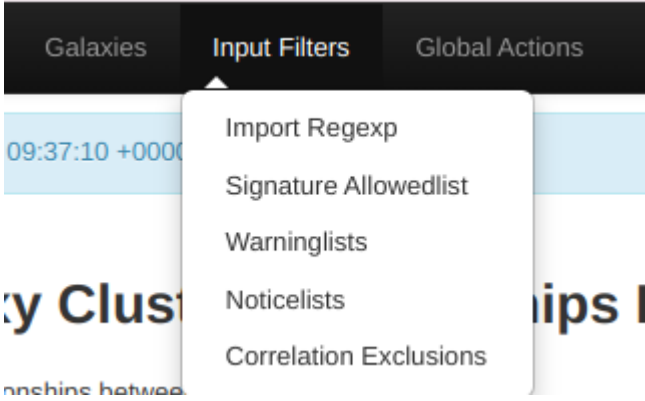


# INPUT FILTERS

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.

| Home              | Event Actions                          | Dashboard                  | Galaxies      | Input Filters   | Global Actions | Sync Actions | Administration | Logs | API | ★ | MISP | Admin | ✉ | Log out |
|-------------------|--|----------------------------|---------------|---|----------------|--------------|----------------|------|-----|---|------|-------|---|---------|
| List Regexp       | New Regexp                             | Perform on existing        | Import Regexp |   |                |              |                |      |     |   |      |       |   |         |
| « previous next » |  |                            |               |   |                |              |                |      |     |   |      |       |   |         |
| ID ↓              | Regexp                                 | Replacement                | Type          | Actions   |                |              |                |      |     |   |      |       |   |         |
| 1                 | /::ProgramData./i                      | %ALLUSERSPROFILE%\         | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 2                 | /::Documents and Settings.All Users./i | %ALLUSERSPROFILE%\         | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 3                 | /::Program Files.Common Files./i       | %COMMONPROGRAMFILES%\      | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 4                 | /::Program Files (x86).Common Files./i | %COMMONPROGRAMFILES(x86)%\ | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 5                 | /::Users\(*.*)\AppData.Local.Temp./i   | %TEMP%\                    | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 6                 | /::ProgramData./i                      | %PROGRAMDATA%\             | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 7                 | /::Program Files./i                    | %PROGRAMFILES%\            | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 8                 | /::Program Files (x86)./i              | %PROGRAMFILES(x86)%\       | ALL           |   |                |              |                |      |     |   |      |       |   |         |
| 9                 | /::Users.Public./i                     | %PUBLIC%\                  | ALL           |   |                |              |                |      |     |   |      |       |   |         |

- **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.

Home

Event Actions

Dashboard

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Logs

API

List Allowedlist

New Allowedlist

Signature Allowedlist

Regex entries (in the standard php regex `/({regex})/({modifier})` format) entered below will restrict matching attributes from being included in the IDS flag sensitive exports (such as NIDS exports).

« previous

next »

| ID   | Name ↓ | Actions |
|--|--------|---------|
| Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0 |        |         |
| <div><div>« previous</div><div>next »</div></div>                                |        |         |

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

Home

Event Actions

Dashboard

Galaxies

Input Filters

Global Actions

Sync Actions

Administration

Logs

API

★

MISP

Admin

📧

Log out

Add Warninglist

List Warninglists

Update Warninglists

Search in Warninglists

# Warninglists

« previous

1

2

next »

last »

AllEnabledDisabled

Enter value to search

Filter

| ID ↑ | Name   | Version  | Description  | Category       | Type     | Entries | Default | Enabled | Actions |
|------|--|----------|--|----------------|----------|---------|---------|---------|---------|
| 87   | List of known Zscaler IP address ranges  | 20230810 | Zscaler IP address ranges<br>(https://config.zscaler.com/api/zscaler.net/hubs/cidr/json/required)  | False positive | cidr     | 66      | ✓       | ✗       | 🔍🗑️🔗    |
| 86   | List of known Wikimedia address ranges   | 20240227 | Wikimedia address ranges (http://noc.wikimedia.org/conf/reverse-proxy.php.txt)   | False positive | cidr     | 62      | ✓       | ✗       | 🔍🗑️🔗    |
| 85   | List of known domains to know external IP  | 8        | Event contains one or more entries of known 'what's my ip' domains   | False positive | hostname | 232     | ✓       | ✗       | 🔍🗑️🔗    |
| 84   | Specialized list of IPv6 addresses belonging to common VPN providers and datacenters     | 20220324 | Specialized list of IPv6 addresses belonging to common VPN providers and datacenters   | False positive | cidr     | 1250    | ✓       | ✗       | 🔍🗑️🔗    |
| 83   | Specialized list of vpn-ipv4 addresses belonging to common VPN providers and datacenters | 20240227 | Specialized list of vpn-ipv4 addresses belonging to common VPN providers and datacenters   | False positive | cidr     | 24049   | ✓       | ✗       | 🔍🗑️🔗    |
| 82   | List of known URL Shorteners domains   | 10       | Event contains one or more entries of known Shorteners domains   | False positive | hostname | 101     | ✓       | ✗       | 🔍🗑️🔗    |
| 81   | University domains   | 20240227 | List of University domains from<br>https://raw.githubusercontent.com/Hipo/university-domains-list/master/world_universities_and_domains.json | False positive | string   | 10265   | ✓       | ✗       | 🔍🗑️🔗    |

### ◦ 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.

[Home](#) [Event Actions](#) [Dashboard](#) [Galaxies](#) [Input Filters](#) [Global Actions](#) [Sync Actions](#) [Administration](#) [Logs](#) [API](#) [★](#) [MISP](#) [Admin](#) [✉](#) [Log out](#)

List Noticelist  
Update Noticelists

## Noticelists

« previous next »

Enter value to search

Filter

| ID | Name | Expanded Name                      | Ref   | Geographical area | Version | Enabled                  | Actions |
|----|------|------------------------------------|---|-------------------|---------|--------------------------|---------|
| 1  | gdpr | General Data Protection Regulation | <a href="http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679">http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679</a> | EU                | 1       | <input type="checkbox"/> |         |

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

« previous next »

- **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.

Revision #5

Created 8 April 2024 18:40:13 by İlayda Durlanık

Updated 8 April 2024 20:42:43 by İlayda Durlanık