Varlık Yönetimi

Bu bölümde profiller, özel alanlar, gözlemlenebilir tipler, vaka durumu, uyarı durumu, analiz şablonları, sınıflandırmalar, att&ck modellerinin nasıl oluşturduğu anlatılacaktır.

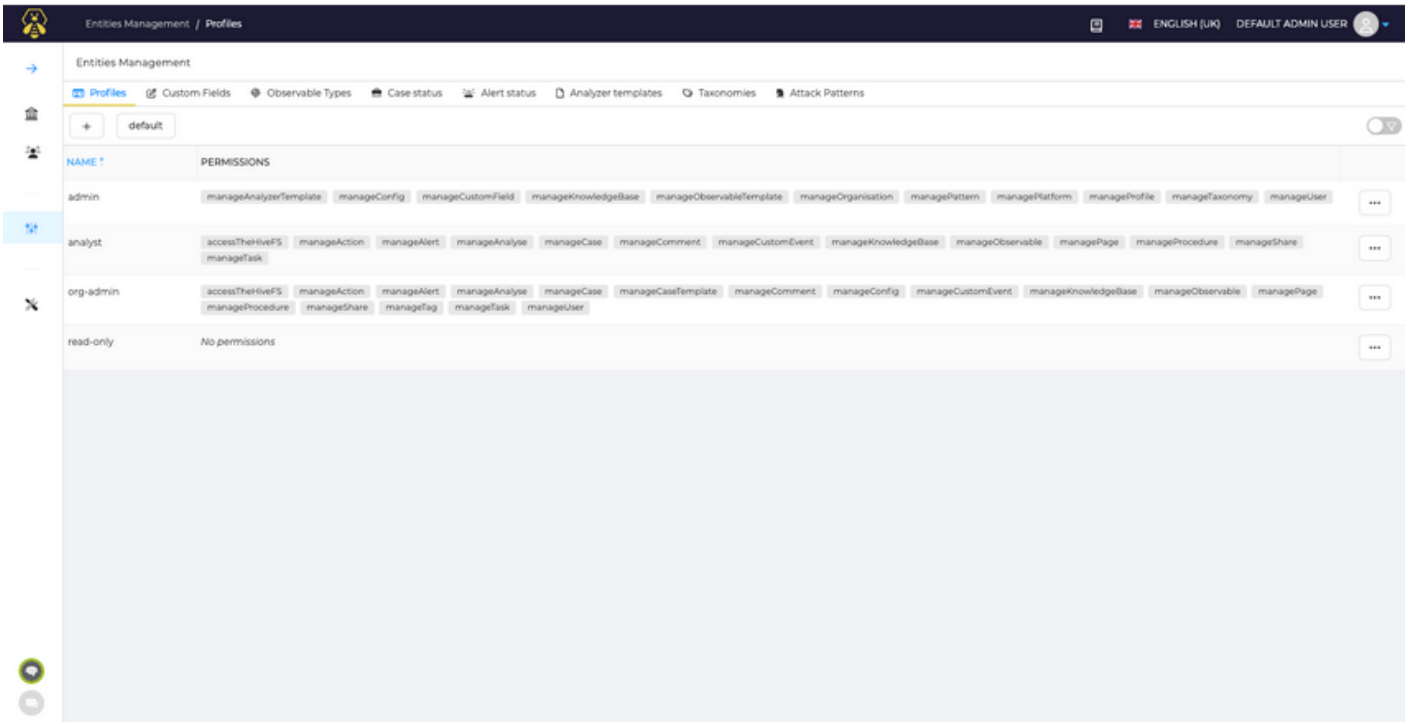
- Profiller
- Özel Alanlar
- Gözlemlenebilir Tipler
- Vaka Durumu
- Uyarı Durumu
- Analiz Şablonları
- Sınıflandırmalar
- Att&ck Modelleri

Profiller

Profiller, Varlıklar Yönetimi sayfasının ilk sekmesinde bulunmaktadır.

Giriş

TheHive, Yöneticiler ve Kuruluşlar için önceden tanımlanmış bir dizi profil ile gelir; bu set, ihtiyaçlarınıza bağlı olarak oluşturabileceğiniz özel profillerle zenginleştirilebilir.



Profilleri güncellemek için geçerli bir lisans gereklidir.

İzinler

Her profil, bir dizi izin tarafından tanımlanır. İki profil türü vardır:

- Yönetim: Admin kuruluşundaki kullanıcılar tarafından platformun yönetimi için kullanılır.
- Kuruluş: İş kuruluşlarında kullanılan.

İzinler, uygulamadaki bir varlık olan Entity ile `manageEntity` adı verilir. Örneğin: `manageCase`. Bir `manageEntity` izni, bir varlığı yazma, güncelleme, silme haklarını içerir.

Profilleri Yönet

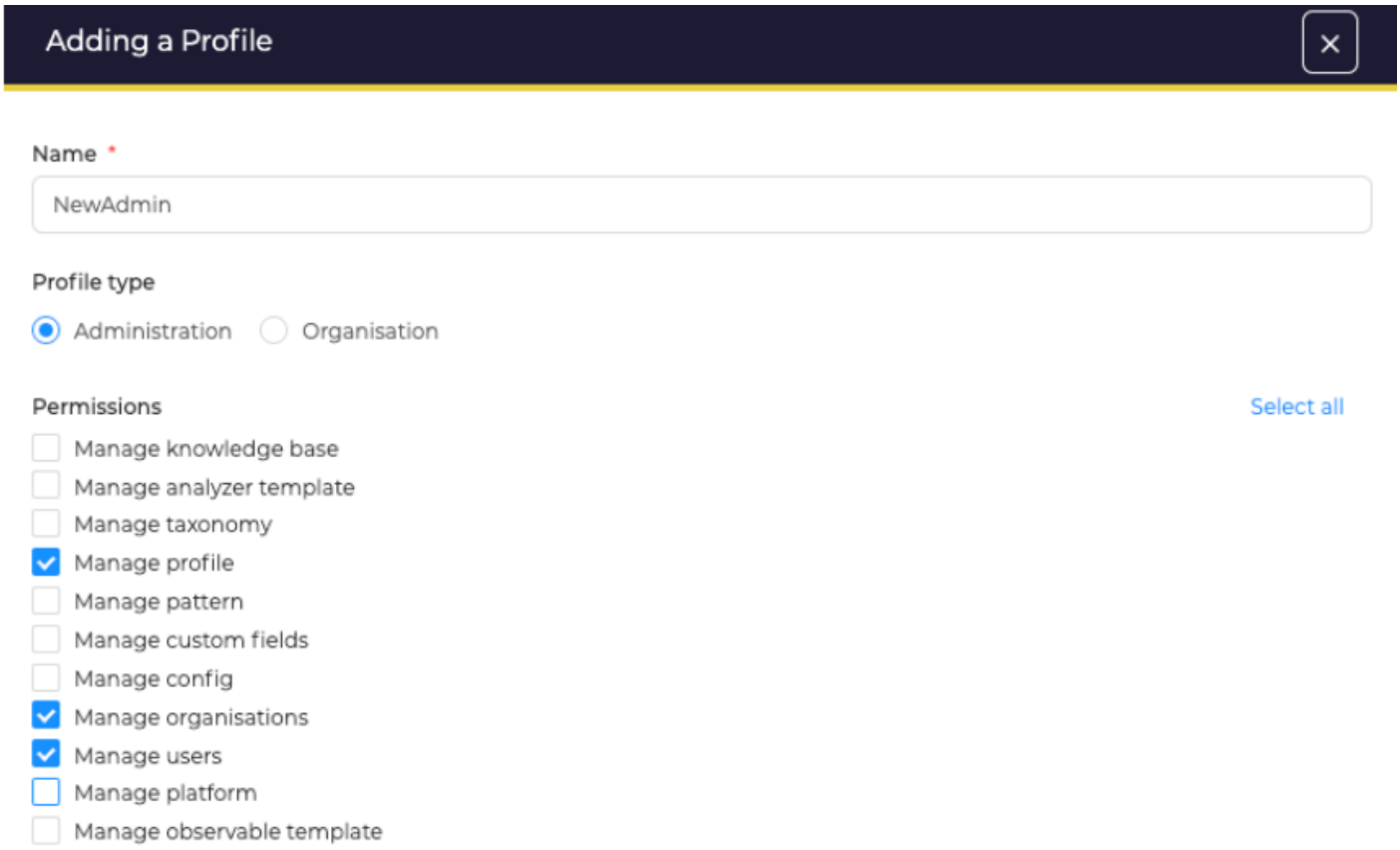
Admin profili hariç, tüm profiller özelleştirilebilir ve silinebilir.

Profil Ekle

- Profil sekmesinde, Entities Management sayfasında "+" düğmesine tıklayarak yeni bir profil ekleyin.
- Ardından oluşturulacak profil türünü seçin ve ilişkilendirilmiş izinleri belirleyin.

Profil Ekleme penceresi açılır.

- Yeni profil için bir Ad girin.
- Profil türünü Seçin.
- O profil türü için İzinleri seçin.
- Profil oluşturma işlemini onaylamak için "Profil Oluşturma" düğmesine tıklayın.



Özel Alanlar

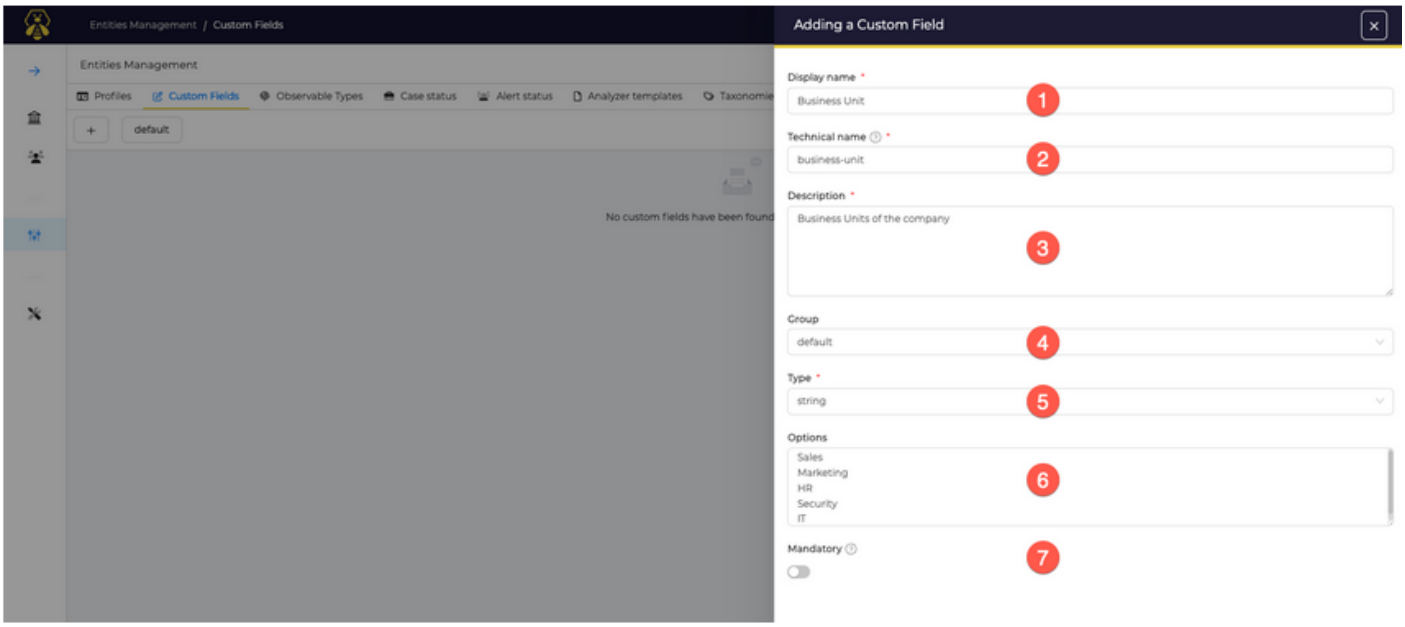
Özel Alanlar, bir Vaka veya Uyarıyı daha fazla bağlam sağlamak, istatistikler veya panolar oluşturmak için kullanılan özel bilgilerle zenginleştirilmiş bilgilerdir.

TheHive'in Yönetici görünümünde tanımlanır ve platformdaki tüm Kuruluşlara sunulur.

Bu Özel Alanlar görünümü, Yönetici alanında mevcuttur: Varlıklar Yönetimi görünümünü açın, ardından Özel Alanlar sekmesini açın.

Özel Alan Oluştur

Yeni bir Özel Alan oluşturmak için "+" simgesine tıklayın.



Yeni bir Özel Alan oluşturmak için aşağıdaki bilgileri doldurun:

- Vakalar ve Uyarılarda görüntülenecek bir isim
- Teknik bir isim. Varsayılan olarak, bu isim otomatik olarak ad ile ayarlanır, ancak gerektiğinde ayarlanabilir. Bu isim, API ile Özel Alanı kullanırken kullanılır.
- Analistlerin Vakalar ve Uyarılarla bu ÖA'yı kullanmasına yardımcı olmak için bir açıklama ekleyin.
- Bu ÖA için bir grup adı tanımlayın.
- ÖA'nın türünü tanımlayın; Birden fazla tür mevcuttur - Dize, Boolean, Tamsayı, Ondalık, Tarih
- Önceden tanımlanmış değerler varsa, bunları doldurun veya bu bir serbest alan ise boş bırakın

- Bu Özel Alanın zorunlu olması ve bir Vakayı kapatmadan önce değerlendirilmesi gerekiyorsa bu seçeneği etkinleştirin.

Sonra, Özel Alan oluşturma işlemini onaylamak için "Özel Alan Oluştur" üzerine tıklayın.

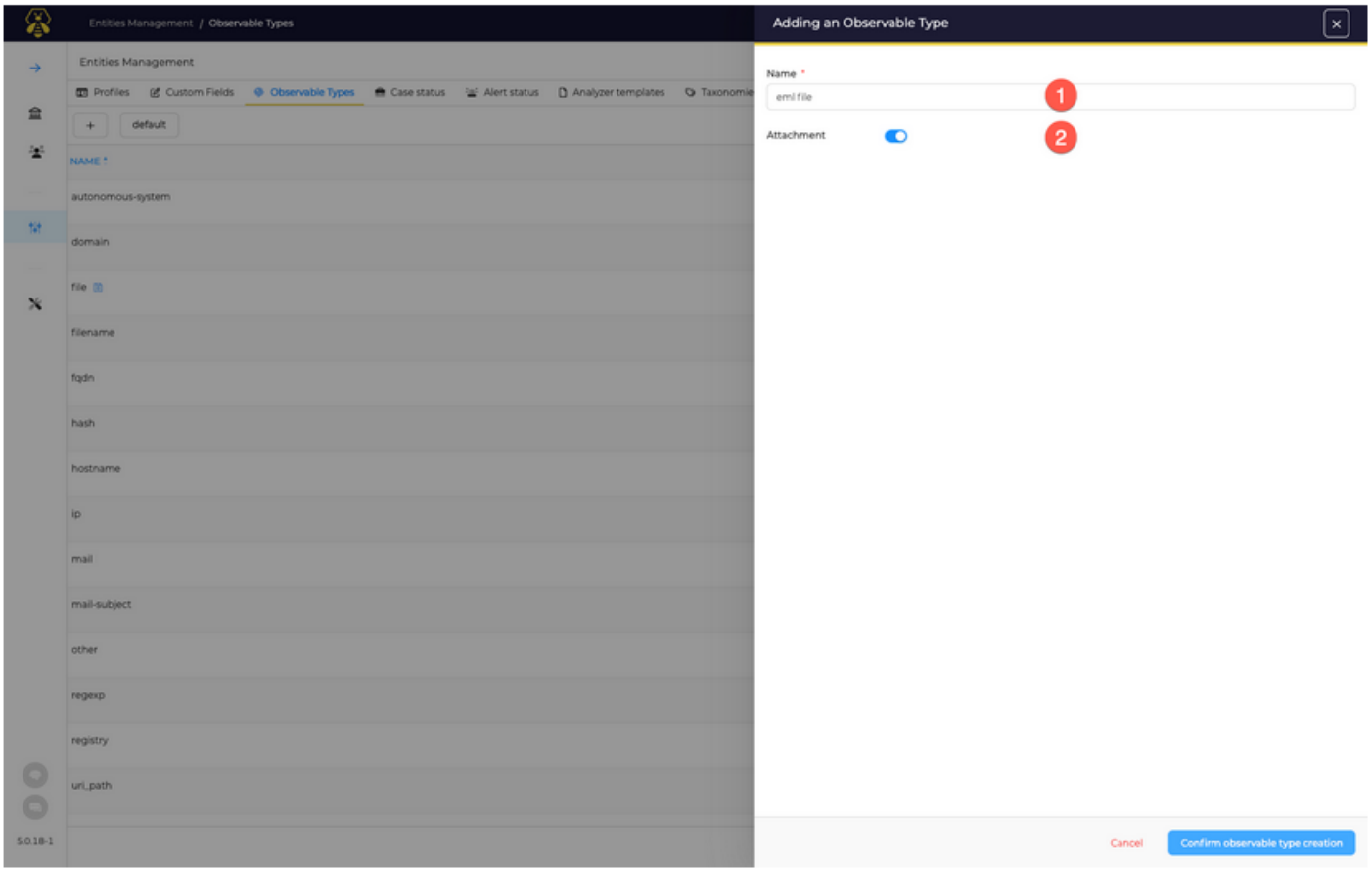
Gözlemlenebilir Tipler

Gözlemlenebilir türler, uygulamada kullanılabilecek Gözlemlenebilirlerin mevcut veri türlerini tanımlar. TheHive, önceden tanımlanmış bir dizi türle gelir ve bu liste özel veri türleriyle zenginleştirilebilir.

Gözlemlenebilir türleri, Yönetici alanında yapılandırılır: Varlıklar Yönetimi'ni açın ve Gözlemlenebilir türler sekmesini seçin.

Yeni Bir Gözlemlenebilir Türü Oluştur

Yeni bir Gözlemlenebilir Türü oluşturmak için "+" simgesine tıklayın.



Bu yeni tür için bir isim belirtin. Bu yeni gözlemlenebilir türünün bir dosya ekine göre tanımlanıp tanımlanmadığını belirleyin. Eğer evet ise, analistler tarafından girilen veri bir dosyadır; değilse, bu bir metin alanıdır.

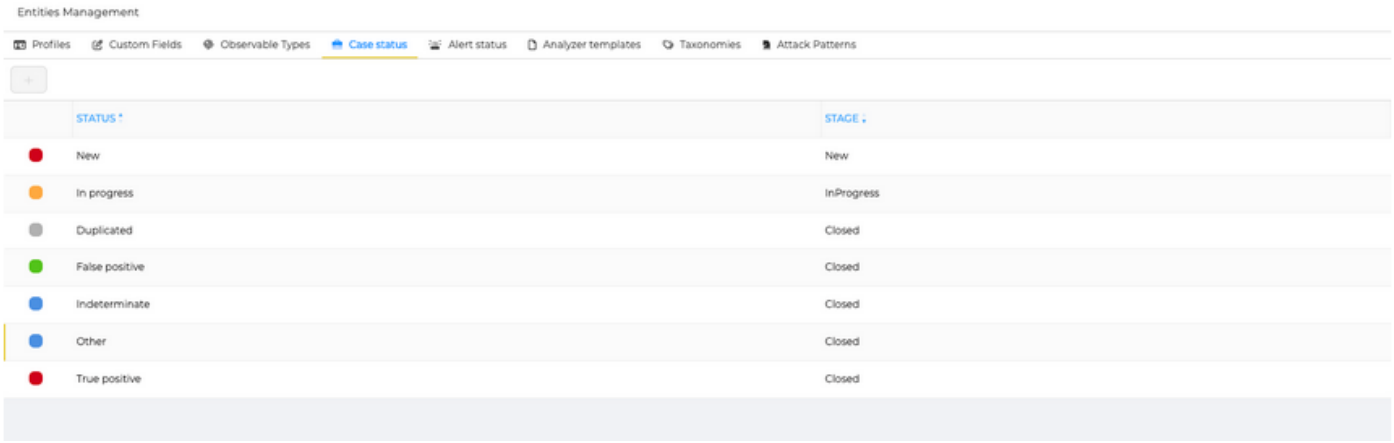
Sonra, Gözlemlenebilir tür oluşturmayı onaylamak için "Gözlemlenebilir tür oluştur" üzerine tıklayın.

Vaka Durumu

Vaka Durumu, Yönetici alanında yapılandırılabilir: Varlıklar Yönetimi sayfasını açın ve Vaka durumu sekmesini seçin.

Giriş

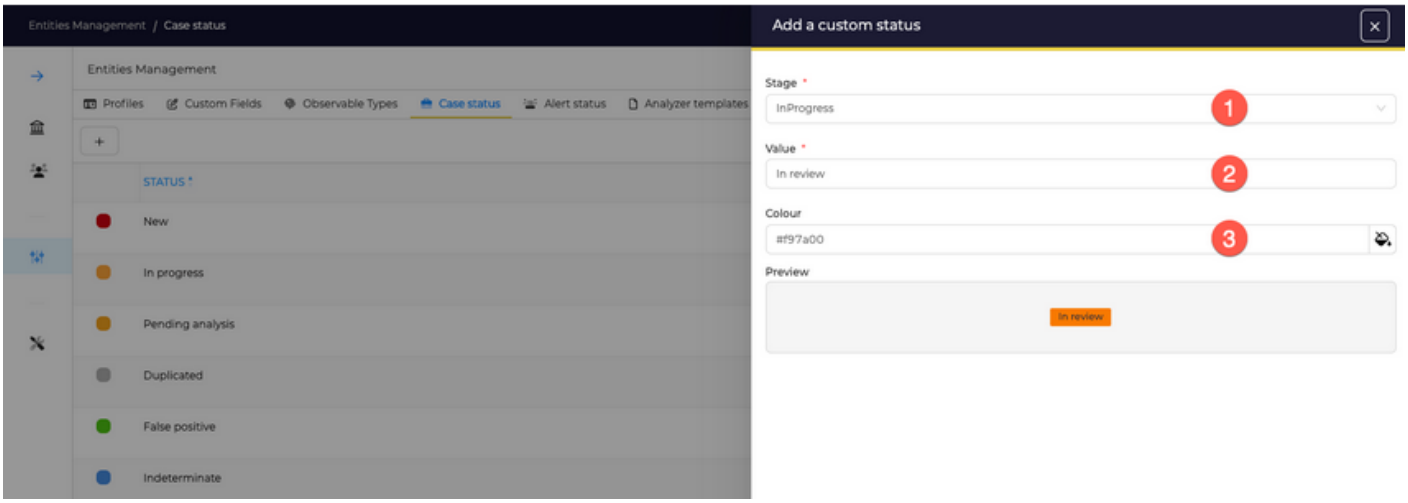
TheHive, bir dizi önceden tanımlanmış durum ile gelir. Her durum bir Aşamaya aittir.



Aşamalar sabitlenmiştir; güncellenemez veya silinemezler ve platforma yeni bir aşama eklenemez. Durumlar oluşturulabilir, güncellenebilir ve silinebilir.

Durum Oluşturma

Yeni bir durum eklemek için "+" simgesine tıklayın.



Bir durum şu özelliklere sahiptir:

- Bir aşama: Yeni durumun aşamasını seçin.

- Bir değer: Yeni durum için bir ad seçin.
- Bir renk: Kullanıcıların uygulamada durumu hızlıca tanımlaması için bir renk seçin.

Durumu Düzenle/Sil

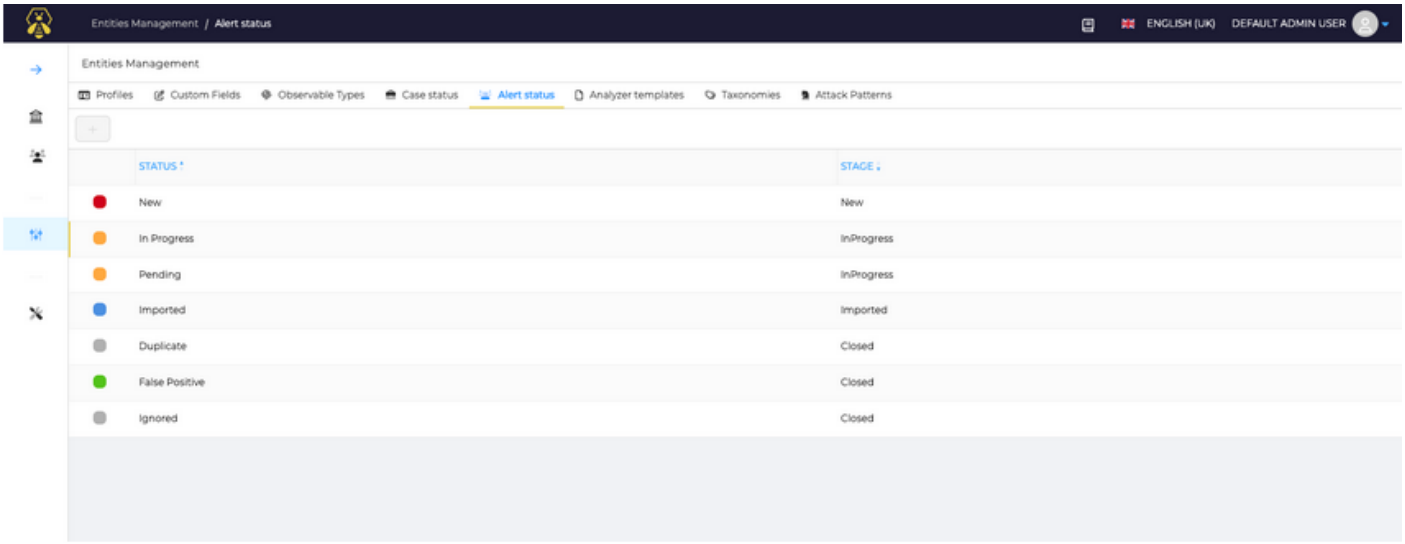
Renk, bir durumu güncellerken yalnızca güncellenebilir.

Uyarı Durumu

Uyarı Durumu, Yönetici alanında yapılandırılabilir: Varlıklar Yönetimi sayfasını açın ve uyarı durumu sekmesini seçin.

Giriş

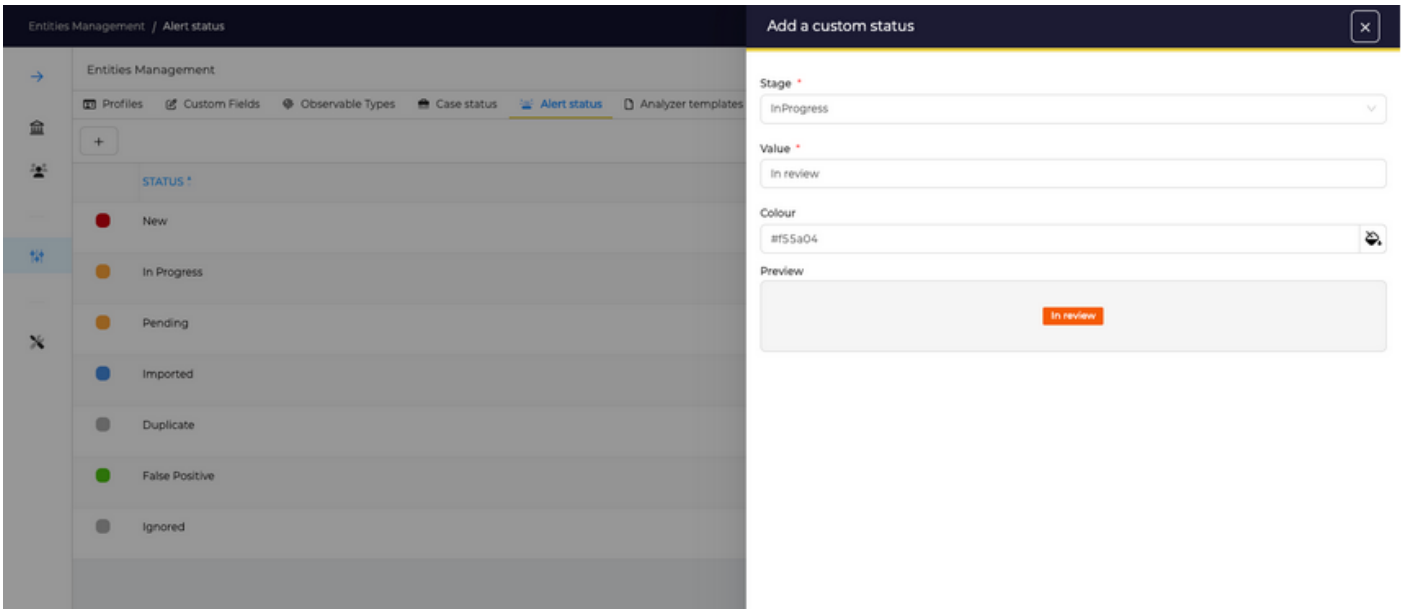
TheHive, bir dizi önceden tanımlanmış durum ile gelir. Her durum bir aşamaya aittir.



Aşamalar sabitlenmiştir; güncellenemez veya silinemezler ve platforma yeni bir aşama eklenemez. Durumlar oluşturulabilir, güncellenebilir ve silinebilir.

Durum Oluşturma

Yeni bir durum eklemek için "+" simgesine tıklayın.



Bir durum, şu özelliklere sahiptir:

- Bir aşama: Yeni durumun aşamasını seçin.
- Bir değer: Yeni durum için bir ad seçin.
- Bir renk: Kullanıcıların uygulamada durumu hızlıca tanımlaması için bir renk seçin.

Durumu Düzenle/Sil

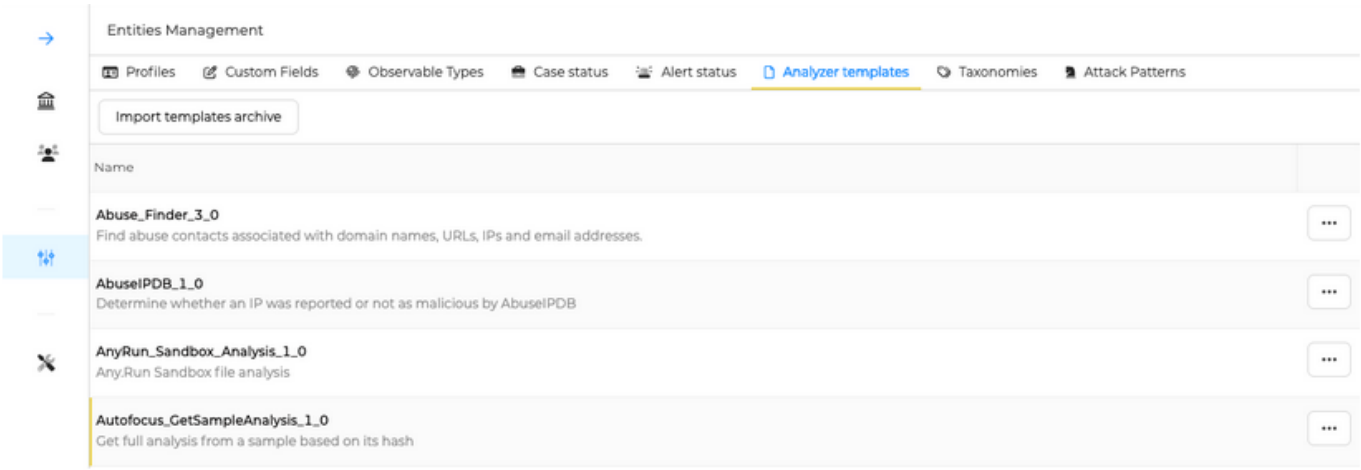
Renk, bir durumu güncellerken yalnızca güncellenebilir.

Analiz Şablonları

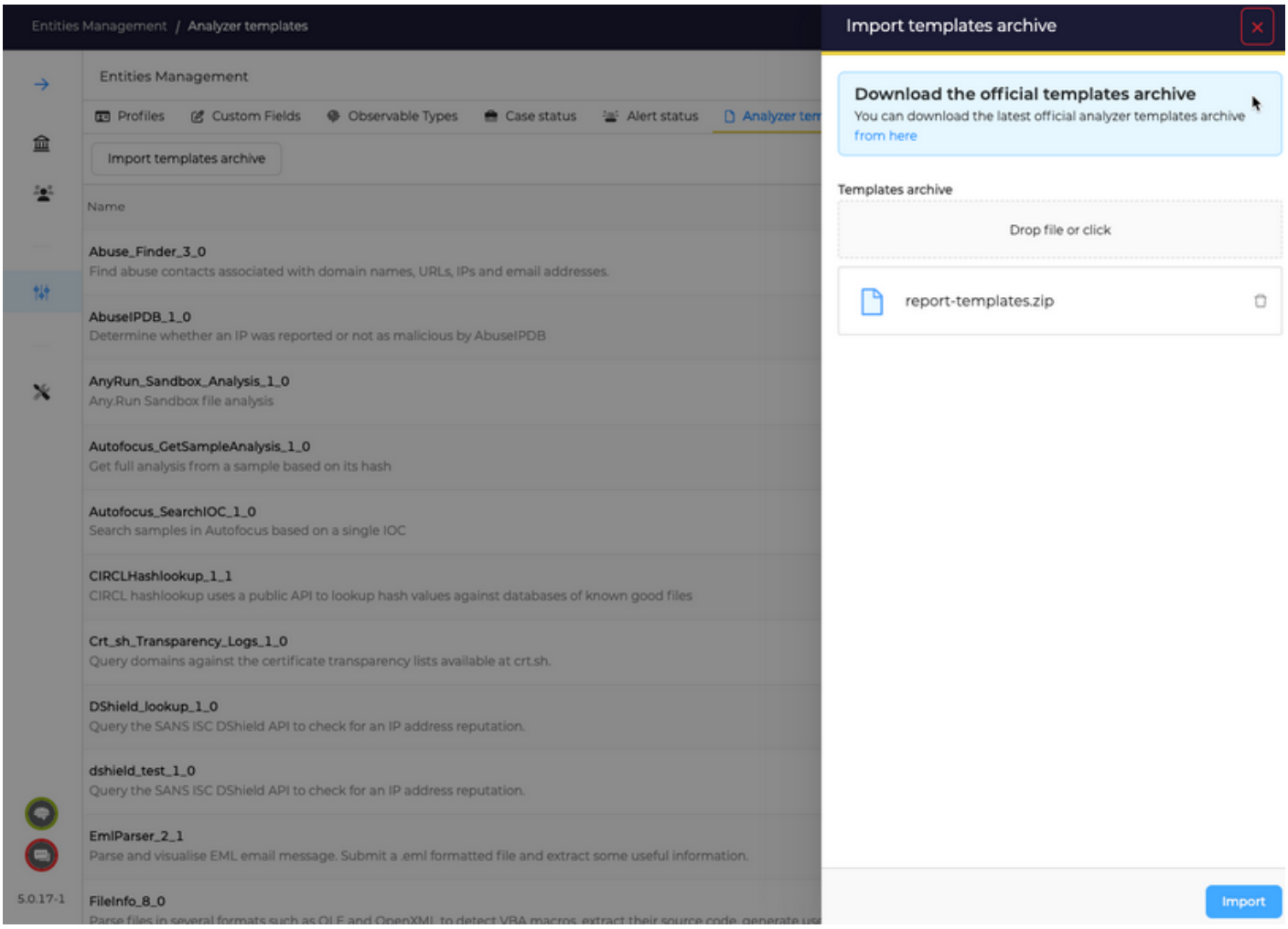
TheHive, analiz raporlarını görüntülemek için HTML şablonlarına ihtiyaç duyar.

Genel Analiz Şablonlarını Kurun veya Güncelleyin

- Yönetici olarak, "Varlık Yönetimi" menüsüne ve "Analiz Şablonlarına" gidin.



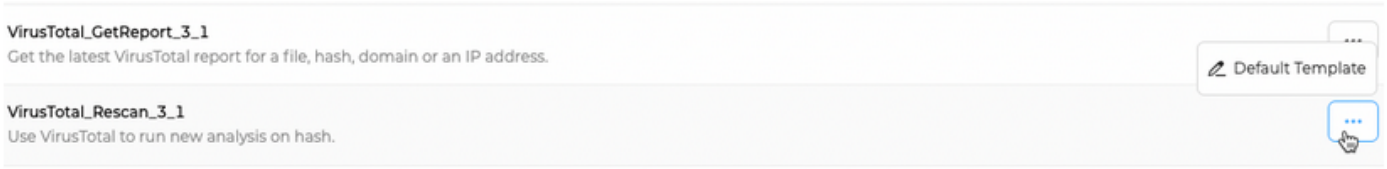
- ZIP arşivini indirin, ekleyin ve İçe Aktar düğmesine tıklayın.



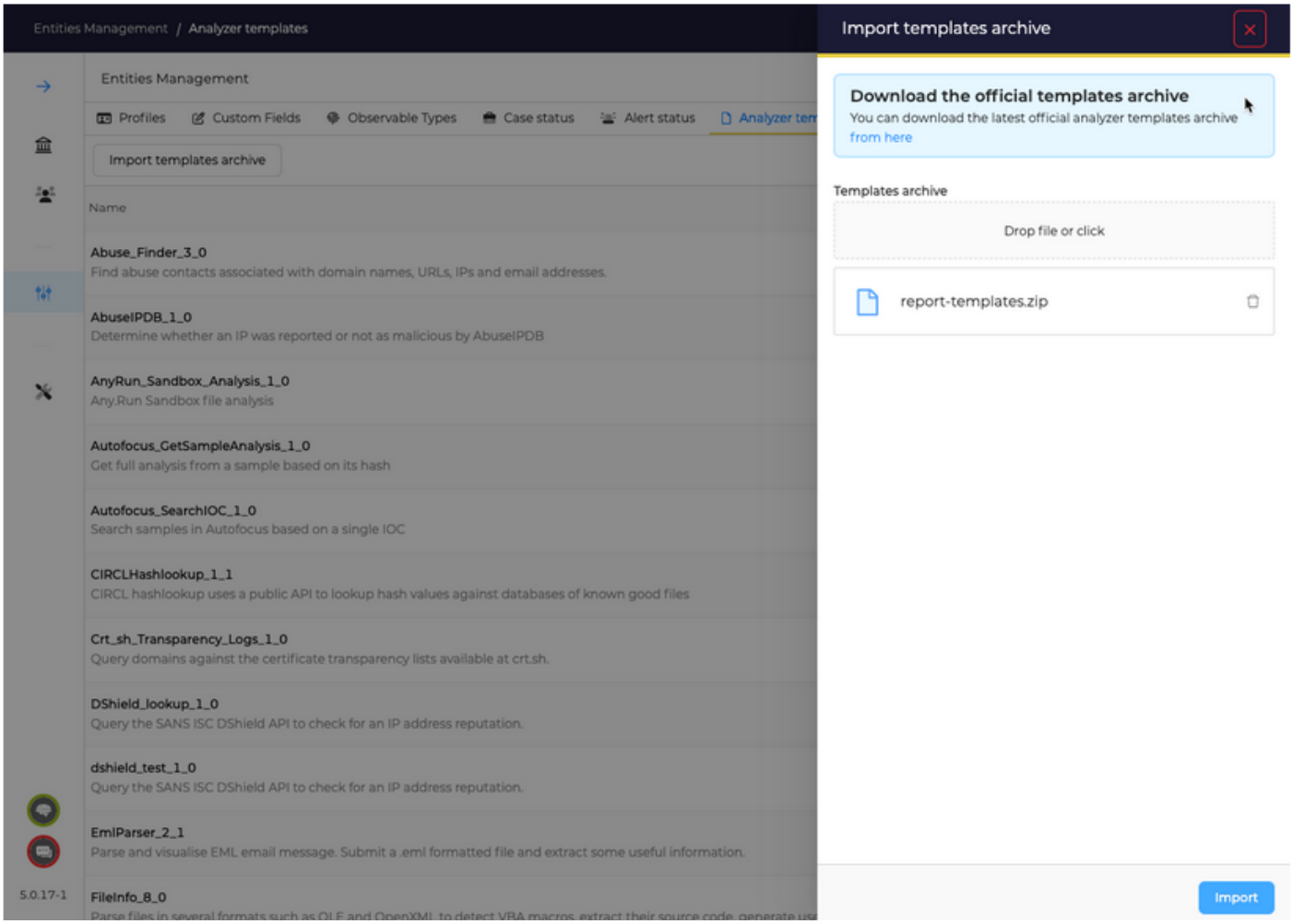
Şablonları Düzenle

Yeni bir Analiz Cortex'te etkinleştirildiğinde ve TheHive için kullanılabilir hale geldiğinde, bu listede bir şablon satırı eklenir.

- Düzenlenecek şablonu bulun



Düzenleyin ve kaydedin

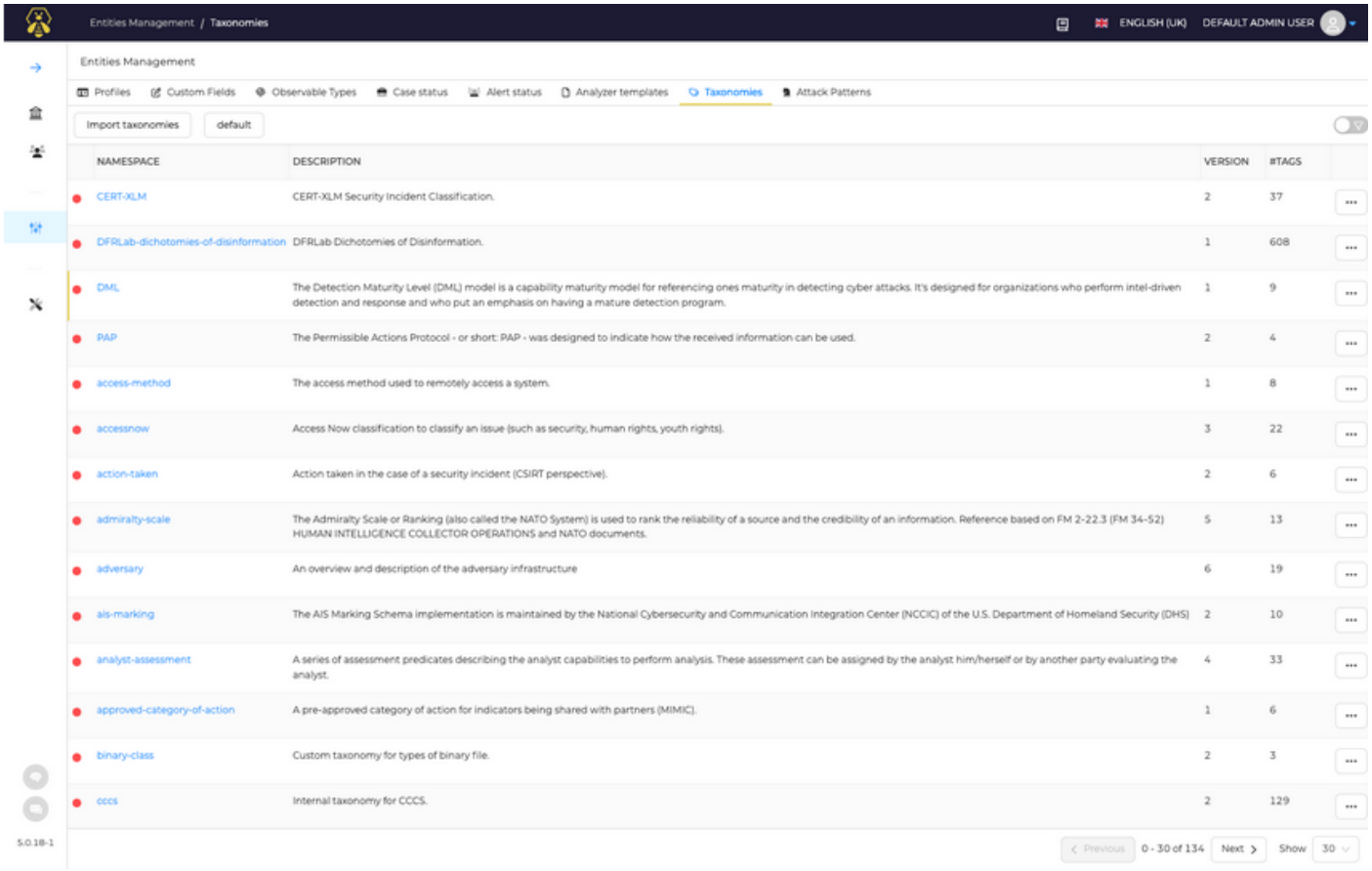


Bağlı analizleri çalıştırmak, yeni şablonun uygulandığı sonuçları görüntülemelidir.

Sınıflandırmalar

Sınıflandırmalar, TheHive'da yapılandırılmış etiketleri tanımlamak için kullanılır. Sınıflandırmalar, Yönetici alanında yapılandırılabilir: Varlıklar Yönetimi'ni açın ve Sınıflandırmalar sekmesini seçin.

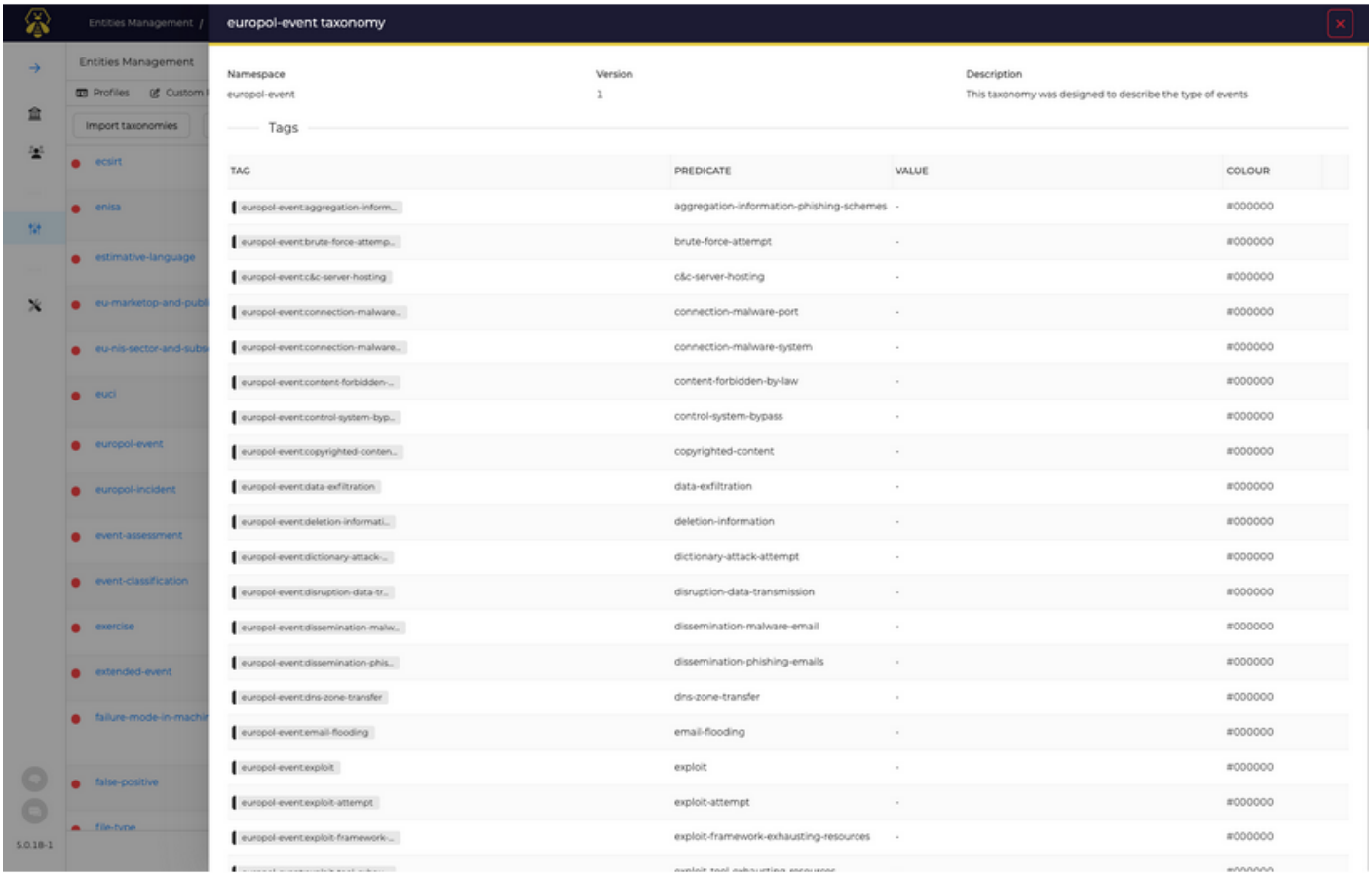
Varsayılan olarak, MISP sınıflandırmaları içe aktarılır.



Bir sınıflandırmadaki mevcut etiketlerin listesini gözden geçirmek için istenen adı tıklayın; bu, etiketlerin listesiyle bir çekmeceyi açacaktır.

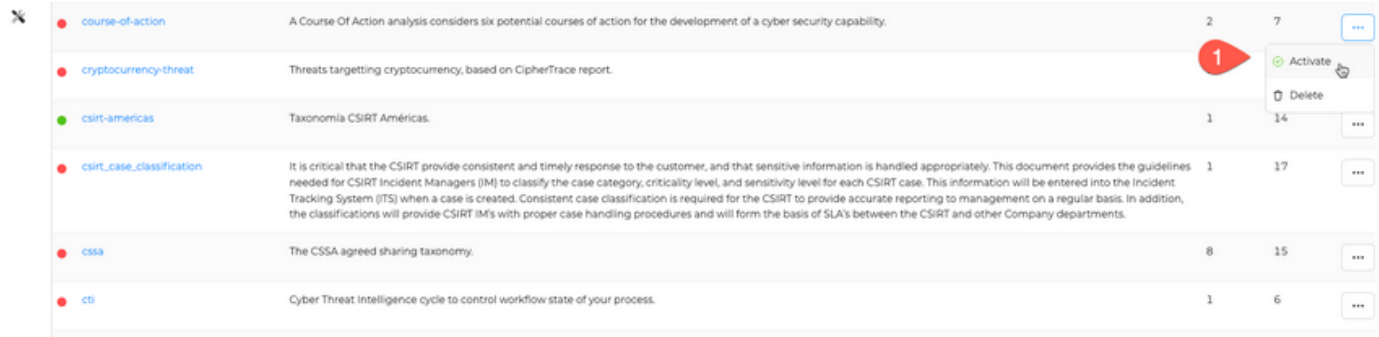
Kullanıcı Bir Sınıflandırmayı Görüntüle

Bir belirli sınıflandırmadaki mevcut etiketlerin listesini gözden geçirmek için istenen adı tıklayın; bu, etiketlerin listesiyle bir çekmeceyi açacaktır.



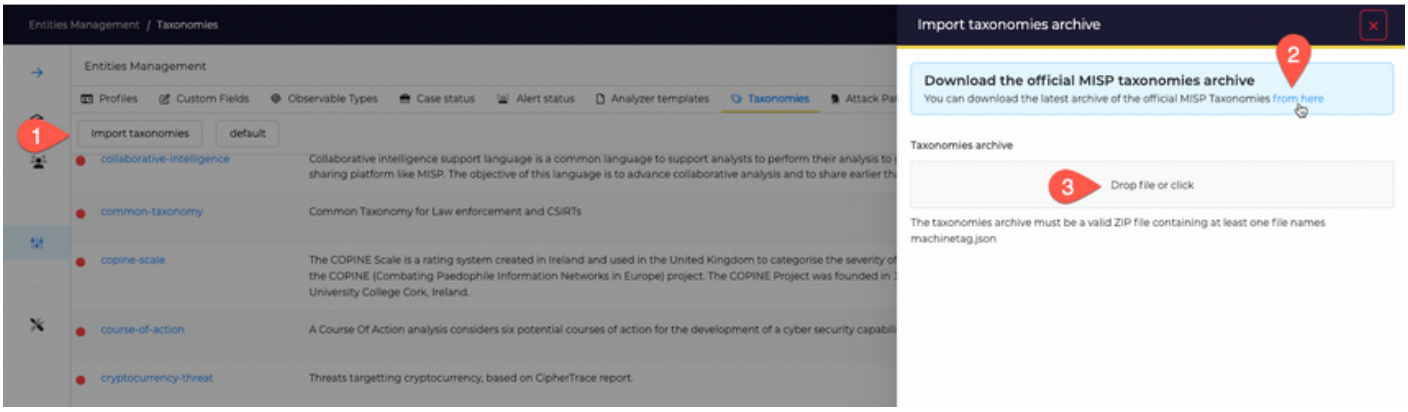
Bir Sınıflandırmayı Etkinleştirme veya Silme

Varsayılan olarak hiçbir sınıflandırma etkin değildir; bu nedenle Vakalarda veya Uyarılarda kullanılamazlar. Vakalarda ve Uyarılarda bir etiket setini kullanmak için ilgili sınıflandırma etkinleştirilmelidir.



Sınıflandırmaları Güncelle

TheHive, kurulum anındaki MISP sınıflandırmaları sürümüyle birlikte gelir. TheHive güncellenirken en son kullanılabilir sürümü güncellemez veya eklemaz. Dolayısıyla, MISP ekibinin yayınladığı en son sürümü almak istiyorsanız bunu manuel olarak güncellemeniz gerekir.



1. Taksonomileri "İçe Aktar" düğmesine tıklayın.
2. Son arşivi buradan indirebilirsiniz: https://github.com/MISP/misp-taxonomies/archive/main.zip
3. İndirilen dosyayı sürükleyip bırakın ve "İçe Aktar" düğmesine tıklayın

Özel Sınıflandırmalar

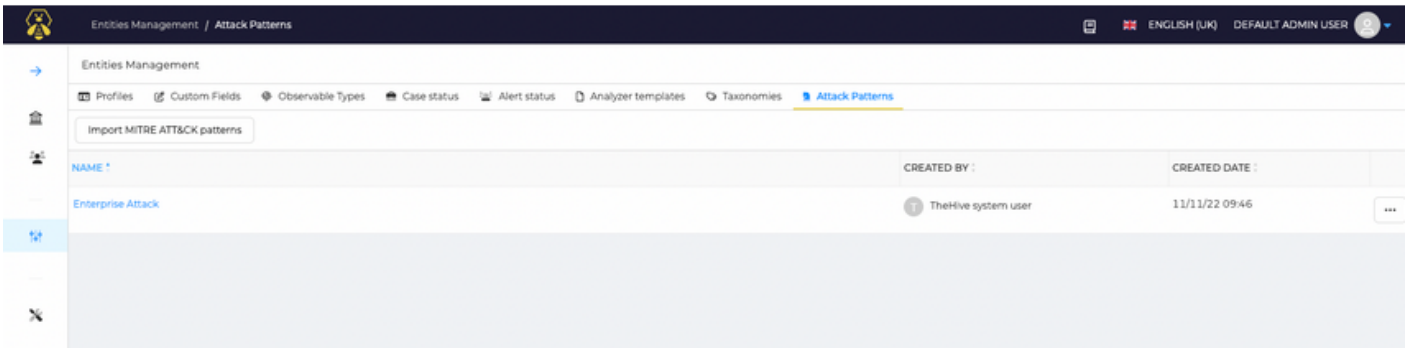
MISP tarafından belirtilen JSON şemasını takip ederek kendi taksonomilerinizi ekleyebilirsiniz. (https://github.com/MISP/misp-taxonomies)

Att&ck Modelleri

Att&ck modelleri yapılandırması, Yönetici alanında mevcuttur: Varlıklar Yönetimi'ni açın, ardından Att&ck Modelleri sekmesine tıklayın.

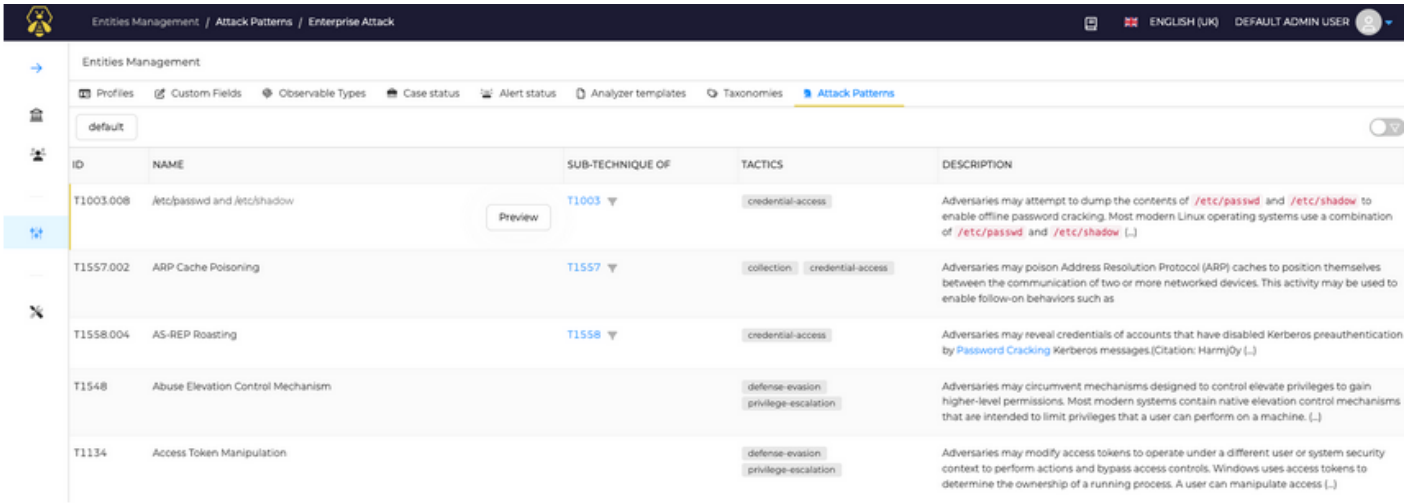
Giriş

Varsayılan olarak, TheHive, MITRE'den Enterprise ATT&CK modelleri ile birlikte gelir. Bu, kurulum süreci sırasında yüklenir ve ilgili tüm tekniklerle birlikte Katalog adı Enterprise Attack oluşturulur.

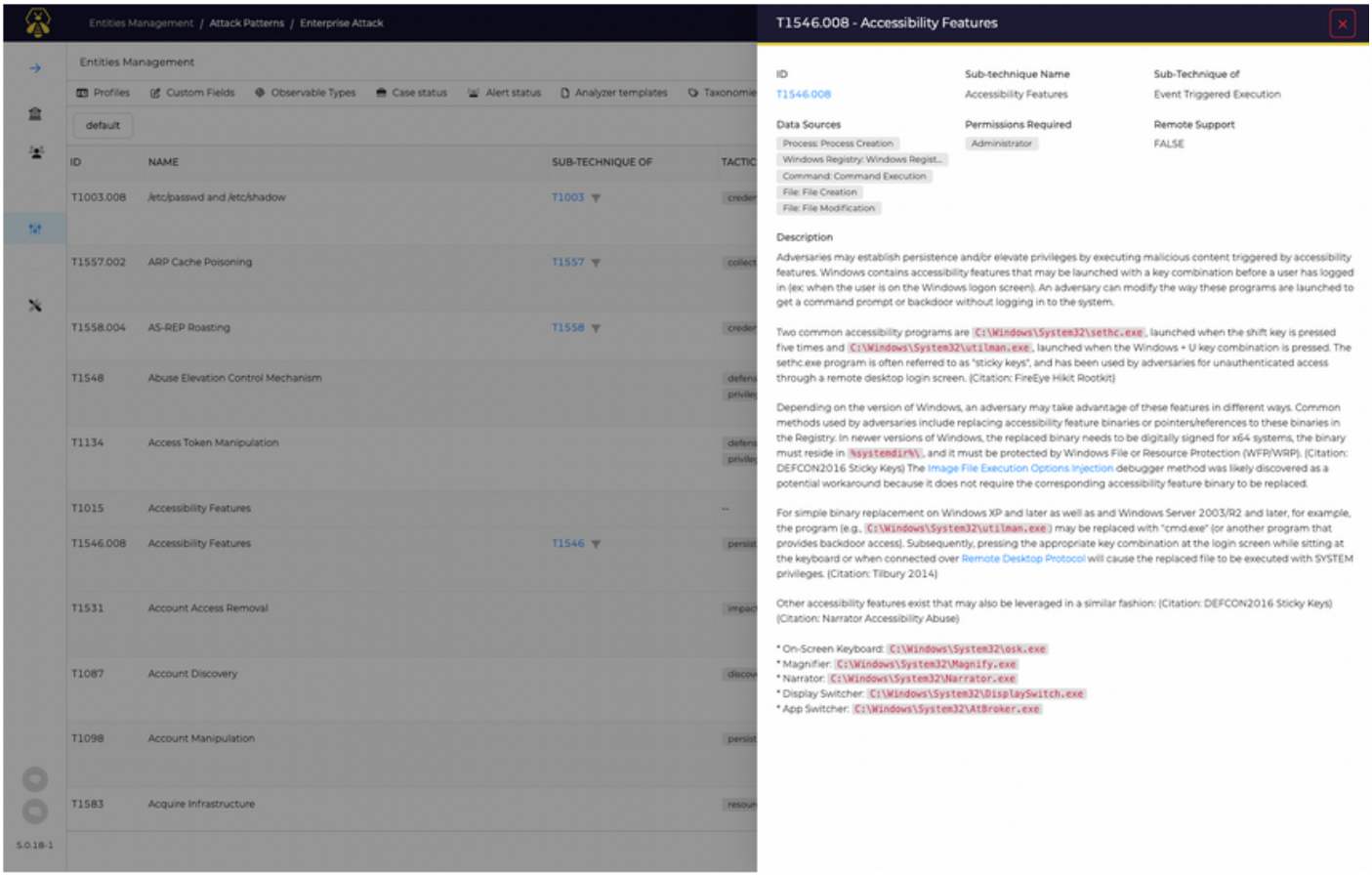


Modelleri Görüntüle

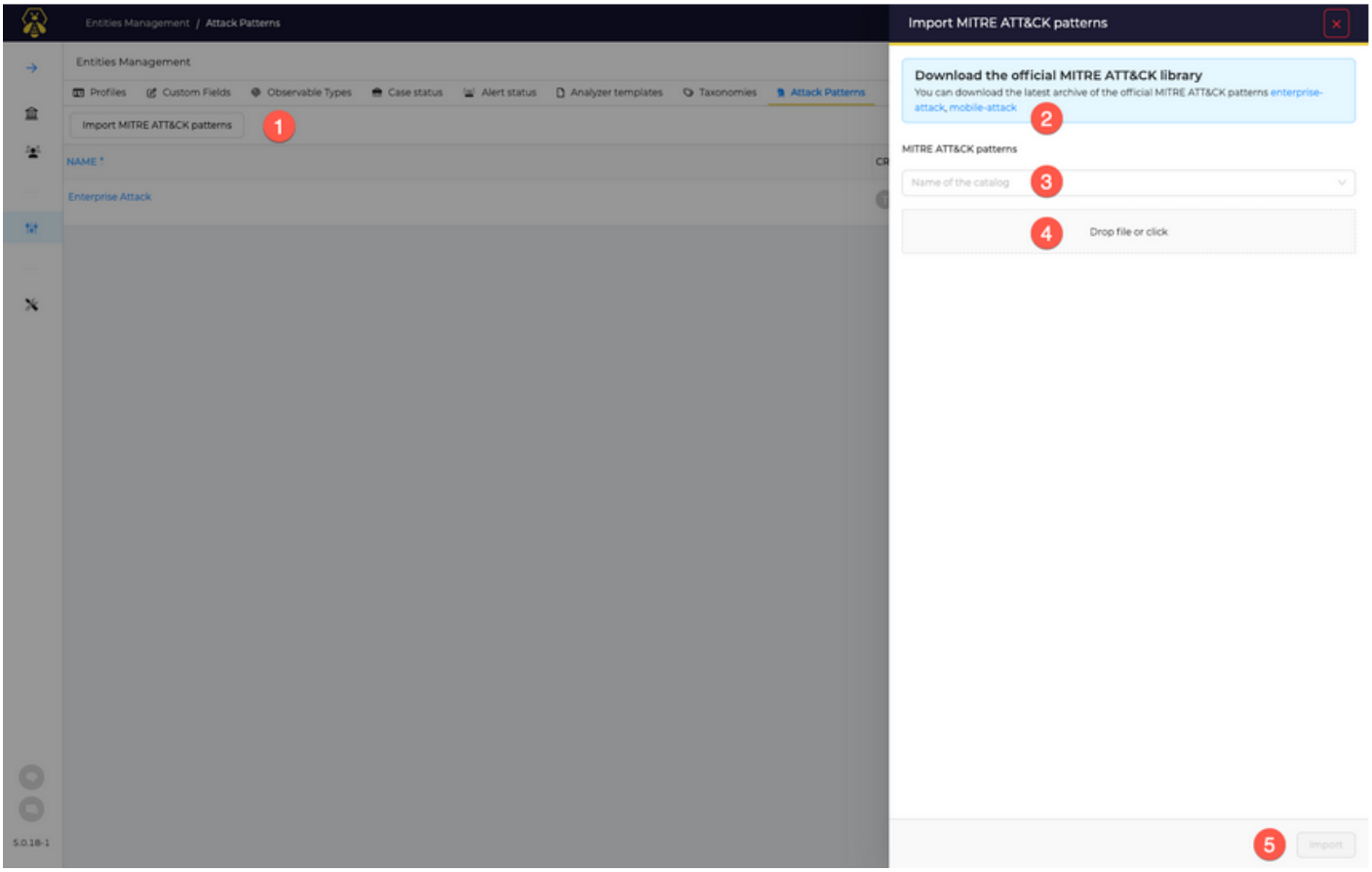
Bir kataloğa dahil edilen modellerin ayrıntılarını görmek için bir kataloğa tıklayın.



Her bir modelin tüm ayrıntıları teknik kimliğine tıklanarak incelenebilir



Kataloglar otomatik olarak güncellenmez, kurulum sırasında gelen Enterprise kataloğu da güncellenmez. Dolayısıyla, çerçevenin en son sürümlerinden yararlanmak istiyorsanız, bunları güncellemeniz gerekir.



Yeni bir katalog eklemek için:

1. "MITRE ATT&CK desenlerini içe aktar" üzerine tıklayın.
2. Kurmak istediğiniz desenleri seçin.
3. Yeni bir katalog oluşturuyorsanız bir katalog adı ekleyin veya güncellemek istediğiniz mevcut bir adı seçin.
4. İndirilen dosyayı sürükleyip bırakın.
5. İçe Aktar düğmesine tıklayın.

Bu işlemler biraz zaman alabilir.