

Giriş

MISP'e giriş, proje hakkında, proje gereksinimlerini ve hızlı başlangıç adımlarını içeren bir bölümdür. Bu bölüm, kullanıcıların MISP platformu hakkında temel bilgiler edinmesini sağlar.

- [Proje Hakkında](#)
 - [Tarihçesi](#)
 - [MISP Nedir?](#)
- [Gereksinimler](#)
 - [MISP Gereksinimleri](#)
- [Hızlı Başlangıç](#)
 - [Oturum Açma](#)
 - [Event](#)
 - [Tag ve Taglist](#)
 - [Free-Text Import Aracı](#)
 - [Feed](#)

Proje Hakkında

Tarihçesi

Christophe Vandeplas Tehdit Göstergeleri (IOCs), e-posta veya pdf belgeleri ile paylaşıyor ve otomatik makineler tarafından ayrıştırılamıyor olmasından fazlasıyla rahatsız olmuştur. Bu nedenle Haziran 2011 civarında, CakePHP ile denemeler yapmaya başladı ve fikrinin bir kanıtını ortaya koymuştur. Bu projeye CyDefSIG: Siber Savunma İmzaları adını verdi.

Temmuz 2011'in ortalarında, kişisel projesini Belçika Savunmasındaki iş yerinde sunmuştur ve geri bildirim oldukça olumlu olmuştur. Belçika Savunmasının CyDefSIG'i resmi olarak kullanmaya başlamasıyla birlikte 2011'in ortalarından itibaren CyDefSIG'e erişim verilmiştir. Bu noktada, Christophe, evde çalışmaya devam ederken iş saatlerinde CyDefSIG'e biraz zaman ayırmasına izin verilmiştir.

Bir noktada NATO bu projeden haberdar olmuştur. Ocak 2012'de projeyi daha detaylı olarak tanıtmak için ilk sunum yapılmıştır. NATO, pazarda sunulan diğer ürünlere göre CyDefSIG'in açıklığını bir avantaj olarak görmüştür. Böylece Andrzej Dereszowski, NATO tarafından ilk kısmi zamanlı geliştirici olmuştur.

Birkaç ay sonra NATO, kodu iyileştirmek ve daha fazla özellik eklemek için tam zamanlı bir geliştiriciyi işe almıştır. Geliştirme süreci o tarihten itibaren başlamıştır. Birçok kişisel projede olduğu gibi lisans henüz açıkça yazılmamıştı, proje kamuoyuna Affero GPL lisansı altında yayınlanacağına karar verilmiştir. Bu kaynak kod mümkün olan en çok insanla paylaşmak ve herhangi bir zarardan korumak içindi.

Ocak 2013'te Andras Iklody, MISP'in başlıca tam zamanlı geliştiricisi olmuştu. Günümüzde, Andras Iklody MISP projesinin baş geliştiricisi ve CIRCL'de çalışıyor.

MISP projesi genişledikçe, artık sadece kötü amaçlı yazılım göstergelerini değil, aynı zamanda sahtekarlık veya güvenlik açığı bilgilerini de kapsıyor. Adı artık MISP Threat Sharing olarak değişti. MISP şimdi bir topluluk projesi, bir grup gönüllü tarafından yönetilmektedir.

MISP Nedir?

MISP, hedeflenen saldırılara, tehdit istihbaratına, mali dolandırıcılık bilgilerine ve güvenlik açığı bilgilerine ilişkin Tehdit Göstergelerini (IOC'ler) paylaşmak, depolamak ve ilişkilendirmek için bir tehdit istihbarat platformudur. Bu platform, sadece siber güvenlik göstergelerini ve kötü amaçlı yazılım analizini depolamak ve paylaşmakla kalmaz, aynı zamanda saldırıları, sahtekarlıkları veya tehditleri tespit etmek ve önlemek için IOC'leri ve bilgileri kullanır.

MISP, organizasyonların karşılaştığı tehditler ve güvenlik açıkları hakkında bir bilgi deposu olarak hizmet eder. Bilgi tutarlı bir yapıya kavuşturulduğunda, aranabilir hale gelir ve güvenlik analistlerinin bilgileri farklı zamanlarda ilişkilendirmesi daha kolay olur. Otomatik olarak benzer bilgileri ilişkilendirir ve bilgileri tutarlı bir formatta depolayarak, kuruluşlar arasında bilgi paylaşımını kolaylaştırır.

Ayrıca, MISP iş ortaklarından, analistlerden, araçlardan ve yayınlardan bilgi toplayan bir araçtır. Bu araç, verileri ilişkilendirir, zenginleştirir ve ekiplerin, toplulukların işbirliği yapmasını sağlar. Bu şekilde, otomatik koruyucu araçları ve analiz araçlarını besleyerek etkili bir şekilde tehditleri tespit etmeye ve önlemeye yardımcı olur.

Gereksinimler

MISP Gereksinimleri

MISP kullanım senaryosunu belirlerken, ilk adım kullanım amacını belirlemektir. Kullanıcı sayısı, alınan veri miktarı, kullanılan veri noktaları, olay sayısı, ilişkilendirme sayısı ve API kullanımı gibi faktörlerin hepsi göz önünde bulundurulmalıdır.

Donanım gereksinimleri oldukça düşüktür; genellikle 2+ çekirdekli ve 8-16 GB belleğe sahip bir web sunucusu yeterlidir, ancak daha fazlası her zaman tercih edilir. Gereksinimler veri kümesi ve kullanıcı sayısına bağlıdır.

Gereksinimleri Etkileyebilecek Bazı Önemli Hususlar:

- Verilerin yüksek oranda ilişkilendirilmesi, bellek ve hesaplama yoğunluğunu artırabilir. Bu durumda, ilişkilendirme oranını düşürmek veya bellek ve CPU kapasitesini artırmak düşünülebilir.
- Örnek sayısı ve ek dosyalar, doğrudan disk kullanımını etkiler.
- Eş zamanlı kullanıcı sayıları, bellek ve CPU kullanımını etkiler.
- Uzak *feedlerin* ve sunucuların önbelleğe alınması, sistemin bellek gereksinimlerini artırır.
- Günlük faaliyetlerin miktarı, veritabanı ve yerel günlük dosyalarının disk gereksinimlerini artırabilir.

Operasyonel Sunucular İçin Örnek Gereksinimler:

- Küçük paylaşım merkezleri ve uç nokta MISP'leri için 16 GB bellek ve 2 vCPU yaygındır.
- Büyük paylaşım toplulukları için 128 GB bellek ve 32 fiziksel CPU çekirdeği önerilir.
- COVID misp topluluğu, 4 vCPU ve 8GB bellek ile binlerce kullanıcıya hizmet verir.
- Eğitim örnekleri, sadece 2GB bellek ve tek bir vCPU üzerinde çalışır (ancak bunun eğitimler / deneyler dışında kullanılması önerilmez).

Veri tabanı:

- MISP'in ana veritabanı MariaDB'ye dayanır.
- Düşük gecikme süresi için SSD kullanılması önerilir.
- Kullanılan depolama türü, gecikmeyi ve kullanılan disk alanını etkileyebilir.

Feed Önbelleği:

- Feedlerden gelen öğeleri önbelleğe almak için RAM kullanılır ve öğeler önbelleğe alınır.
- Varsayılan olarak kullanılabilir feedler etkinleştirilmiş ise, tüm feedlerin 1.2GB'a kadar bellek kullanabileceği unutulmamalıdır.

Hızlı Başlangıç

Oturum Açma

MISP varsayılan kimlik bilgileri:

Username:	admin@admin[.]test
Password:	admin

olarak belirlenmiştir.

Kurulum aşamasında `.env` dosyası içinde yapılan konfigürasyonlar sırasında `username` ve `password` alanlarına yazacağınız bilgiler geçerli olacaktır. Boş bırakıldığı takdirde varsayılan `username` ve `password` kullanılır.

```
# Email/username for user #1, defaults to MISP's default (admin@admin.test)
ADMIN_EMAIL=
# name of org #1, default to MISP's default (ORGNAME)
ADMIN_ORG=
# defaults to an automatically generated one
ADMIN_KEY=
# defaults to MISP's default (admin)
ADMIN_PASSWORD=
# defaults to 'passphrase'
GPG_PASSPHRASE=
# defaults to 1 (the admin user)
CRON_USER_ID=
# defaults to 'https://localhost'
BASE_URL=
```

Parola Güncelleme

Komut satırı aracılığıyla parola güncelleme yapılabilir.

```
sudo -u www-data /var/www/MISP/app/Console/cake Password admin@admin.test Password1234
```

NOT: Verilen komut docker konteyner içinde çalıştırılmalıdır. Docker konteynerine geçmek için aşağıdaki adımlar uygulanır;

```
cd /opt/misp-docker
```

- Çalışan docker konteynerlerine erişelim.


```
docker ps
```

- misp-core docker konteynerinin id değeri kopyalanır. Ve aşağıda verilen komut ile docker konteynerine giriş yapılır.

```
docker exec -it [konteyner_id] bash
```

- Konteyner id değeri bilinmiyorsa aşağıdaki komut kullanılabilir.

```
docker compose exec -it misp-core bash
```

Ayrıca MISP arayüzü aracılığıyla da parola güncellemesi yapılabilir.

- Administration -> List users sayfası içinde bulunan *Actions* menüsünde aşağıda gösterilen buton kullanılır.



- Manuel olarak aşağıda gösterildiği şekilde parola değişikliği yapılabilir.

Change Password

New password ⓘ

Confirm new password

Confirm with your current password

Submit

Parola Politikası

[12]: Parola en az 12 karakter uzunluğunda olmalı.

[A-Z]: En az bir büyük harf içermeli.

[0-9]: Bir rakam veya özel bir karakter içermeli.

[a-z]: En az bir küçük harf karakteri içermeli.

Event

MISP'e *Event* eklemek, güvenlik profesyonellerinin tehditleri daha iyi anlamalarını, savunma stratejilerini geliştirmelerini ve genel olarak siber güvenliği artırmalarını sağlar.

- "Event Actions" menüsü içinde "Add Event" butonu kullanılarak yeni bir Event oluşturulabilir.

[Home](#) [Event Actions](#) [Dashboard](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#)

The event created will be visible to the organisations having an account on this platform, but not synchronised to other

[List Events](#)
[Add Event](#)
[Import from...](#)
[REST client](#)
[List Attributes](#)
[Search Attributes](#)
[View Proposals](#)
[Events with proposals](#)
[View delegation requests](#)
[View periodic summary](#)
[Export](#)
[Automation](#)

Add Event

Date

2024-04-07

Distribution *i*

This community only

Threat Level *i*

High

Analysis *i*

Initial

Event Info

Quick Event Description or Tracking Info

Extends Event

Event UUID or ID. Leave blank if not applicable.

Submit

- Distribution (Dağıtım):** Oluşturulan bilgilerin kısıtlı bir grupta ya da herkese açık dağıtılabileceği seçeneklerini belirler.
- Threat Level (Tehdit Seviyesi):** Oluşturulan *Event*'in düşük, orta ve yüksek olmak üzere 3 ayrı önem derecesini belirtir.
- Event Info (Olay Bilgisi):** Oluşturulan *Event* hakkında genel bilgileri içerir. Bu, olayın adı, tanımı, zaman damgası, kaynakları vb. içerebilir.
- GFI Sandbox(opsiyonel):** MISP *Event*'i, kötü amaçlı yazılım analizi için GFI Sandbox gibi bir çözümle ilişkilendirilebilir. Bu, tehditlerin analiz edilmesine ve kötü amaçlı faaliyetlerin tespit edilmesine yardımcı olabilir.

5. **Does it extend (Uzatma var mı)(opsiyonel):** Bu, MISP *Event'inin* genişletilip genişletilmediğini belirtir. Yani, *Event'e* daha fazla ayrıntı veya bağlantılar eklenip eklenmediğini ifade eder.
- "Submit" butonu ilgili alanları doldurduktan sonra bir sonraki aşamaya geçmek için kullanılır.
 - *Event* oluşturulduktan sonra, "View Event" içinde *Event'e* ait özellikler belirlenebilir.

The event has been saved

View Event

View Correlation Graph

View Event History

Edit Event

Delete Event

Add Attribute

Add Object

Add Attachment

Add Event Report

Populate from...

Enrich Event

Merge attributes from...

Publish Event

Publish (no email)

Contact Reporter

Download as...

Add Event to Collection

List Events

Add Event

DEMO -multi-domain

Event ID160

UUID6ebc51bd-eb34-4a4c-b710-c042c884502a

Creator orgORGNAME

Owner orgORGNAME

Creator useradmin@admin.test

Protected Event (experimental)Event is in unprotected mode. Switch to protected mode

Tags

Date2024-04-07

Threat LevelHigh

AnalysisInitial

DistributionThis community only

Warnings

Content: Your event has neither attributes nor objects, whilst this can have legitimate reasons (such as purely creating an event with an event report or galaxy clusters), in most cases it's a sign that the event has yet to be fleshed out.

Contextualisation: Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.

PublishedNo

#Attributes0 (0 Objects)

Last change2024-04-07 19:13:24

Modification map

Sightings0 (0) - restricted to own organisation only

PivotsGalaxyEvent graphEvent timelineCorrelation graphATT&CK matrixEvent reportsAttributesDiscussion

X 160: DEMO -multi-d...

Galaxies

< previousnext >view all

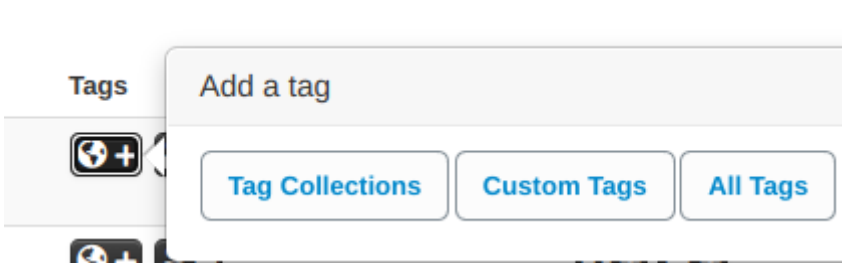
+Scope toggleDeletedDecay scoreContextRelated TagsFiltering tool

Date ↑ContextPatternTimeValueTimeGalaxiesCommentCorrelateRelated EventsEvent hits

Tag ve Taglist

"Event Actions" sekmesi içinde "List Attributes" klasöründe eklenilen eventlere ait özellikler bulunur.

Tag eklemek için 3 seçenek bulunmaktadır. Bunlar;



Tag Collections (Etiket Koleksiyonları):

- Etiket koleksiyonları, belirli bir konsepti veya kategoriyi temsil eden bir grup etiketten oluşur.

Custom Tags (Özel Etiketler):

- Özel etiketler, kullanıcıların kendi ihtiyaçlarına göre tanımladığı ve oluşturduğu etiketlerdir.

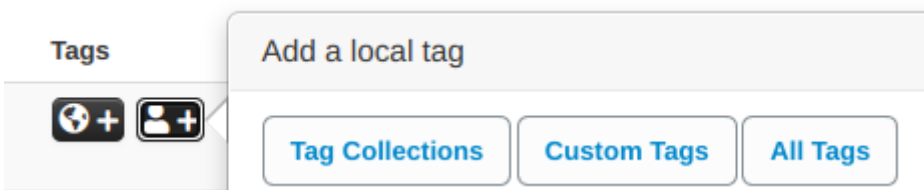
All Tags (Tüm Etiketler):

- Tüm etiketler, platformda kullanılabilir olan tüm etiketlerin bir listesini temsil eder.

LOCAL TAGS:

MISP'te "Local Tags" veya "Yerel Etiketler", kullanıcılar tarafından oluşturulan ve yalnızca belirli bir MISP örneği içinde geçerli olan etiketlerdir. Bunlar genellikle özel bir organizasyonun ihtiyaçlarına veya spesifik analiz gereksinimlerine uygun olarak tanımlanır ve kullanılır.

Local tag eklemek için 3 seçenek bulunmaktadır. Bunlar;

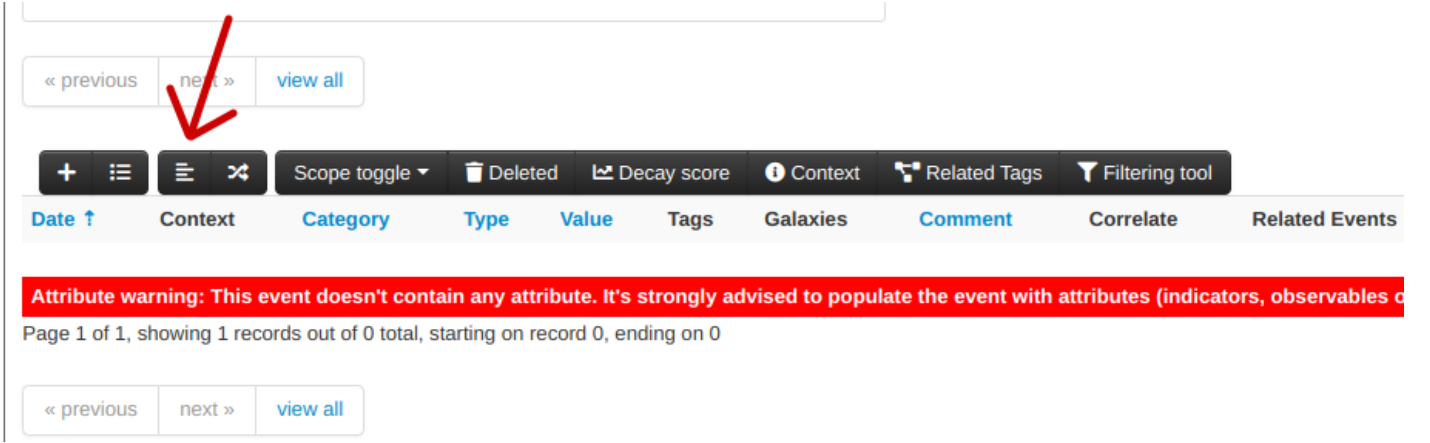


Local tag ekleme özellikler ile tag ekleme özellikleri aynı işlevi görmektedir. Fakat local tag yalnızca bir organizasyona özeldir.

Free-Text Import Aracı

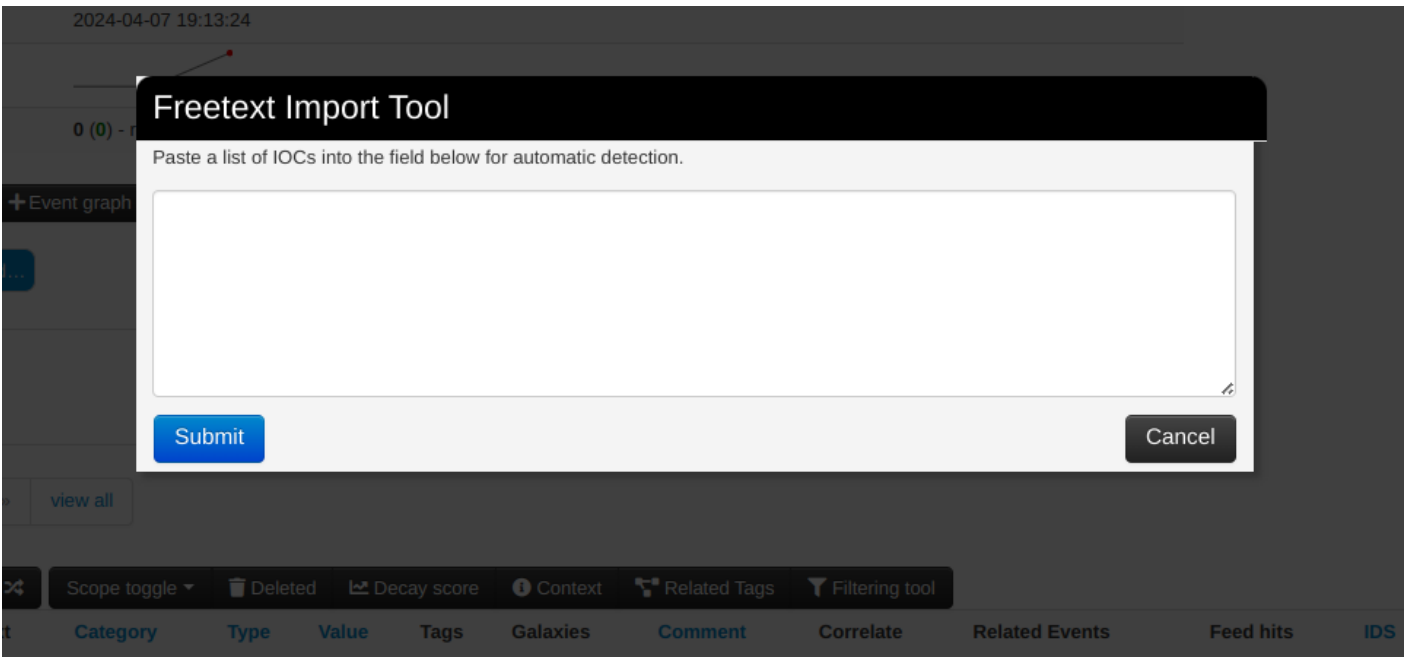
Free-Text Import aracı, metin tabanlı verileri hızlı ve etkili bir şekilde MISP'e aktarmak için kullanılan bir araçtır. Bu araç, metin belgelerinde veya başka bir metin formatında bulunan tehdit bilgilerini MISP formatına dönüştürerek, tehdit istihbaratı paylaşımını ve analizini kolaylaştırır. Bu sayede kullanıcılar, tehdit verilerini elle girme gibi zaman alıcı işlemlerle uğraşmak zorunda kalmadan, hızlıca MISP platformuna aktarabilirler.

- Aşağıda gösterildiği gibi, oluşturulan Event içinde metin tabanlı verilerin MISP'e aktarılması sağlanır.



The screenshot shows the MISP interface with the Free-Text Import tool. A red arrow points to the 'next' button in the navigation bar. The interface includes a search bar, navigation buttons ('previous', 'next', 'view all'), a toolbar with icons for adding, deleting, and filtering, and a table with columns for Date, Context, Category, Type, Value, Tags, Galaxies, Comment, Correlate, and Related Events. A red warning banner at the bottom states: 'Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables)'. Below the banner, it says 'Page 1 of 1, showing 1 records out of 0 total, starting on record 0, ending on 0'.

- Pop-up içerisinde,IOC'lerin (Indicators of Compromise) yapıştırılması istenmektedir. Bu, kullanıcının metin tabanlı tehdit bilgilerini veya IOC'leri belirli bir formatta girerek MISP'e aktarmasını sağlar.



The screenshot shows the Free-Text Import Tool pop-up window. The window has a title bar 'Freetext Import Tool' and a subtitle 'Paste a list of IOCs into the field below for automatic detection.' Below the subtitle is a large text input field. At the bottom of the window are two buttons: 'Submit' and 'Cancel'. The background shows the MISP interface with the same navigation bar and table as the previous screenshot.

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 aktarılabılır.

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

[List Feeds](#)[Search Feed Caches](#)[Add Feed](#)[Import Feeds from JSON](#)[Feed overlap analysis matrix](#)[Export Feed settings](#)

Add MISP Feed

Add a new MISP feed source.

☐ Enabled

☐ Caching enabled

☐ Lookup visible

☐ Disable correlation

Name

Provider

Input Source

Network

URL

Source Format

MISP Feed

Any headers to be passed with requests (for example: Authorization)

Line break separated list of headers in the "headername: value" format

Add Basic Auth

Distribution

All communities

Default Tag

None

Filter rules:

Modify

Submit

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.