

ADMINISTRATOR KONSOLE > BERICHTE

Panther SIEM

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/panther-siem/>

Panther SIEM

Panther ist eine Plattform für Sicherheitsinformationen und Ereignisverwaltung (SIEM), die mit Bitwarden Organisationen verwendet werden kann. Benutzer der Organisation können die [Ereignisaktivität](#) mit der Bitwarden-App auf ihrem Panther-Überwachungssystem überwachen.

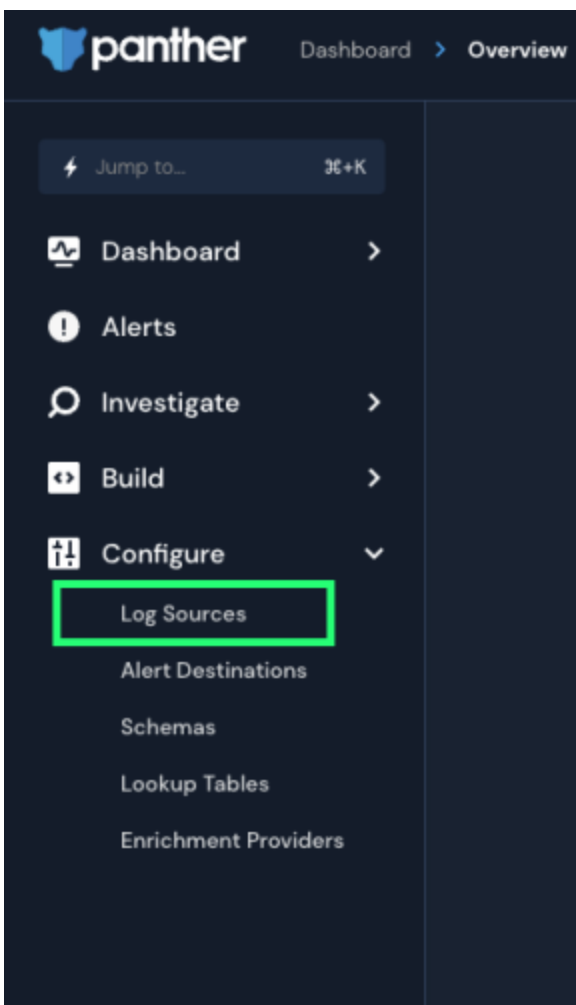
Einrichtung

Erstellen Sie ein Panther-Konto

Um zu beginnen, benötigen Sie ein Panther-Konto und ein Dashboard. Erstellen Sie ein Panther-Konto auf ihrer [Website](#).

Initialisieren Sie Panther Bitwarden Log Quelle

1. Greifen Sie auf das Panther-Dashboard zu.
2. Im Menü öffnen Sie das Dropdown-Menü **Konfigurieren** und wählen **Log-Quellen** aus.



Panther Log Sources

3. Wählen Sie **Ihre Protokolle an Bord**.

Log Sources

Onboard logs for detection and investigation.



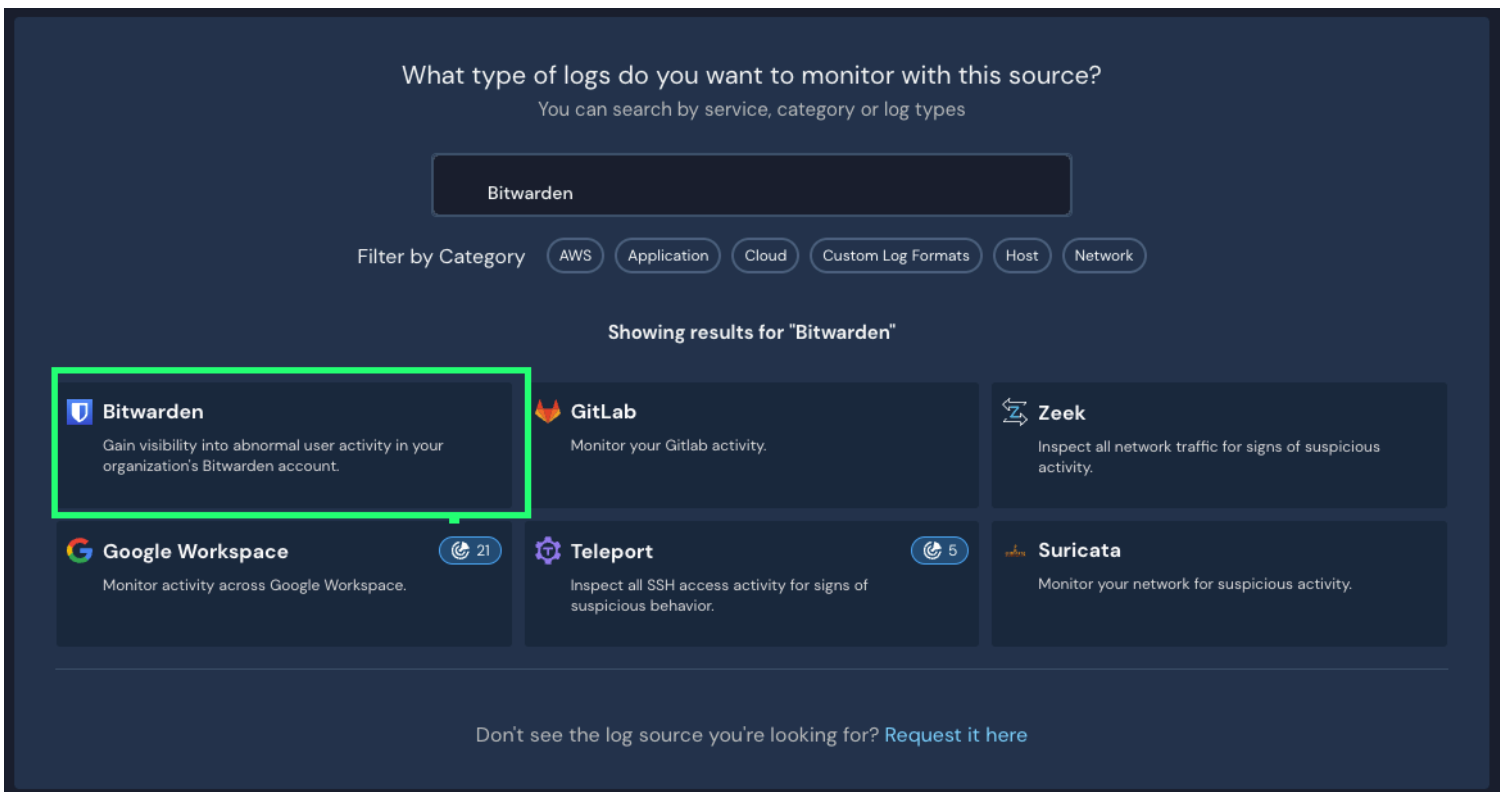
It's empty in here

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

[Onboard your logs](#)

Panther Onboard logs

4. Suchen Sie **Bitwarden** im Katalog.



Elastic Bitwarden integration

5. Klicken Sie auf die **Bitwarden** Integration und wählen Sie **Einrichtung starten**.

Verbinden Sie Ihre Bitwarden Organisation

Nachdem Sie **Setup starten** ausgewählt haben, werden Sie zum Konfigurationsbildschirm weitergeleitet.

Note

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

1. Geben Sie einen Namen für die Integration ein und wählen Sie dann **Einrichten** aus.

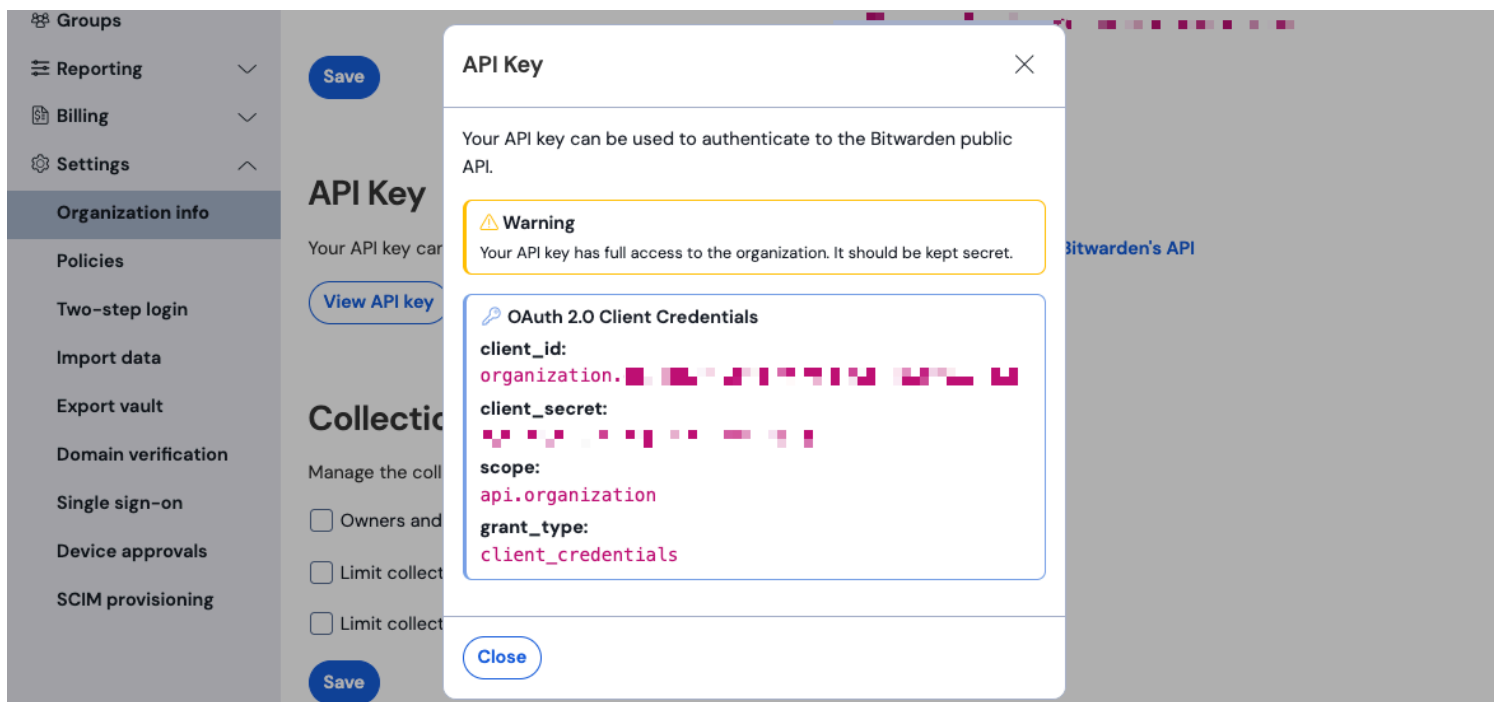
2. Als nächstes müssen Sie auf die **Client ID** und das **Client Secret** Ihrer Bitwarden Organisation zugreifen. Lassen Sie diesen Bildschirm geöffnet, melden Sie sich in einem anderen Tab in der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktschalter (☰):

The screenshot displays the Bitwarden web interface. On the left, a dark blue sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. Below these are Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red box highlights the sidebar, and a red arrow points to 'Secrets Manager'. The main area is titled 'All vaults' and features a 'FILTERS' panel on the left with a search bar and a list of vault categories. The main list shows several vaults:

| <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... | ⋮ |

Produktwechsler

3. Navigieren Sie zu dem Bildschirm "Organisationsinformationen" in den **Einstellungen** Ihrer Organisation und wählen Sie die Schaltfläche **API-Schlüssel anzeigen**. Sie werden aufgefordert, Ihr Master-Passwort erneut einzugeben, um auf Ihre API-Schlüsselinformationen zugreifen zu können.



Organisation API Informationen

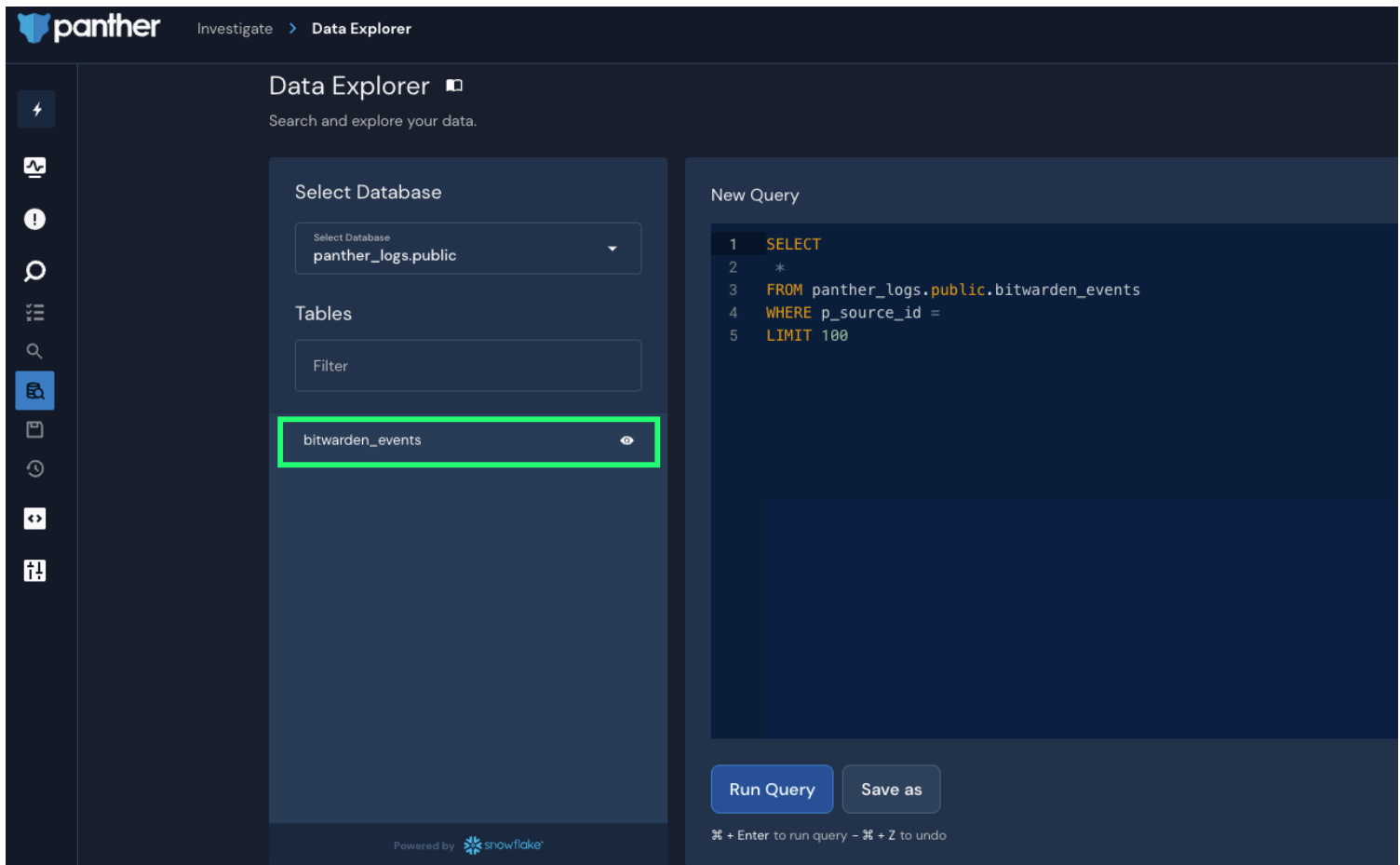
4. Kopieren und fügen Sie die Werte `client_id` und `client_secret` an ihren jeweiligen Stellen auf der Bitwarden App-Einrichtungsseite ein. Nachdem Sie die Informationen eingegeben haben, fahren Sie fort, indem Sie erneut **Einrichten** auswählen.
5. Panther wird einen Test zur Integration durchführen. Sobald ein erfolgreicher Test abgeschlossen wurde, haben Sie die Möglichkeit, Ihre Einstellungen anzupassen. Schließen Sie die Einrichtung ab, indem Sie auf **Ansicht Log-Quelle** drücken.

Note

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

Beginnen Sie mit der Überwachung der Daten

1. Um mit der Überwachung von Daten zu beginnen, gehen Sie zum Haupt-Dashboard und wählen Sie **Untersuchen** und **Daten-Explorer**.
2. Auf der Seite "Data Explorer" wählen Sie die `panther_logs.public` Datenbank aus dem Dropdown-Menü aus. Stellen Sie sicher, dass auch `bitwarden_events` in der Ansicht ist.



Panther Data Explorer

3. Sobald Sie alle erforderlichen Auswahlmöglichkeiten getroffen haben, wählen Sie **Abfrage ausführen**. Sie können die Abfrage auch für eine spätere Verwendung **Speichern unter**.
4. Eine Liste von Bitwarden-Ereignissen wird am unteren Bildschirmrand erstellt.

| | object | type | itemid | collectionid | groupid | policyid | memberid | actingUserid | installat |
|---------------------------|--------|------|--------|--------------|---------|----------|----------|--------------|-----------|
| View JSON | event | 1700 | null | null | null | | null | | null |
| View JSON | event | 1700 | null | null | null | | null | | null |
| View JSON | event | 1700 | null | null | null | | null | | null |
| View JSON | event | 1400 | null | null | | | null | | null |
| View JSON | event | 1000 | null | null | null | | null | | null |

Panther Event Logs

5. Ereignisse können erweitert und in JSON angezeigt werden, indem **Ansicht JSON** ausgewählt wird. ☹.

```
{
  actingUserId: [REDACTED]
  date:
  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:
  p_schema_version: 0
  p_source_id: [REDACTED]
  p_source_label: [REDACTED]
  type: 1000
}
```

Panther JSON Object

Für zusätzliche Informationen zu Bitwarden Organisation Veranstaltungen, siehe [hier](#). Zusätzliche Optionen für spezifische Anfragen sind verfügbar, siehe die [Panther Daten Explorer](#) Dokumentation für weitere Informationen.