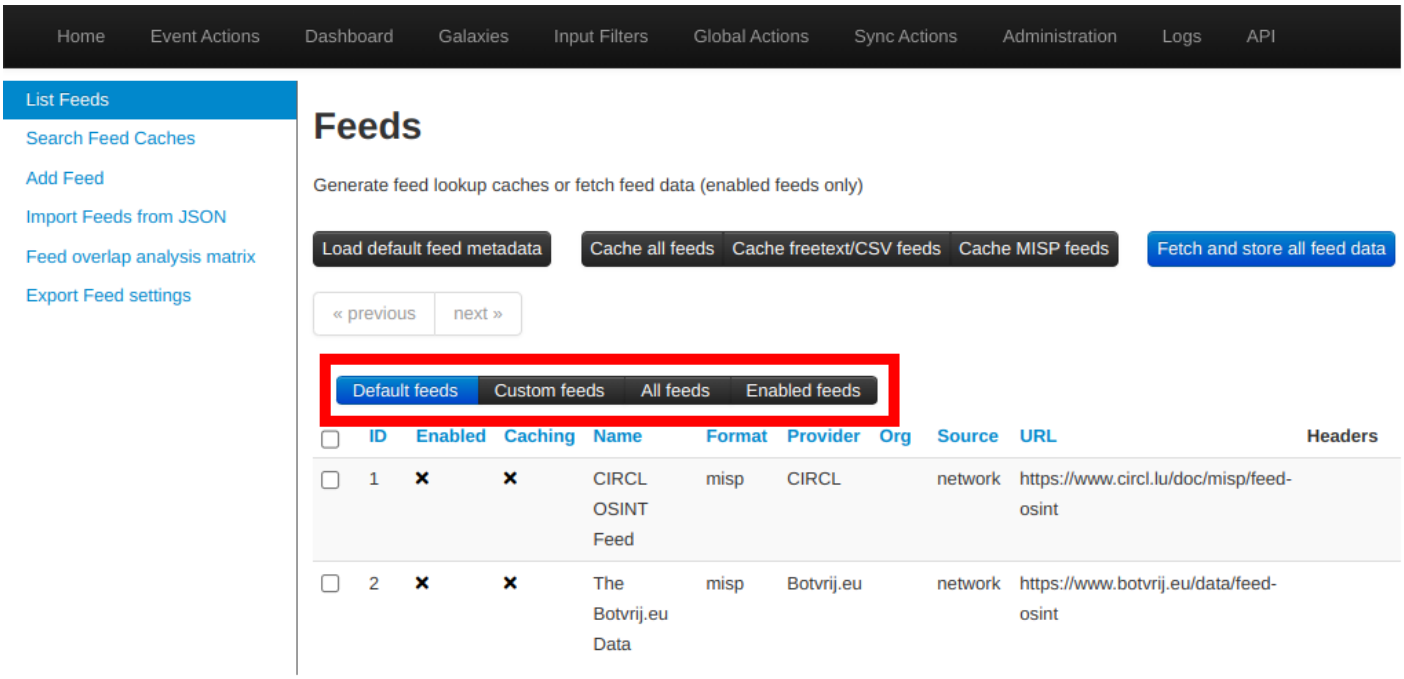
Örneğin, bir güvenlik tehdidi MISP üzerinde tespit edildiğinde, MISP Sync Actions aracılığıyla bu bilgi bir SIEM (Security Information and Event Management) sistemi ile senkronize edilerek, SIEM sistemi o tehdide karşı otomatik olarak koruma politikalarını güncelleyebilir veya alarm üretebilir.



- **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.

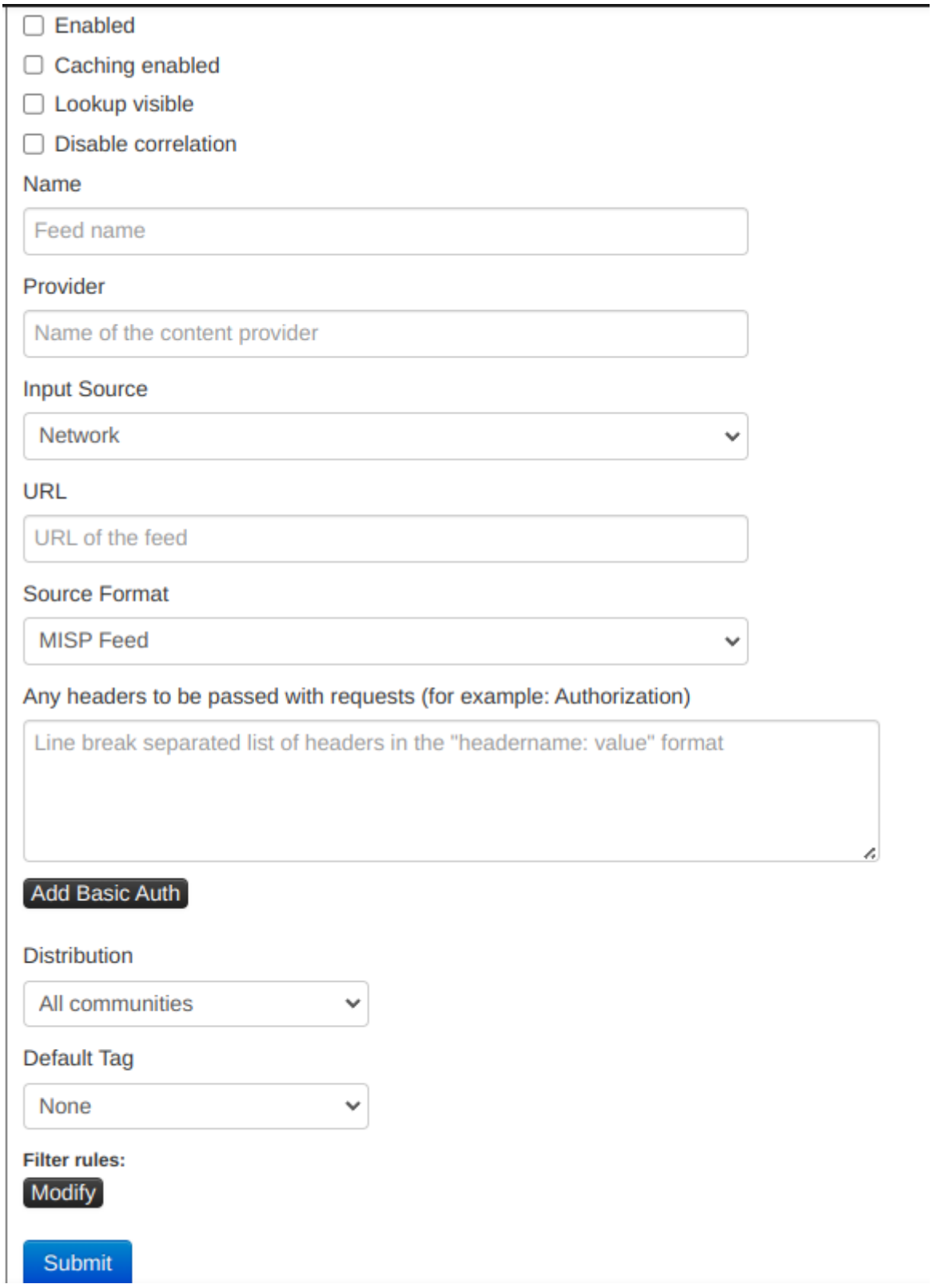
Belirli aralıklarla otomatik güncelleme yapmak için, MISP platformunda genellikle bir zamanlama ayarı bulunur. Bu ayar, ne sıklıkla "feed"lerin güncelleneceğini belirlemek için kullanılır. Ayarlar, genellikle MISP'in yönetim arayüzünde veya yapılandırma dosyalarında yapılır.

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.

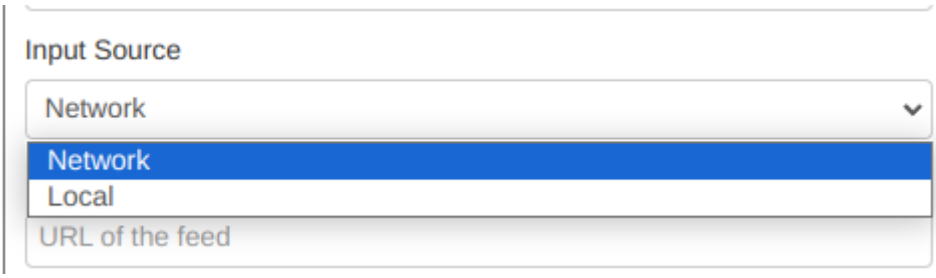
Lookup visible: İşaretlenmediğinde, korelasyonlar sadece sizin için görünür; işaretlendiğinde ise, korelasyonlar diğer kullanıcılar tarafından da görünür.

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.

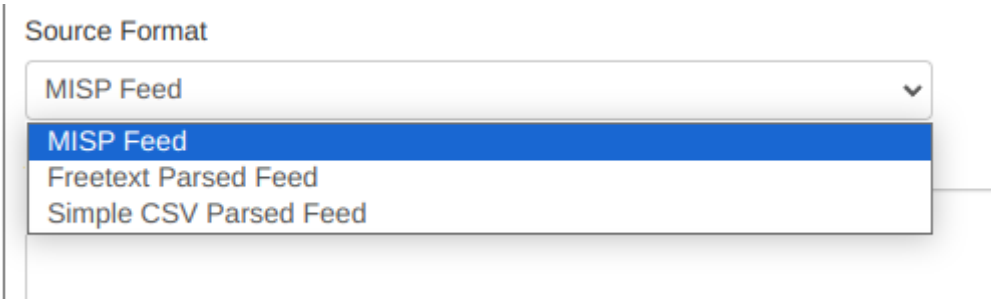
Input Source: Giriş kaynağı belirlenir. İki seçenek vardır:



- **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.

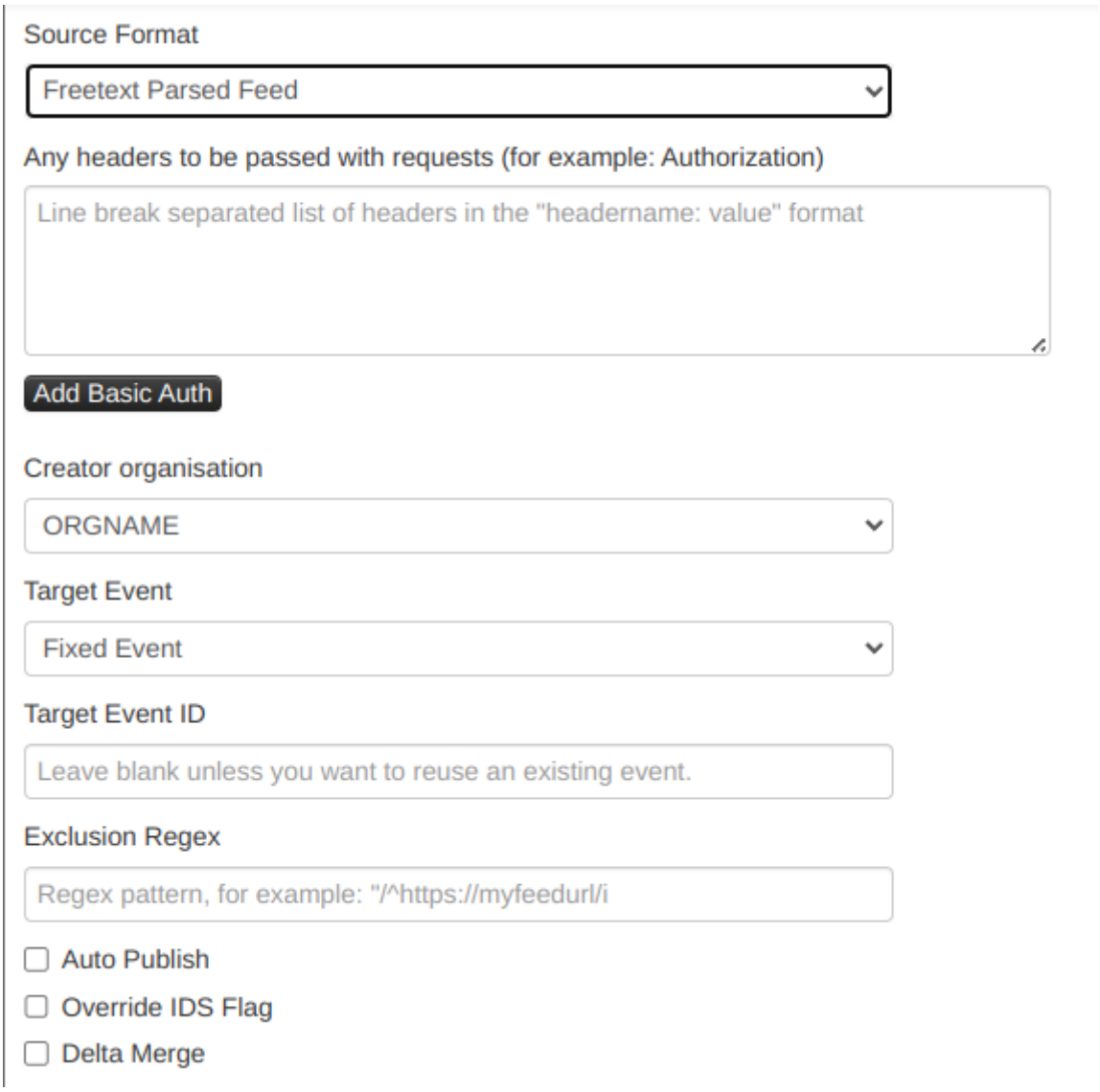


MISP Feed: Kaynak, MISP "Event"leri gibi JSON biçimli dosyaların bir listesine işaret eder.

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

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

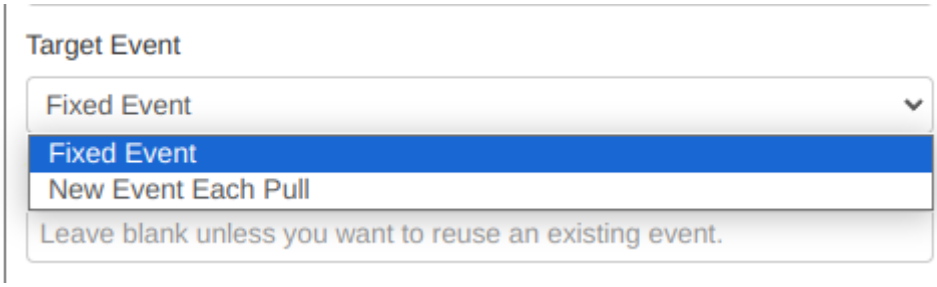
NOT: Freetext Parsed Feed seçeneği seçildiği takdirde yeni alanlar açılacaktır.



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.

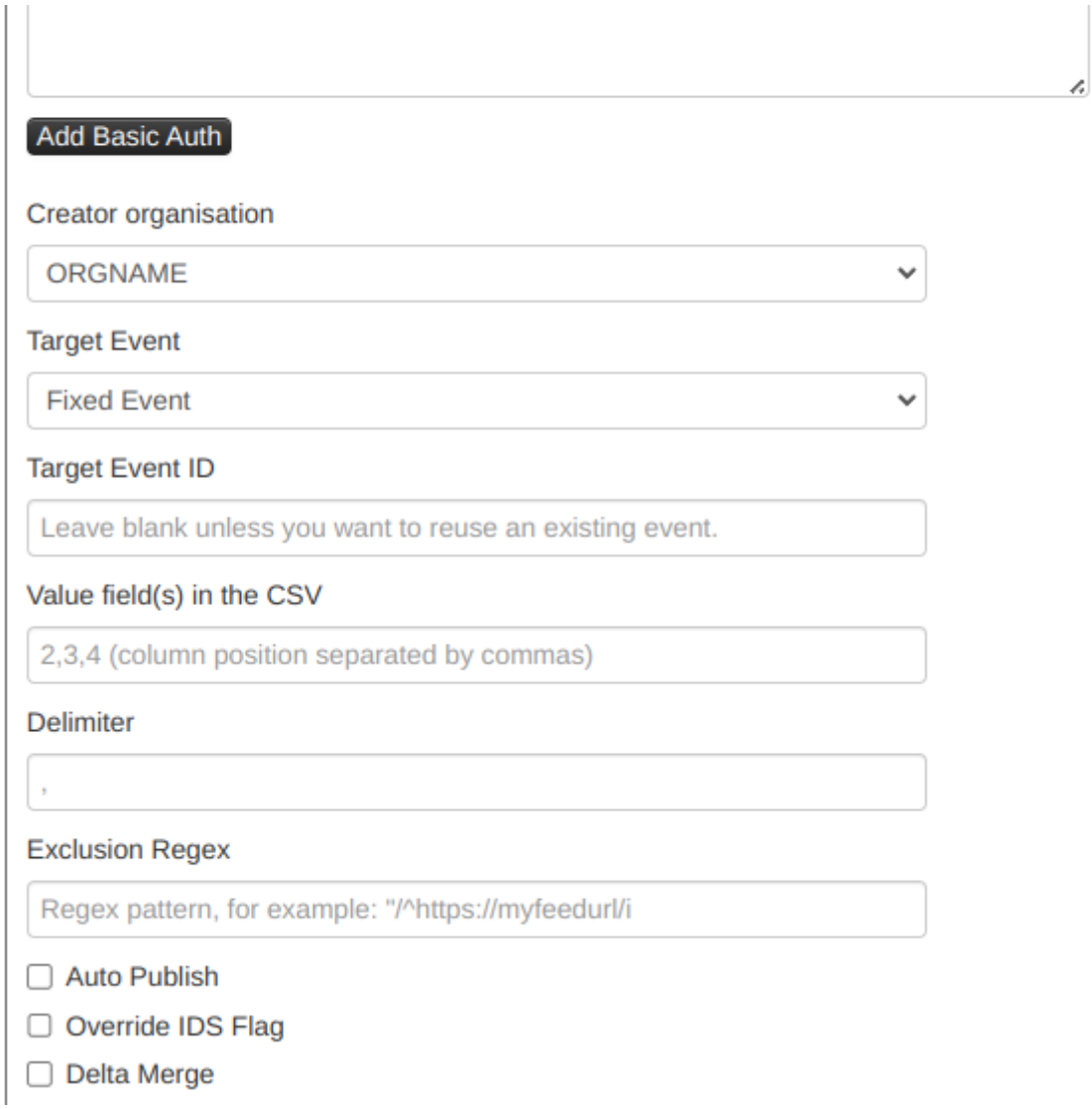
Exclusion Regex: Atlanması gereken IoC'leri tespit etmek için bir regex deseni eklenebilir. Örneğin, gerçek raporun / "feed"in herhangi bir referansını hariç tutmak için kullanışlı olabilir.

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

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

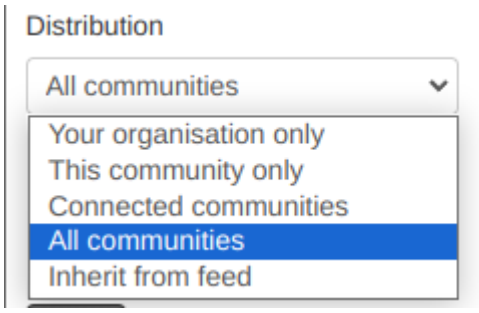
Delta Merge: İşaretlendiğinde, yalnızca en son alınan "feed"den özellikler saklanır, eski olanlar (geçici olarak) silinir.

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.

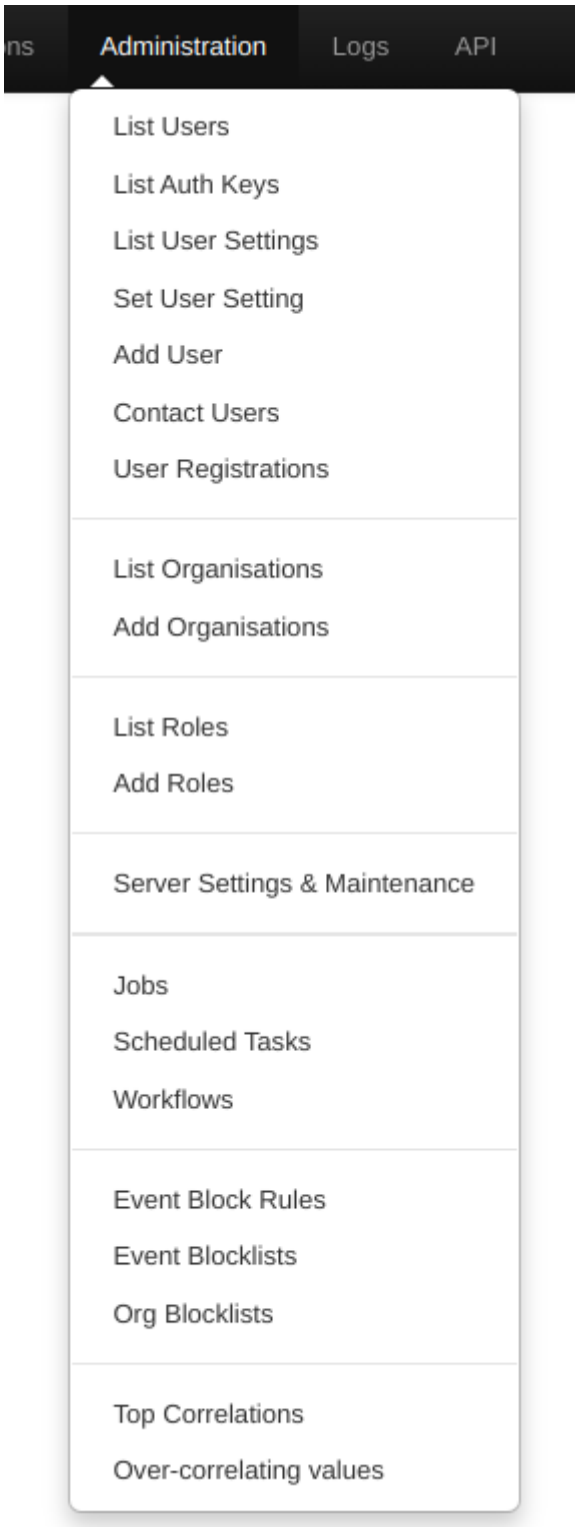
Filter Rules: Hangi "Event"lerin ya da kuruluşların izin verildiği veya engellendiği tanımlanabilir.

- **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.

ADMINISTRATIONS

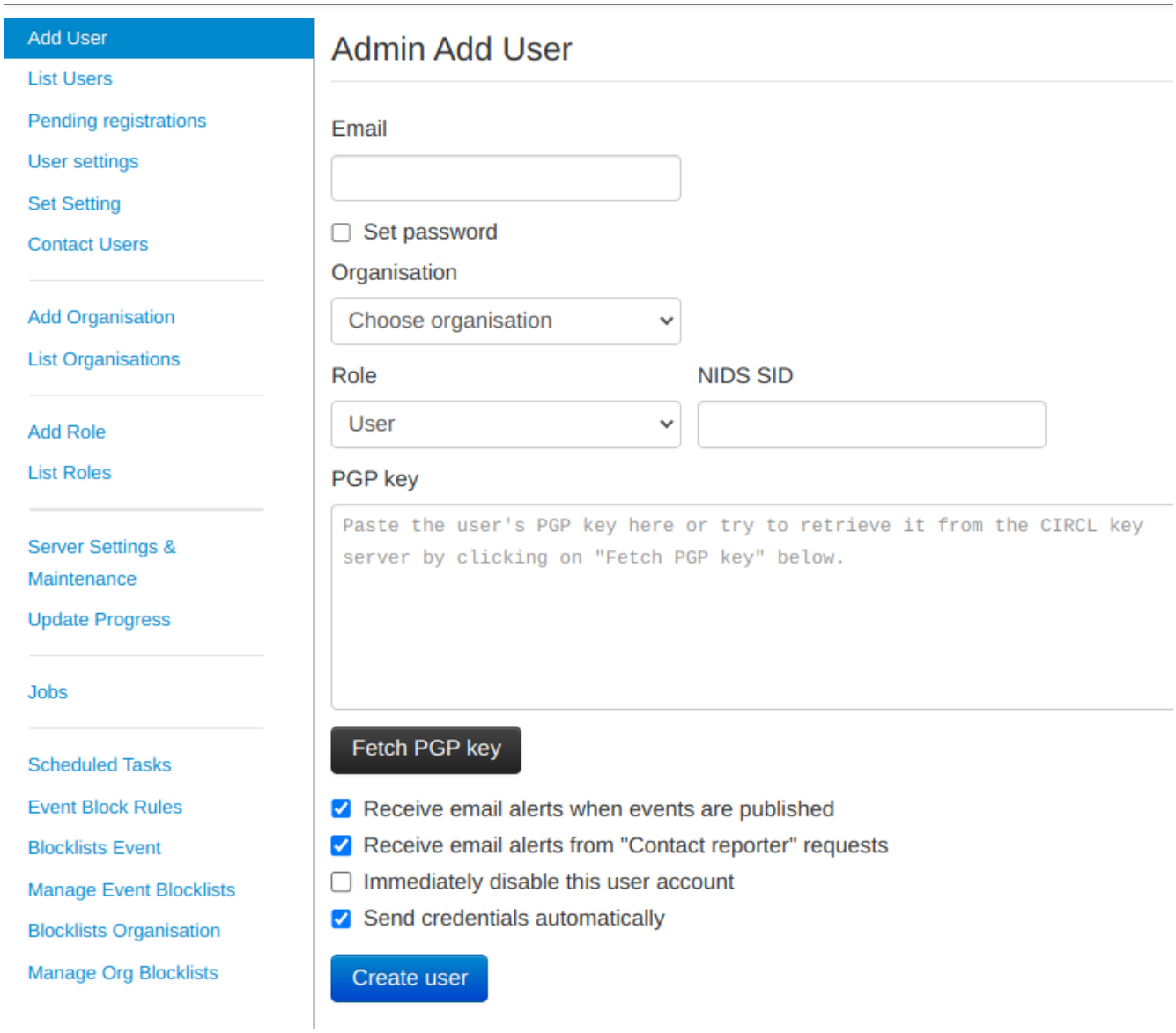
Yöneticiler kullanıcı hesaplarını ve kullanıcı rollerini ekleyebilir, düzenleyebilir veya kaldırabilir. Roller, olayların yayınlanması, REST arayüzünün kullanımı veya verilen role ait herhangi bir kullanıcının senkronizasyonu gibi belirli özelliklere erişim haklarını tanımlar.

Site yöneticileri kullanıcıların şifrelerini sıfırlamanın veya şifreli e-mail yoluyla onlarla iletişime geçmenin mümkün olduğu bir iletişim formuna da erişebilir.



- **List Users:** Şu anda kayıtlı olan kullanıcılar görüntülenebilir, değiştirilebilir veya silinebilir.
- **List Auth Keys:** Gelişmiş yetkilendirme anahtarı sisteminden alınan yetkilendirme anahtarlarının bir listesini ve bunların yorumlarını gösterir. Yetkilendirme anahtarı, bilgisayar sistemlerine erişim izni sağlayan bir kimlik doğrulama aracıdır. Özel bir dizi karakter veya sayıdan oluşur ve belirli kaynaklara erişim izni verir.
- **List User Setting:** Kullanıcı ayarlarını listeler.
- **Set User Setting:** Kullanıcılar için kullanıcıya özel ayarları belirler.
- **Add User:** Kuruluşlar için yeni bir kullanıcı hesabı oluşturulabilir. Site yöneticileri, herhangi bir kuruluş için kullanıcı hesapları oluşturabilirler.

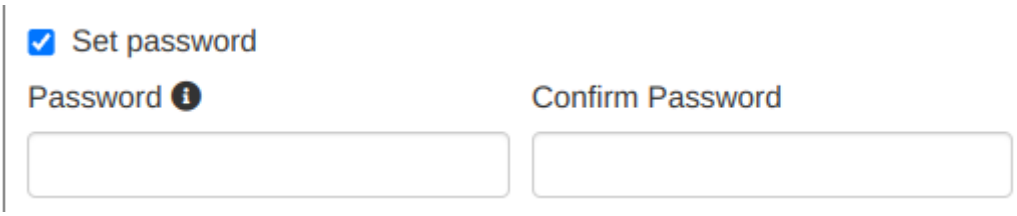
Yeni bir kullanıcı eklemek için soldaki yönetim menüsündeki "Add User" butonu ile yeni bir kullanıcı eklenebilir.



E-Mail: Kullanıcı e-mail adresi, kullanıcı adı olarak giriş yapmak ve otomatik e-mailleri göndermek için bir adres olarak kullanılacaktır.

Set Password: Kullanıcı için geçici bir kullanıcı şifresi tanımlamak isteniyorsa kutu işaretlenir. Eğer istenmiyorsa, bir şifre oluşturmak ve bunu kullanıcıya e-mail ile göndermek için 'List Users' görünümündeki 'reset password' butonu kullanılmalıdır.

Password: 'Set Password' işaretlendiğinde yalnızca bu metin kutusu görüntülenir. Kullanıcı için ilk girişten sonra değiştirmesi gereken geçici bir şifre tanımlanmalıdır. Parola MISP Parola politikasına uygun olmalıdır.



Organisation: Kullanıcı için organizasyon seçilmesini sağlayan açılır bir listedir.Organizasyon hakkında detaylı bilgi aşağıda verilmiştir.

Role: Kullanıcının ait olması gereken bir rol grubunun seçilmesini sağlayan açılır bir listedir. Roller, kullanıcıya atanan kullanıcı ayrıcalıklarını tanımlar. Roller hakkında detaylı bilgi aşağıda verilmiştir.

Authkey: Belirtilen kullanıcının benzersiz yetkilendirme anahtarıdır ve otomatik olarak atanır. (kullanıcı bunu sıfırlayabilir ve yeni bir anahtar alabilir). Bir sunucuyu başka bir sunucuya bağlamak için kullanılır, ancak kullanıcının yetkilendirme izni etkinleştirilmiş bir rolle atandığından emin olunması gerekir.

NIDS SID: Ağ sızma algılama sisteminde kullanılan bir imza kimliğidir. Kullanıcı tarafından oluşturulan Snort kuralları, kullanıcının tanımladığı ofsetle başlayan artan bir SID ile dışa aktarılır. Ofset belirtilmemişse, varsayılan olarak bir SID atanır, ancak bu bir rastgele değer olabilir.

Sync user for: Eğer bu seçenek ayarlanırsa, yerel kullanıcı bir uzak sunucudan çekim yaparken seçilen sunucunun itme kuralları da uygulanır. Bu seçenek, yönetici, Kuruluş Yöneticisi ve Senkronizasyon kullanıcı rolü için kullanılabilir.

> **Çekim (Pull)**: Bir cihazın veya sistemdeki bir kaynağın, diğer bir kaynaktan veri almak için aktif olarak talepte bulunması anlamına gelir. Yani, veri kaynağı, belirli bir zaman aralığında veya belirli bir olay gerçekleştiğinde veriyi çeken cihaz veya sistemdir. Örneğin, bir kullanıcının e-posta istemcisi, sunucudaki yeni e-postaları çekmek için düzenli aralıklarla sunucuya talepte bulunur.
>
> **İtme (Push)**: Bir cihazın veya sistemdeki bir kaynağın, veriyi otomatik olarak hedefe gönderdiği eylemidir. Kaynak, veri değişiklikleri olduğunda veya belirli bir koşul gerçekleştiğinde veriyi hedefe iletir. Örneğin, bir sunucu, yeni bir dosya oluşturulduğunda veya var olan bir dosya değiştirildiğinde, bu değişiklikleri hedef cihaza veya sisteme itebilir.

Gpgkey: Sistem üzerinden gönderilen e-mailleri şifrelemek için kullanılan anahtarı temsil eder.

Fetch GnuPG (PGP) key: GnuPG genel anahtarını getirir. GnuPG'nin genel anahtarı, diğer kullanıcıların verileri şifrelemek için kullandığı, herkese açık bir anahtardır.

Receive alerts when events are published: Bu seçenek, bir "Event" yayımlandığında yeni bir kullanıcıyı, otomatik olarak oluşturulan e-postaların alıcı

listesine ekleyecektir.

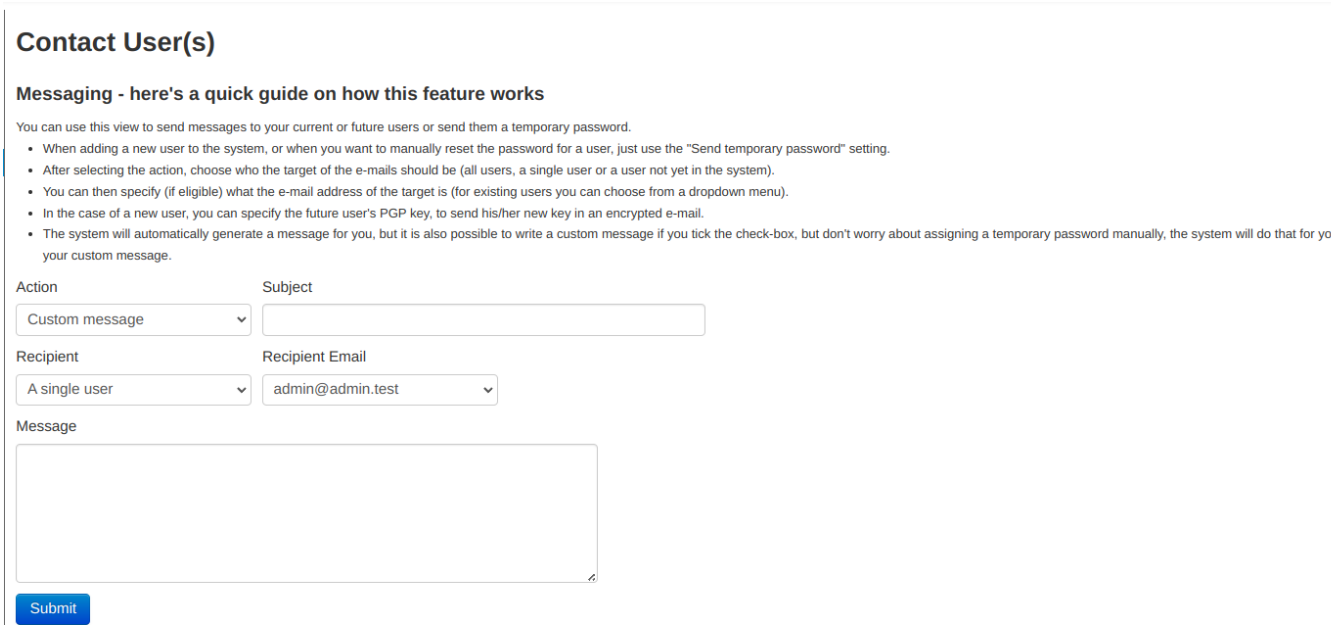
Receive alerts from "contact reporter" requests: Olayın raporlayıcısı veya kaynaklarından daha fazla bilgi sağlamalarını istemek için yapılan bir iletişim isteğidir.

Immediately disable this user account: Kullanıcı hesabını hemen devre dışı bırakma işlemini belirtir. Bu seçeneği işaretlediğinizde, kullanıcı hesabı derhal etkisiz hale getirilir ve kullanıcı o andan itibaren sistemde erişim hakkını kaybeder.

Send credentials automatically: Otomatik olarak kimlik bilgilerini gönderme işlemini belirtir. Bu seçeneği işaretlediğinizde, kullanıcıya otomatik olarak bir kullanıcı adı ve şifre gönderilir. Bu, genellikle yeni bir kullanıcı hesabı oluşturulduğunda veya bir kullanıcının şifresi sıfırlandığında kullanılır. Kullanıcıya kimlik bilgileri e-mail yoluyla gönderilir ve böylece kullanıcı, hesabına erişim sağlayabilir.

- **Contact Users:** Bu görünüm, mevcut veya gelecekteki kullanıcılara mesaj göndermek veya onlara geçici bir şifre göndermek için kullanılabilir.

Site yöneticileri, tüm kullanıcılara veya bireysel kullanıcılara e-mail göndermek için "Contact Users" özelliğini kullanabilir. GnuPG (PGP) anahtar setine sahip olan kullanıcılar e-maillerini şifrelenmiş olarak alacaklardır.



Action: Belirli bir e-mail türünü açıklar; ya özel bir ileti ya da şifre sıfırlama işlemi için kullanılır. Şifre sıfırlama e-postaları, otomatik olarak geçici bir şifreyi içeren bir mesajı alt kısmına ekler ve kullanıcının şifresini otomatik olarak bu yeni geçici şifreyle değiştirir.

Subject: Özel bir e-mail durumunda, buraya bir konu satırı girilebilir.

Recipient: Bu özellik, üç farklı kullanıcı grubuna ulaşmanıza olanak tanır:

1. **Tüm Kullanıcılar**:Platformdaki tüm kullanıcılara ulaşılmasını sağlar.

2. **Tek Bir Kullanıcıya**: Belirli bir kullanıcıya özel bir mesaj gönderilmesine olanak tanır. Tüm kullanıcıların e-mail adreslerinin bulunduğu ikinci bir açılır liste oluşturarak gerçekleştirilir.
3. **Potansiyel Gelecekteki Kullanıcılara**: Gelecekteki kullanıcıların hedef alınmasını sağlar. e-mail adresi için bir metin alanı ve bir GnuPG (PGP) genel anahtarı için bir metin alanı sağlayarak gerçekleştirilir. Bu şekilde henüz platforma katılmamış kişilere de ulaşabilirsiniz.

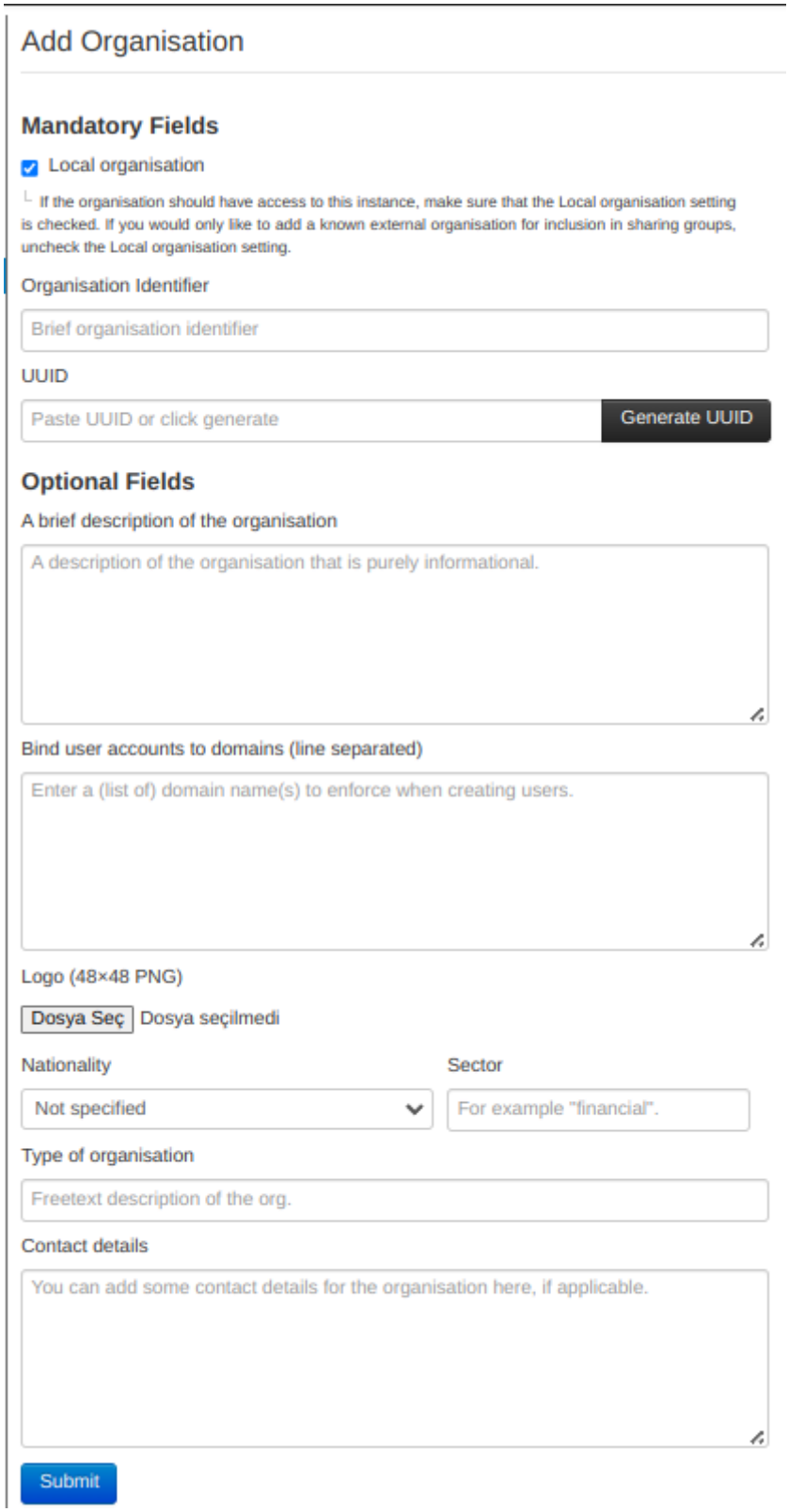
Message: Şifre sıfırlamaları ve hoş geldin mesajları için kullanılabilir. Kendi mesajınızı yazabilirsiniz (geçici bir anahtar ve imza ile birlikte eklenecektir) veya sistem tarafından otomatik olarak bir tane oluşturmasına izin verebilirsiniz.

Not: Sisteme yeni bir kullanıcı eklerken veya bir kullanıcının şifresini manuel olarak sıfırlamak isterken sadece "Send credentials automatically" ayarı kullanılır.

Uyarı: GnuPG (PGP) örneği anahtarı, yalnızca MISP örneği tarafından kullanılan ve yalnızca bildirimleri imzalamak için kullanılan GnuPG (PGP) anahtarıdır. MISP örneğinde kullanılan GnuPG (PGP) anahtarı başka hiçbir yerde kullanılmamalı ve değerli olmamalıdır.

- **Organisations:** Her kullanıcı bir kuruluşa aittir. Yöneticiler bu organizasyonu yönetebilir.

  Add Organisation:



Local Organisation: Organizasyonun bu örneğe erişimi olması gerekiyorsa, onay kutusunu işaretlenir. Yalnızca paylaşım gruplarına dahil etmek için bilinen bir dış organizasyon eklemek isteniyorsa, işaret kaldırılır.

Organisation Identifier: Organizasyon adı girilir.

Bir resim eklemek istenirse, 'Sunucu Ayarları' menüsünü kullanılarak web sunucusuna bir dosya eklenmelidir. Resmin aynı adı taşıması gerekir.

Uuid: **E**vrensel olarak benzersiz tanımlayıcı anlamına gelir. UUID'ler genellikle bilgisayar sistemlerinde benzersiz kimlikler oluşturmak için kullanılır.

> MISP çoklu örneği arasında organizasyon paylaşımı yapmak istiyorsanız, aynı Uuid'yi kullanabilirsiniz.

Nationality: Organizasyonun ülkesini seçmek için açılır listeden bir seçenek belirtilebilir.

Sector: Organizasyonun faaliyet gösterdiği sektör belirtilebilir (finansal, ulaşım, telekomünikasyon vb.).

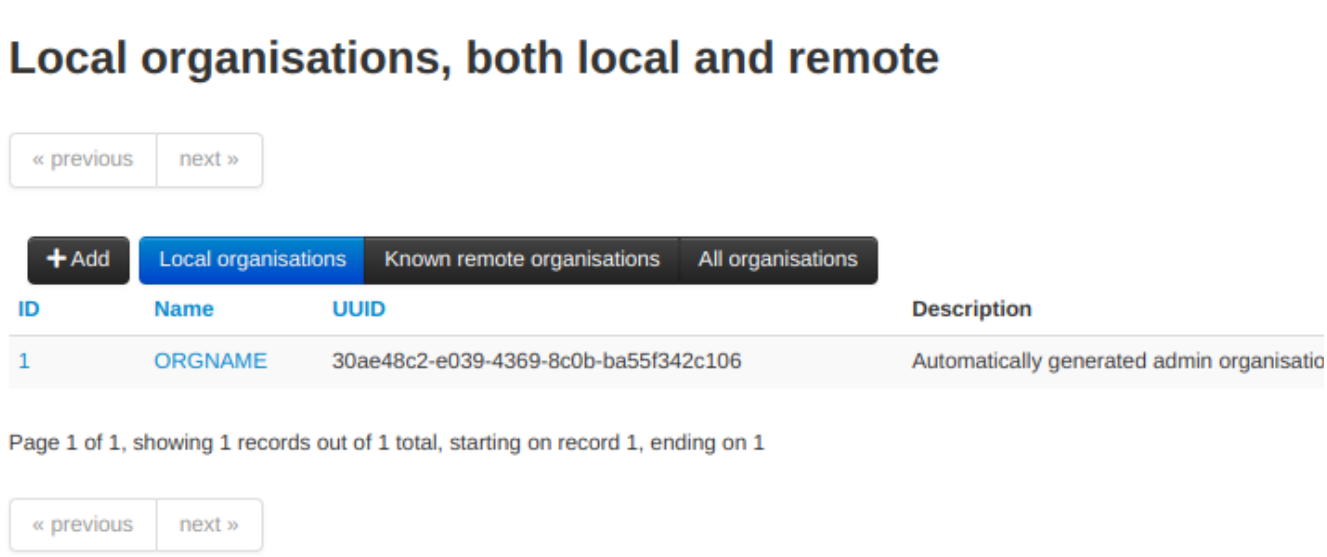
Type of Organisations: Organizasyonun türü belirtilebilir.

Contact Details: Organizasyon için bazı iletişim bilgileri eklenebilir.

List Organisations: Bir sistem veya platformda bulunan organizasyonların bir listesini görüntülemek için kullanılır.

Bu menü, kullanıcıların belirli bir kategorideki veya belirli bir özellikteki organizasyonları bulmasına ve bunlarla etkileşime geçmesine olanak tanır. Örneğin, bir veri paylaşım platformunda, "List Organization" menüsü, kullanıcıların kayıtlı olan tüm organizasyonların isimlerini, ülkelerini, sektörlerini ve iletişim bilgilerini görüntülemesine olanak sağlayabilir.

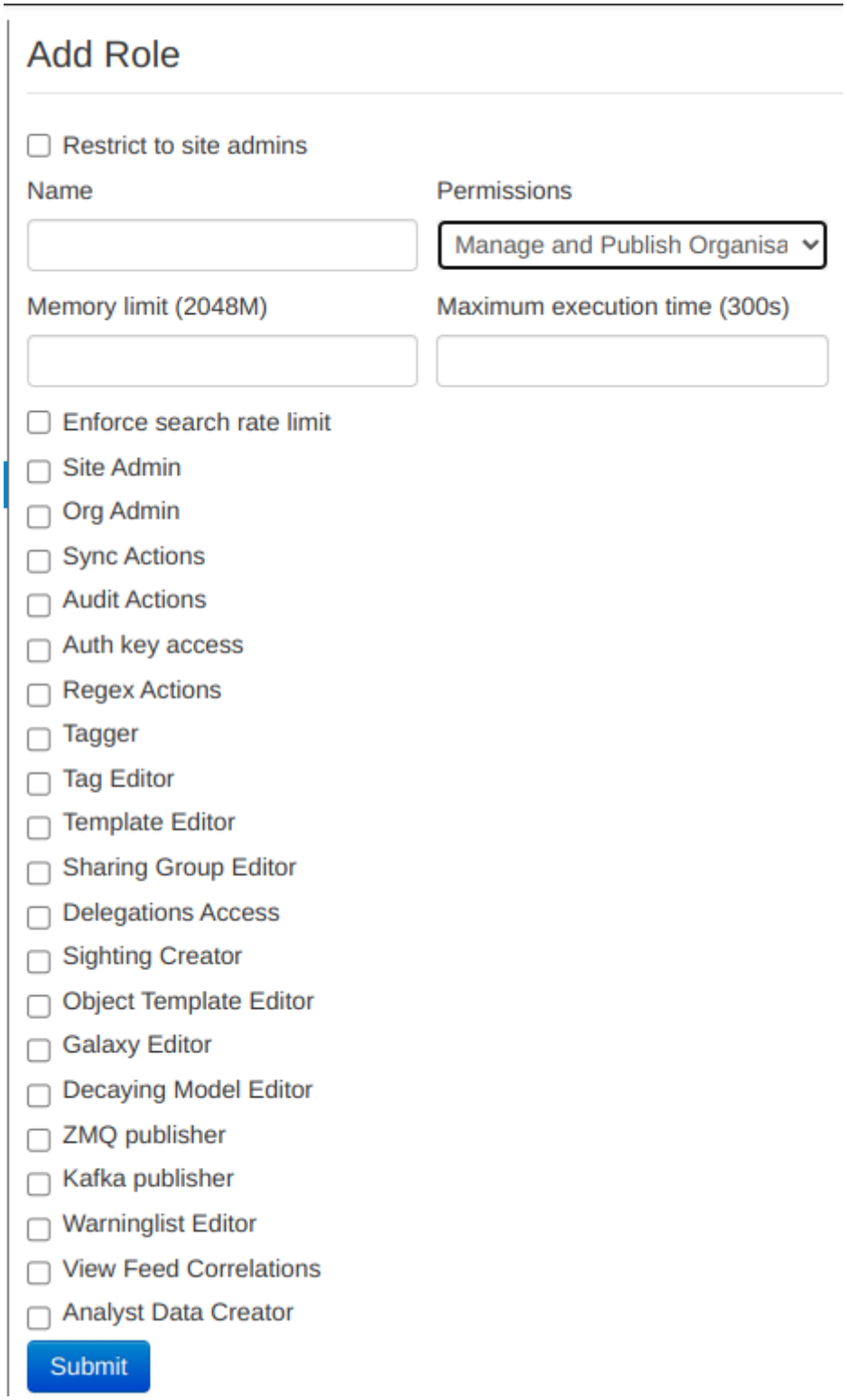
Kullanıcıların istedikleri organizasyonları aramalarına, filtrelemelerine ve bu organizasyonlarla ilgili daha fazla bilgi almak veya iletişime geçmek için gerekli adımları atmalarına imkan tanır.



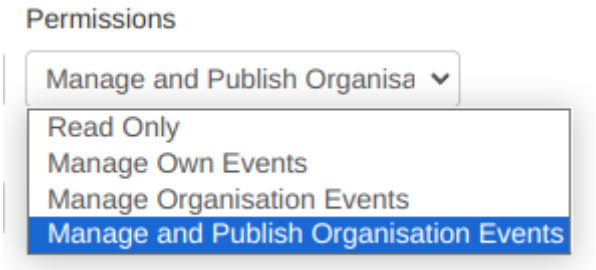
Bu görünümde yerel organizasyonları (Local Organizations), uzak organizasyonları (Known remote organizations) veya her ikisini birden (All organization) filtrelemek için 3 seçenek vardır.

- **Roles:** Kullanıcılara ayrıcalıklar, rol gruplarına atayarak verilir. Rol grupları, etkinliklerle ne yapabileceklerini belirleyen dört seçenekten birini kullanır; ayrıca dört ek ayrıcalık yükseltme ayarı sağlar.

  Add Roles: Yeni bir rol oluştururken, oluşturulacak rol için bir ad girilmesi, açılır menüyü ve ilgili onay kutularını kullanarak izinlerin ayarlanması gerekecektir.



  Permisions:



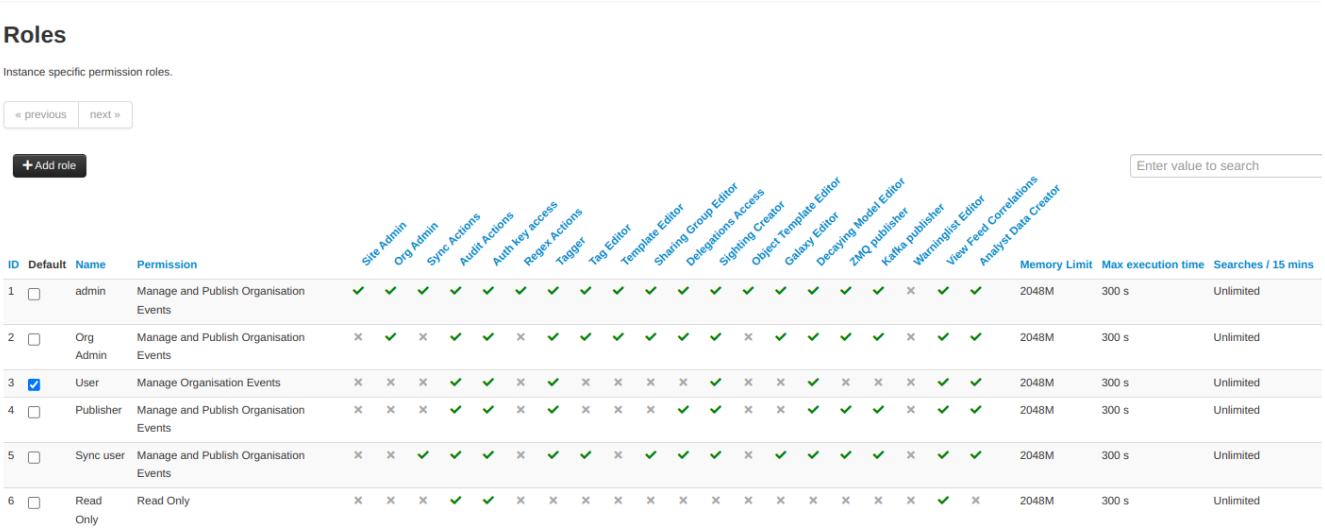
Read Only: Kullanıcının, kuruluşunun erişim sahibi olduğu "Event"lere göz atmasına izin verir, ancak veritabanında herhangi bir değişiklik yapılmasına izin vermez.

Manage Own Events: Kullanıcıların kendi "Event"lerini oluşturmasına, değiştirmesine veya silmesine olanak tanır, ancak bunları yayınlayamazlar.

Manage Organisation Events: Kullanıcıların, organizasyonlarının bir üyesi tarafından oluşturulan "Event"leri oluşturmasına veya değiştirmesine ve silmesine olanak tanır.

Manage and Publish Organisation Events: Kullanıcılara yukarıdakilerin tümünü yapma ve kuruluşlarının etkinliklerini yayınlama hakkı verir.

List Roles: Bir sistem veya platformda tanımlanmış olan rollerin bir listesini görüntülemek için kullanılır. Bu özellik, sistem yöneticilerinin hangi kullanıcıların hangi rollerle ilişkilendirildiğini kolayca görmelerini sağlar.



- **Blocklists and block rules:** Belirli etkinlik veya organizasyonların sisteme eklenmesini engellemek mümkündür. Yöneticiler engellenen ögeler listesine ekleyebilir, düzenleyebilir veya silebilir.

Event Blocklist: Bir etkinliğin örneğe eklenmesini engeller. Var olan bir "Event"i bloke etmek, "Event"in kaldırılmasına neden olmaz. Event hala düzenlenebilir durumda olacaktır.

Event bloke etme işlevselliği varsayılan olarak etkindir. Event bloke etme etkinleştirildiğinde, silinen eventler otomatik olarak "event Blocklist"ine eklenir. Event bloke etme işlevselliğini

etkinleştirme/devre dışı bırakma işlemi, MISP ayarlar görünümü kullanılarak yapılabilir.

Event Block Rules: "Event"lerin eklenmesini veya senkronize edilmesini engellemek için basit bir etiket filtresi eklenmesine olanak tanır.

Kullanım Senaryoları

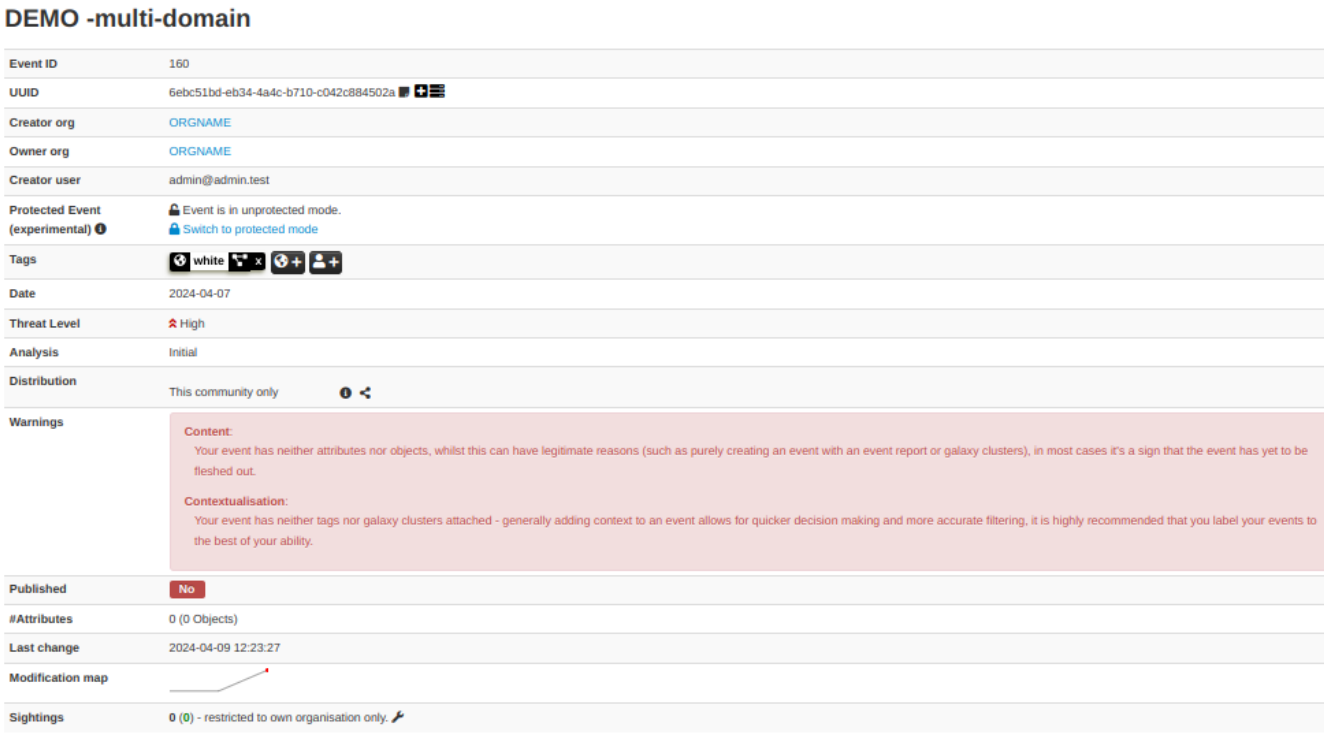
Best Practise

(TAG) Etiketleme:

- **"Event" düzeyinde etiketleme ve "Attribute" düzeyinde etiketleme:**

  Eventin tamamına etiket(TAG) eklenebilir. Daha ayrıntılı bir spesifikasyon için etiketler attribute düzeyinde de yerleştirilebilir. Kullanıcının her attribute hakkında daha ayrıntılı ve seçici bir görünüm sunmasına olanak tanır.

  Aşağıda verilen örnekte "Event" düzeyinde etiket ayarlanmıştır.



NOT: Hem "Event" hem de tüm "Attribute"lar için etiket eklemek yanlış bir uygulama olacaktır.

"Event" düzeyinde etiket örnekleri:

Traffic Light Protocol (TLP): İstihbarat paylaşımının nasıl gerçekleştirileceğini belirlemek için dört renkli basit bir şema kullanır. Bu şema, paylaşılan bilginin hassasiyetini ve kısıtlamalarını belirleyerek, doğru paylaşımın sağlanmasına yardımcı olur.

TLP'nin temel amacı, bilgiyi sınıflandırarak, hangi çevrelere hangi düzeyde paylaşılabileceğini belirlemektir. Bu, doğru kişilere doğru bilgiyi sağlamanın yanı sıra, gereksiz dağıtımı

önleyerek güvenlik risklerini azaltmaya da yardımcı olur.

Confidence: Paylaşılan verinin kalitesi ve güvenilirliği hakkında bir değerlendirme sunar. Verilerin kalitesi büyük farklılıklar gösterebilir ve paylaşım sırasında bu verilerin doğrulanıp doğrulanmadığı önemlidir.

Güven etiketi, verinin güvenilir bir tehdit göstergesi olduğuna veya en azından güvenilir bir gösterge olduğuna inanıldığını belirtir.

Permissible Actions Protocol (PAP): Veri sınıflandırması için daha gelişmiş bir yaklaşım sunar. Bu protokol, alınan verinin, bireysel bir şirket veya topluluk içindeki tehlikeleri aramak için nasıl kullanılabileceğini belirlemeye yöneliktir.

Bu etiketler, her bir etkinliğin hangi koşullarda ve nasıl paylaşılacağını belirlemek için kullanılır.

(DISTRIBUTION) Dağıtımı Ayarlama: Etiketleme gibi, miras alma özelliği de mümkün olduğunca kullanılmalıdır. Bu, özellikle paylaşım grupları (sharing groups) kullanılırken performans üzerindeki etkileri sınırlamak için önemlidir. Miras alma, bir olayın veya "Event"in "Attribute"lerini veya etiketlerini, üst düzeydeki bir kategoriden veya gruplardan otomatik olarak devralma yeteneğidir.

Sharing groups: MISP'deki paylaşım grupları, kullanıcıların kendi örneklerinden organizasyonların yanı sıra doğrudan veya dolaylı olarak bağlı örneklerden organizasyonları dahil etmelerine olanak tanıyan Eventler/Attributeler için yeniden kullanılabilir dağıtım listeleri oluşturmanın daha ayrıntılı bir yoludur.

Kullanıcı Soruları ve Cevapları

- Lider tehdit istihbaratı analisti olarak, BİT altyapılarına ve kuruluşlarına yönelik saldırıları önleyebilmek için tehditleri yakalamaya odaklanan bir ekibe liderlik etmek istiyorum.
  - Canlı Kontrol Panelini kullanarak ekiplerin gerçek zamanlı olarak neler yaptığını izleyin.
- Bir tehdit analisti olarak, kötü amaçlı yazılımlara nasıl karşı koyacağımı bilmek için kötü amaçlı yazılımları araştırmak, analiz etmek ve tersine mühendislik yapmak istiyorum.
  - **"Event"lere Dosya ve Kötü Amaçlı Yazılım Örnekleri Ekleyin ve İndirin:**
    - MISP panelinizden ilgili etkinliğe gidin.
    - Dosyalar sekmesine gidin ve istediğiniz kötü amaçlı yazılım örneklerini ekleyin.
    - Eğer mevcutsa, kötü amaçlı yazılım örneklerini indirin ve analiz için yerel araştırma ortamlarınıza aktarın.
  - **Kötü Amaçlı Yazılım Olaylarında Karma ve İlgili Bilgileri Arayın:**
    - MISP panelinizden arama aracını kullanarak kötü amaçlı yazılım olaylarındaki karmaları, IP'leri, etki alanlarını ve URL'leri arayın.
    - Bu aramaları gerçekleştirerek, belirli bir kötü amaçlı yazılımın veya tehdidin yaygınlığını ve etkisini değerlendirin.
  - **Kötü Amaçlı Yazılım Örnekleri Karma ve İlgili Bilgileri Ekleyin:**
    - Kötü amaçlı yazılım olaylarınıza kötü amaçlı yazılım örnekleri karmalarını ekleyin.
    - Bu karmaları ekleyerek, benzer kötü amaçlı yazılım örneklerinin izlenmesini ve analiz edilmesini sağlayın.
  - **Korelasyon Grafiği ve Genişletme Modülleri ile Gözlemlenebilirleri İnceliyin:**
    - MISP panelinizde korelasyon grafiklerini kullanarak, gözlemlenebilirler arasındaki ilişkileri analiz edin.
    - Genişletme modüllerini kullanarak, IoC'lerin doğruluğunu kontrol edin ve yanlış pozitifleri ele.
  - **MISP Dışındaki Veri Kaynaklarını Sorgulayarak Kötü Amaçlı Yazılım Olaylarını Zenginleştirin:**
    - MISP panelinizde bulunan modüller aracılığıyla, MISP dışındaki veri kaynaklarını sorgulayarak kötü amaçlı yazılım olaylarını zenginleştirin.
    - Bu sayede, kötü amaçlı yazılım olayları hakkında daha fazla detay ve context elde edin.
  - **Dinamik Kötü Amaçlı Yazılım Analizi Korelasyonları Gerçekleştirin:**
    - İlgili analiz araçlarına (örneğin, VirusTotal, VMRay) kötü amaçlı yazılım örneklerini göndererek, dinamik analiz sonuçlarını alın.

    - Bu sonuçları MISP panelinizdeki kötü amaçlı yazılım olaylarıyla ilişkilendirerek, daha kapsamlı bir tehdit analizi yapın.
- Lider tehdit istihbaratı analisti olarak, güvenlik duruşunu geliştirebilmek için tehdit verilerini, eyleme dönüştürülebilir tehdit istihbaratına dönüştürmek istiyorum.
    - Dış kaynaklardan veri alımı yapın
    - "Feed"leri ekleyin
    - "Event"leri ve "Attribute"leri etiketler, taksonomiler ve galaksiler kullanarak bağlamlandırın.
- Tehdit Analisti olarak, tehdit bilgilerini üçüncü taraflarla paylaşmak istiyorum, böylece ortak bir durum farkındalığı kazanabiliriz.
    - MISP örneğinde farklı dağıtım modellerini kurun
    - Olayları ve öznitelikleri örnekler arasında senkronize edin
    - Bir kuruluşun paylaşım politikasını karşılamak için filtreleme işlevlerini kullanın
    - Bilgileri, pentest bilgilerini, kötü amaçlı yazılım örneklerini, zafiyetleri içeride ve dışarıda paylaşın
- Tehdit Analisti olarak, tehditleri izlemek ve canlı verilere erişmek istiyorum, böylece ciddi bir hasara neden olmadan tehditleri yönetebilirim.
    - Göstergelerin listelerini içe aktarın ve IoC'lerin "Feed"lerde mevcut olup olmadığını kontrol edin.
    - Widget'ları kullanarak istatistikleri ve gözlemleri izleyin
    - Canlı verileri ve istatistikleri MISP Dashboard aracılığıyla bir veya daha fazla MISP örneğinden gösterin
- Tehdit Analisti olarak, çeşitli kaynaklardan gelen göstergeleri toplamak ve karşılaştırmak istiyorum, böylece çeşitli tehditler arasındaki bağlantıları kurabilirim.
    - Topluluklara katılın ve "Feed"lere abone olun
    - "Event"leri ekleyin ve belirli "Feed"lere "Event"ler atayın
    - MISP'in otomatik korelasyon motorunu kullanarak göstergeleri karşılaştırın
    - MISP'te mevcut olan "Feed"leri analiz edin
    - Korelasyon grafiğini kullanarak "Event"leri ve "Attribute"leri bağlayın
    - Modülleri kullanarak "Attribute"ler üzerinde daha fazla bilgi edinin
    - Galaksileri kullanarak "Event"leri kötü amaçlı yazılımlar, tehdit aktörleri vb. ile ilişkilendirin (örneğin ATT&CK)
- Tehdit Analisti olarak, yeni tehditleri araştırırken sorgular yapabilmek için tehdit verilerinin yapılandırılmış bir veritabanına sahip olmak istiyorum.
    - Bilgileri STIX formatında yapılandırılmış bir formatta depolayın
    - Serbest metin içe aktarma aracını kullanarak yapılandırılmamış raporları içe aktarın
    - MISP'i güvenlik ve sahtekarlık tehdit istihbaratı için merkezi bir merkez olarak kullanın. OSINT ve ticari beslemelerden göstergeleri bir araya getirerek tehdit istihbaratını merkezileştirin
    - "False-Positive"leri ve kopyaları kaldırın
    - Gözlemler tarafından puanlanan göstergeleri değerlendirin
    - Üçüncü taraflardan tehdit istihbaratı veya "Feed"lerini içe aktarın. "Feed"leri oluşturmak için veri deposunun filtrelenmiş alt kümelerini oluşturun
    - Değerlendirme için doğrudan "Feed"leme verilerini önizleyin ve karşılaştırın
- Tehdit Analisti olarak, ham tehdit verilerini zenginleştirerek ve bağlamsallaştırarak harekete geçirilebilir istihbarat üretebilmek istiyorum.
    - Taksonomileri kullanarak saldırgan TTP'lerini anlayın

    - Galaksileri ve taksonomileri kullanarak riskleri ve olayları kategorize edin
    - Etiket koleksiyonlarını kullanarak bilgileri hızlı bir şekilde sınıflandırın
    - Gözlem kaynakları hakkında bilgilerle gözlemleri bağlamsallaştırın
    - IDS'lerin dışa aktarımını etiketlerle zenginleştirin
    - Gözlemleri gözlemleme bilgilerini kullanarak bozulma ve göstergeleri puanlayın
    - MISP'in daha zengin veri yapısı kullanarak karmaşık senaryoları tanımlayın ve görselleştirin
    - MISP nesneleri (object) kullanarak "Attribute"lerin gelişmiş kombinasyonlarını sağlayın
- Tehdit Analisti olarak, tehditleri araştırarak bilgisayar sistemlerini saldırılardan korumak istiyorum.
    - MISP topluluklarından ilgili verileri bulun. Birden çok kaynaktan gelen yeni MISP olaylarını ve uyarıları önizleyin, örneğin e-posta raporları, CTI sağlayıcıları ve SIEM'ler
    - Belirli bir IOC içeren olaylar için bir MISP örneğine sorgu yapın. Diğer MISP olayları, öznitelikler, nesneler, etiketler ve galaksilere göz atın
    - "Event"ler oluşturun, IoC'ler ekleyin ve etiketler kullanarak bağlamsallaştırın
    - Bir olayı bileşenlerine, nesnelerine, etiketlerine, galaksilere ve/veya ilgili "Event"lere dönüştürün
    - Galaksiler ve ilgili "Event"ler aracılığıyla daha fazla ayrıntıya göz atın
    - Kullanılan Cytomic Orion API gibi araçlardan belirli MISP göstergelerinin gözlemlendiğini kontrol etmek için sorgular yapın ve ardından bunları MISP olaylarına eklemek için görme ayrıntılarını içe aktarın
    - Kullanıcılar, betikler ve IDS'ler tarafından toplanan Gözlemlerden tehditleri önceliklendirin.
    - Kullanıcılar, betikler ve IDS'ler tarafından bildirilen Gözlemler kullanılarak göstergeleri bozulma/sona erme durumlarına göre sona erdirin