

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.

The screenshot displays the Alerts interface for an alert with ID -28896. The interface is divided into several sections:

- Header:** Alerts / internal (#mail_4376) / Description. A search icon and a "CREATE CASE" button are visible on the right.
- Left Sidebar:** Contains navigation icons for home, alerts, and search. A notification badge with the number "9" is present.
- Main Content Area:**
 - Alert Details:** Mail reported by [redacted], _id -28896, Created by Florian Perret, Created at 02/12/2021 15:15, Import date 02/12/2021 15:27.
 - Tags:** TLP:AMBER, PAP:AMBER, SEV:MEDIUM.
 - Source:** Malspam.
 - Reference:** mail_4376.
 - Type:** internal.
 - Occurred date:** 02/12/2021 15:15.
- Right Panel:**
 - General:** (4) Observables, (0) TTPs, Similar Cases, Similar Alerts, Responders.
 - Tags:** source:siem, log-source:ids.
 - Description:** User kyle has reported the following suspicious email.
 - Summary:** Description.
 - Custom Fields:** Add default.
 - business-unit:** Add ICT.
 - location:** Add Paris.

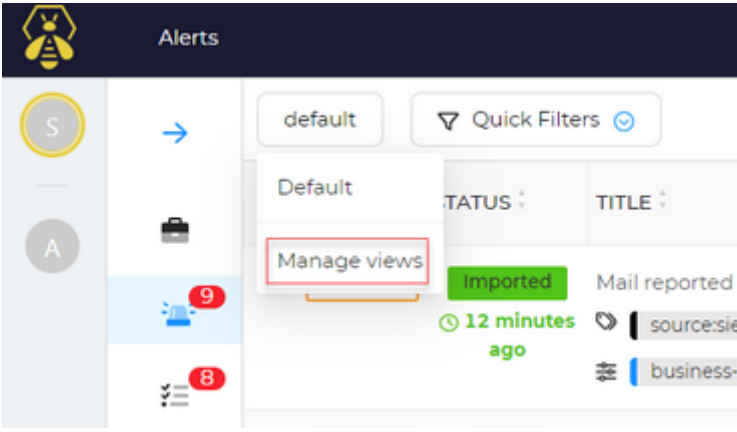
Görünümleri yönetin

Bu bölümde, görünümleri yönetme hakkında bilgi bulabilirsiniz.

Görünümleri yönetmek için:

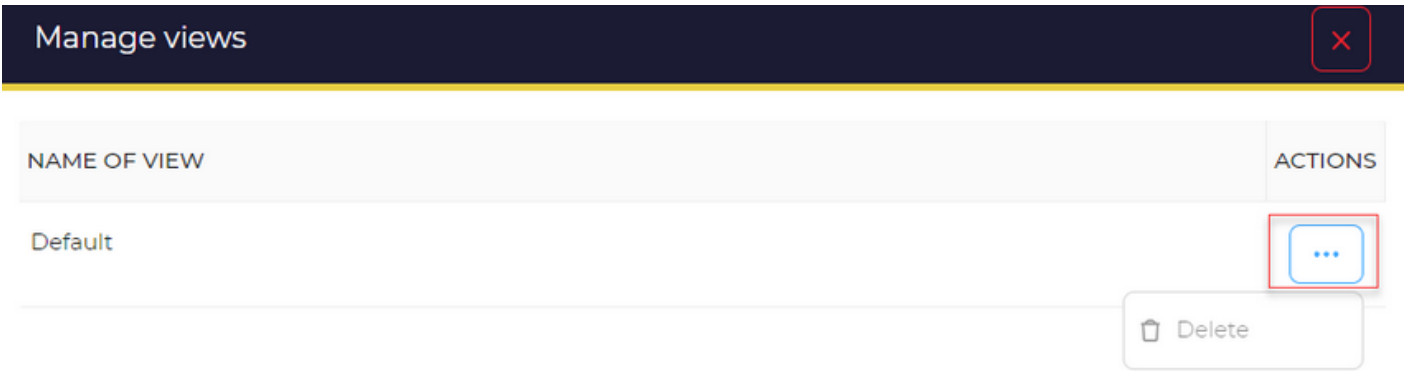
Varsayılan(default) düğmesine tıklayın.

Listeden Görünümleri Yönet(Manage Views) üzerine tıklayın.



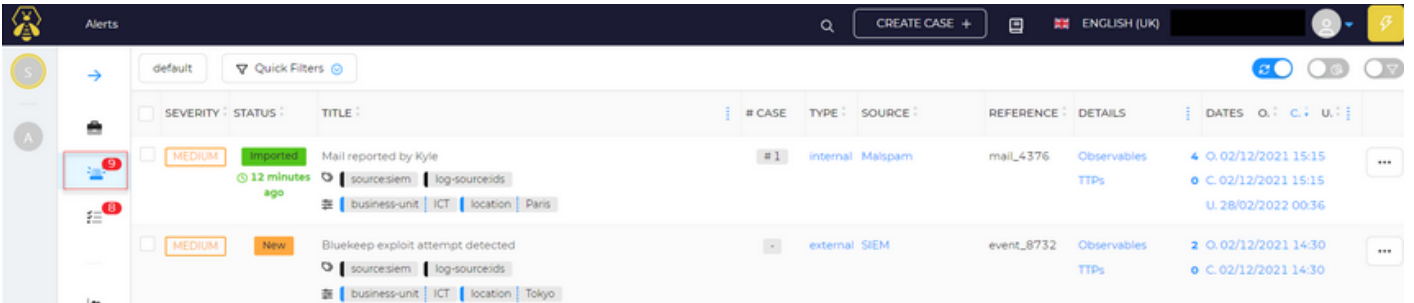
Yeni bir sayfa açılır. Görünümün Adı (Name of the view) ve ilgili Eylemler (Actions) yer alır.

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



Uyarıları Yönet

Uyarılara başvurmak için çeşitli seçenekler mevcuttur.

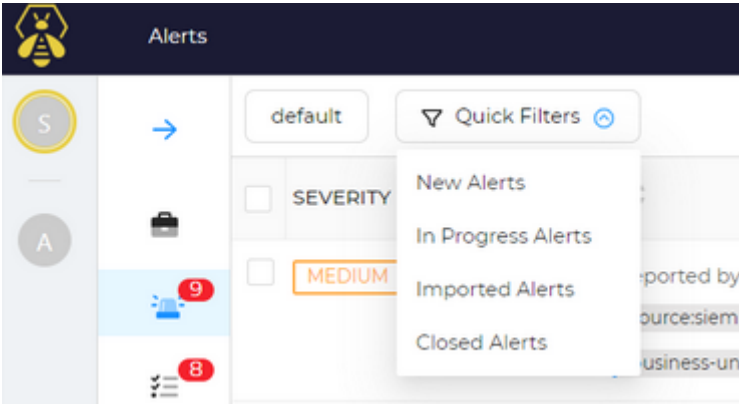


Hızlı Filtreler

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:

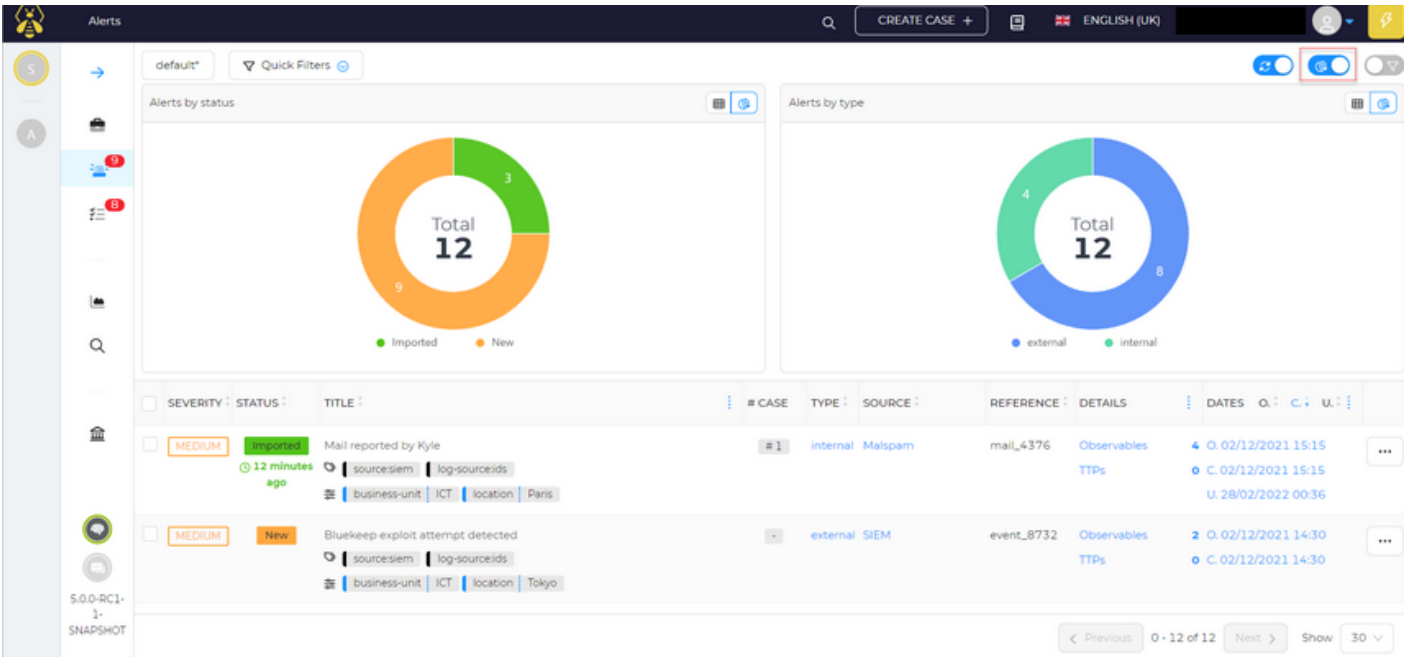
- Uyarılar sayfasında, Otomatik yenileme düğmesini açın.



İstatistikler

İstatistikleri görüntülemek için:

- Uyarılar sayfasında, İstatistikler geçiş düğmesini açtığınızda istatistikler görüntülenecektir.

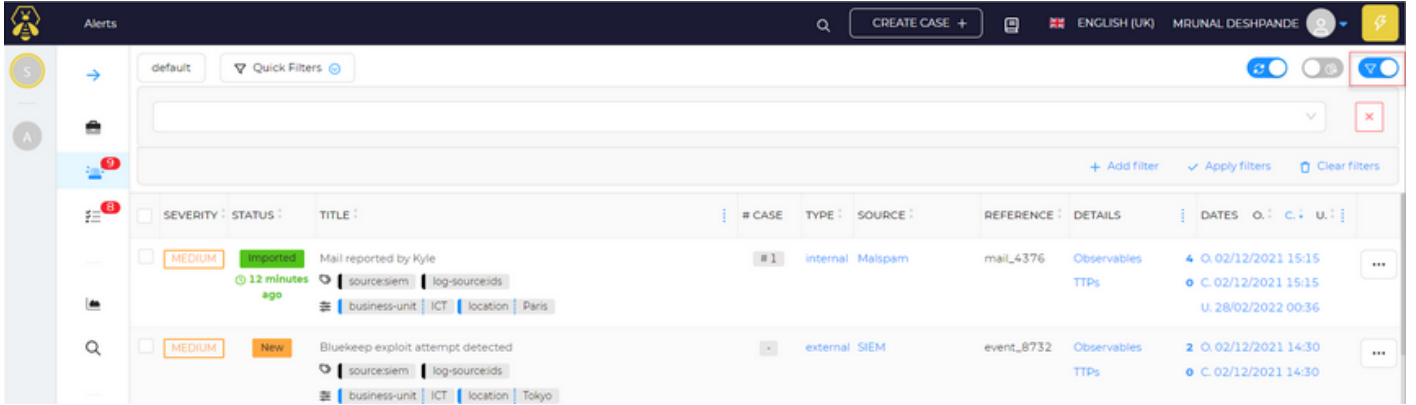


Filtreler

Filtre uygulamak için:

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

- Gerekli alana Filtre Uygula.



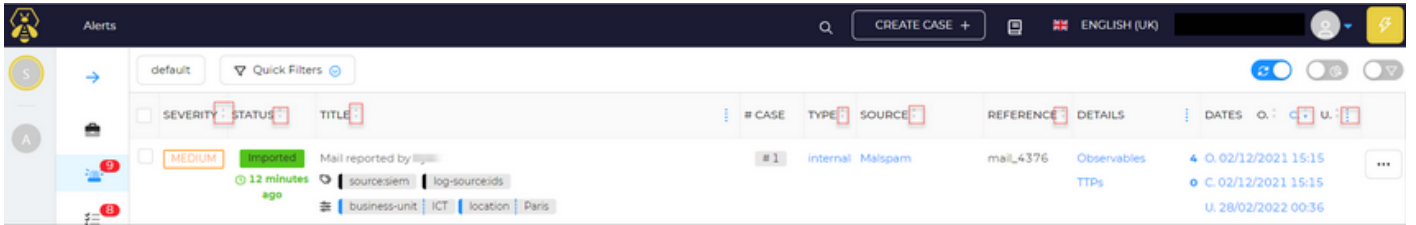
- Listedeki filtreleri seçin.
- Filtreleri uygula ögesine tıklayın.
- (İsteğe bağlı) Uygulanan tüm filtreleri temizlemek için Filtreleri temizle ögesine tıklayın.

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.



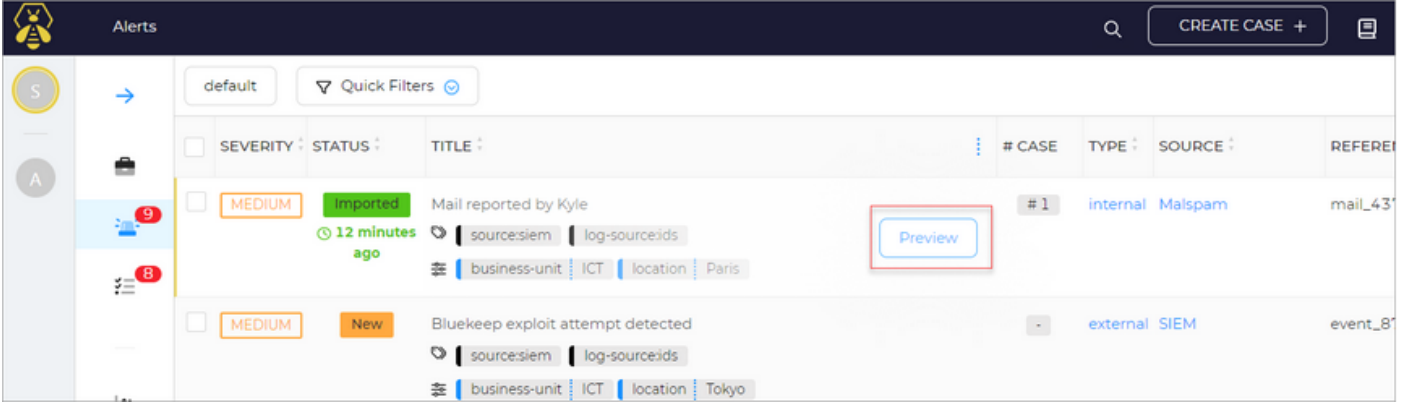
Önizleme Uyarıları

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.



The screenshot shows the Alerts interface with a table of alerts. The table has columns for SEVERITY, STATUS, TITLE, # CASE, TYPE, SOURCE, and REFERENCE. The first alert is highlighted with a red box around the 'Preview' button.

SEVERITY	STATUS	TITLE	# CASE	TYPE	SOURCE	REFERENCE
MEDIUM	Imported 12 minutes ago	Mail reported by Kyle source:siem log-sourceids business-unit: ICT location: Paris	# 1	internal	Malspam	mail_43
MEDIUM	New	Bluekeep exploit attempt detected source:siem log-sourceids business-unit: ICT location: Tokyo	-	external	SIEM	event_8

Uyarı ayrıntıları önizleme penceresi açılır.

Alert preview

_id ~28896 Created by Created at 02/12/2021 15:15 Last reviewed by
Last reviewed at 28/02/2022 00:53 Import date 02/12/2021 15:27

TLP:AMBER	Type	Reference	Observables
PAP:AMBER	internal	mail_4376	4
SEV:MEDIUM	Source	Occurred date	TTPs
	Malspam	02/12/2021 15:15	0

Title
Mail reported by Kyle

Tags
source:siem log-source:ids

Case #1 **Import date** 02/12/2021 15:27

Description
User kyle has reported the following suspicious email

Status
● Imported

Summary
Description

Custom Fields Add
default 3

business-unit Add **location** Add
ICT Paris

Actions [Go to details](#)

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.

Custom Fields [Add](#)

default 3 v

business-unit [Add](#) location [Add](#)

ICT v Paris v

Enter a value... v Enter a value... v

Uyarı Detayları

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

Alert preview

[_id ~28896](#) [Created by](#) [Created at 02/12/2021 15:15](#) [Last reviewed by](#)

[Last reviewed at 28/02/2022 01:35](#) [Import date 02/12/2021 15:27](#)

TLP:AMBER	Type	Reference	Observables 4
PAP:AMBER	internal	mail_4376	
SEV:MEDIUM	Source	Occurred date	TTPs 0
	Malspam	02/12/2021 15:15	

Title

Mail reported by Kyle

Tags

[source:siem](#) [log-source:ids](#)

Case #1 Import date 02/12/2021 15:27

[Start](#) [Close](#) [Track new updates](#) [Responders](#) [Unlink](#)

[Actions](#) [Go to details](#)

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.

Alerts / internal (#mail_4376) / Description

CREATE CASE +

ENGLISH (UK)

Mail reported by Kyle

_id -28896

Created by Florian Perret

Created at 02/12/2021 15:15

Import date 02/12/2021 15:27

TLP:AMBER PDP:AMBER SEV:MEDIUM

Source Malspam

Reference mail_4376

Type internal

Occurred date 02/12/2021 15:15

Status Imported

Case #1

Import date 02/12/2021 15:27

General (4) Observables (0) TTPs Similar Cases Similar Alerts Responders

Tags sourcesiem log-sourceids

Description User kyle has reported the following suspicious email

Summary Description

Custom Fields Add

default 3 v

business-unit Add location Add

ICT Paris

Comments

Type a comment...

Comment

Eylemler

Mevcut eylemlerden herhangi birini kullanabilirsiniz.

Status

Imported

Summary

Description

Start

Close

Track new updates

Responders

Unlink

location Add

Paris

3 v

Actions ^

Go to details

Başlangıç

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

Status
● Imported

Summary
Description

Start
x Close
Track new updates
Responders
Unlink

location ? Add

Paris

3 v

Actions ^

Go to details

Kapatma

Bir görevi kaldırmak için Kapat seçeneğine tıklayın.

Yeni bir pencere açılır.

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

Change the alert status



Status *

New



Summary

Rich text editor toolbar with icons for bold, italic, underline, list, link, code, table, image, and link.

Preview ?

Enter a summary...

Cancel

Confirm

Yeni Güncellemeleri İzle/Görmezden Gel

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

success



Alert(s) followed successfully!

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

success



Alert(s) unfollowed successfully!

Bağlantı Kaldırma

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

! Are you sure you want to unlink this alert?

Cancel

OK

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.



- By title
 By case number

Merge

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.

The screenshot shows a security alert management interface. The top navigation bar includes a search icon, a 'CREATE CASE +' button, and a language selector set to 'ENGLISH (UK)'. The main area displays a table of alerts with columns for SEVERITY, STATUS, TITLE, # CASE, TYPE, SOURCE, REFERENCE, DETAILS, and DATES. A context menu is open over the second alert, showing options: Start, Close, Ignore new updates, New case from selection, Merge selection into case, and Responders. The 'New case from selection' option is highlighted with a red box.

SEVERITY	STATUS	TITLE	# CASE	TYPE	SOURCE	REFERENCE	DETAILS	DATES
MEDIUM	Imported	Mail reported by [redacted]	#1	internal	Mailspam	mail_4376	Observables TTPs	4 O. 02/12/2021 15:15 C. 02/12/2021 15:15 U. 28/02/2022 00:36
MEDIUM	New	Bluekeep exploit attempt detected	-	external	SIEM	event_8732	Observables TTPs	2 O. 02/12/2021 14:30 C. 02/12/2021 14:30 U. 02/12/2021 14:30
LOW	Imported	Port scan attempt detected	#2	external	SIEM	event_8743	Observables TTPs	2 O. 02/12/2021 14:30 C. 02/12/2021 14:30 U. 02/12/2021 14:30
MEDIUM	New	Security Software discovery on host	-	internal	EDR	edr_8419	Observables TTPs	2 O. 02/12/2021 02:41 C. 02/12/2021 02:41 U. 02/12/2021 02:41
MEDIUM	Imported	Connection to account from unusual region	#3	internal	EDR	edr_8416	Observables TTPs	2 O. 02/12/2021 02:41 C. 02/12/2021 02:41 U. 02/12/2021 02:41

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.



How do you want to create your case?



Empty case



From template



From archive (.thar)



From MISP (.json)

Genel

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

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

Pencerenin sağ bölümünde, 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.

Custom Fields [Add](#)

default 3 v

business-unit ? [Add](#) location ? [Add](#)

ICT v Paris v

Enter a value... Enter a value...

Alerts / internal (#mail_4376) / Description

CREATE CASE + ENGLISH (UK)

Mail reported by Kyle

_id -28896
Created by [redacted]
Created at 02/12/2021 15:15
Import date 02/12/2021 15:27

TLP:AMBER PAP:AMBER SEV:MEDIUM

Source
Malspam

Reference
mail_4376

Type
internal

Occurred date
02/12/2021 15:15

Status
Imported

Case
#1

Import date
02/12/2021 15:27

General (4) Observables (0) TTPs Similar Cases Similar Alerts Responders

Tags
source:em log-source:ids

Description
User Kyle has reported the following suspicious email

Summary
Description

Custom Fields [Add](#)

default 3 v

business-unit ? [Add](#) location ? [Add](#)

ICT v Paris v

Comments

Type a comment...

Comment

Yanıtlayanlar

Yanıt verenleri çalıştırın

Yanıtlayanlar seçeneğine tıklayın.

Yeni bir pencere görünür.

Arama kutusunda belirli bir yanıtlayıcıyı arayın.

Run responder jobs on current alert



Search for a specific responder

Yanıtlayanları Görüntüle

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

General (4) Observables (0) TTPs Similar Cases Similar Alerts **Responders**

No responder reports available!

Benzer Uyarıları görüntüleyin

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

General (4) Observables (0) TTPs Similar Cases **Similar Alerts** Responders

default

TITLE : CREATED AT : OBSERVABLES : IOCS : MATCHES

SEVERITY : STATUS : Filter by title 0 0 SELECT

MEDIUM **New** Security Software discovery on host 02/12/2021 02:41 50% (1/2) 0% (0/1) username (1)

source:EDR origin:endpoint

location : Seattle business-unit : VIP


Benzer vakaları görüntüleyin

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

TITLE	CREATED AT	OBSERVABLES	IOCS	MATCHES	ACTION
Filter by title		0	0	SELECT	Clear filters
#1 Phishing -Mail reported by	02/12/2021 15:27	66% (4/6)	33% (1/3)	mail (1) uri (1) mail-subject (1) username (1)	
#3 EDR -Connection to account from unusual region	02/12/2021 15:54	50% (1/2)	0% (0/1)	username (1)	

TTPS'yi Görüntüleyin

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

General	(4) Observables	(0) TTPs	Similar Cases	Similar Alerts	Responders
default					
 No TTPs have been found.					

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.

Alerts / internal (#mail_4376) / Observables

CREATE CASE +

ENGLISH (UK)

Mail reported by [redacted]

General (4) Observables (0) TTPs Similar Cases Similar Alerts Responders

default

FLAGS DATA TYPE VALUE/FILENAME DATES S. C. U.

TLP:AMBER	PAP:AMBER	SEVMEDIUM	TLP:AMBER	mail-subject	Claim your prize!	S	02/12/2021 15:15		
			PAP:AMBER		None	C	02/12/2021 15:15		
					No report(s) available				
TLP:AMBER			TLP:AMBER	mail	sayz[.]dota@gmail[.]com	S	02/12/2021 15:15		
			PAP:AMBER		None	C	02/12/2021 15:15		
					No report(s) available				
TLP:AMBER			TLP:AMBER	username	kyie	S	02/12/2021 15:15		
			PAP:AMBER		Targeted	C	02/12/2021 15:15		
					No report(s) available				
TLP:AMBER			TLP:AMBER	url	hxpx://u842504ngz[.]ha004[.]t[.]justns[.]ru/tatim/tim/	S	02/12/2021 15:15		
			PAP:AMBER		None	C	02/12/2021 15:15		
					No report(s) available				

< Previous 0 - 4 of 4 Next > Show 30 v

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