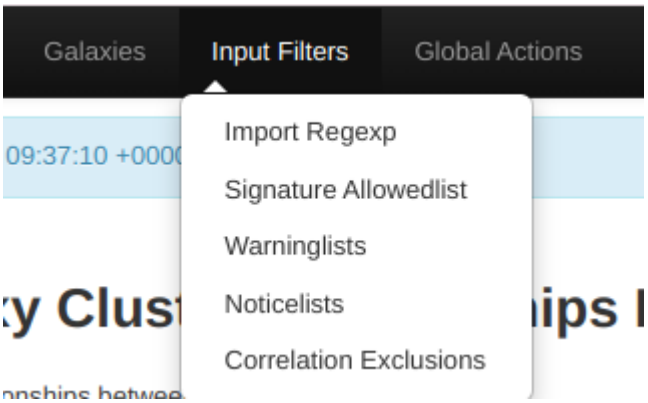
INPUT FILTERS

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

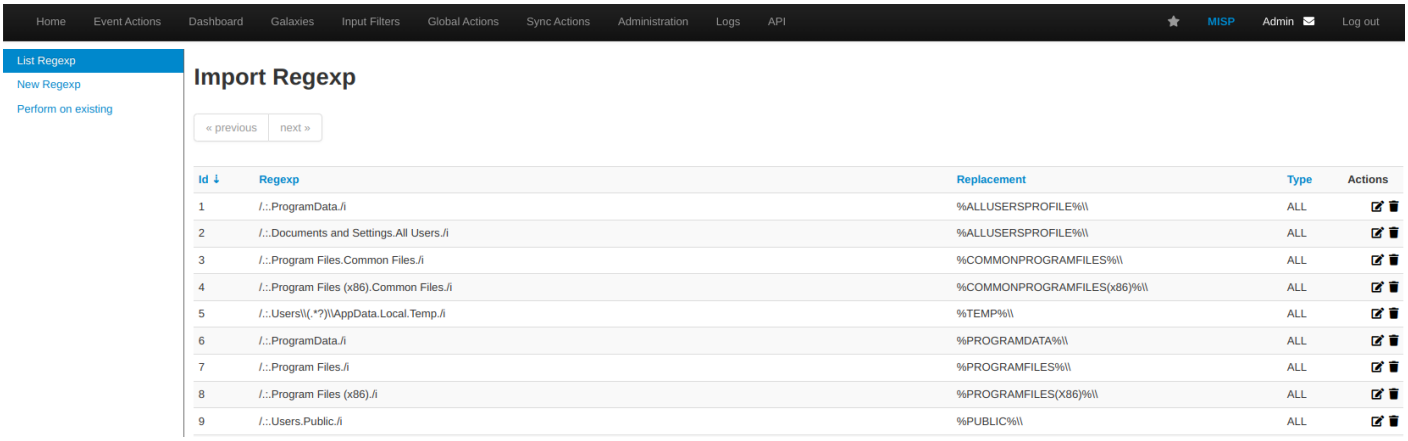
Bu filtreler, kullanıcıların veri girişini doğrulamak, belirli veri türlerini kabul etmek veya reddetmek, düzenli ifadeleri kullanarak veri biçimlerini kontrol etmek ve kötü amaçlı veya istenmeyen verileri engellemek gibi işlevlere sahiptir. Kullanıcılar, MISP giriş filtreleri aracılığıyla veri kalitesini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

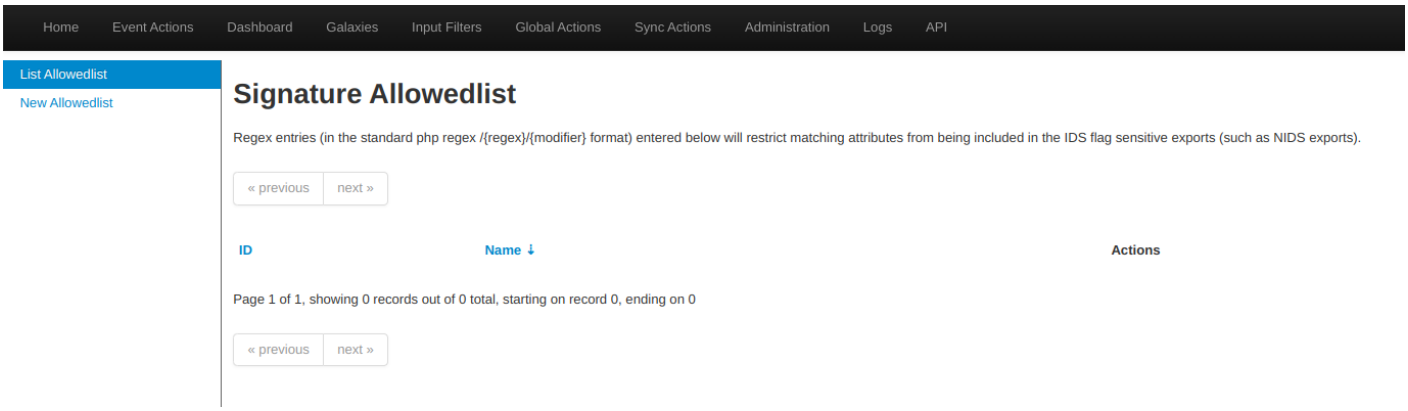
Bu alanda belirtilen düzenli ifadeler, içeri aktarılan verilerin belirli bir formata veya desene uyması gerektiğini belirtir. Örneğin, e-mail adresleri, URL'ler veya dosya adları gibi belirli veri türlerinin doğruluğunu kontrol etmek için kullanılabilirler. Bu şekilde, yanlış veya zararlı verilerin sisteme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



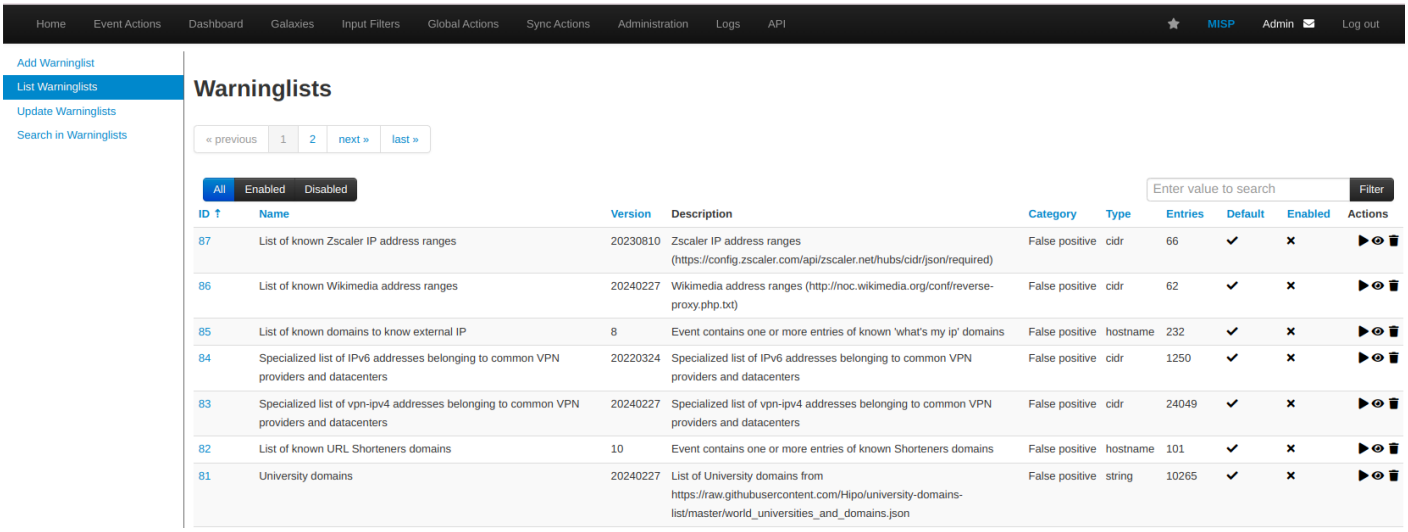
- **Signature Allowedlist:** İçeri aktarılan verilerin belirli imzaları veya desenleri içermesine izin verilen bir izin listesini tanımlar.

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:**

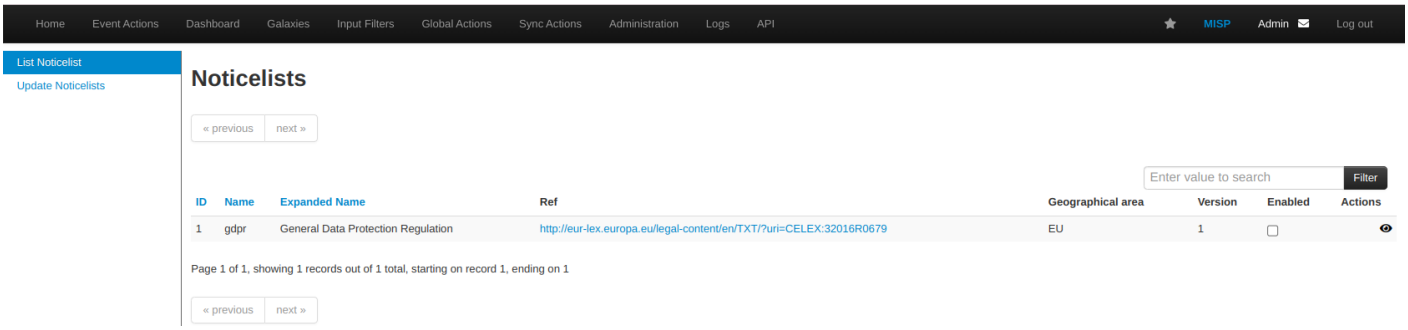
Varsayılan olarak, MISP, warninglist olarak adlandırılan belirli veri listelerindeki özelliklerin (attribute) sadece bir tür bayrağı belirli olduğunda eşleşmeleri tetikler. Ancak bu davranış, MISP'in yapılandırma ayarlarından biri olan "MISP.warning_for_all" parametresi "true" olarak ayarlandığında değiştirilebilir.

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.

Revision #5
Created 8 April 2024 18:40:13 by İlayda Durlanık
Updated 8 April 2024 20:42:43 by İlayda Durlanık