Uyarılar (Alerts)

Bu bölümde Uyarılar hakkında bilgi bulabilirsiniz.

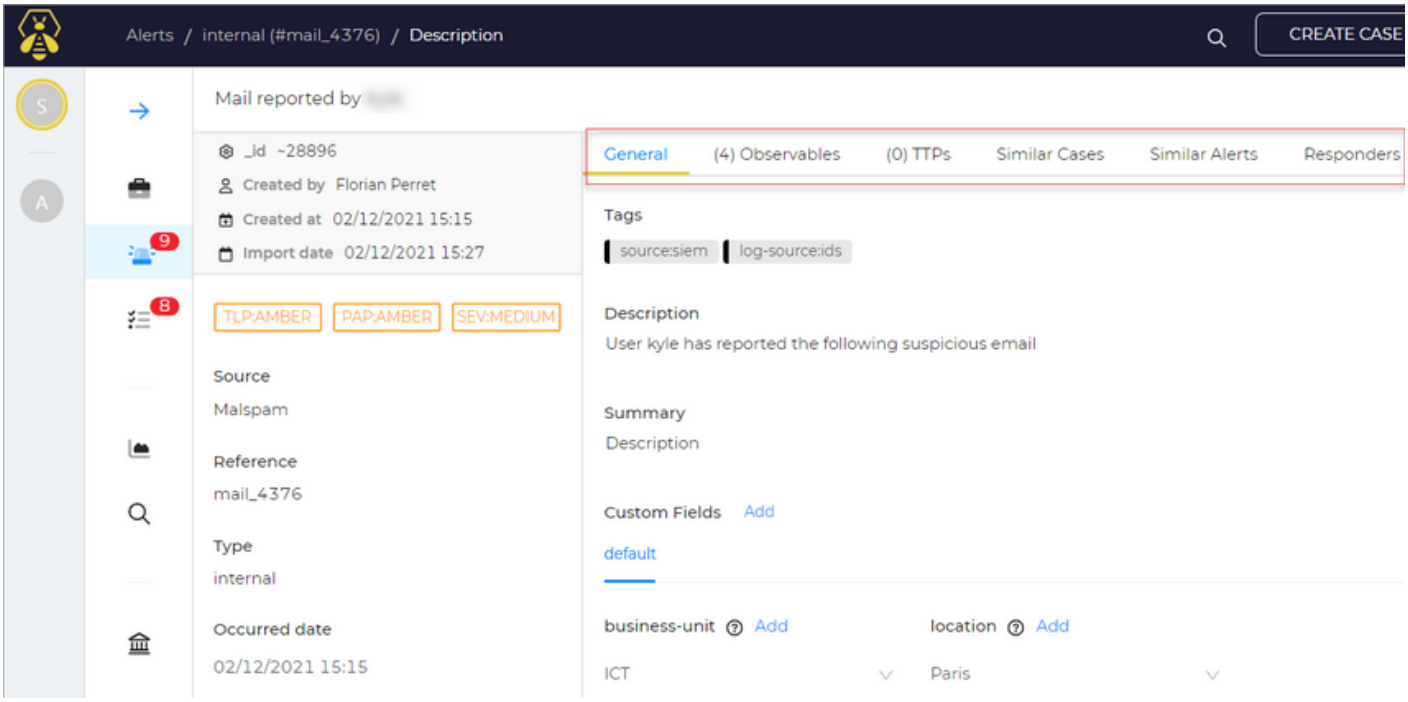
Uyarılar, mevcut güvenlik sorunları, zafiyetler ve saldırılar hakkında zamanında bilgi sağlar.

Uyarı Ayrıntılarını Görüntüleme

Uyarı ayrıntılarını görüntülemek için:

Listede herhangi bir uyarıya tıklayabilirsiniz.

Uyarılar sayfası, uyarılar hakkında daha fazla ayrıntıya sahip olan çeşitli sekmeleri içerir; genel sekme, gözlemlenebilirler, TTP'ler, benzer vakalar, benzer uyarılar, yanıtlayıcılar sekmesi.

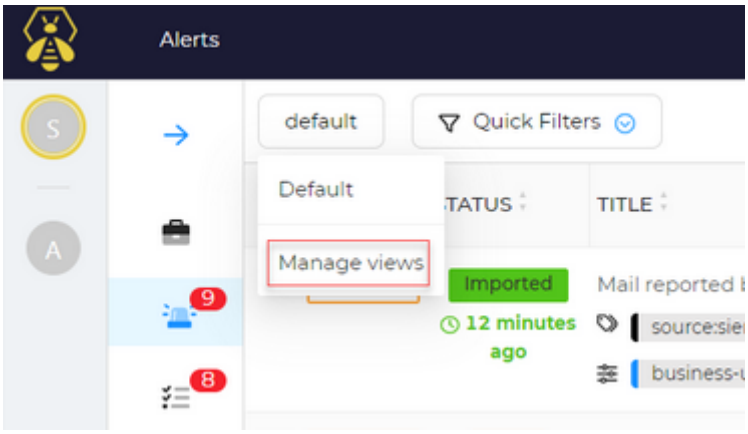


Görünümleri yönetin

Bu bölümde, görünümleri yönetme hakkında bilgi bulabilirsiniz.

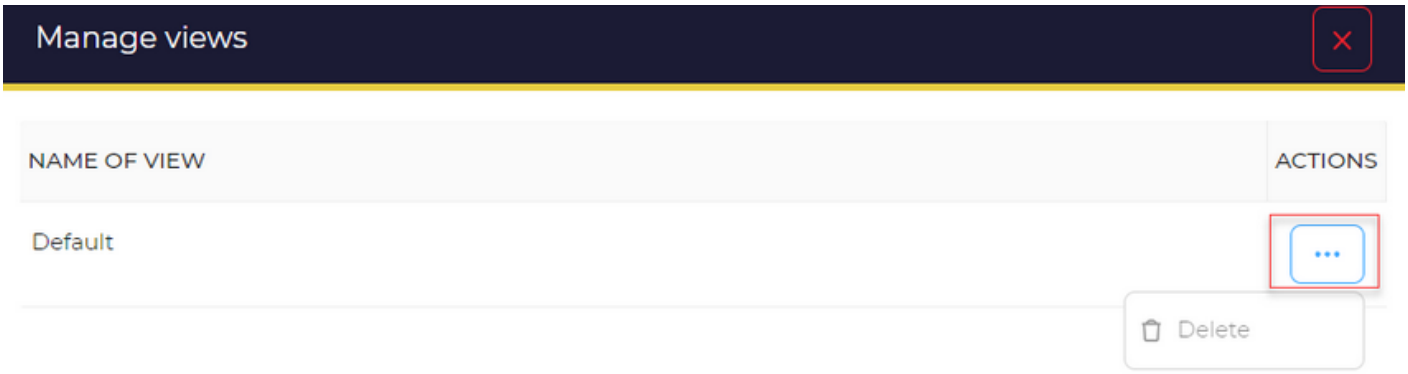
Görünümleri yönetmek için:

Varsayılan(default) düğmesine tıklayın.
Listeden Görünümleri Yönet(Manage Views) üzerine tıklayın.



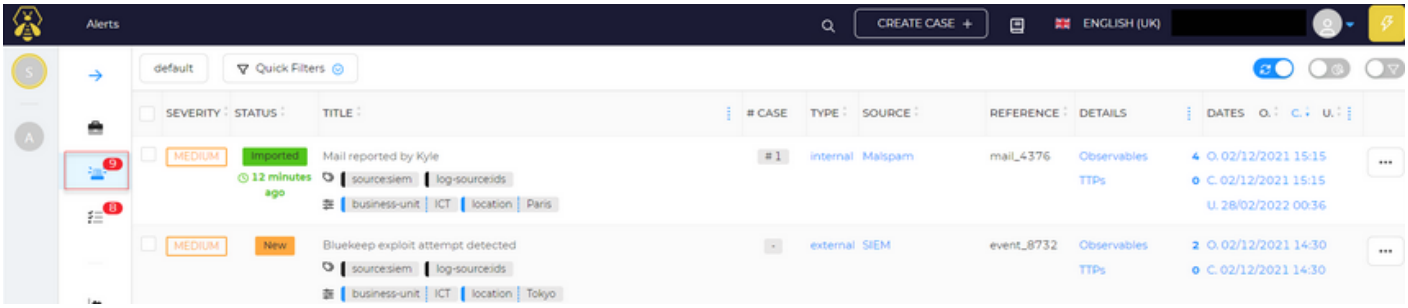
Yeni bir sayfa açılır. Görünümün Adı (Name of the view) ve ilgili Eylemler (Actions) yer alır.

Silmek istediğiniz görünümün adına karşılık gelen üç noktaya **(...)** tıklayın.
Sil (Delete) öğesine tıklayın.



Uyarıları Yönet

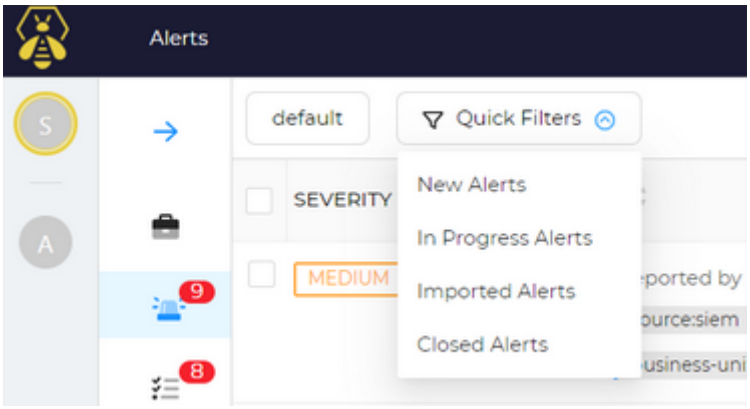
Uyarılara başvurmak için çeşitli seçenekler mevcuttur.



Hızlı Filtreler

Hızlı filtre uygulamak için:

Hızlı Filtre (Quick Filter) seçeneğine tıklayın.
Liste, aralarından seçim yapabileceğiniz seçenekleri görüntüler.



Otomatik Yenileme

Otomatik yenileme seçeneği, bir sayfayı otomatik olarak yenilemenizi sağlar.

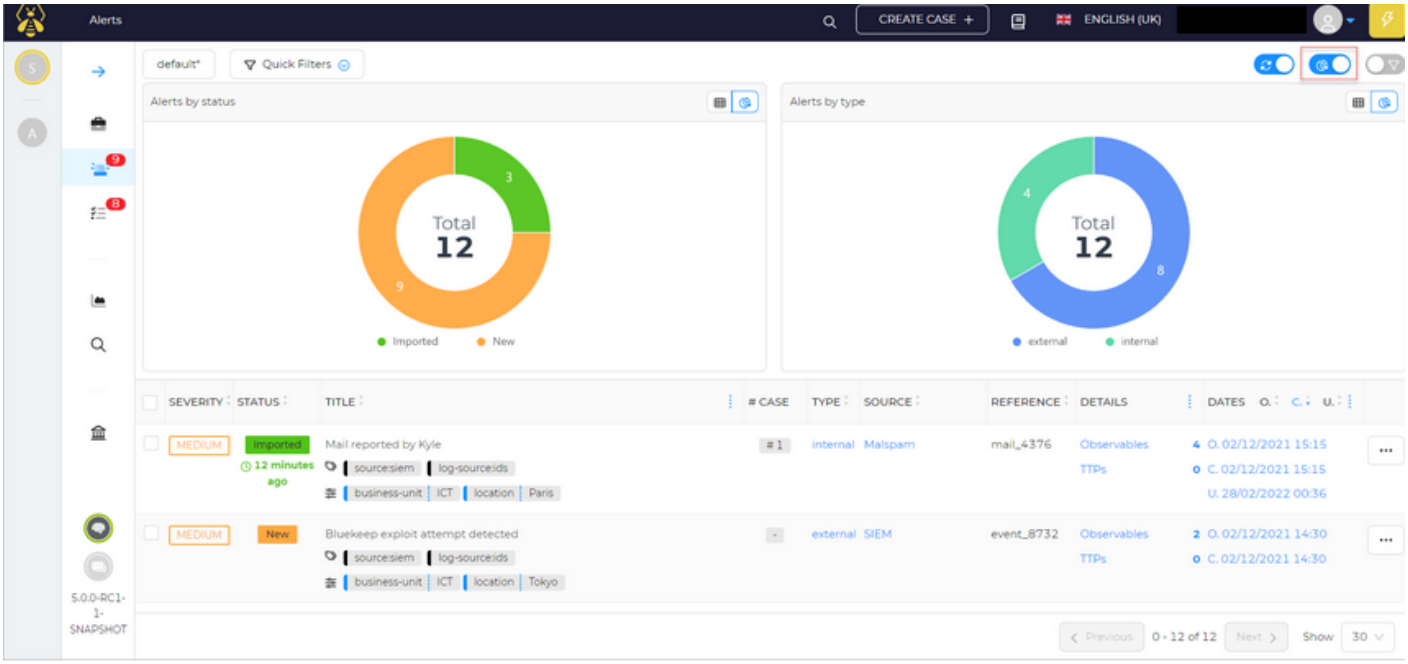
Otomatik yenileme gerçekleştirmek için:

- Uyarılar sayfasında, Otomatik yenileme düğmesini açın.

İstatistikler

İstatistikleri görüntülemek için:

- Uyarılar sayfasında, İstatistikler geçiş düğmesini açtığınızda istatistikler görüntülenecektir.

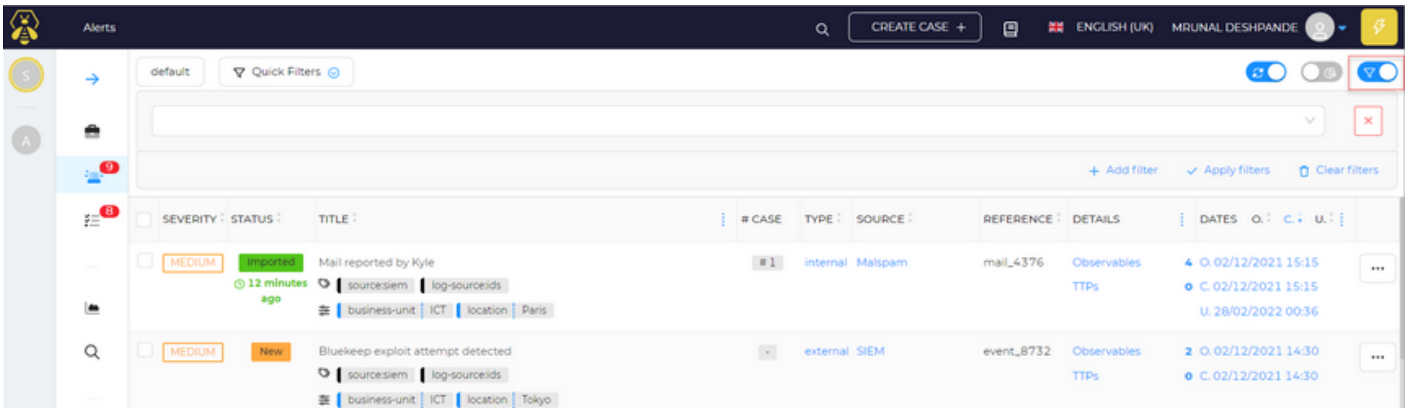


Filtreler

Filtre uygulamak için:

Uyarılar sayfasında, Filtreler geçiş düğmesini açın.
Filtre ekle'ye tıklayın.

- Gerekli alana Filtre Uygula.



- Listeden filtreleri seçin.
- Filtreleri uygula öğesine tıklayın.
- (İsteğe bağlı) Uygulanan tüm filtreleri temizlemek için Filtreleri temizle öğesine tıklayın.

Sıralama

Sıralama herhangi bir alan değeri üzerinde gerçekleştirilebilir.

Sıralamak için:

- Uyarılar sayfasında, belirli bir dosya adına göre sıralama yapmak için yukarı/aşağı doğru işaret eden küçük oka tıklayın.

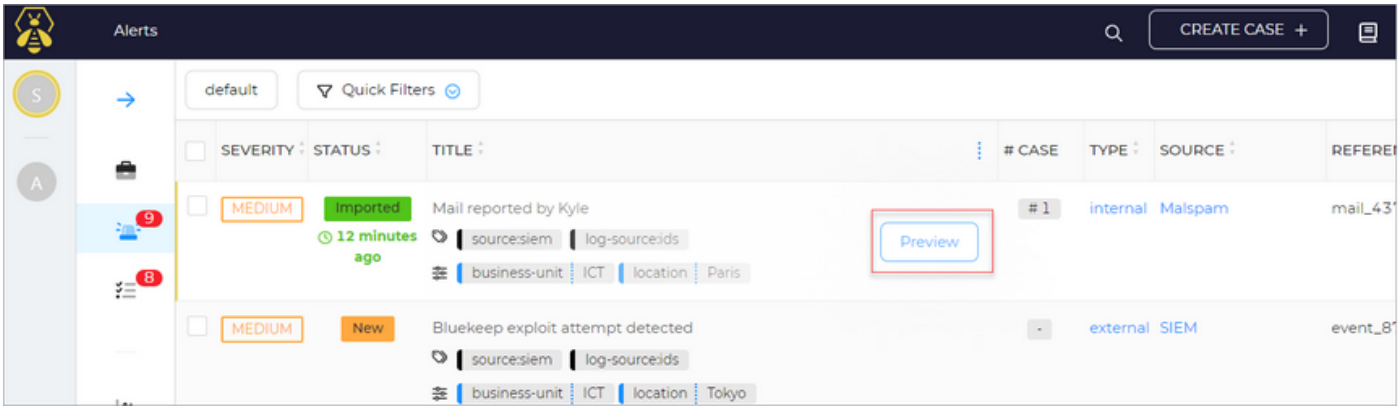
Önizleme Uyarıları

Bu bölümde uyarıları ve ilgili ayrıntıları önizleme hakkında bilgi bulabilirsiniz.

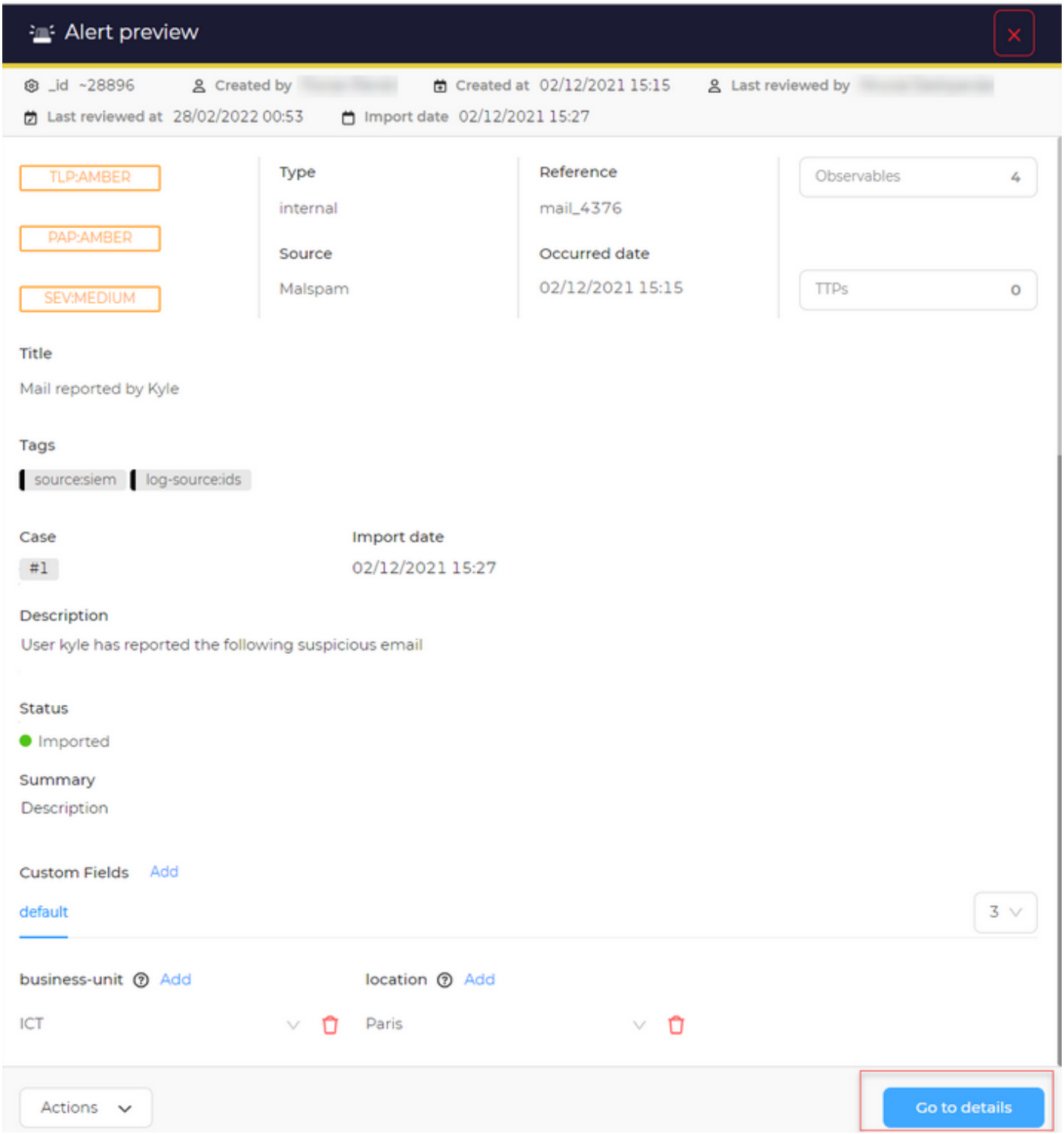
Uyarı ayrıntılarını önizlemek için:

Uyarılar listesi sayfasında, belirli uyarı adına karşılık gelen bir Önizleme düğmesi vardır.

Önizleme (Preview) seçeneğine tıklayın.



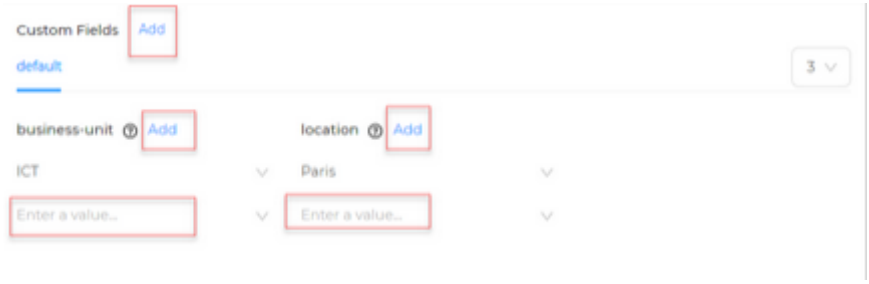
Uyarı ayrıntıları önizleme penceresi açılır.



Uyarının kimliği, oluşturulma tarihi, son gözden geçirme tarihi, içe aktarma tarihi, TLP, PAP ve önem derecesi ayrıntıları, başlığı, etiketleri, açıklaması, durumu ve özeti gibi ayrıntıları görebilirsiniz.

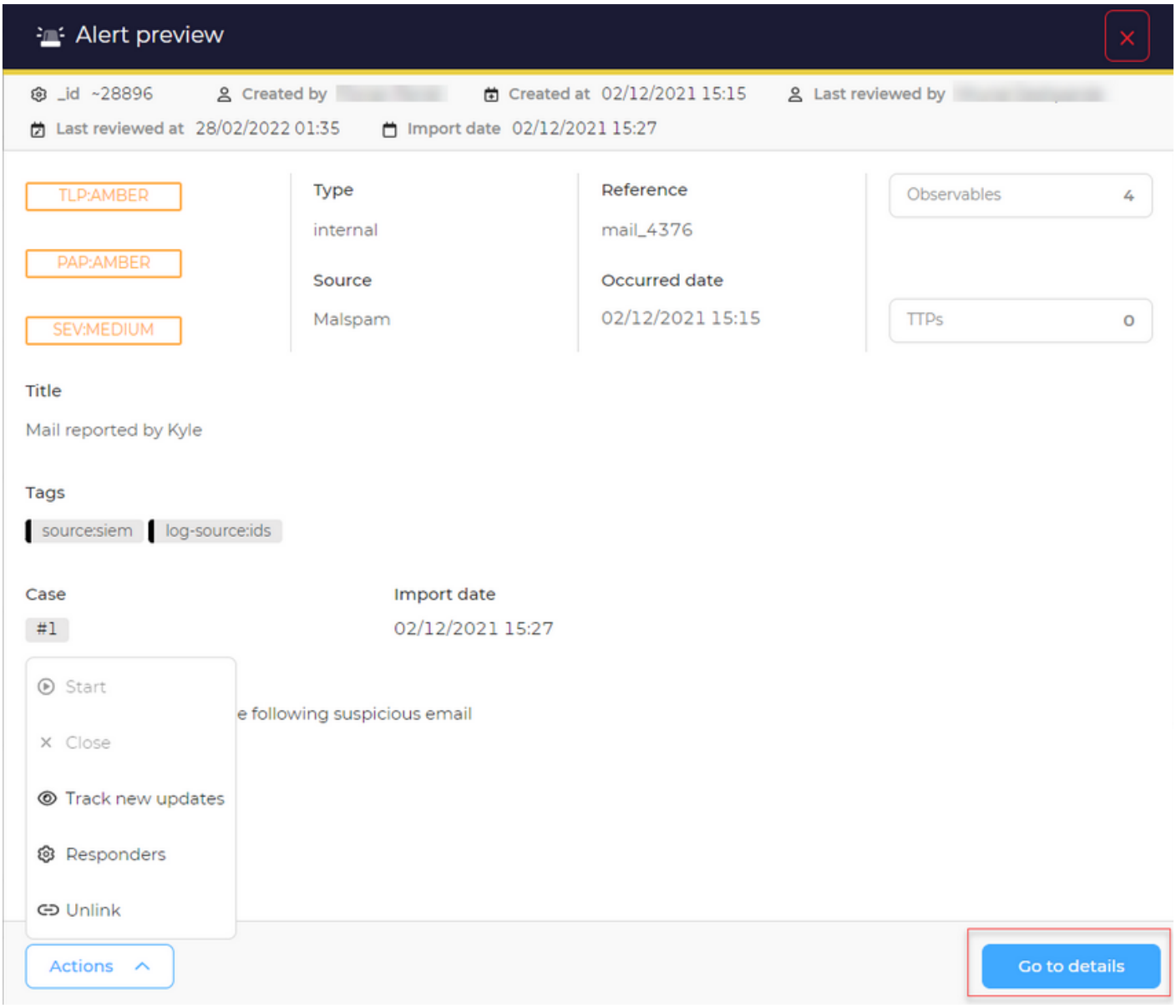
Özel alanlar (Bkz. Özel alanlar ekleme), iş birimi ve konum ayrıntıları ekleyin.

- İş birimi ve konum ayrıntılarını girmek için Ekle'ye (Add) tıklayın.



Uyarı Detayları

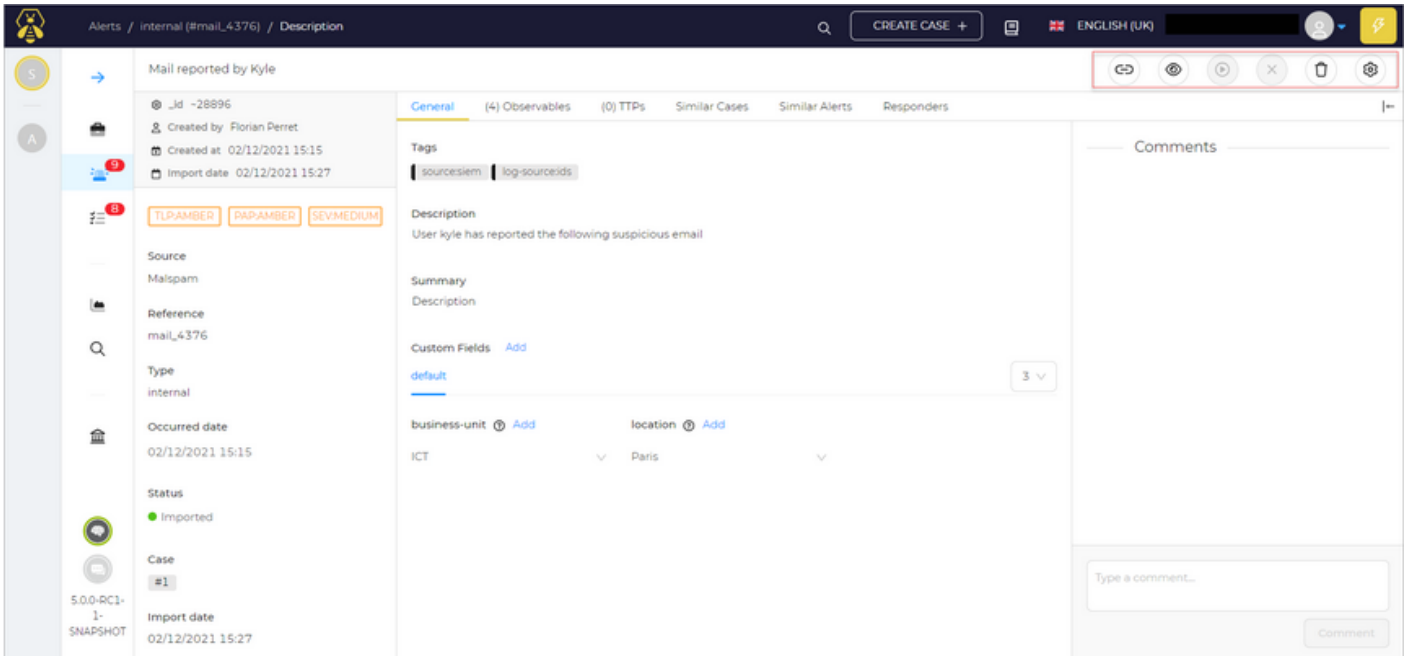
Uyarı hakkında daha fazla ayrıntı görüntülemek için Ayrıntılara git (Go to details) düğmesine tıklayın.



Uyarı Ayrıntıları Menüsü

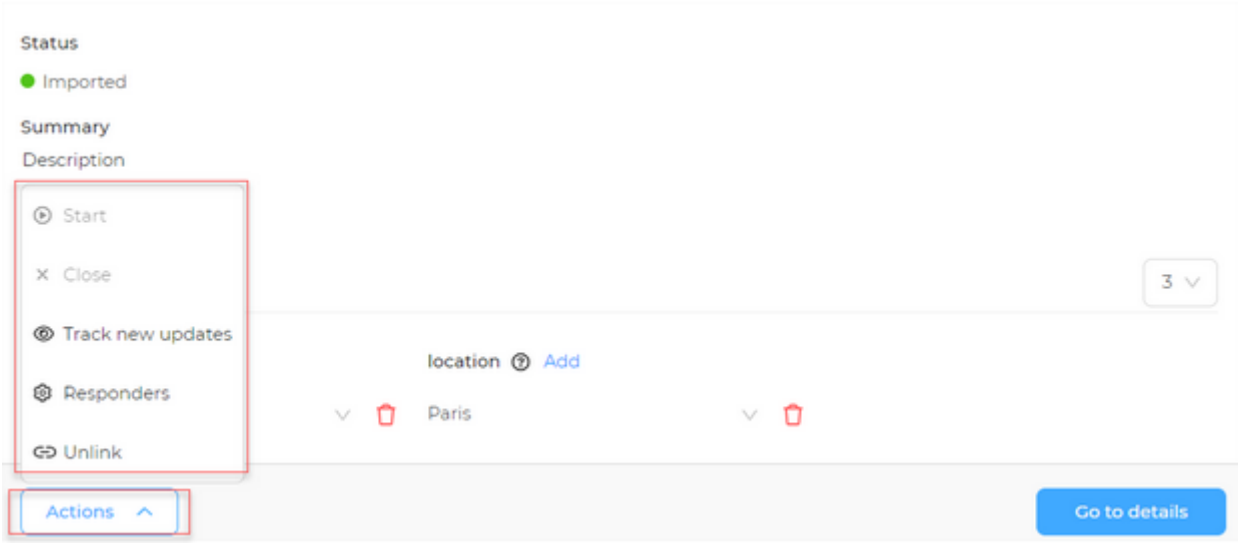
Uyarı hakkında daha fazla ayrıntı görüntülemek için Ayrıntılara git düğmesine tıklayın.

Sayfanın üst kısmında, başlatma, kapatma, yeni güncellemeleri izleme/görmezden gelme, uyarıların bağlantısını kaldırma ve yanıtlayıcıları çalıştırma gibi birçok görev seçeneği mevcuttur.



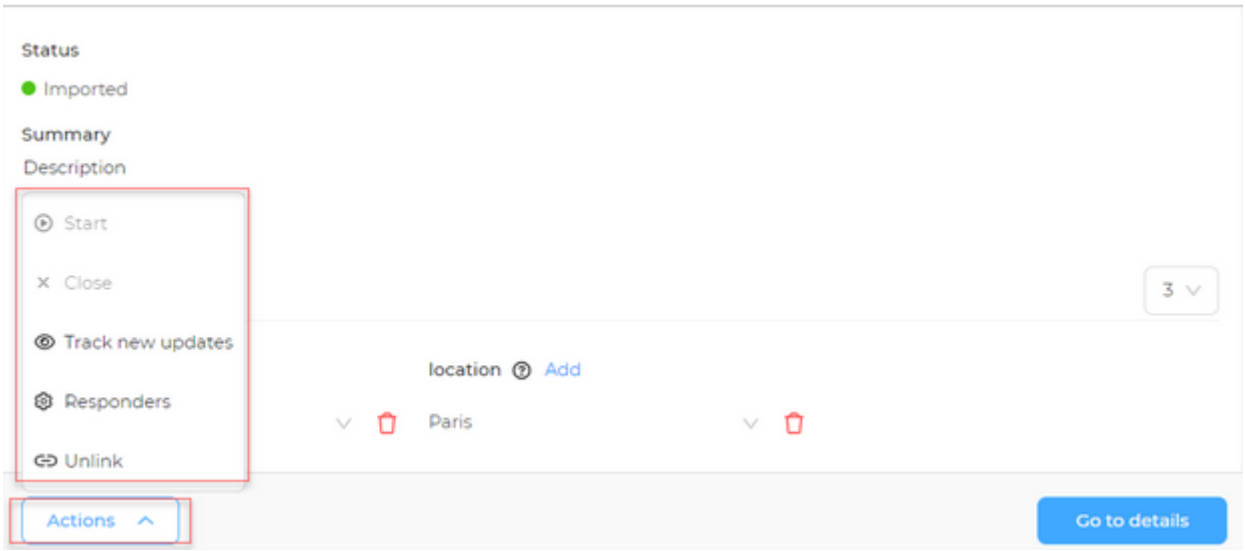
Eylemler

Mevcut eylemlerden herhangi birini kullanabilirsiniz.



Başlangıç

Bir uyarı başlatmak için Başlat (Start option) seçeneğine tıklayın.

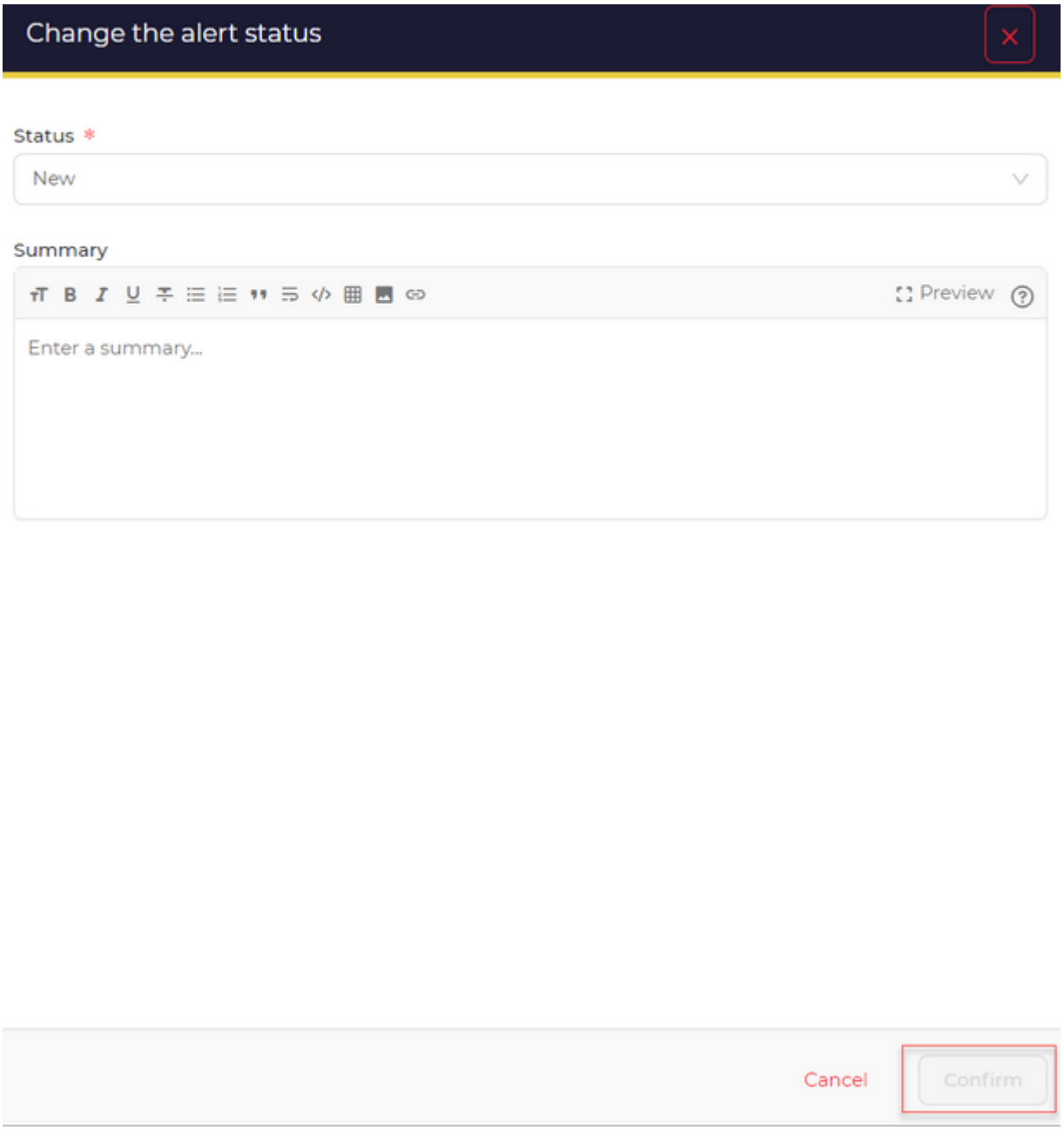


Kapatma

Bir görevi kaldırmak için Kapat seçeneğine tıklayın.

Yeni bir pencere açılır.

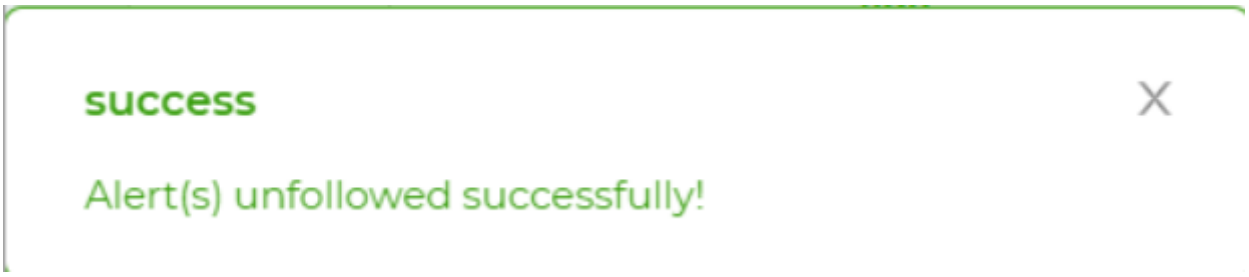
1. Listeden Durum(Status) öğesini seçin.
2. Özeti (Summary) Değiştirin
3. Görevleri ve vakayı kapat düğmesine (Close tasks and case) tıklayın.



Yeni Güncellemeleri İzle/Görmezden Gel

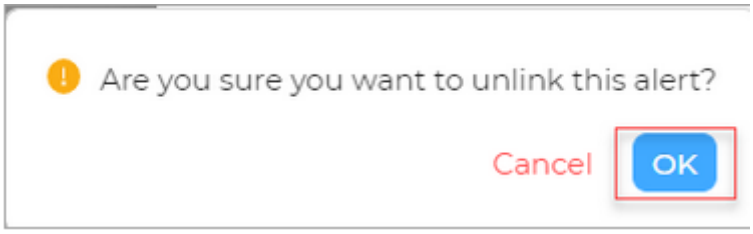
1. Bir uyarıyı izlemek için Yeni Güncellemeleri İzle (Track New Updates) seçeneğine tıklayın.
2. Bir başarı mesajı görüntülenir.

1. Bir uyarıyı yok saymak için Yeni Güncellemeleri Yoksay seçeneğine tıklayın.
2. Bir başarı mesajı görüntülenir.



Bağlantı Kaldırma

1. Bir uyarının bağlantısını kaldırmak için Bağlantıyı Kaldır seçeneğine tıklayın.
2. Tamam düğmesine tıklayın.

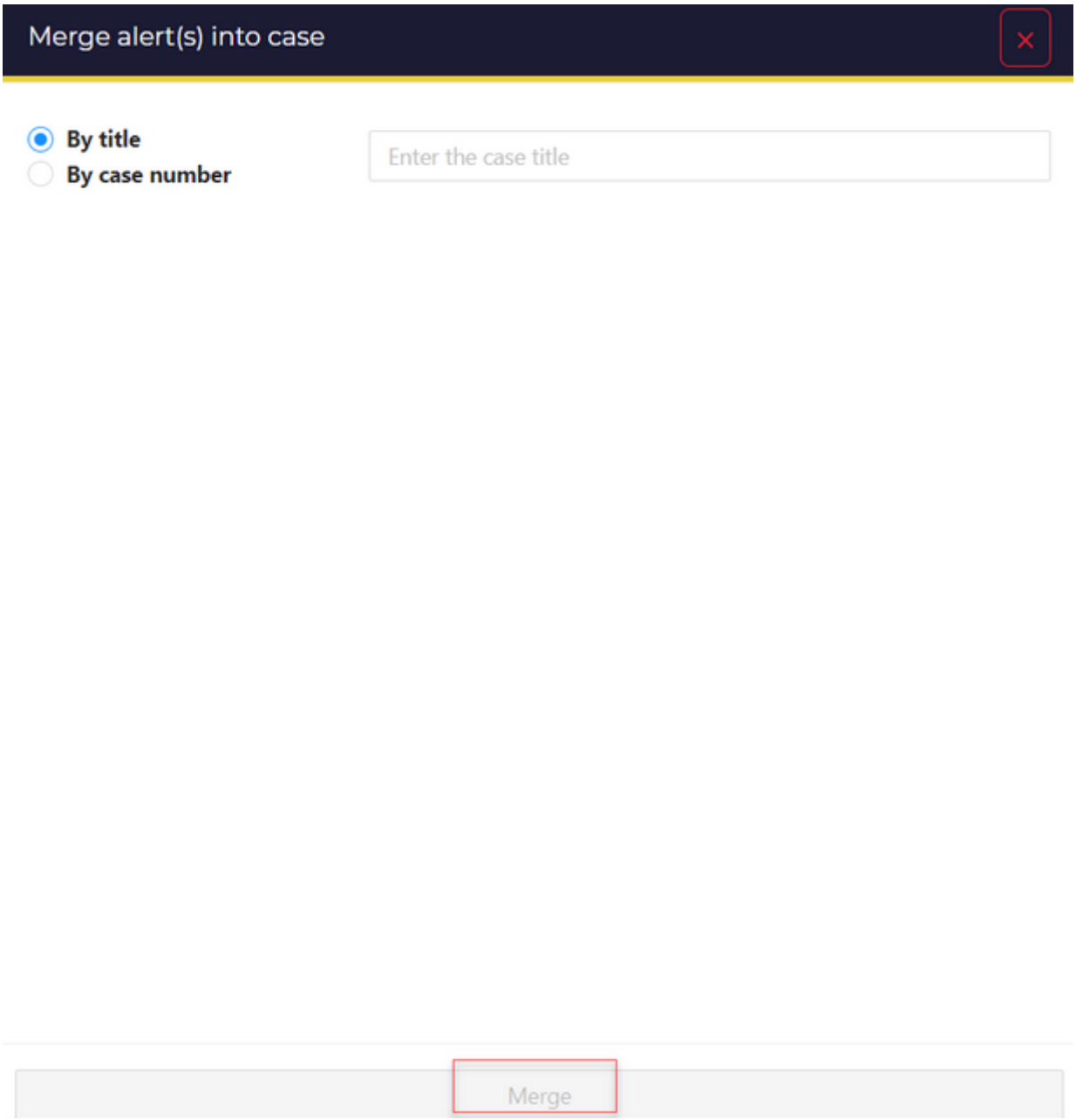


Uyarıları Birleştir

Tüm uyarıların listelendiği ana sayfada çeşitli uyarılar bulunmaktadır. Bazıları yeni, bazıları içe aktarılmış. Uyarıları birleştir / seçimi vakaya birleştir seçeneği yalnızca listedeki Yeni uyarılar için kullanılabilir.

Uyarıları birleştirmek için:

1. Uyarı ayrıntıları sayfasına gidin.
2. Verileri birleştirmek için uyarıyı seçin
3. Uyarıları birleştir'e tıklayın.

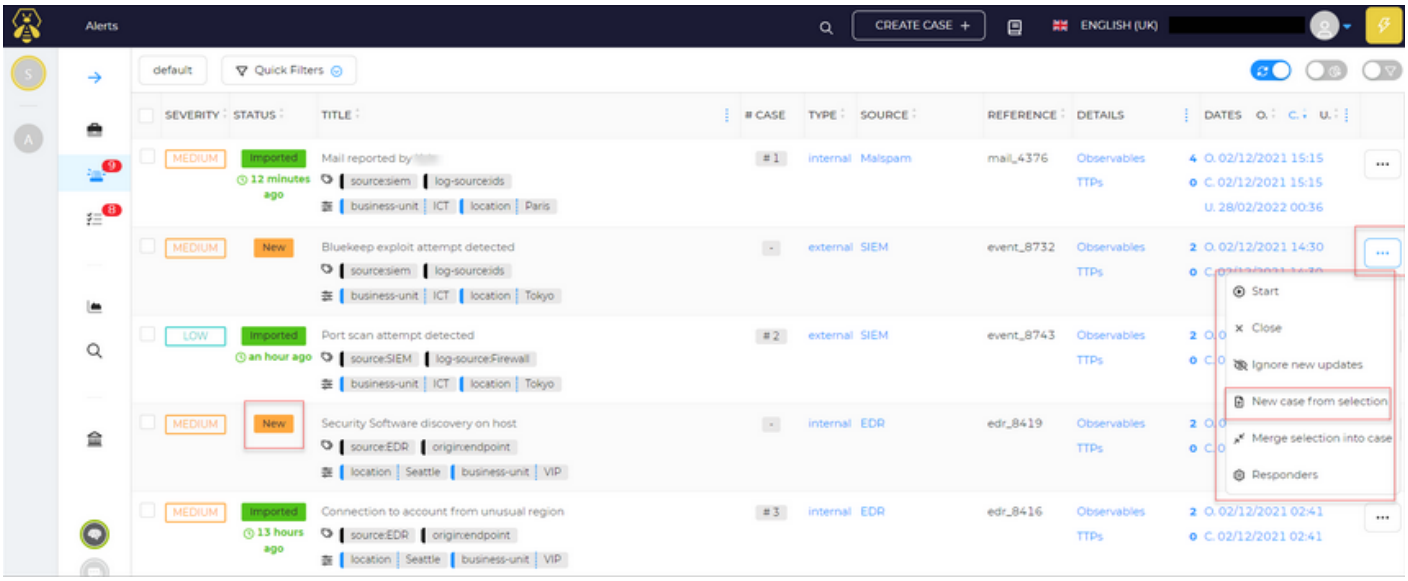


İki vakayı birleştirmek, kaynak vakaları kaldırır ve birleştirilen tüm verilerle yeni bir vaka oluşturur.

Seçimden Yeni Vaka

Bu bölümde seçimden yeni bir vaka oluşturma hakkında bilgi bulabilirsiniz.

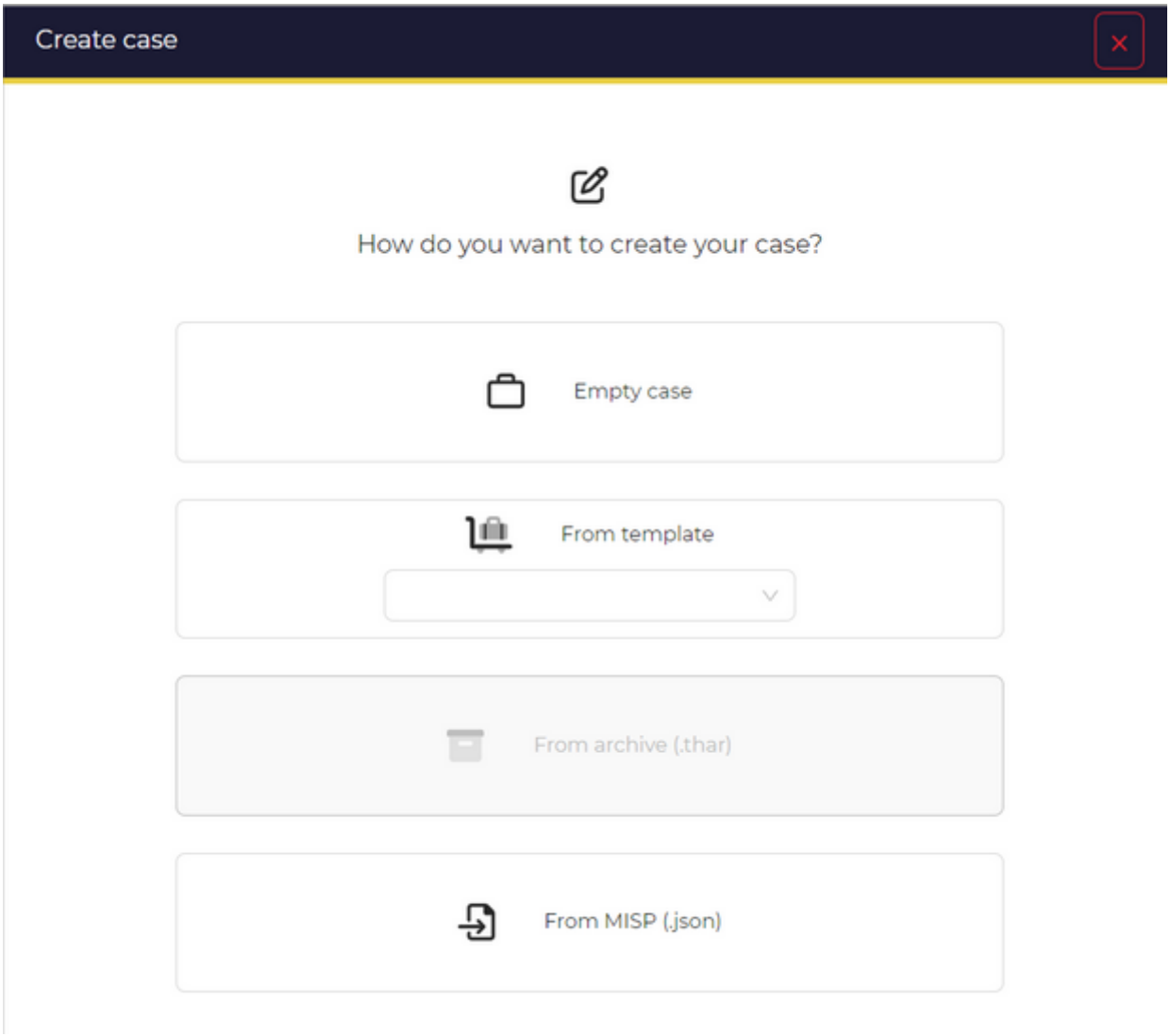
Tüm uyarıların listelendiği ana sayfada çeşitli uyarılar bulunmaktadır. Bazıları yeni, bazıları içe aktarılmış. Seçimden yeni vaka seçeneği sadece listedeki yeni ihbarlar için kullanılabilir.



Seçimden yeni bir vaka eklemek için:

1. Uyarı ayrıntıları sayfasına gidin.
2. Yeni vaka eklemek istediğiniz uyarıyı seçin.
3. Seçim seçeneğinden Yeni Vaka'ya tıklayın.

Yeni bir pencere açılır.



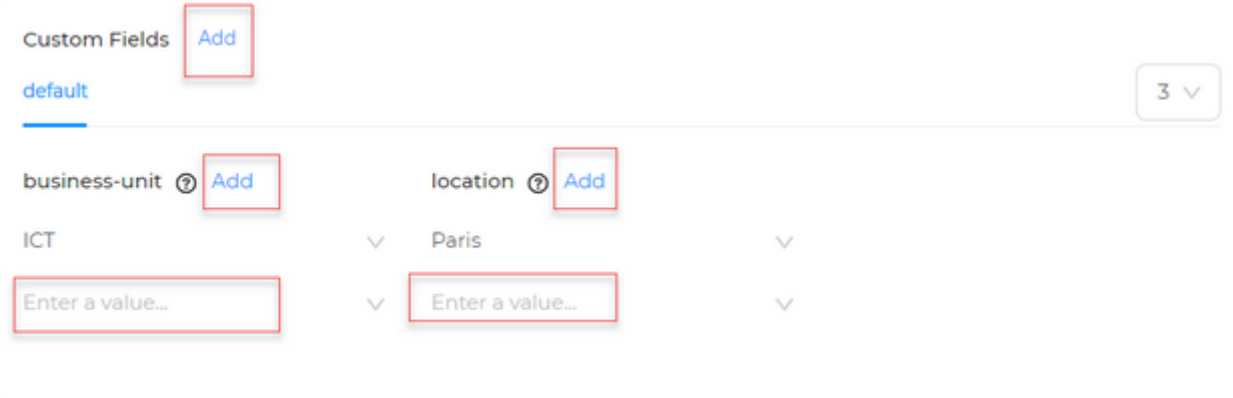
Genel

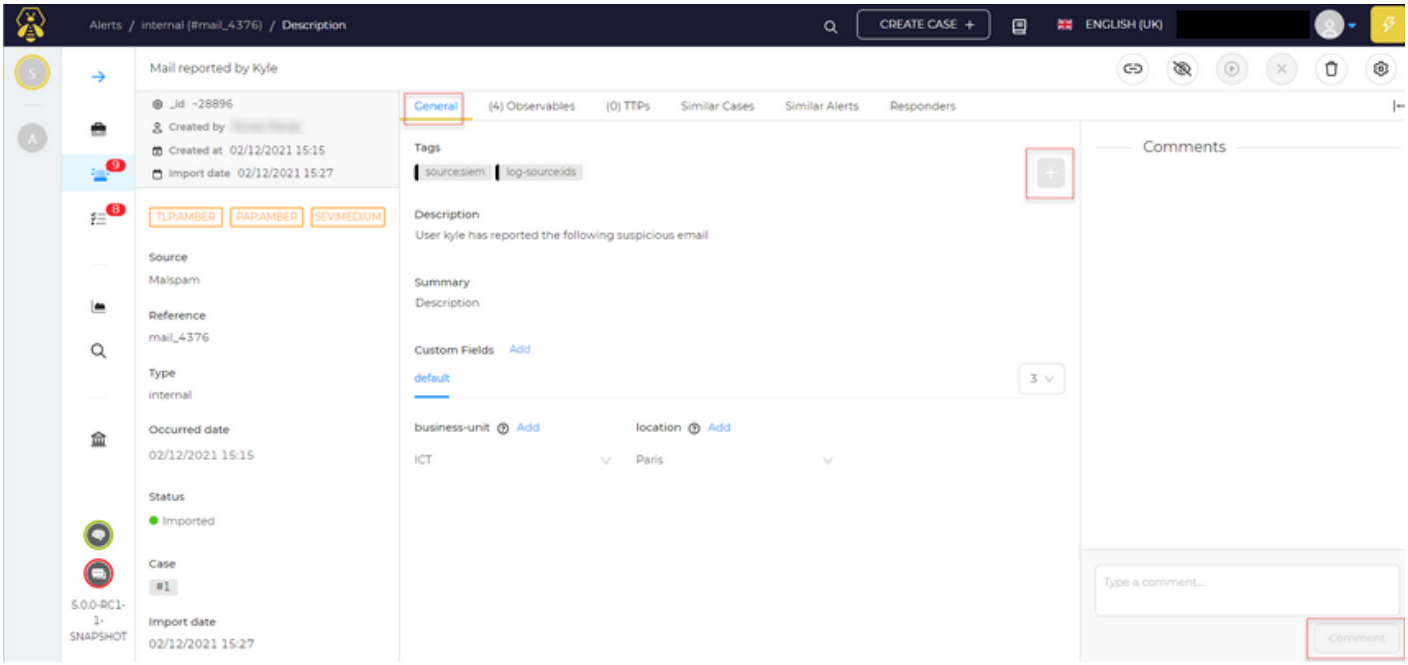
Genel sayfadaki bilgiler şablonlardan gelir ve otomatik olarak doldurulur. Pencerenin sol bölmesinde oluşturulan kişi, oluşturulan tarih, TLP, PAP, önem derecesi ayrıntıları, uyarının durumu, başlangıç tarihi ve görev tamamlama ayrıntıları gibi ayrıntıları görebilirsiniz.

Pencerenin sol bölmesinde PAP, TLP ve Önem derecesini yapılandırabilirsiniz. Daha fazla ayrıntı için Uyarı Ayrıntılarını Yapılandırma bölümüne bakın

Pencerenin sağ bölmesinde, varsa Yorumları (Comments) girin.
Yorum (Comment) düğmesine tıklayın.
Etiketler ekleyin. (Vakalar bölümünde Etiket eklemeye bakın).
Açıklamayı girin.
Özel alanlar (Custom fields) ekleyin.

İlgili iş birimi ve konum ayrıntılarını girmek için Ekle'ye tıklayın.





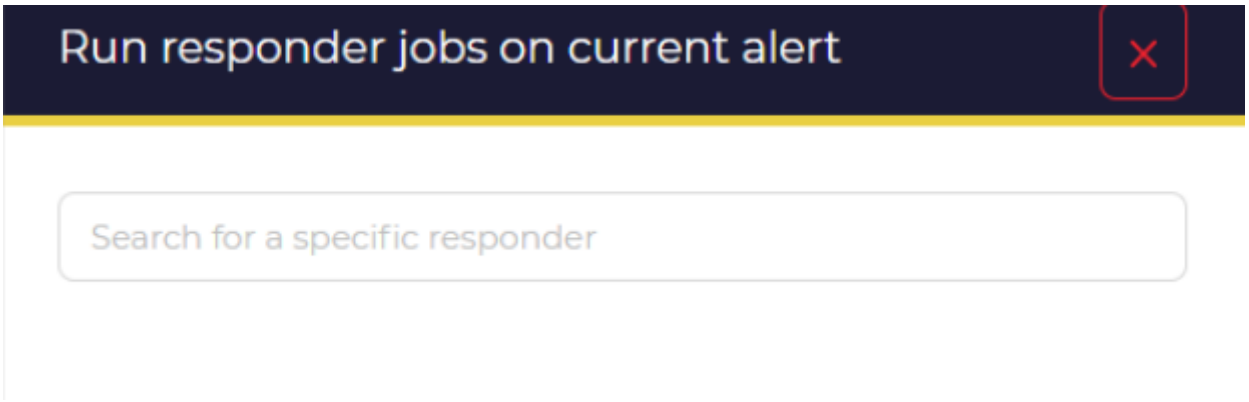
Yanıtlayanlar

Yanıt verenleri çalıştırın

Yanıtlayanlar seçeneğine tıklayın.

Yeni bir pencere görünür.

Arama kutusunda belirli bir yanıtlayıcıyı arayın.

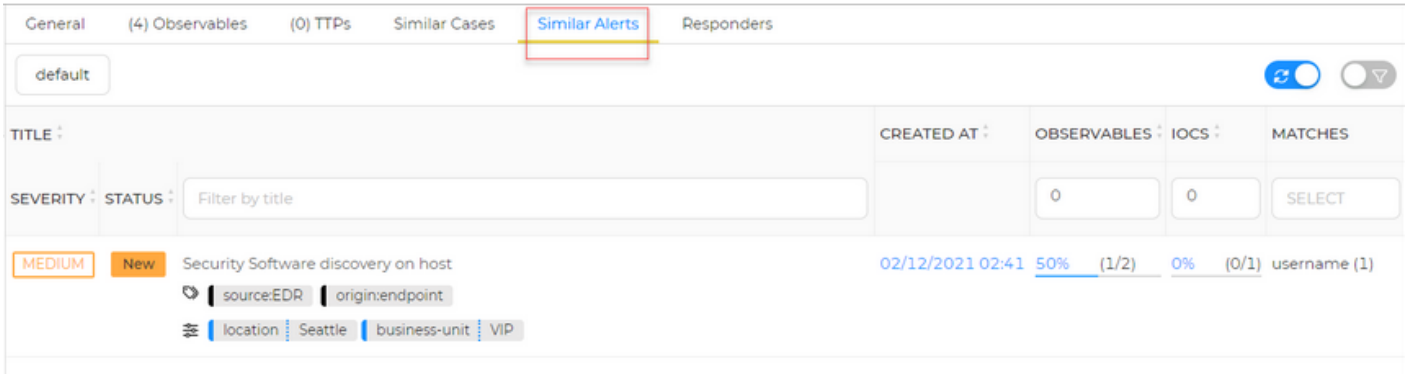


Yanıtlayanları Görüntüle

Responder, ağların altyapısı üzerinde yapılan güvenlik sızma testlerinde kullanılabilecek bir araçtır.

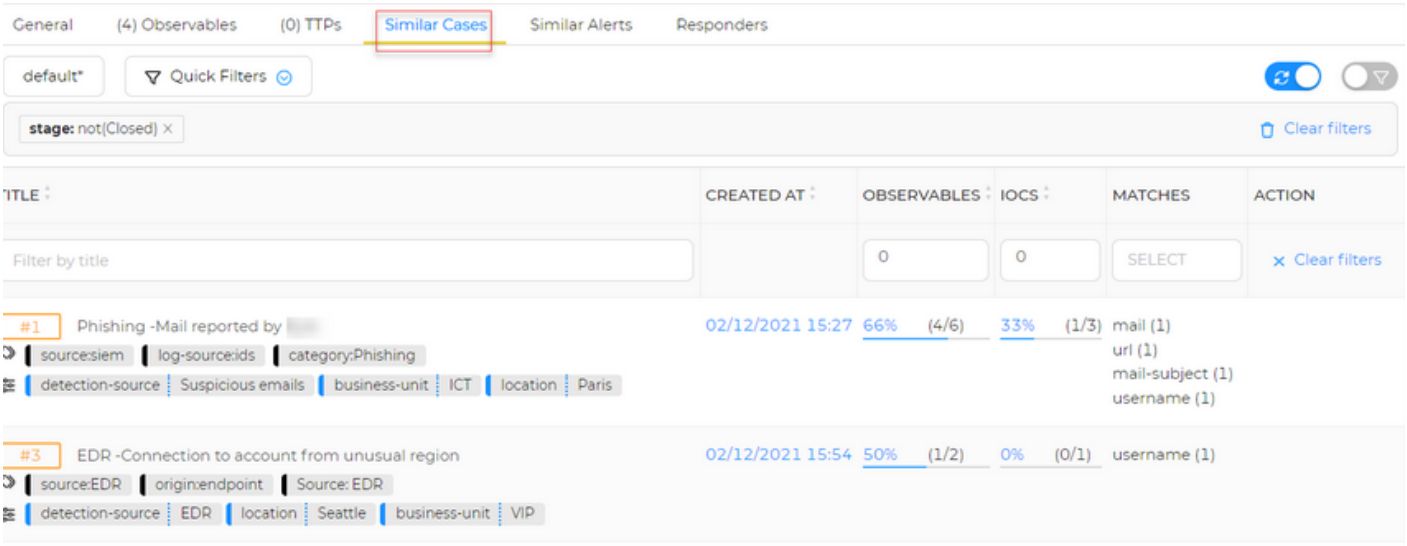
Benzer Uyarıları görüntüleyin

Bu bölümde, aşağıda listelenen tüm benzer uyarılar hakkında bilgi bulabilirsiniz.



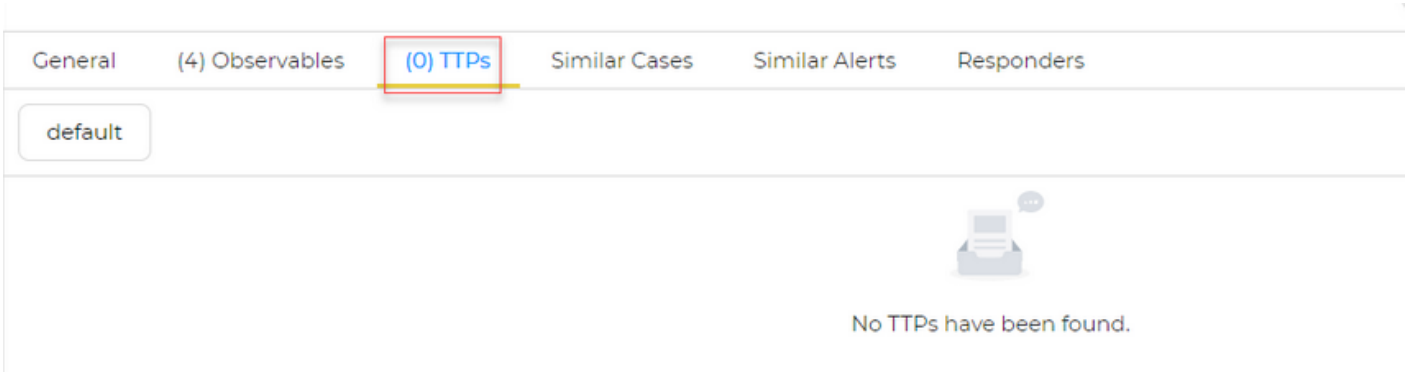
Benzer vakaları görüntüleyin

Bu bölümde, aşağıda listelenen tüm benzer vakalar hakkında bilgi bulabilirsiniz.



TTPS'yi Görüntüleyin

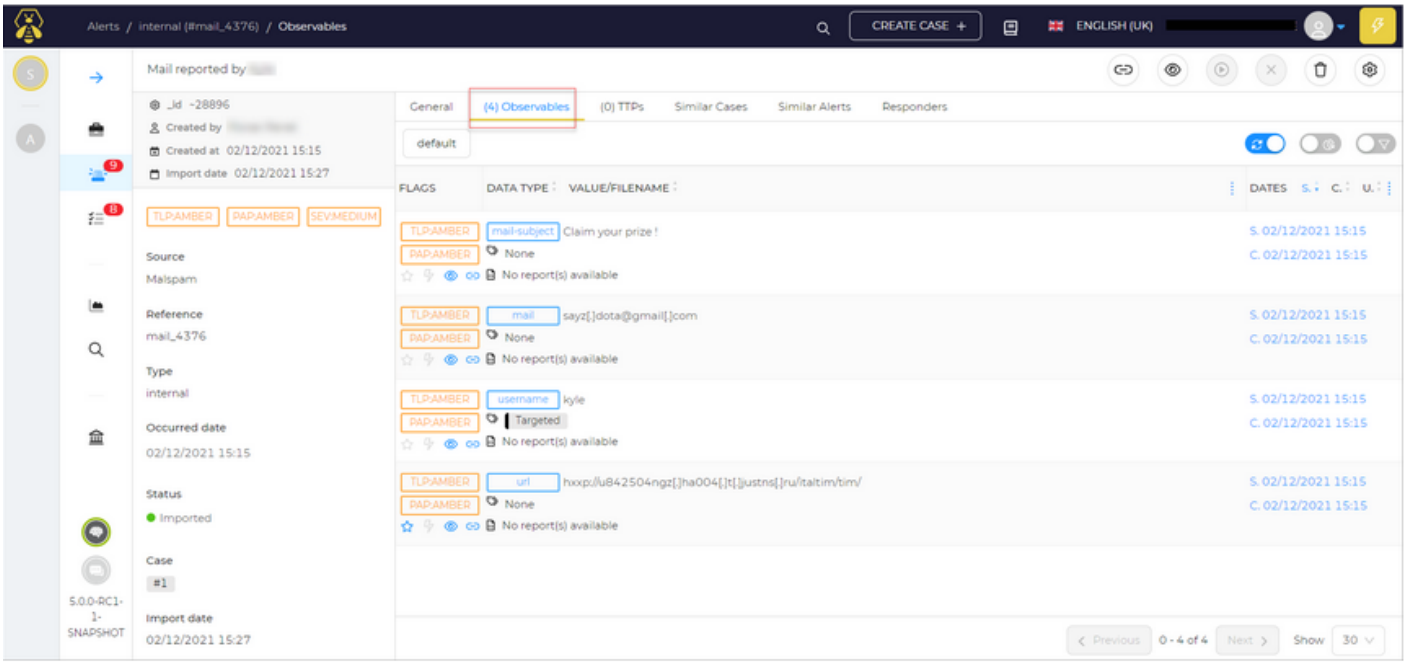
Taktikler, teknikler ve prosedürler (TTP'ler), belirli bir tehdit aktörü veya tehdit aktörleri grubuyla ilişkili faaliyet kalıpları veya yöntemlerdir.



Gözlemlenebilirleri Görüntüle

Bu bölümde gözlemlenebilirleri görüntüleme hakkında bilgi bulabilirsiniz.

TheHive uygulamasını yüklediğinizde, IP ve e-posta adresleri, URL'ler, alan adları, dosyalar veya karmalar gibi önceden tanımlanmış bir dizi gözlemlenebilirle birlikte gelir.



Kendi gözlemlenebilir tipinizi tanımlayabilirsiniz. Tüm Gözlemlenebilir Türlerin listesini görebilirsiniz.

Revision #3
Created 10 April 2024 07:10:56 by Güldeniz Akca
Updated 13 April 2024 15:15:31 by Güldeniz Akca