ADMINISTRATOR KONSOLE > BERICHTE

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

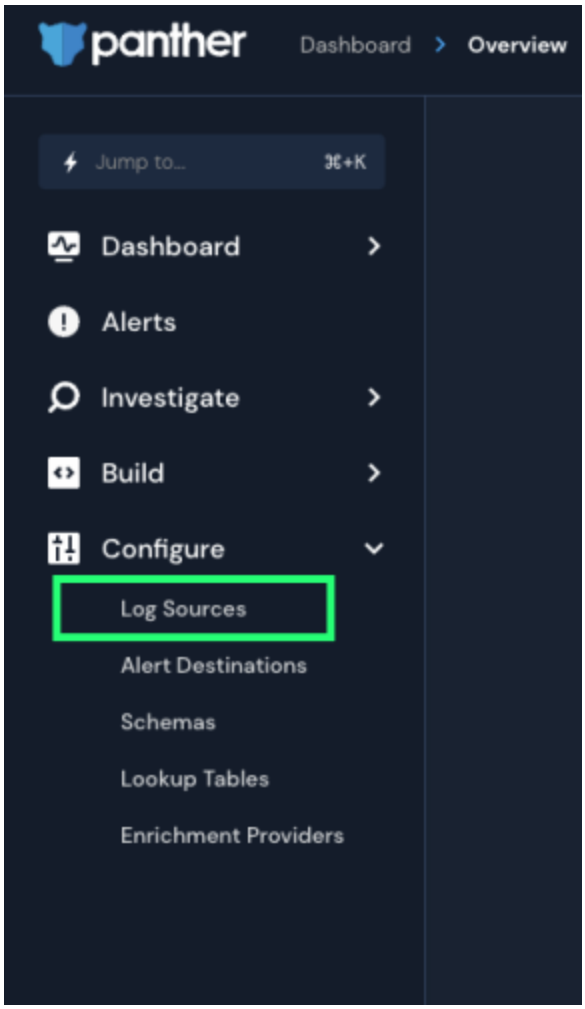
Erstellen Sie ein Panther-Konto

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

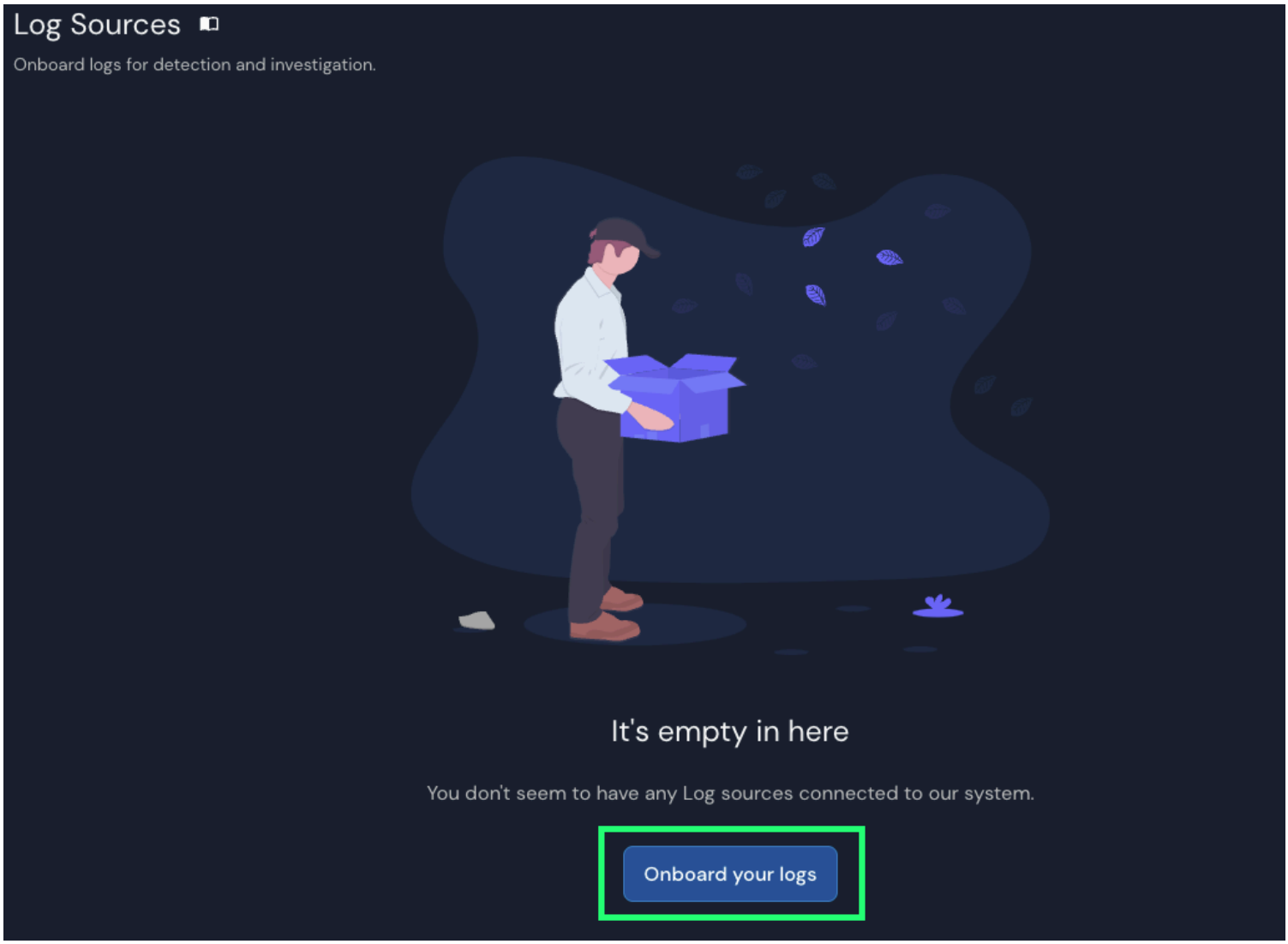
1. Greifen Sie auf das Panther-Dashboard zu.

2. Im Menü öffnen Sie das Dropdown-Menü **Konfigurieren** und wählen **Log-Quellen** aus.



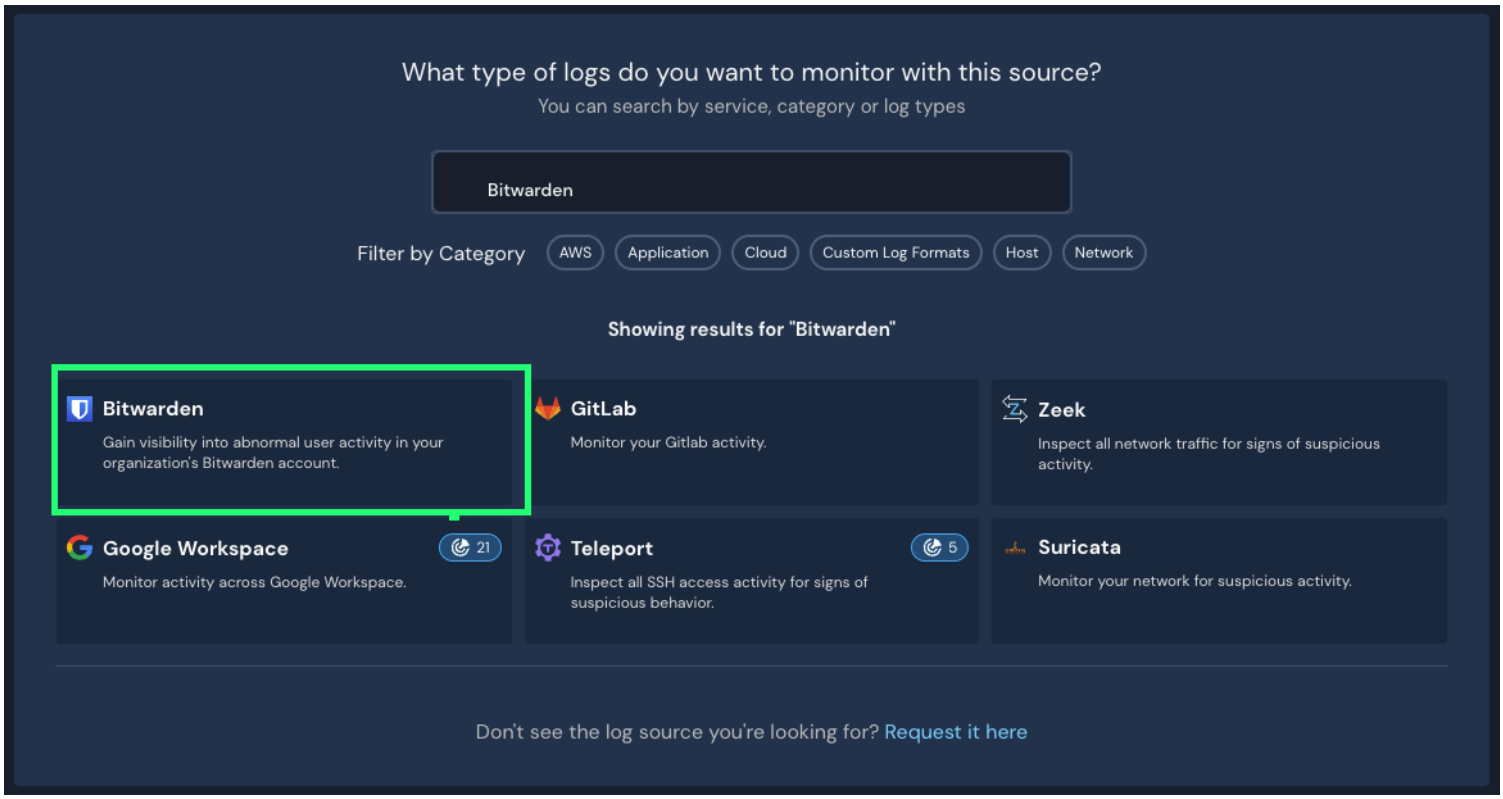
Panther Log Sources

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



Panther Onboard logs

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



Elastic Bitwarden integration

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

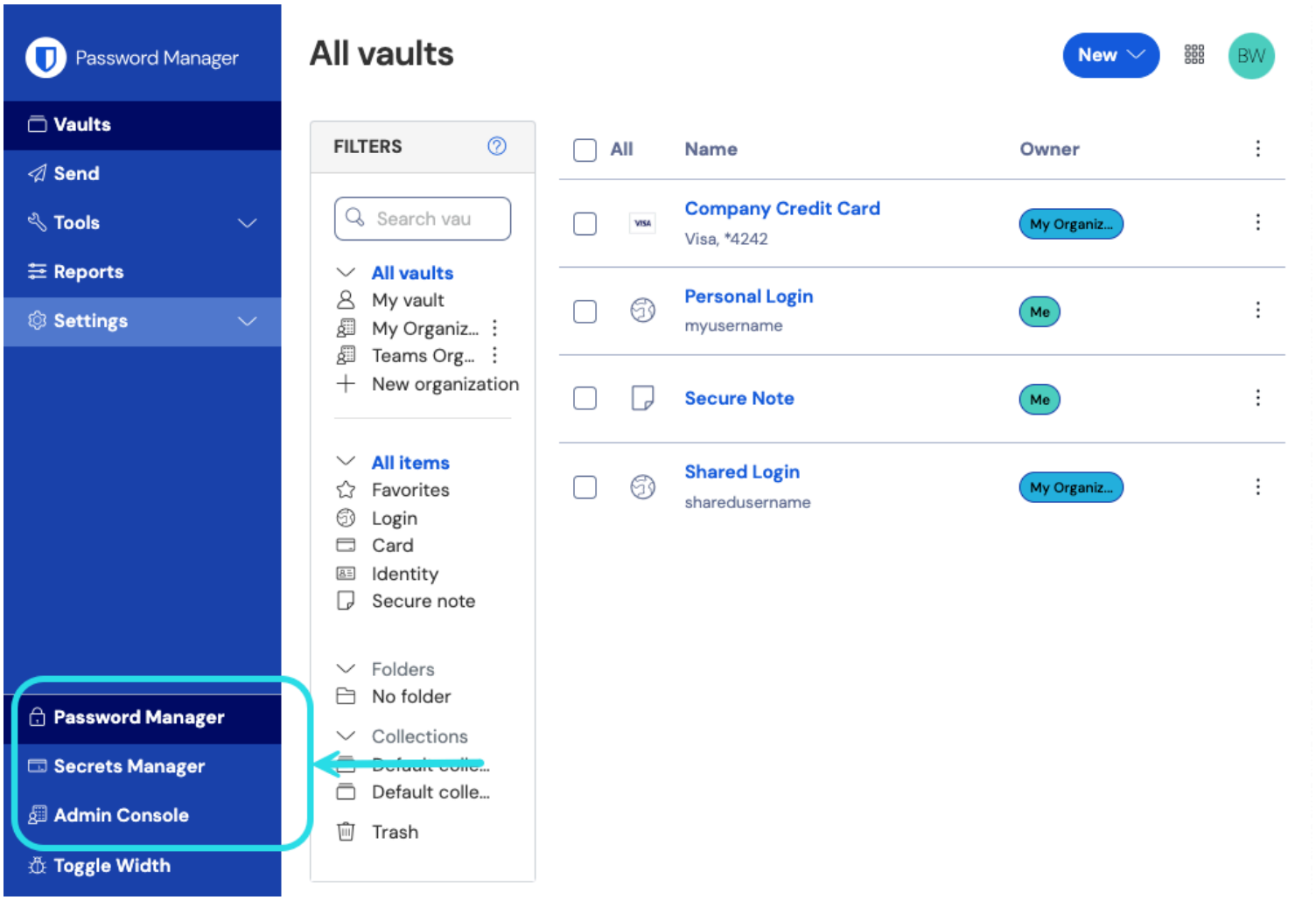
Verbinden Sie Ihre Bitwarden Organisation

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

> **ⓘ Note**
> Panther SIEM services are only available for Bitwarden cloud hosted organizations.

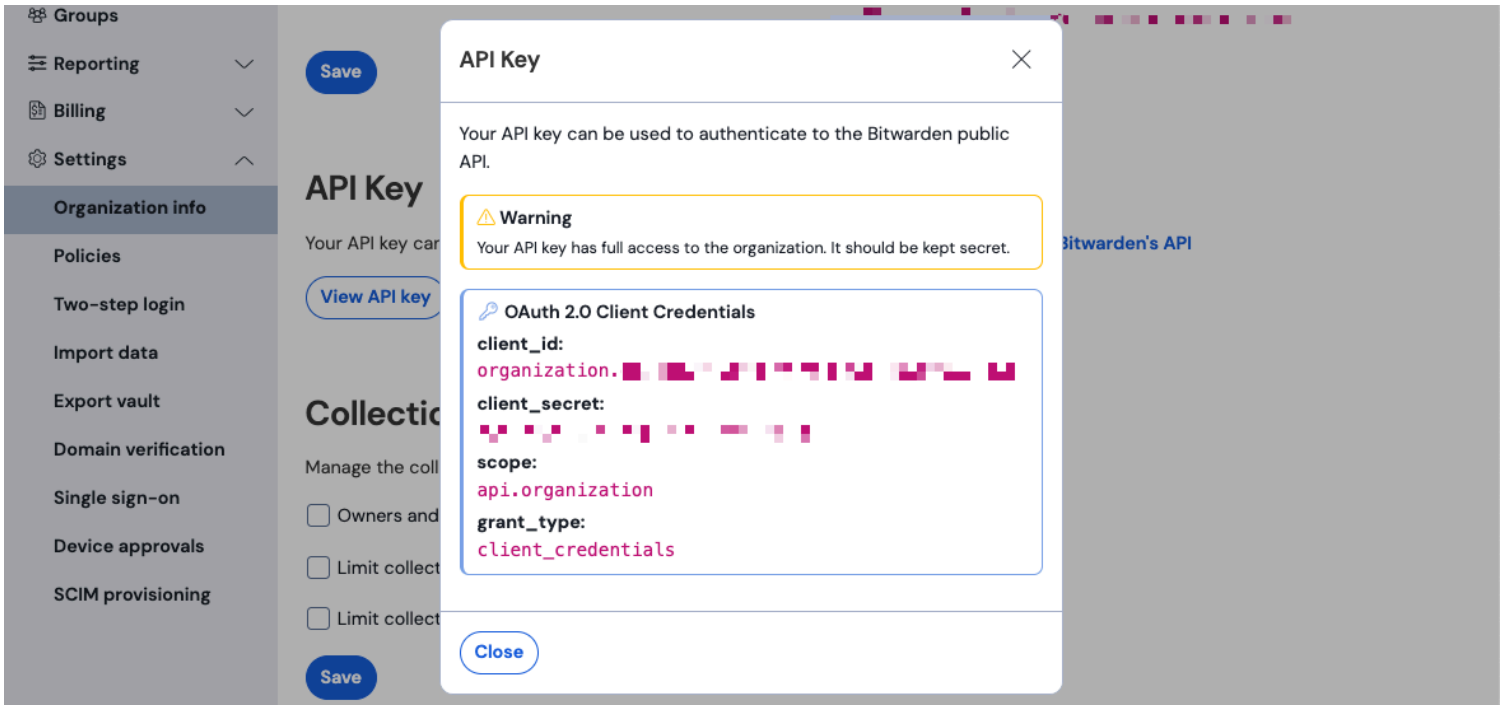
1. Geben Sie einen Namen für die Integration ein und wählen Sie dann **Einrichten.** aus.

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 Produktumschalter (⊞):



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.

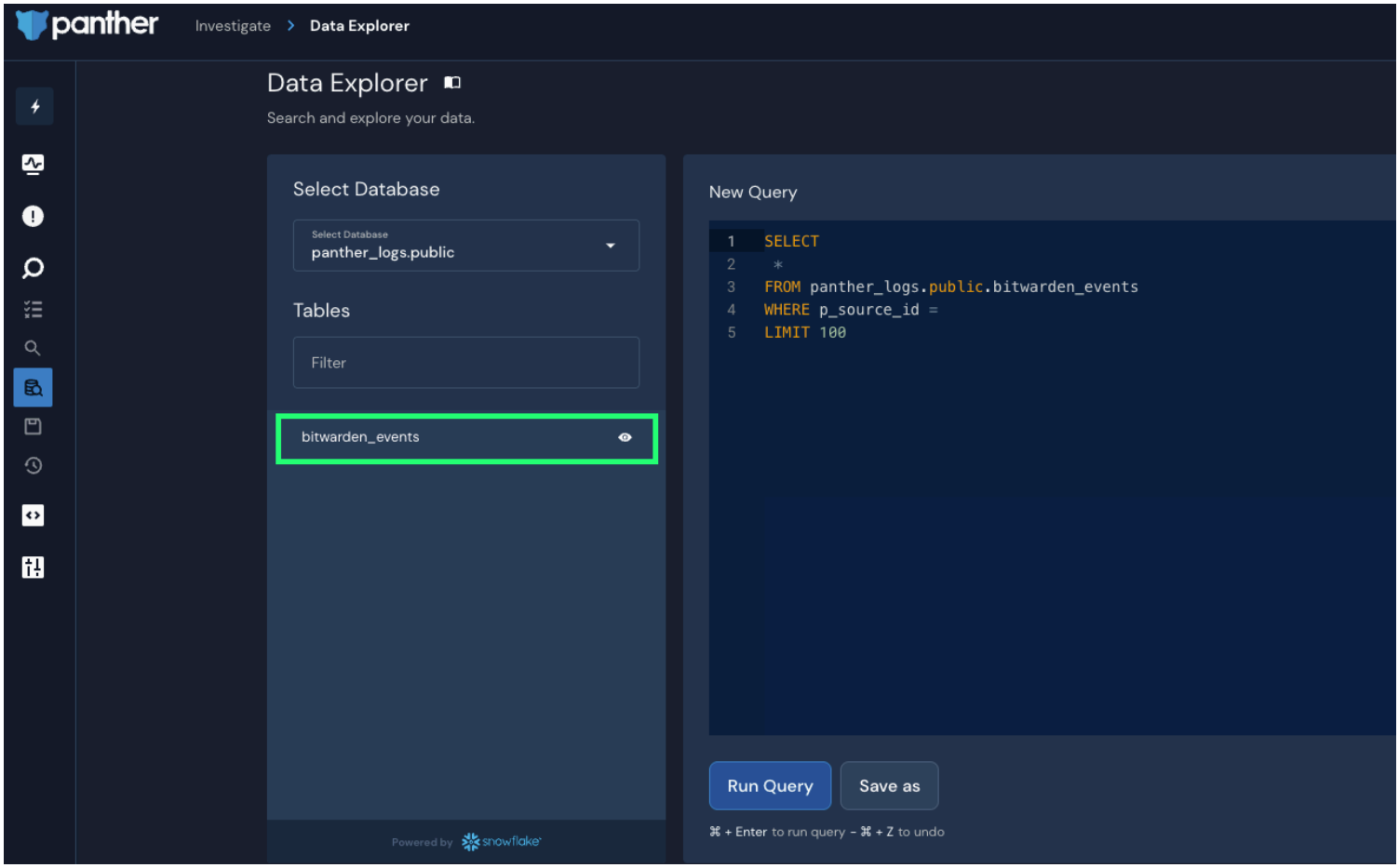
5. Panther wird einen Test zur Integration durchführen. Sobald ein erfolgreicher Test abgeschlossen wurde, haben Sie die Möglichkeit, Ihre Einstellungen anzupassen. Schließen Sie die Einrichtung ab, indem Sie auf **Ansicht Log-Quelle** drücken.

> **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**.

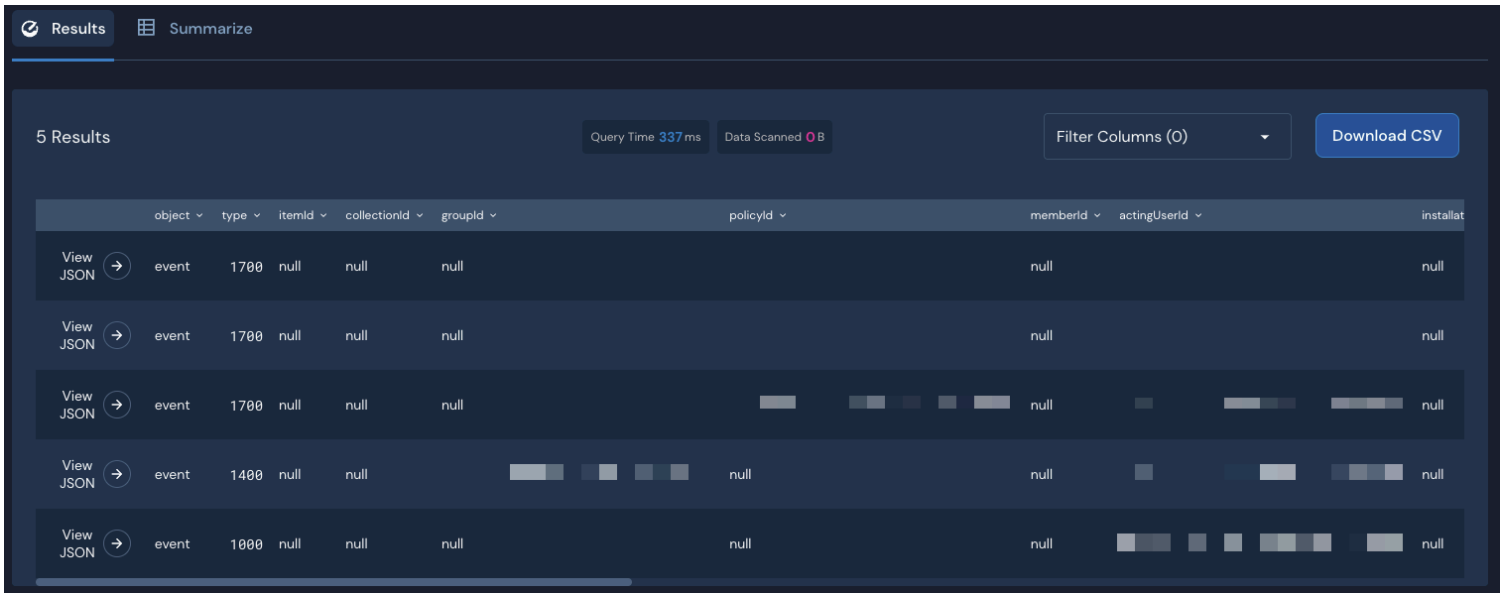
2. Auf der Seite "Data Explorer" wählen Sie die `panther_logs.public` Datenbank aus dem Dropdown-Menü aus. Stellen Sie sicher, dass auch `bitwarden_events` in der Ansicht ist.



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.



Panther Event Logs

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

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.