

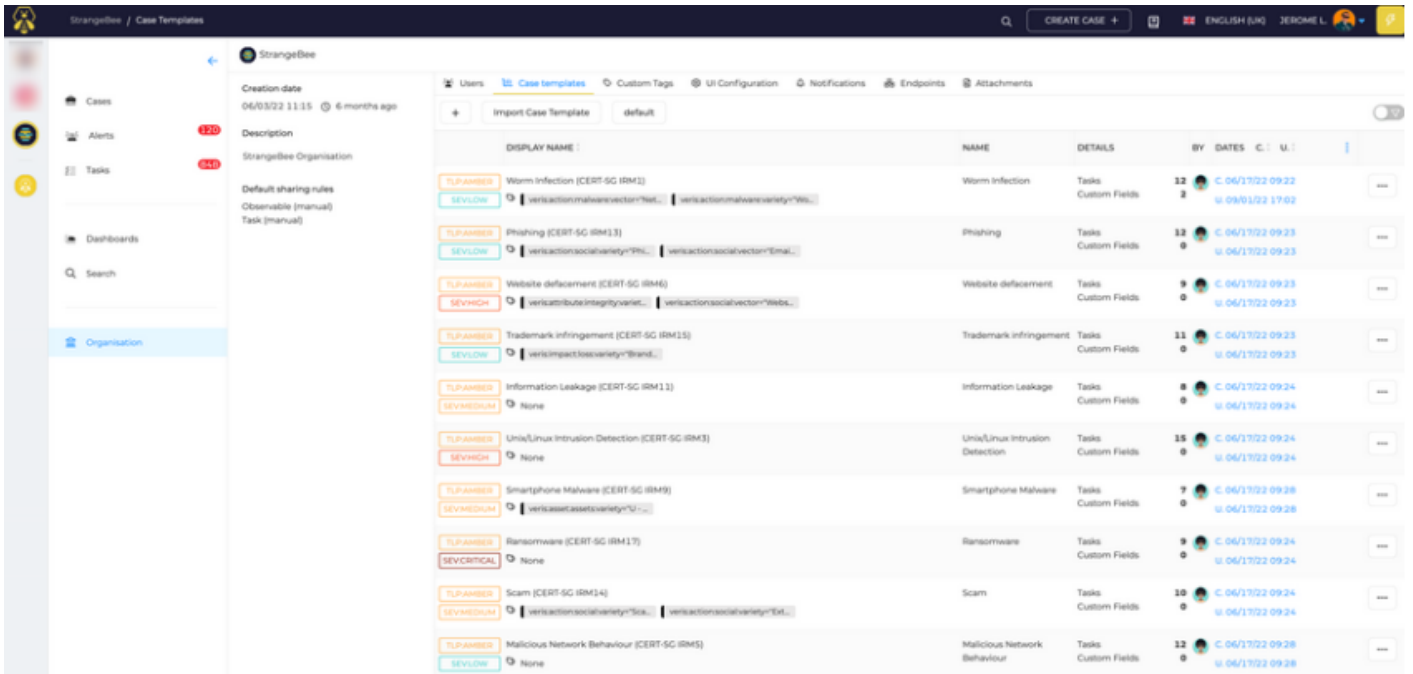
Şablonlar

Vaka Şablonlarını Tanımlama

Bu bölüm, kuruluşunuz için hazırladığınız Vaka şablonlarını içerir.

Vaka Şablonlarının Listesi

Vaka şablonlarının listesine, Kuruluş menüsünü açarak, ardından Şablonlar sekmesini ve Vakalar sekmesini açarak erişebilirsiniz.



| DISPLAY NAME | NAME | DETAILS | BY | DATES | C.I. | U.I. |
|--|--------------------------------|------------------------|----|--|------|------|
| TLP:AMBER SEVLOW Worm Infection (CERT-SG IRM2) | Worm Infection | Tasks Custom Fields | 12 | C: 06/1/2022 09:22 U: 09/9/2022 17:02 | | |
| TLP:AMBER SEVLOW Phishing (CERT-SG IRM13) | Phishing | Tasks Custom Fields | 12 | C: 06/1/2022 09:23 U: 06/1/2022 09:23 | | |
| TLP:AMBER SEVHIGH Website defacement (CERT-SG IRM4) | Website defacement | Tasks Custom Fields | 9 | C: 06/1/2022 09:23 U: 06/1/2022 09:23 | | |
| TLP:AMBER SEVLOW Trademark infringement (CERT-SG IRM15) | Trademark infringement | Tasks Custom Fields | 11 | C: 06/1/2022 09:23 U: 06/1/2022 09:23 | | |
| TLP:AMBER SEVNONE Information Leakage (CERT-SG IRM13) | Information Leakage | Tasks Custom Fields | 8 | C: 06/1/2022 09:24 U: 06/1/2022 09:24 | | |
| TLP:AMBER SEVHIGH Unix/Linux Intrusion Detection (CERT-SG IRM3) | Unix/Linux Intrusion Detection | Tasks Custom Fields | 15 | C: 06/1/2022 09:24 U: 06/1/2022 09:24 | | |
| TLP:AMBER SEVNONE Smartphone Malware (CERT-SG IRM9) | Smartphone Malware | Tasks Custom Fields | 7 | C: 06/1/2022 09:28 U: 06/1/2022 09:28 | | |
| TLP:AMBER SEVCRITICAL Ransomware (CERT-SG IRM17) | Ransomware | Tasks Custom Fields | 9 | C: 06/1/2022 09:24 U: 06/1/2022 09:24 | | |
| TLP:AMBER SEVNONE Scam (CERT-SG IRM14) | Scam | Tasks Custom Fields | 10 | C: 06/1/2022 09:24 U: 06/1/2022 09:24 | | |
| TLP:AMBER SEVLOW Malicious Network Behaviour (CERT-SG IRM5) | Malicious Network Behaviour | Tasks Custom Fields | 12 | C: 06/1/2022 09:28 U: 06/1/2022 09:28 | | |

Yeni bir Vaka şablonu oluşturmak için düğmesine tıklayın.

Yeni Vaka Şablonu

Adding a Case Template

Prefix
Case template title prefix...

Name
Worm infection

Display name
Worm infection (CERT-5G (RM1))

TLP
TLP-CLEAR TLP-GREEN **TLP-AMBER** TLP-AMBER-STRICT TLP-RED

PAP
PAP-CLEAR PAP-GREEN **PAP-AMBER** PAP-RED

Severity
LOW MEDIUM HIGH CRITICAL

Tags
CERT:5G:malicious-coder:worm

Description
Worm infection

Tasks

| | | |
|---|------|--------|
| Preparation - Preparation | Edit | Delete |
| Identification - Detect the infection | Edit | Delete |
| Identification - Identify the infection | Edit | Delete |
| Containment - Containment | Edit | Delete |
| Remediation - Identify | Edit | Delete |
| Remediation - Test | Edit | Delete |
| Remediation - Deploy | Edit | Delete |
| Remediation - Recovery | Edit | Delete |
| Aftermatch - Report | Edit | Delete |
| Aftermatch - Capitalize | Edit | Delete |

Custom fields

| | | |
|------------------------|------|--------|
| string - business-unit | Edit | Delete |
|------------------------|------|--------|

Pages

| | |
|--------------------------|--------|
| Aftermatch - Learn | Remove |
| Aftermatch - Post Mortem | Remove |

Cancel Confirm case template addition

Yapılandırma Parametreleri

Önek

Bu şablonla oluşturulan bir Vakanın başlığına öne eklenen dize

Ad

Vaka şablonunun adı. API ile Vaka şablonunu tanımlamak için kullanılır

Görüntülenen Ad

Arayüzde görüntülenen Vaka şablonunun adı

TLP

Bu şablonla oluşturulan Vakanın varsayılan TLP'si

PAP

Bu şablonla oluşturulan Vakanın varsayılan PAP'ı

Ciddiyet

Bu şablonla oluşturulan Vakanın varsayılan

Ciddiyeti Etiketler

Bu şablonla oluşturulan Vakalara eklenecek etiketlerin listesi

Açıklama

Değiştirilmediği takdirde, bu şablonla oluşturulan Vakaların varsayılan açıklaması

Görevler

Şablonlara görevler ekleyin. Bunlar, bu şablonla oluşturulan Vakalara otomatik olarak eklenir

Özel Alanlar

Şablona Özel alanlar ekleyin. Özel alanlar için varsayılan değer de ayarlanabilir

Sayfalar

Şablona sayfa şablonları ekleyin. Bunlar, bu şablonla oluşturulan Vakalara otomatik olarak eklenir

Dışa Aktarım/İçe Aktarım

Vaka Şablonunu Dışa Aktarma

Vaka şablonları, seçenek ... simgesine tıklayarak ve |-> Dışa Aktar seçeneğini seçerek JSON dosyaları olarak dışa aktarılabilir.

| | | | | | | |
|-------------------------------------|---|-------------------------|------------------------|--------|--|-----|
| TLP:AMBER SEV:LOW | Phishing (CERT-SG IRM16) None | IRM-16-Phishing | Tasks Custom Fields | 6 0 | C. 2022-12-07 18:13 U. 2022-12-08 15:35 | ... |
| TLP:AMBER SEV:HIGH | Website Defacement (CERT-SG IRM6) None | IRM-6-WebsiteDefacement | Tasks Custom Fields | 6 0 | C. 2022-12-06 15:13 U. 2022-12-06 16:01 | ... |
| TLP:AMBER SEV:LOW | Blackmail (CERT-SG IRM8) None | IRM-8-Blackmail | Tasks Custom Fields | 6 0 | C. 2022-12-06 15:13 U. 2022-12-06 16:01 | ... |
| TLP:AMBER SEV:HIGH | Insider Abuse (CERT-SG IRM 12) None | IRM-12-InsiderAbuse | Tasks Custom Fields | 6 0 | C. 2022-12-06 17:31 U. 2022-12-06 17:31 | ... |

Bir Vaka Şablonunu İçe Aktarma

Vaka Şablonunu İçe Aktar düğmesine tıklayın ve içe aktarılacak JSON formatlı dosyayı seçin.

Importing a Case Template

Case Template
You can use the exported case template directly from TheHive platform

Attachment

Drop file or click

worm-infection.json

The file must be a valid JSON file

Name of case template

smishing infection

The name of the case template is unique, rename it if you already use this name

Sayfa Şablonlarını Tanımlama

Bu bölüm, kuruluşunuz için hazırladığınız Sayfa şablonlarını içerir.

Sayfa Şablonlarının Listesi

Organizasyon menüsünü, ardından Şablonlar sekmesini ve Sayfalar sekmesini açarak listeye erişin.

| CATEGORY : | TITLE : | DETAILS | BY | DATES | C. : | U. : | |
|------------|-------------|-----------------------|----|---------------------|------|------|-----|
| Aftermatch | Post Mortem | Linked case templates | 2 | C. 27/06/2023 08:32 | | | ... |
| Aftermatch | Learnt | Linked case templates | 2 | C. 27/06/2023 08:32 | | | ... |

Yeni bir Sayfa şablonu oluşturmak için "+"düğmesine tıklayın.

Yeni Sayfa Şablonu

create a new page template

Title

Enter a title

Category

Enter a category

Content

Preview

Yapılandırma Parametreleri

Başlık

Sayfa şablonu başlığı. API ile Sayfa şablonunu tanımlamak için kullanılır. Ayrıca şablon bir vakada kullanıldığında sayfa başlığı olarak da kullanılır.

Kategori

Sayfaları ortak bir tema altında gruplamak için kategori. Vakada sayfa ağacı olarak kullanılır.

İçerik

Sayfa şablonu bir vakada kullanıldığında varsayılan sayfa içeriği.

Dışa Aktarım/İçe Aktarım

Bir Sayfa Şablonunu Dışa Aktar

Sayfa şablonları, seçenek ... simgesine tıklayarak ve |-> Dışa Aktar seçeneğini seçerek JSON dosyaları olarak dışa aktarılabilir.

Users Templates Custom Tags UI Configuration Notifications Endpoints Functions^{BETA} Attachments

Cases Pages Reports

+ Import Page Template default

| CATEGORY : | TITLE : | DETAILS | BY | DATES | C. : | U. : | |
|------------|-------------|-----------------------|----|---------------------|------|------|-----|
| Aftermatch | Post Mortem | Linked case templates | 2 | C. 27/06/2023 08:32 | | | ... |
| Aftermatch | Learnt | Linked case templates | 2 | C. 27/06/ | | | ... |

- Edit
- Export page template
- Delete

Sayfa Şablonunu İçe Aktar

Sayfa Şablonunu İçe Aktar düğmesine tıklayın ve içe aktarılacak JSON formatlı dosyayı seçin.

Importing a Page Template

Page Template
You can use the exported page template directly from TheHive platform

Attachment

Drop file or click

aftermatch-learnt.json

The file must be a valid JSON file

Title of page template

Learnt

Rapor Şablonlarını Tanımlama

Bu bölüm, kuruluşunuz için hazırladığınız rapor şablonlarını içerir.

Rapor Şablonlarının Listesi

Rapor şablonlarının listesine, Kuruluş menüsünü açarak, ardından Şablonlar sekmesini ve Raporlar sekmesini açarak erişebilirsiniz.

Template

Add variable ▾

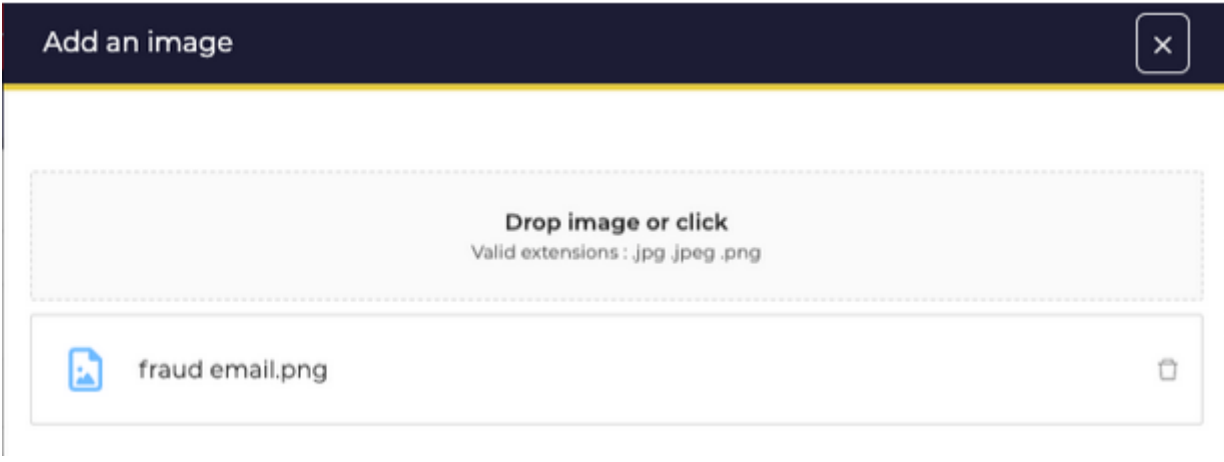


Preview ?

```
# {{case.title}}  
  
Case ID: {{case.number}}  
Date and Time of Incident: {{case.startDate}}  
Severity Level: {{case.severity}}  
TLP: {{case.tlp}}  
PAP: {{case.pap}}
```

Metin Widget'ı

İçerik tanımlamak için bir metin kutusu tanımlamak mümkündür.

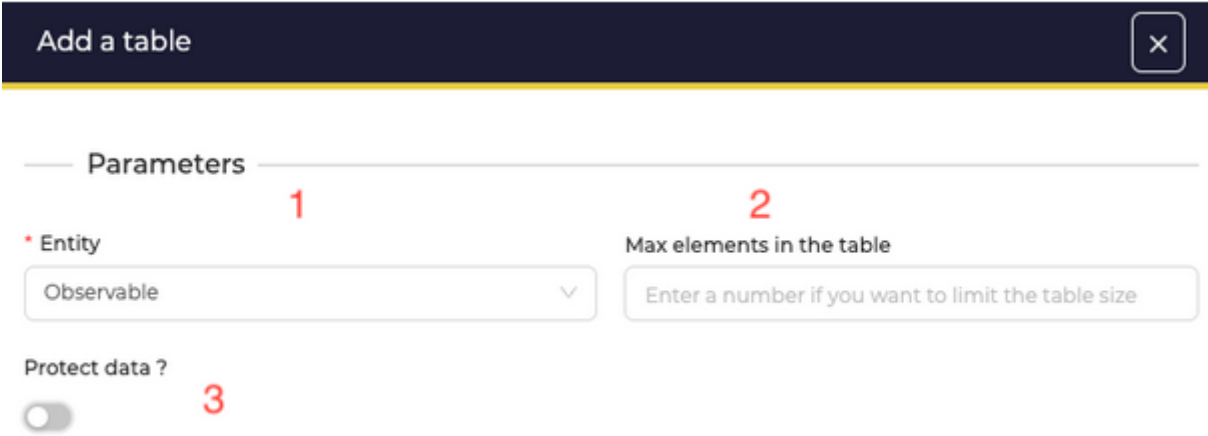


Tablo Bileşeni

Vaka öğelerini içeren tablolar ekleyin.

Parametreler :

- **Varlık Tanımlama:** Hangi vaka öğelerinin tabloda görüntüleneceğini seçmek için varlık tanımlayın.
- **Maksimum Öğe Sayısı:** Tabloda görüntülenecek maksimum öğe sayısını tanımlamak mümkündür.
- **Bilgi Koruması:** Gözlemlenenlerin görüntülenmesinde bilgi korumasını etkinleştirmek mümkündür.



Veri Sütunları

- Bileşen eklendiğinde, en ilgili bilgiler otomatik olarak ön seçilir. Bununla birlikte, yeni sütunlar her zaman eklenebilir.
- Sütunların sırasını yeniden tanımlamak için sürükleyin ve bırak kullanılabilir.
- Son olarak, herhangi bir sütunu silmek için öğenin çarpı düğmesine tıklayarak silmek mümkündür.

Data list

- title ×
- group ×
- assignee × **2**
- status ×
- startDate ×

1 + Add a line

Tasks logs ? ⓘ

Sorts

No sort selected [Add a sort](#)

Filters

- description
- dueDate
- endDate
- flag
- mandatory
- _createdAt
- _createdBy
- _updatedAt

Sıralamalar

- Tablo bilgilerinin sıralanması mümkündür.
- Tablonun hangi verilere göre filtrelenmesi gerektiğini belirtin.
- Sıralama düzenini seçin.
- Birden fazla sıralama verisi ekleyin.
- Gereksiz sıralama verilerini silin.

1 Sorts

- 2** tip **3** desc ×
- _createdAt asc **5** ×

4 + Add a sort

Filtreler

- Tabloya veri miktarını sınırlamak için filtreler ekleyebilirsiniz.

- Seçilen varlıktan herhangi bir bilgiyi seçin.
- Filtrenmesi gereken operatörü belirtin.
- Kontrol değerlerini tanımlayın.
- Birden çok filtre eklenebilir.
- Bir filtreyi silmek için çarpı düğmesini kullanın.
- Son olarak, uygulanacak tüm filtreleri temizleyebilirsiniz.

1 Filters

6

sighted: true x

pap: not(red) x

tip: not(amber+strict, red) x

5+ Add filter
 7 Clear filters

Veri Listesi

Vaka öğelerini içeren bir liste ekleyin.

Parametreler:

- Liste içinde görüntülenecek vaka öğelerini seçmek için varlık tanımlayın.
- Listede görüntülenecek maksimum öğe sayısını tanımlamak mümkündür.
- Gözlemlenenlerin görüntülenmesinde bilgi korumasını etkinleştirmek mümkündür.

Add a table
x

Parameters

1

* Entity

2

Max elements in the table

Protect data ?

3

Veri Listesi

- Bileşen eklendiğinde, en ilgili bilgiler otomatik olarak ön seçilir. Ancak, istenilen zaman yeni veriler eklenebilir.
- Verilerin sırasını yeniden tanımlamak için sürükle ve bırak yöntemi kullanılabilir.
- Son olarak, herhangi bir veriyi silmek için öğenin üzerinde bulunan çarpı düğmesine tıklanabilir.

Data list

title x

group x

assignee x

status x

startDate x

1 + Add a line

Tasks logs ?

Sorts

No sort selected [Add a sort](#)

Filters

description

dueDate

endDate

flag

mandatory

_createdAt

_createdBy

_updatedAt

Sıralamalar

- Liste bilgilerini sıralamak mümkündür.
- Listenin hangi verilere göre filtrelenmesi gerektiğini belirtin.
- Sıralama düzenini seçin.
- Birden fazla sıralama verisi ekleyin.
- Gereksiz sıralama verilerini silin.

1 Sorts

2 tlp desc 3

_createdAt asc 5 x

4 + Add a sort

Filtreler

- Listenin içindeki verileri sınırlamak için filtreler ekleyebilirsiniz.
- Seçilen varlıktan herhangi bir bilgiyi seçin.
- Filtrenmesi gereken operatörü belirtin.
- Kontrol değerlerini tanımlayın.
- Birden çok filtre ekleyebilirsiniz.
- Bir filtreyi silmek için çarpı düğmesini kullanın.
- Son olarak, uygulanacak tüm filtreleri temizleyebilirsiniz.

1 Filters

sighted true 6

pap 3 not 4 red

tlp not amber+strict red

2

sighted: true x pap: not(red) x tlp: not(amber+strict, red) x

5 + Add filter 7 Clear filters

Altbilgi

Altbilgi, metin biçimlendirme içeriği ile oluşturulur. Altbilgiyi tanımlamak zorunlu değildir.

Template

Add variable v

RT B I U T L R S C D G H I J K L M N O P Q R S T U V W X Y Z

Preview ?

```
Reporter : {{case._createdBy}}
Assignee : {{case.assignee}}
Close date : {{case.closedDate}}
```

Bileşenleri Düzenleme

- Bir bileşen rapora eklendiğinde, istenilen konuma sürüklenerek bırakılabilir.
- Bir öğeyi raporun sonuna yerleştirmek için istenen bileşen düğmesine tıklanabilir.
- Bileşenlerin sırası istenildiği zaman yeniden düzenlenebilir.
- Başlık ve altbilgi hareket ettirilemez.

The screenshot shows a report editor interface with the following components:

- Top Navigation:** Users, Templates (selected), Custom Tags, UI Configuration, Notifications, Endpoints, Functions^{BETA}, Attachments.
- Report Editor:** Cases, Pages, Reports (selected). A red '2' is next to the text editor icon.
- Task List:** A section with fields for Title, Group, Assignee, Status, StartDate, EndDate, and Logs. A red '3' is next to the 'Observable Table' icon.
- Observable Table:** A table with columns: dataType, data, _createdAt, tip, pap.
- Bottom:** A dashed box with a red '1' and the text 'Drag me here!'.

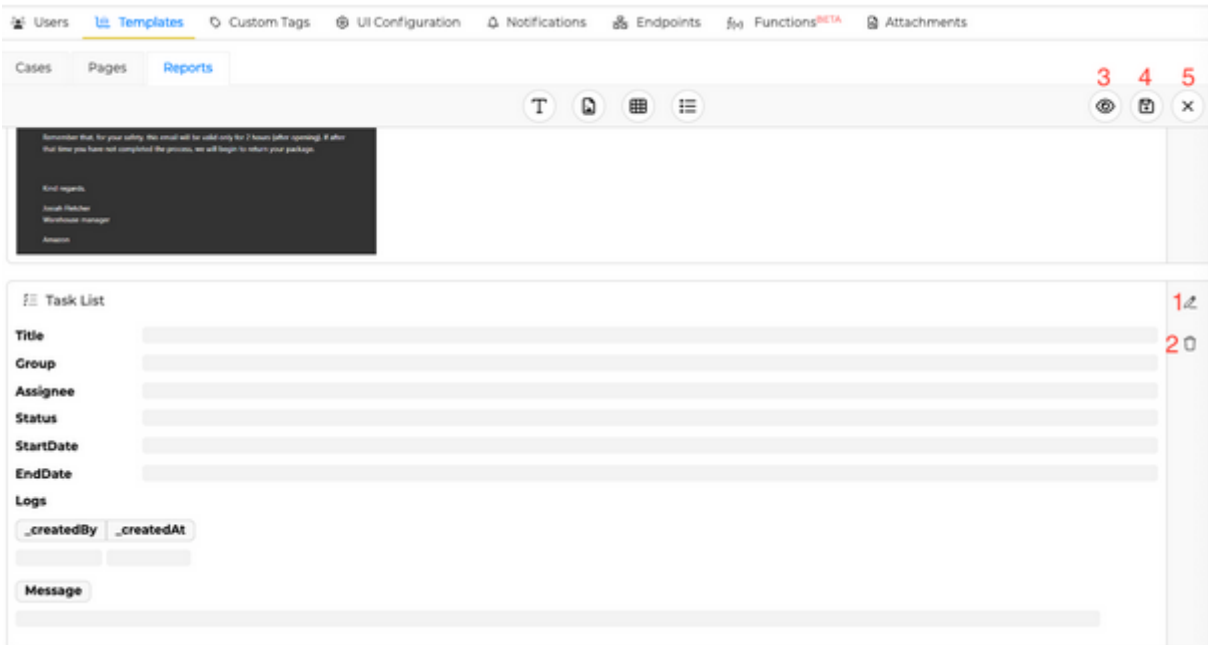
Rapor Üzerindeki İşlemler

- Rapor içindeki herhangi bir bileşeni düzenleme

- Başlık ve altbilgi hariç herhangi bir bileşeni silme
- Raporu önizleme



- Raporu istediğiniz zaman kaydedin
- Rapor listesine dönmek için rapor düzenlemeden çıkın



Revision #2

Created 9 April 2024 12:49:39 by Güldeniz Akca

Updated 17 April 2024 17:26:47 by Güldeniz Akca