

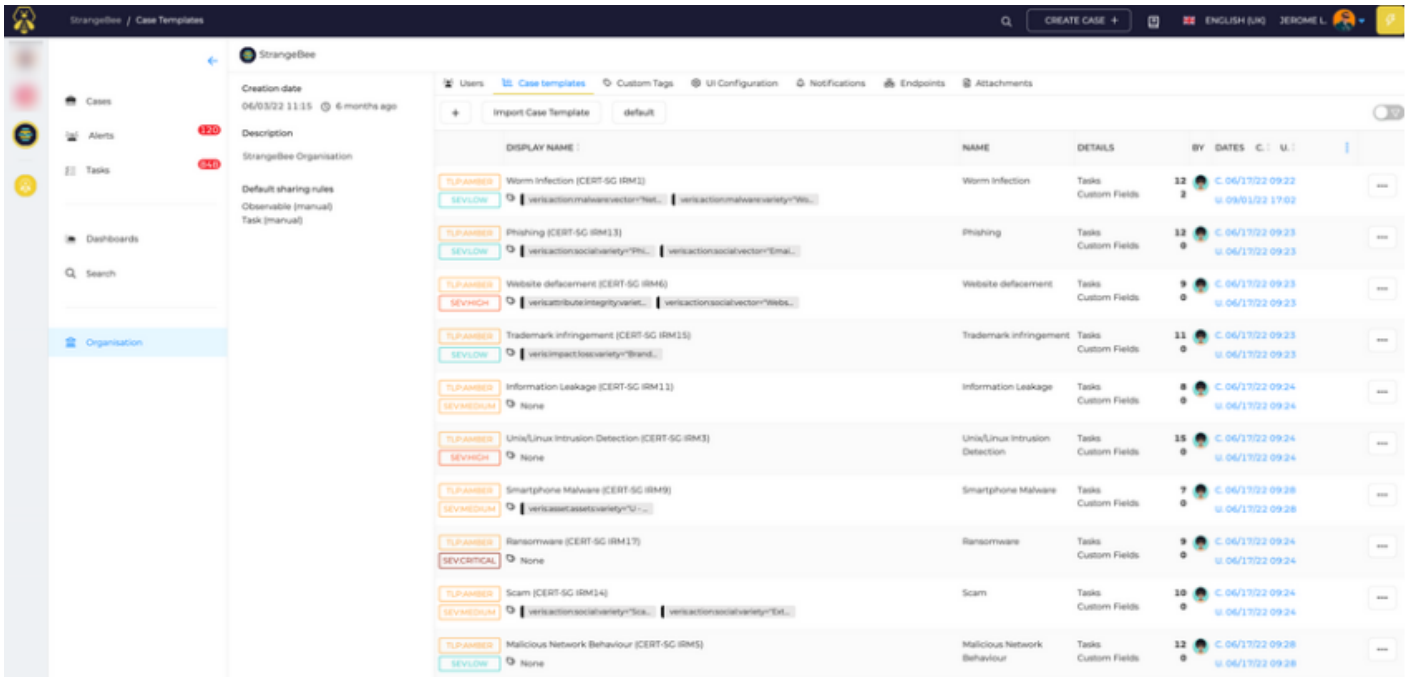
Şablonlar

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 Worm Infection (CERT-SG IRM2) SEV:LOW	Worm Infection	Tasks Custom Fields	12	C: 04/1/2022 09:22 U: 09/9/2022 17:02		
TLP:AMBER Phishing (CERT-SG IRM13) SEV:LOW	Phishing	Tasks Custom Fields	12	C: 04/1/2022 09:23 U: 04/1/2022 09:23		
TLP:AMBER Website defacement (CERT-SG IRM4) SEV:HIGH	Website defacement	Tasks Custom Fields	9	C: 04/1/2022 09:23 U: 04/1/2022 09:23		
TLP:AMBER Trademark infringement (CERT-SG IRM15) SEV:LOW	Trademark infringement	Tasks Custom Fields	11	C: 04/1/2022 09:23 U: 04/1/2022 09:23		
TLP:AMBER Information Leakage (CERT-SG IRM13) SEV:MEDIUM	Information Leakage	Tasks Custom Fields	8	C: 04/1/2022 09:24 U: 04/1/2022 09:24		
TLP:AMBER Unix/Linux Intrusion Detection (CERT-SG IRM3) SEV:HIGH	Unix/Linux Intrusion Detection	Tasks Custom Fields	15	C: 04/1/2022 09:24 U: 04/1/2022 09:24		
TLP:AMBER Smartphone Malware (CERT-SG IRM9) SEV:MEDIUM	Smartphone Malware	Tasks Custom Fields	7	C: 04/1/2022 09:28 U: 04/1/2022 09:28		
TLP:AMBER Ransomware (CERT-SG IRM17) SEV:CRITICAL	Ransomware	Tasks Custom Fields	9	C: 04/1/2022 09:24 U: 04/1/2022 09:24		
TLP:AMBER Scam (CERT-SG IRM14) SEV:MEDIUM	Scam	Tasks Custom Fields	10	C: 04/1/2022 09:24 U: 04/1/2022 09:24		
TLP:AMBER Malicious Network Behaviour (CERT-SG IRM5) SEV:LOW	Malicious Network Behaviour	Tasks Custom Fields	12	C: 04/1/2022 09:28 U: 04/1/2022 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 - Learnit

Remove

Aftermatch - Post Mortem

Remove

Cancel

Confirm case template edition

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.

<div>TLP:AMBER</div> <div>SEV:LOW</div>	Phishing (CERT-SG IRM16)	IRM-16-Phishing	Tasks Custom Fields	6 0	<div><div></div><div>C. 2022-12-07 18:13</div><div>U. 2022-12-08 15:35</div></div>	...
<div>TLP:AMBER</div> <div>SEV:HIGH</div>	Website Defacement (CERT-SG IRM6)	IRM-6-WebsiteDefacement	Tasks Custom Fields	6 0	<div><div></div><div>C. 2022-12-06 15:13</div><div>U. 2022-12-06 15:13</div></div>	...
<div>TLP:AMBER</div> <div>SEV:LOW</div>	Blackmail (CERT-SG IRM8)	IRM-8-Blackmail	Tasks Custom Fields	6 0	<div><div></div><div>C. 2022-12-06 15:13</div><div>U. 2022-12-06 15:13</div></div>	<div><div>Edit</div><div>Export case template</div><div>Delete</div></div>
<div>TLP:AMBER</div> <div>SEV:HIGH</div>	Insider Abuse (CERT-SG IRM 12)	IRM-12-InsiderAbuse	Tasks Custom Fields	6 0	<div><div></div><div>C. 2022-12-06 17:31</div><div>U. 2022-12-06 17:31</div></div>	...

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.

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. 27/06/2023 08:32					...

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

Yeni Sayfa Şablonu

Users	Templates	Custom Tags	UI Configuration	Notifications	Endpoints	Functions	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/			...
							...

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

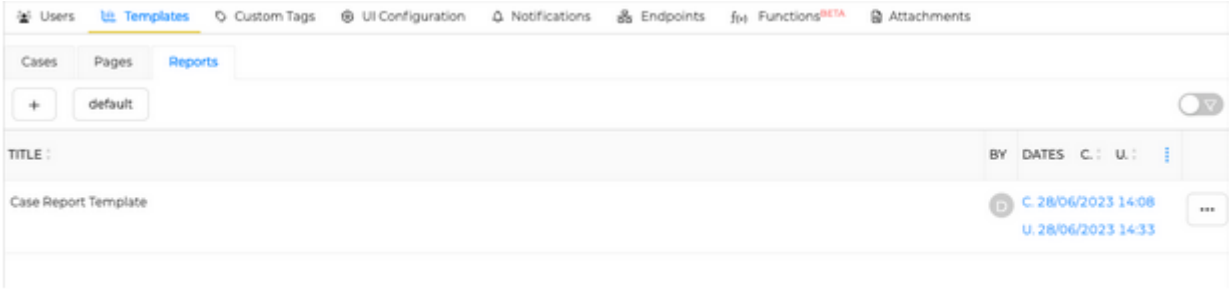
Learnt

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.



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

Yeni Rapor Şablonu

Create a report template

Title

Case Report Template

Description

This template provides a structured format for documenting and reporting cybersecurity cases. It includes relevant information such as case details, incident analysis, actions taken, and recommendations for enhancing security measures.

Yapılandırma Parametreleri

Rapor başlığını ve açıklamasını tanımlayın.

Başlık

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

Açıklama

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

İçerik

Sayfa şablonu bir vakada kullanıldığında varsayılan sayfa içeriği.

Ardından, başlık, altbilgi ve widget listesinden oluşan rapor içeriğini tanımlayın.

Başlık

Başlık, basit metin biçimlendirme içeriğinden oluşur. Bir başlık belirtmek zorunlu değildir

Template

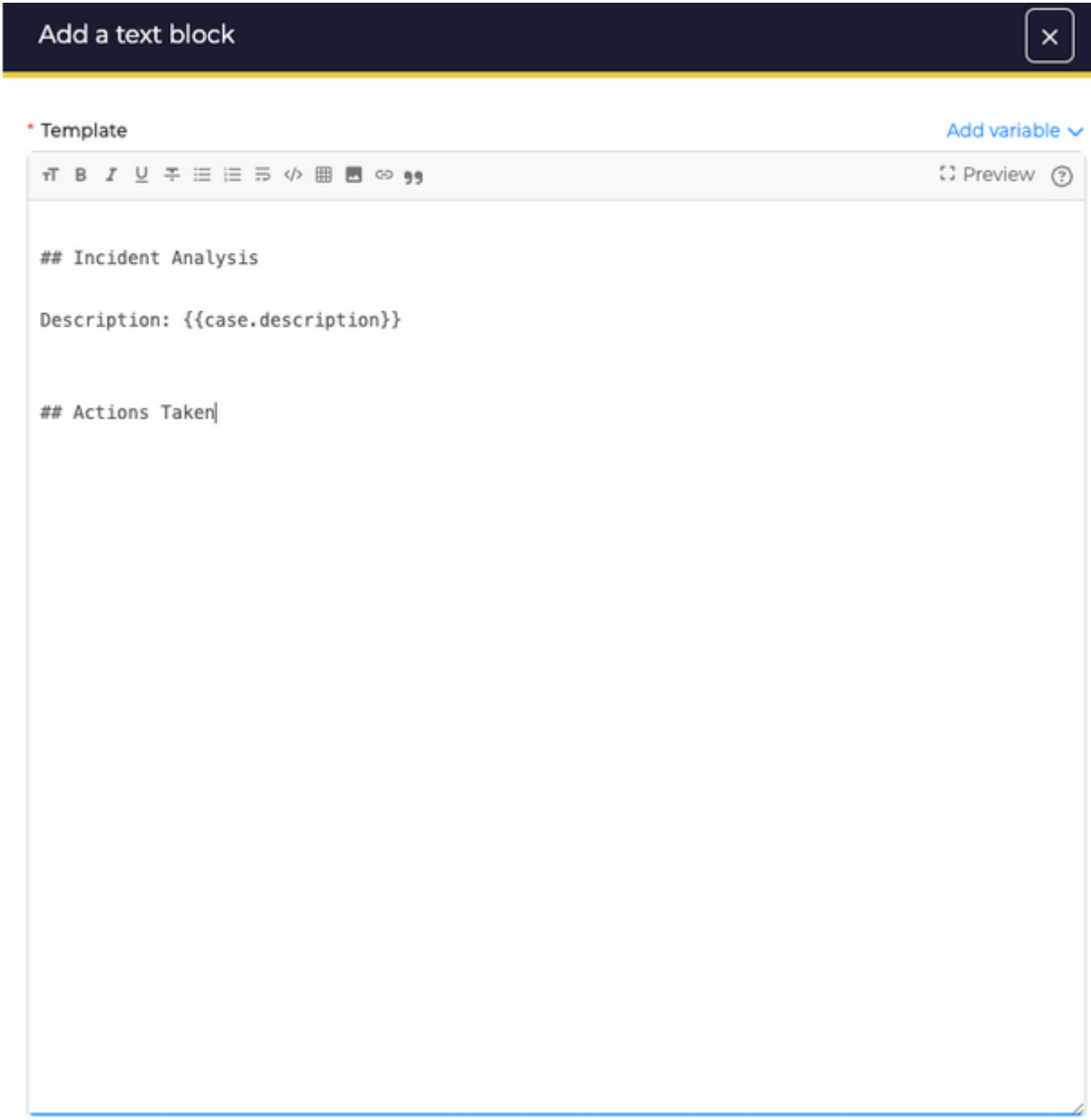
[Add variable](#) ▼

Preview

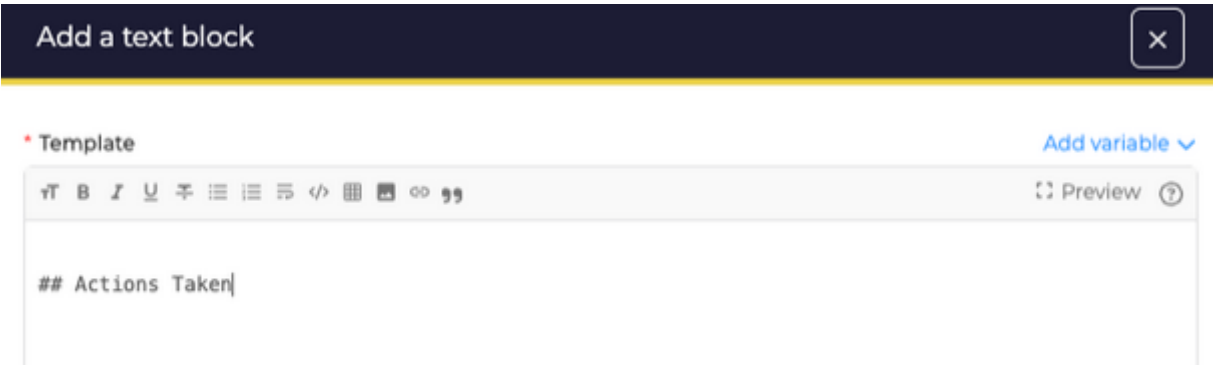
```
# {{case.title}}  
  
Case ID: {{case.number}}  
Date and Time of Incident: {{case.startDate}}  
Severity Level: {{case.severity}}  
TLP: {{case.tlp}}  
PAP: {{case.pap}}
```

Metin Widget'ı

İçerik tanımlamak için bir metin kutusu tanımlamak mümkündür.



Bileşenler arasına ayrı başlıklar eklemek için bir metin kutusu tanımlanabilir.




Görüntü Bileşeni


Görüntüleri bilgisayar dosyalarında aratarak ekleyin veya sürükleyip bırakarak ekleyin

Add an image

Drop image or click

Valid extensions : .jpg .jpeg .png

 fraud email.png



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.

Add a table

Parameters

1

• Entity

Observable

▼

2

Max elements in the table

Enter a number if you want to limit the table size

Protect data ?

3

☐

Veri Sütunları

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

Data list

title

group

assignee

status

startDate

2

3

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 filtreleneceği gerektiğini belirtin.
- Sıralama düzenini seçin.
- Birden fazla sıralama verisi ekleyin.
- Gereksiz sıralama verilerini silin.

1 Sorts

2 tip

3 desc

5

4 + Add a sort

Filtreler

- Tabloya veri miktarını sınırlamak için filtreler ekleyebilirsiniz.

- Seçilen varlıktan herhangi bir bilgiyi seçin.
- Filtrelenmesi 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

sighted

true

×

6

pap

3

not

4

red

×

tip

not

amber+strict

red

×

2

×

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 ×

Parameters

1

Entity

Observable

2

Max elements in the table

Enter a number if you want to limit the table size

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

group

assignee

status

startDate

Tasks logs ?

Sorts

No sort selected

Add a sort

Filters

1 + Add a line

description

dueDate

endDate

flag

mandatory

_createdAt

_createdBy

_updatedAt

Sıralamalar

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

1 Sorts

2 tlp 3 desc 5 x

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

2

sighted true 3 not 4 red 6

pap 3 not 4 red

tlp not amber+strict red

5 + Add filter 7 Clear filters

Altbilgi

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

Add variable

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.

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

Cases | Pages | Reports

2 T [Icon] [Icon] [Icon]

We feel responsible for you not getting what you are entitled to and for apologies we have decided to switch your customer self @cloudnet166132670 over to a premium plan.

If you want to remove it all this week, please configure everything here:

https://aws.amazon.com/opsworks/instances/?ref=AWS_OpsWorks_Instance_Pricing_Page

Remember that, for your safety this email will be valid only for 7 hours (after opening). If after that time you have not completed the process, we will begin to return your package.

Kind regards,

Josiah Fletcher
Workhouse Manager
Amazon

Task List

Title	Group	Assignee	Status	StartDate	EndDate

Logs

_createdBy _createdAt

Message

Observable Table

dataType	data	_createdAt	tip	pap

1 Drag me here!

Rapor Üzerindeki İşlemler

- Rapor içindeki herhangi bir bileşeni düzenleme

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

CasesPagesReports

{{case.title}}

Case ID: {{case.number}}

Date and Time of Incident: {{case.startDate}}

Severity Level: {{case.severity}}

TLP: {{case.tlp}}

PAP: {{case.pap}}

Incident Analysis

Description: {{case.description}}

Actions Taken

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

UsersTemplatesCustom TagsUI ConfigurationNotificationsEndpointsFunctionsBETAAttachments

CasesPagesReports

T

345

Remember that, for your safety, this email will be valid only for 7 hours after opening. If after that time you have not completed the process, we will begin to return your package.

Kind regards,

Isaac Fletcher

Workhouse manager

Amigos

Task List

1

2

Title

Group

Assignee

Status

StartDate

EndDate

Logs

_createdBy

_createdAt

Message

Revision #2

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

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