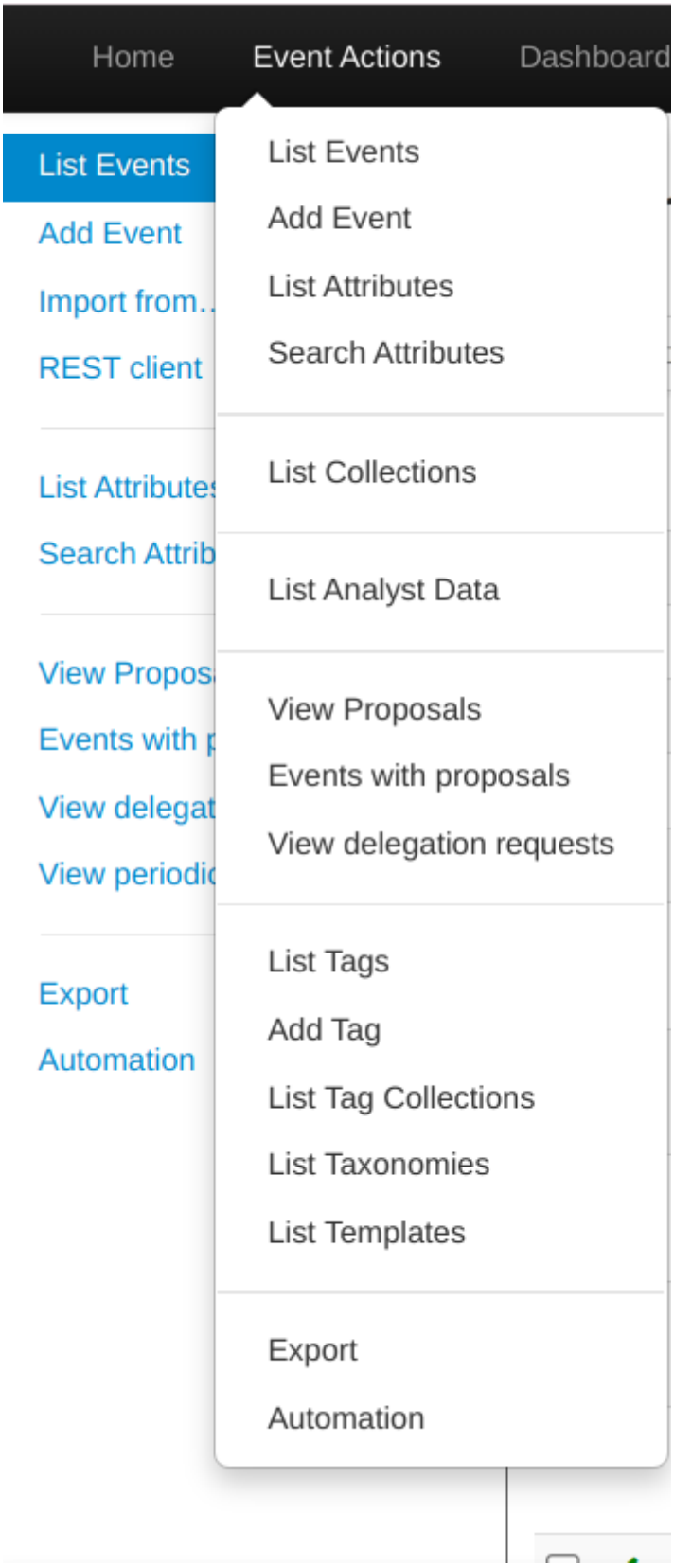
EVENT ACTIONS

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.

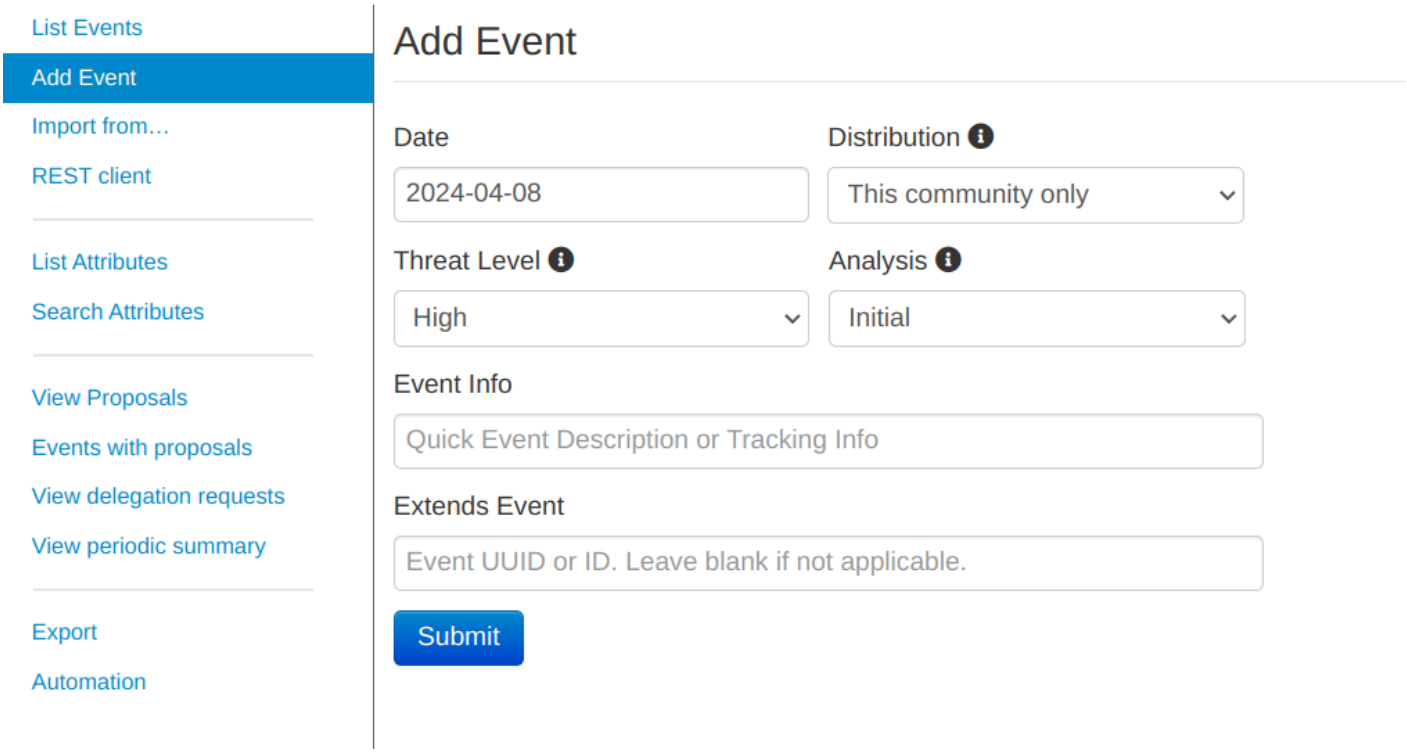
Event Action menüsü farklı kategoriler içerir ve her biri farklı işlevleri temsil eder:



- **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.

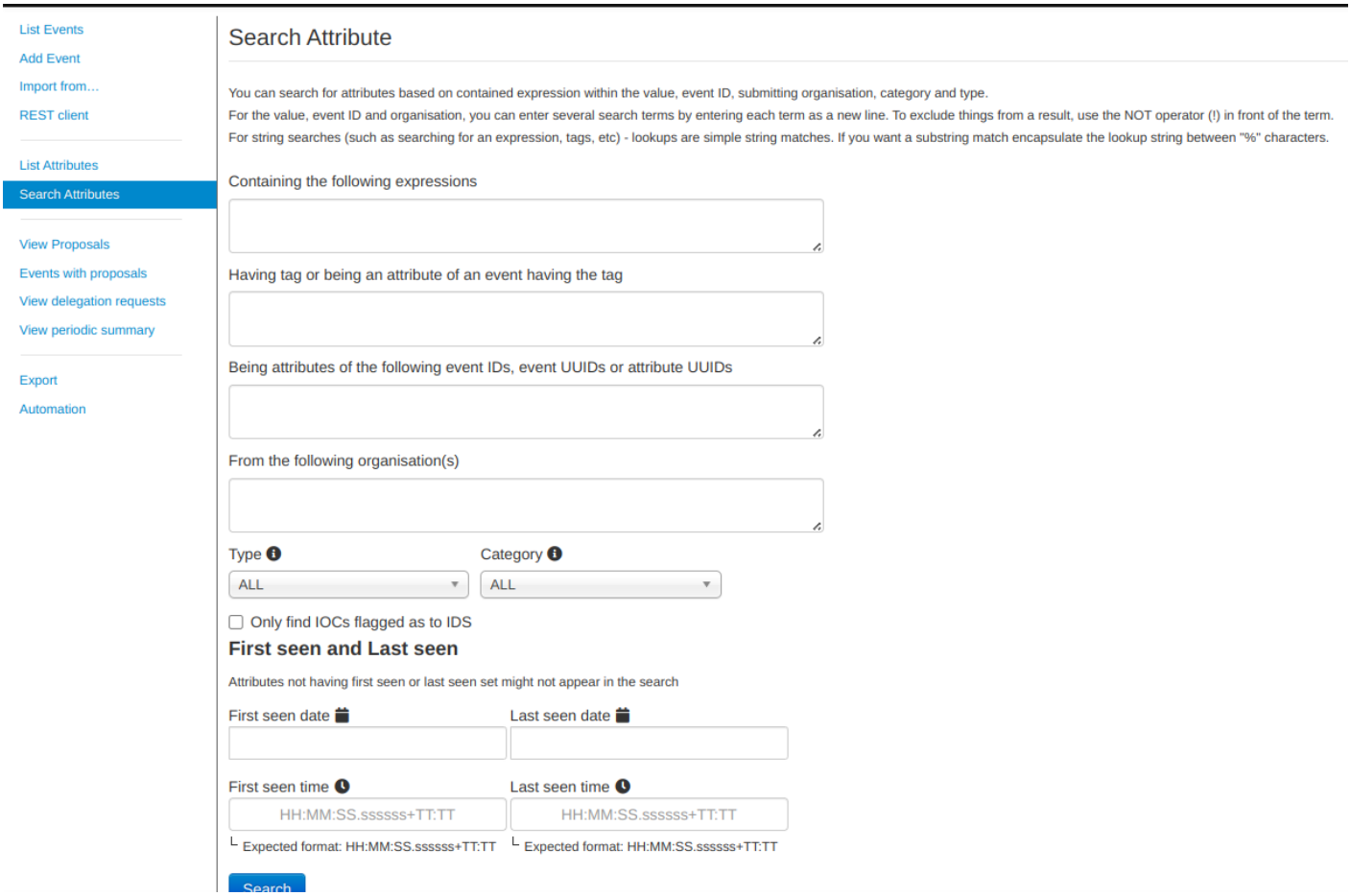
Devam eden: Analiz devam ediyor.

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.

Revision #5
Created 8 April 2024 12:32:11 by İlayda Durlanık
Updated 9 April 2024 19:00:26 by İlayda Durlanık