

BEHEERCONSOLE > RAPPORTAGE

Panther SIEM

Panther SIEM

Panther is een SIEM-platform (Security Information and Event Management) dat kan worden gebruikt met Bitwarden-organisaties. Gebruikers van een organisatie kunnen [gebeurtenisactiviteiten](#) volgen met de Bitwarden app op hun Panther monitoringsysteem.

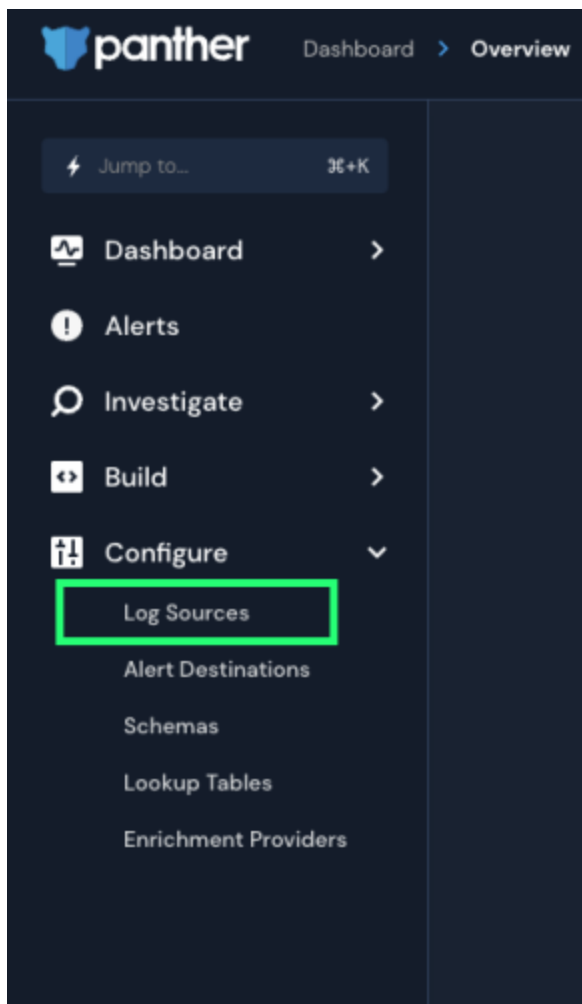
Setup

Maak een Panther-account aan

Om te beginnen heb je een Panther account en dashboard nodig. Maak een Panther-account aan op hun [website](#).

Panther Bitwarden logbron initialiseren

1. Ga naar het Panther dashboard.
2. Open in het menu de vervolgkeuzelijst **Configure** en selecteer **Log Sources**.



Panther Log Sources

3. Selecteer **Aan boord van je logboeken**.

Log Sources

Onboard logs for detection and investigation.



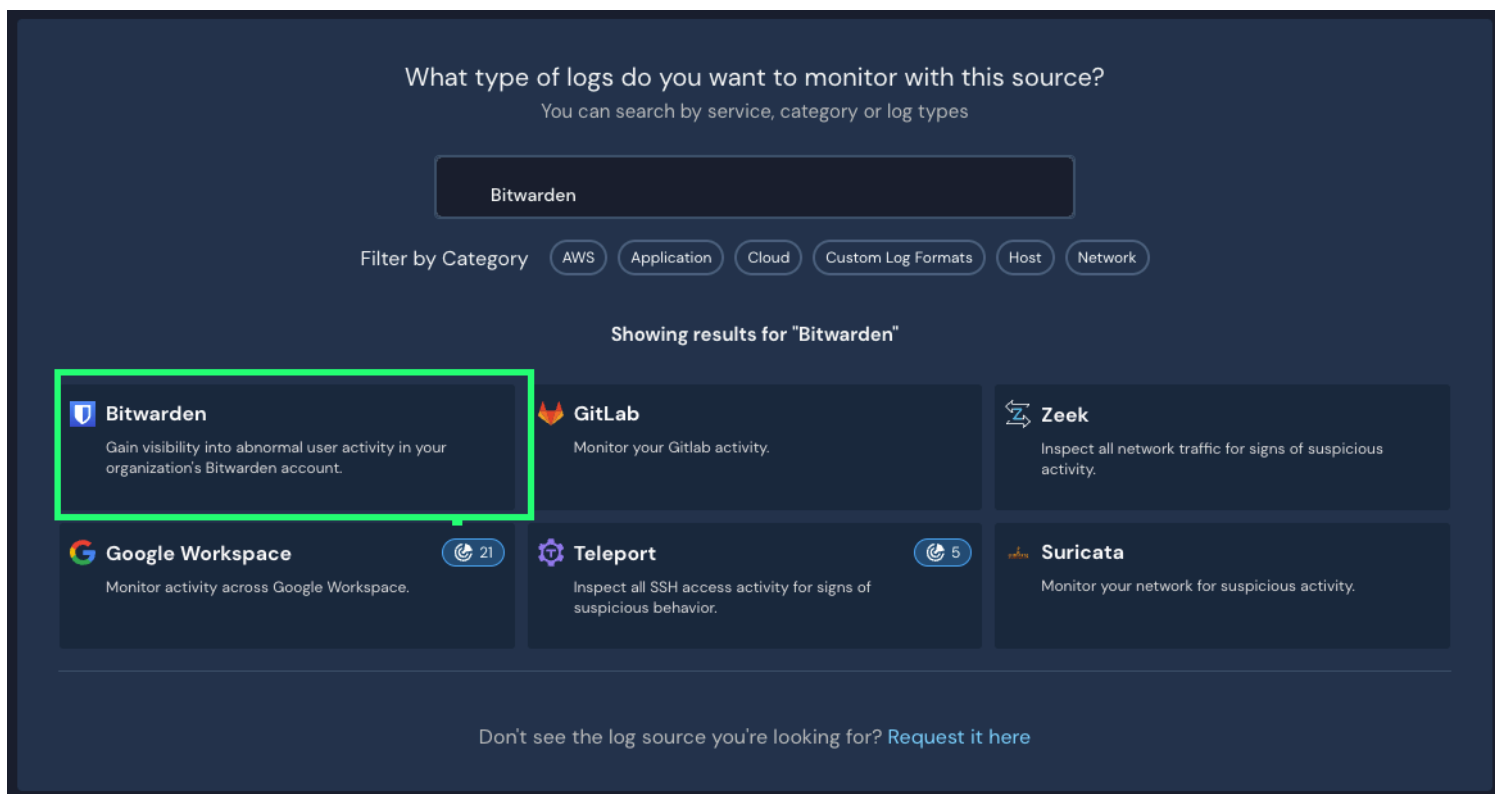
It's empty in here

You don't seem to have any Log sources connected to our system.

[Onboard your logs](#)

Panther Onboard logs

4. Zoek **Bitwarden** in de catalogus.



Elastic Bitwarden integration

5. Klik op de **Bitwarden-integratie** en selecteer **Start Setup**.

Verbind uw Bitwarden-organisatie

Nadat je **Start Setup** hebt geselecteerd, kom je in het configuratiescherm.

Note

Panther SIEM services are only available for Bitwarden cloud hosted organizations.

1. Voer een naam in voor de integratie en selecteer **Setup**.
2. Vervolgens moet u toegang krijgen tot de **klant-ID** en **het klantgeheim** van uw Bitwarden-organisatie. Als u dit scherm open houdt, logt u op een ander tabblad in op de Bitwarden webapp en opent u de beheerconsole met de productswitcher (☰):

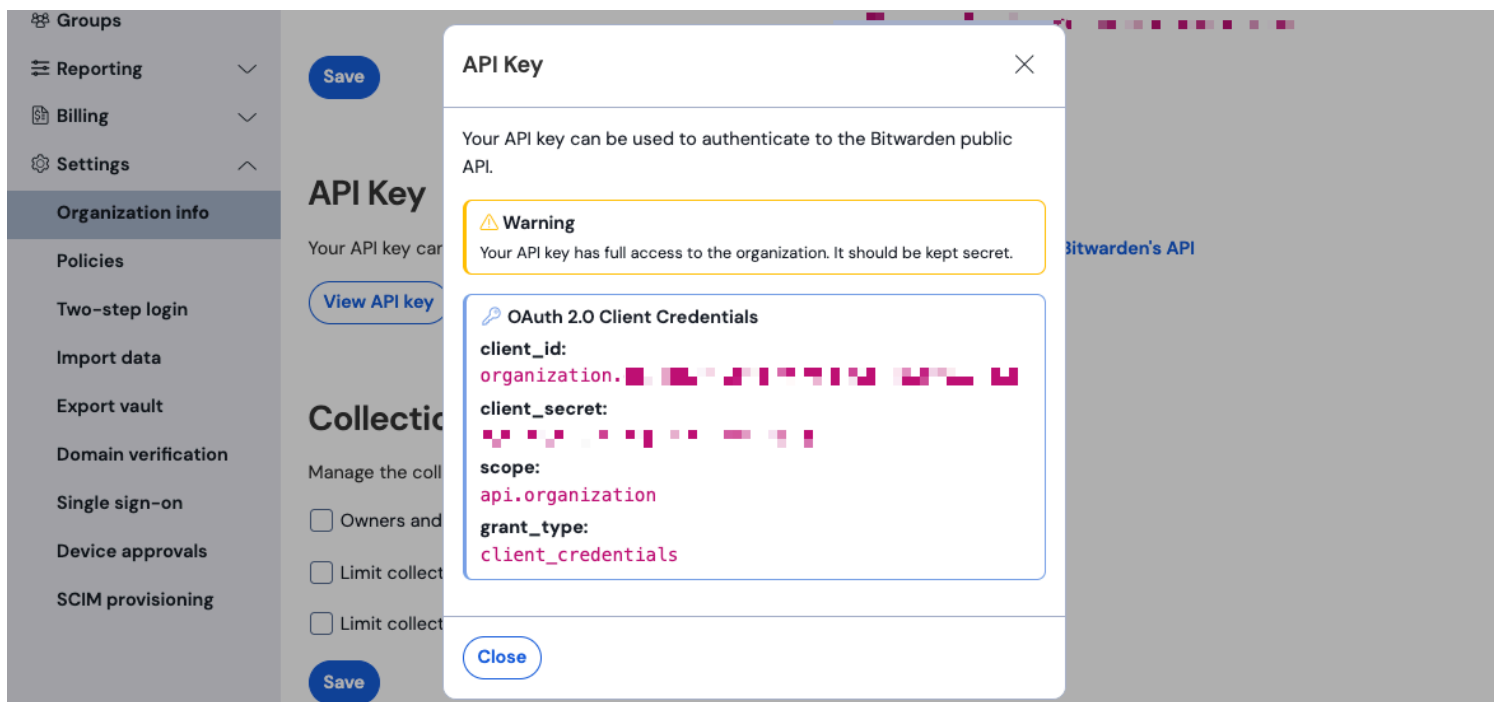
Filters:

- Search vaults
- All vaults
 - My vault
 - My Organiz...
 - Teams Org...
 - New organization
- All items
 - Favorites
 - Login
 - Card
 - Identity
 - Secure note
- Folders
 - No folder
- Collections
 - Default colle...
 - Default colle...
- Trash

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Product switcher

3. Navigeer naar het scherm **Instellingen** → Organisatie-info van je organisatie en selecteer de knop **API-sleutel weergeven** . U wordt gevraagd uw hoofdwachtwoord opnieuw in te voeren om toegang te krijgen tot uw API-sleutelgegevens.



Organisatie api info

4. Kopieer en plak de `client_id` en `client_secret` waarden op hun respectievelijke locaties op de Bitwarden App instellingspagina. Nadat u de informatie hebt ingevoerd, gaat u verder door **Setup** opnieuw te selecteren.
5. Panther zal de integratie testen. Na een succesvolle test krijgt u de optie om uw voorkeuren aan te passen. Voltooi de installatie door op **View Log Source** te drukken.

Note

Panther may take up to 10 minutes to ingest data following the Bitwarden App setup.

Begin met het monitoren van gegevens

1. Om te beginnen met het monitoren van gegevens, ga je naar het primaire dashboard en selecteer je **Onderzoeken** en **Gegevensverkener**.
2. Selecteer op de pagina Data Explorer de database `panther_logs.public` in het vervolgkeuzemenu. Zorg ervoor dat `bitwarden_events` ook wordt bekeken.

The screenshot shows the Panther Data Explorer interface. On the left is a navigation sidebar with icons for home, alerts, search, and other functions. The main area is titled "Data Explorer" and contains a "Select Database" dropdown menu set to "panther_logs.public". Below it is a "Tables" section with a search filter and a list of tables. The table "bitwarden_events" is highlighted with a red box. To the right is a "New Query" editor with the following SQL code:

```
1 SELECT
2 *
3 FROM panther_logs.public.bitwarden_events
4 WHERE p_source_id =
5 LIMIT 100
```

At the bottom of the query editor are "Run Query" and "Save as" buttons. The interface is powered by Snowflake.

Panther Data Explorer

3. Zodra je alle vereiste selecties hebt gemaakt, selecteer je **Query uitvoeren**.
Je kunt ook **opslaan om** de query op een ander moment te gebruiken.
4. Onderaan het scherm verschijnt een lijst met Bitwarden-evenementen.

object	type	itemid	collectionid	groupid	policyid	memberid	actingUserid	installat
event	event	1700	null	null	null	null	null	null
event	event	1700	null	null	null	null	null	null
event	event	1700	null	null	null	null	null	null
event	event	1400	null	null	null	null	null	null
event	event	1000	null	null	null	null	null	null

Panther Event Logs

5. Gebeurtenissen kunnen worden uitgebreid en bekeken in JSON door **View JSON** te selecteren. ☺.

```
{
  actingUserId: [REDACTED]
  date: [REDACTED]
  device: 9
  ipAddress: [REDACTED]
  object: event
  p_any_ip_addresses: [ ] 1 item
  p_event_time: [REDACTED]
  p_log_type: Bitwarden.Events
  p_parse_time: [REDACTED]
  p_row_id: [REDACTED]
  p_schema_version: 0
  p_source_id: [REDACTED]
  p_source_label: [REDACTED]
  type: 1000
}
```

Panther JSON Object

Kijk [hier](#) voor meer informatie over evenementen van Bitwardenorganisaties. Extra opties voor specifieke queries zijn beschikbaar, zie de documentatie van [Panther Data Explorer](#) voor meer informatie.