

Arama (Search)

Vakalara Göre Ara

Vakalara göre arama yapmak için:

Eğer vakalara göre arama yapmak istiyorsanız

- Sol tarafta, "Vakalar"a tıklayın.
- Uygulanan filtreleri kaldırmak için "Tümünü Temizle" seçeneğini kullanarak arama kriterlerini belirleyebilirsiniz.
- Yeni filtreler eklemek için "Yeni Filtreler Ekle" butonuna tıklayın.
- Listedeki gerekli filtreleri seçin. (örneğin, _oluşturan, boş değil vs.)
- Alt kısımdaki "Arama" düğmesine tıklayın.

The screenshot displays the Search interface with three main sections:

- Search Scope:** A sidebar on the left with a search icon and a list of categories: Cases (highlighted), Tasks, Task logs, Observables, Alerts, Jobs, and Audit Logs.
- Search Filter / Cases:** A central panel with a search bar and a filter section. It shows "1 filter(s) applied" with a dropdown menu for "_createdBy" set to "is not empty". There are buttons for "Add new filter" and "Clear all".
- Search Results:** A right panel showing 3 records found. The results are listed with details such as "EDR -Connection to account from unusual region", "Port scan attempt detected", and "Phishing -Mail reported by Kyle". Each result includes a date, a status (New, In progress), and a source (source:EDR, source:SIEM, log-source:Firewall).

Uyarılara Göre Ara

Eğer bir kullanıcı alertlara göre arama yapmak istiyorsa:

- Sol tarafta, "Alertler"e tıklayın.
- Bir kullanıcı, uygulanan filtreleri kaldırmak için "Tümünü Temizle" seçeneğini kullanarak arama kriterlerini belirleyebilir.
- Yeni filtreler eklemek için "Yeni Filtreler Ekle" düğmesine tıklayın.

- Listedeki gerekli filtreleri seçin.
- Alt kısımdaki "Arama" düğmesine tıklayın.

Arama sonuçları sayfanın sağ tarafında görüntülenir.

The screenshot displays the Search interface with the following components:

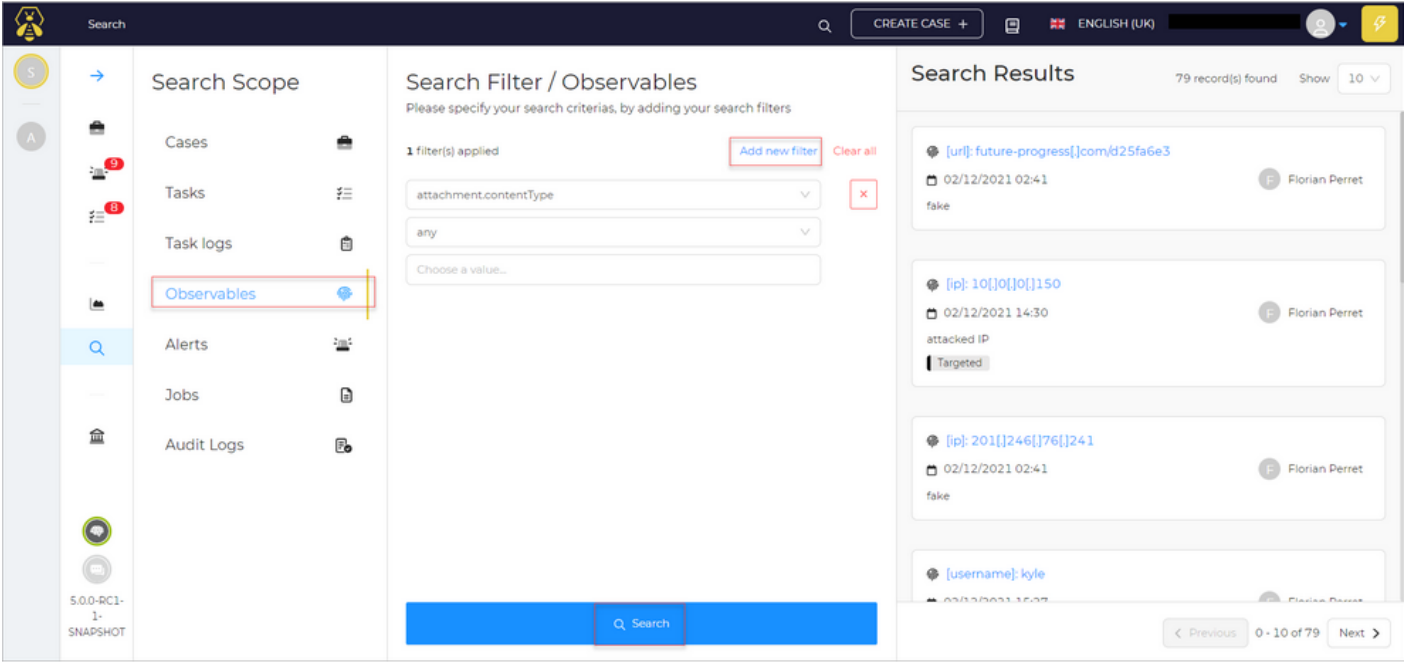
- Search Scope:** A sidebar on the left with a search bar and a list of categories: Cases list, Alerts (9), Tasks (13), Dashboards, Search (highlighted), and Organisation. A secondary list on the right includes Cases, Tasks, Task logs, Observables, Alerts (highlighted), Jobs, and Audit Logs.
- Search Filter / Alerts:** A central panel titled "Please specify your search criteria, by adding your search filters". It shows 1 filter(s) applied: "computed.handlingDuration" with a value of "eq". Buttons for "Add new filter" and "Clear all" are present. A "Search" button is at the bottom.
- Search Results:** A panel on the right showing 12 record(s) found. It displays two alert entries:
 - Port scan attempt detected:** 02/12/2021 14:30, Type: external, Source: SIEM, Reference: event_8743. Description: SIEM automated alert: Port scan attempt from 117[.]215[.]213[.]101 against TOU-W10-1234 (ip: 10.0.0.150). Log source: Firewall.
 - Connection to account from unusual region:** 02/12/2021 02:41, Type: internal, Source: EDR, Reference: edr_8416. Description: The user account connected from unusual region (Russia). Log source: EDR.

Gözlemlenebilirliğe Göre Ara

Gözlemlenebilirliğe göre arama yapmak isterseniz:

- Sol tarafta, "Gözlemlenebilirlik"e tıklayın.
- Uygulanan filtreleri kaldırmak için "Tümünü Temizle" seçeneğini kullanarak arama kriterlerinizi belirleyebilirsiniz.
- "Yeni Filtreler Ekle" düğmesine tıklayarak yeni filtreler ekleyin.
- Listedeki gerekli filtreleri seçin.
- Alt kısımdaki "Arama" düğmesine tıklayın.

Arama sonuçları sayfanın sağ tarafında görüntülenir.



İşlere Göre Arama

- Sol tarafta, "İşler"e tıklayın.
- Uygulanan filtreleri kaldırmak için "Tümünü Temizle" seçeneğini kullanarak arama kriterlerini belirleyebilirsiniz.
- "Yeni Filtreler Ekle" düğmesine tıklayarak yeni filtreler ekleyin.
- Listedeki gerekli filtreleri seçin.
- Alt kısımdaki "Arama" düğmesine tıklayın.

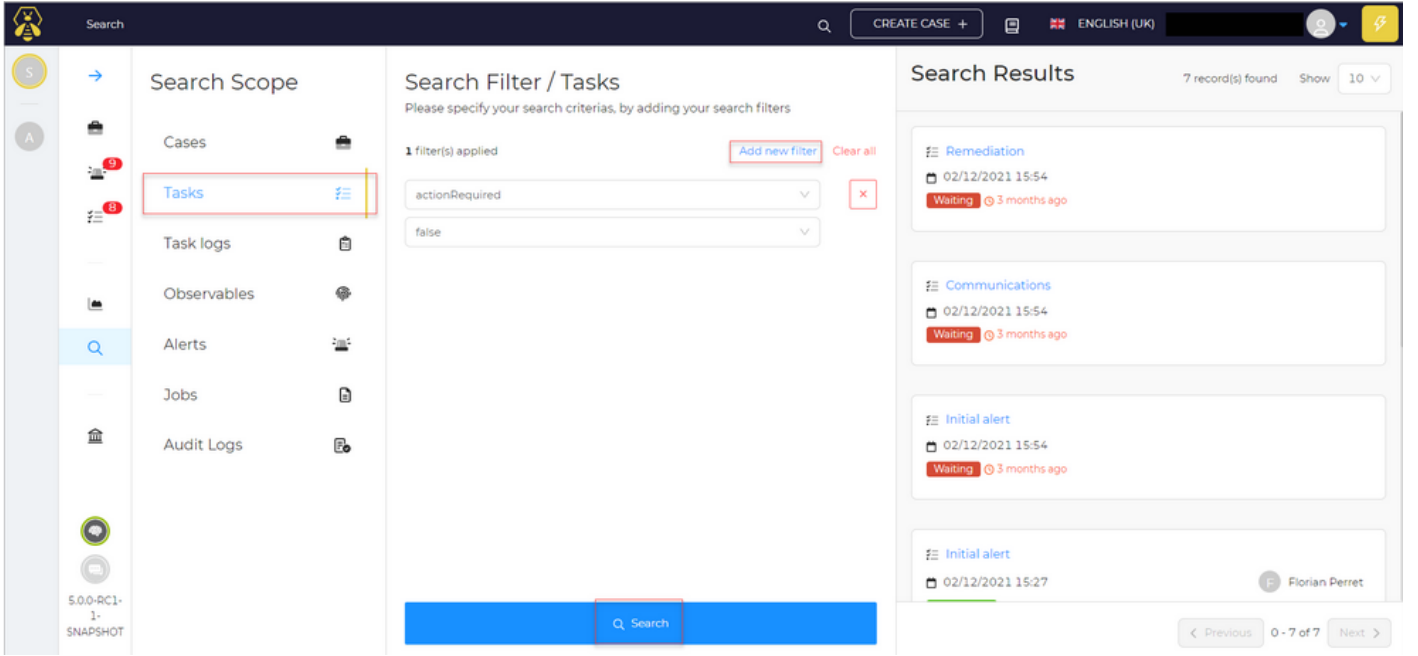
Arama sonuçları sayfanın sağ tarafında görüntülenir.

Görevlere Göre Arama

Görevlere göre arama yapmak için:

- Sol tarafta, "Görevler"e tıklayın.
- Uygulanan filtreleri kaldırmak için "Tümünü Temizle" seçeneğini kullanarak arama kriterlerini belirleyebilirsiniz.
- "Yeni Filtreler Ekle" düğmesine tıklayarak yeni filtreler ekleyin.
- Listedeki gerekli filtreleri seçin.
- Alt kısımdaki "Arama" düğmesine tıklayın.

Arama sonuçları sayfanın sağ tarafında görüntülenir.



Görev Günlüklerine Göre Arama

Görev günlüklerine göre arama yapmak için:

- Sol tarafta, "Görev Günlükleri"ne tıklayın.
- Uygulanan filtreleri kaldırmak için "Tümünü Temizle" seçeneğini kullanarak arama kriterlerini belirleyebilirsiniz.
- "Yeni Filtreler Ekle" düğmesine tıklayarak yeni filtreler ekleyin.
- Listedeki gerekli filtreleri seçin.
- Alt kısımdaki "Arama" düğmesine tıklayın.

Arama sonuçları sayfanın sağ tarafında görüntülenir.

S

A

9

6

5.0.0-RC1-1-SNAPSHOT

Search

→

Cases

Tasks

Task logs

Observables

Alerts

Jobs

Audit Logs

Search Filter / Task logs

Please specify your search criterias, by adding your search filters

1 filter(s) applied

attachments.name

is not empty

Add new filter

Clear all

Q Search

Search Results

2 record(s) found

Show 10

Message by florian@strangebee.com

07/12/2021 15:56

additional logs

Message by florian@strangebee.com

02/12/2021 16:29

Mail reported by kyle, EML file provided in observables

< Previous

0 - 2 of 2

Next >

Revision #2

Created 11 April 2024 17:42:14 by Güldeniz Akca

Updated 13 April 2024 14:59:52 by Güldeniz Akca