

管理者コンソール > レポート

パンサー SIEM

ヘルプセンターで表示:

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

パンサー SIEM

Pantherは、Bitwarden組織で使用できるセキュリティ情報およびイベント管理（SIEM）プラットフォームです。組織のユーザーは、パンサー監視システム上のBitwardenアプリでイベントの活動を監視することができます。

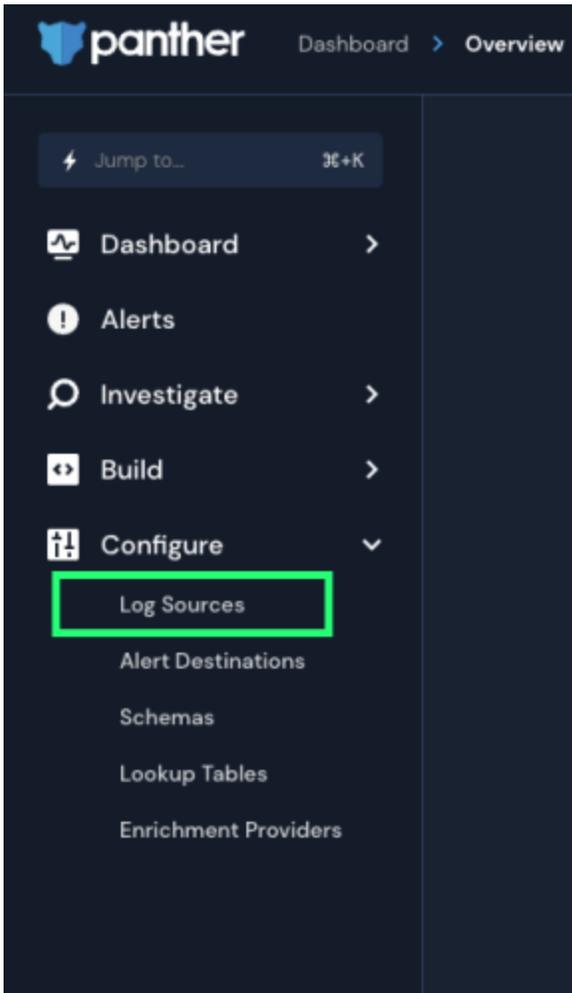
設定

パンサーアカウントを作成します

開始するには、パンサーアカウントとダッシュボードが必要です。彼らの[ウェブサイト](#)でパンサーアカウントを作成してください。

Panther Bitwarden ログソースを初期化します

1. パンサーダッシュボードにアクセスしてください。
2. メニューで、**設定**ドロップダウンを開き、**ログソース**を選択します。



Panther Log Sources

3. あなたのログを**オンボード**に選択します。

Log Sources

Onboard logs for detection and investigation.



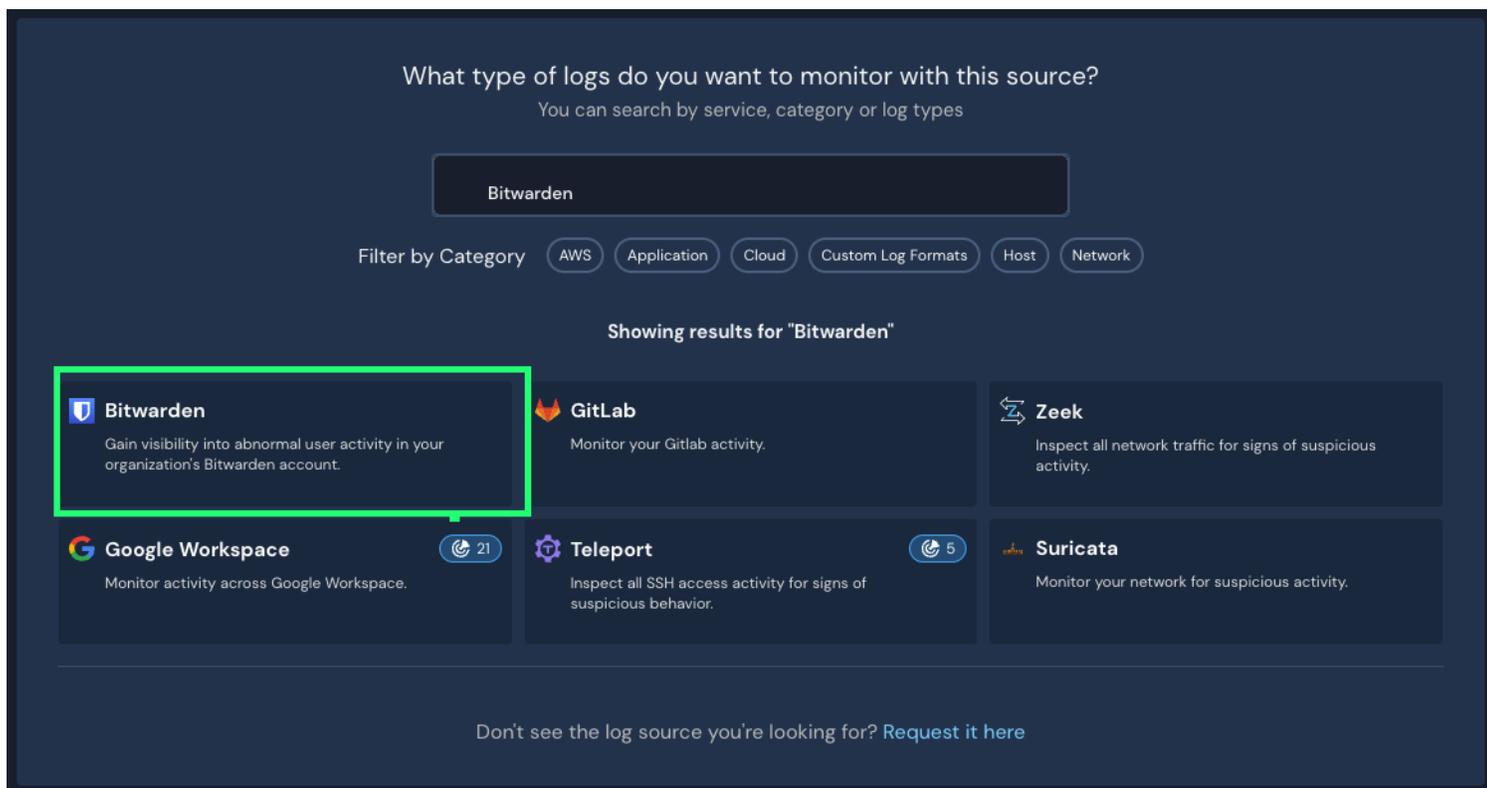
It's empty in here

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

[Onboard your logs](#)

Panther Onboard logs

4. カタログでBitwardenを検索してください。



Elastic Bitwarden integration

5. **Bitwarden**の統合をクリックし、**セットアップを開始**を選択します。

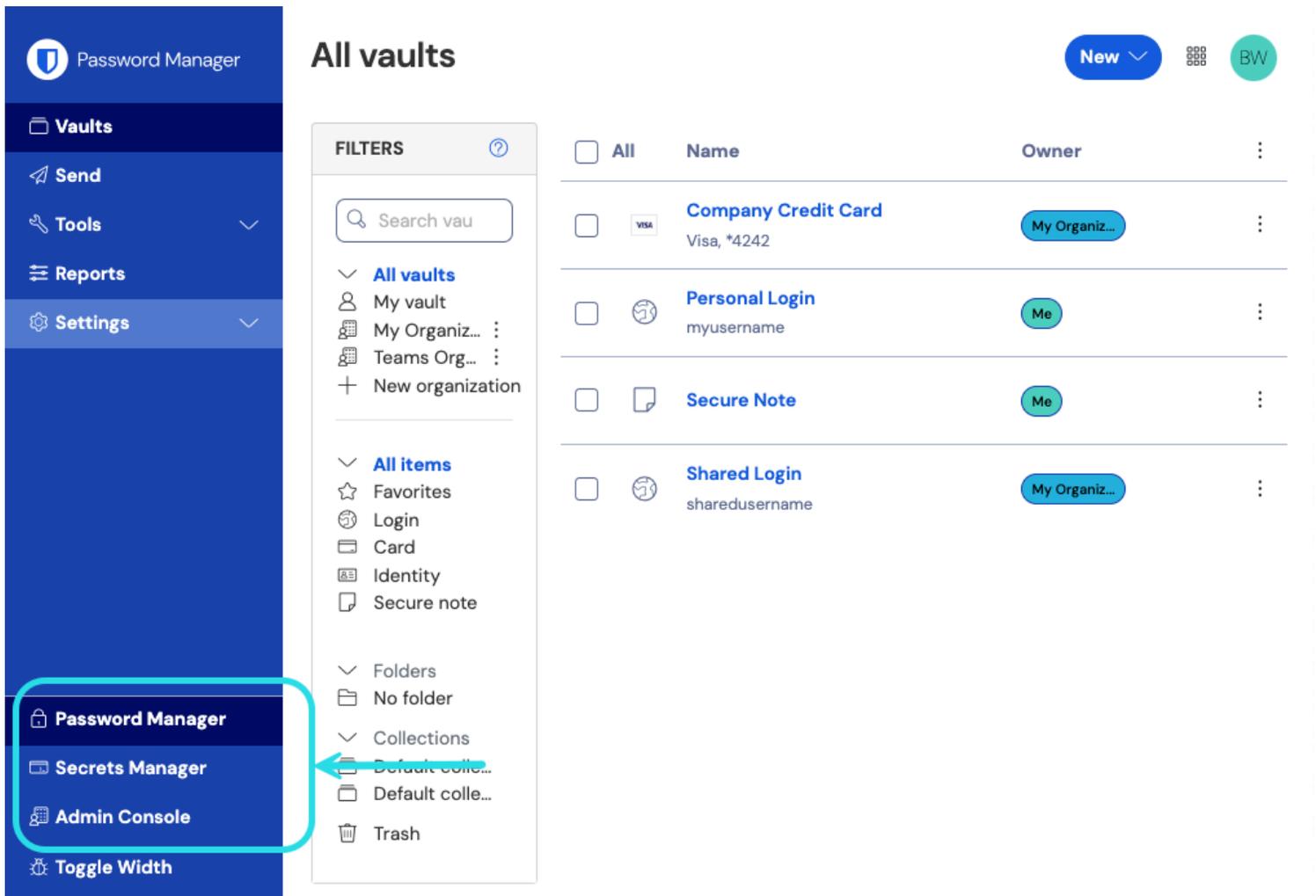
あなたのBitwarden組織を接続してください

セットアップを開始を選択した後、設定画面に移動します。

Note

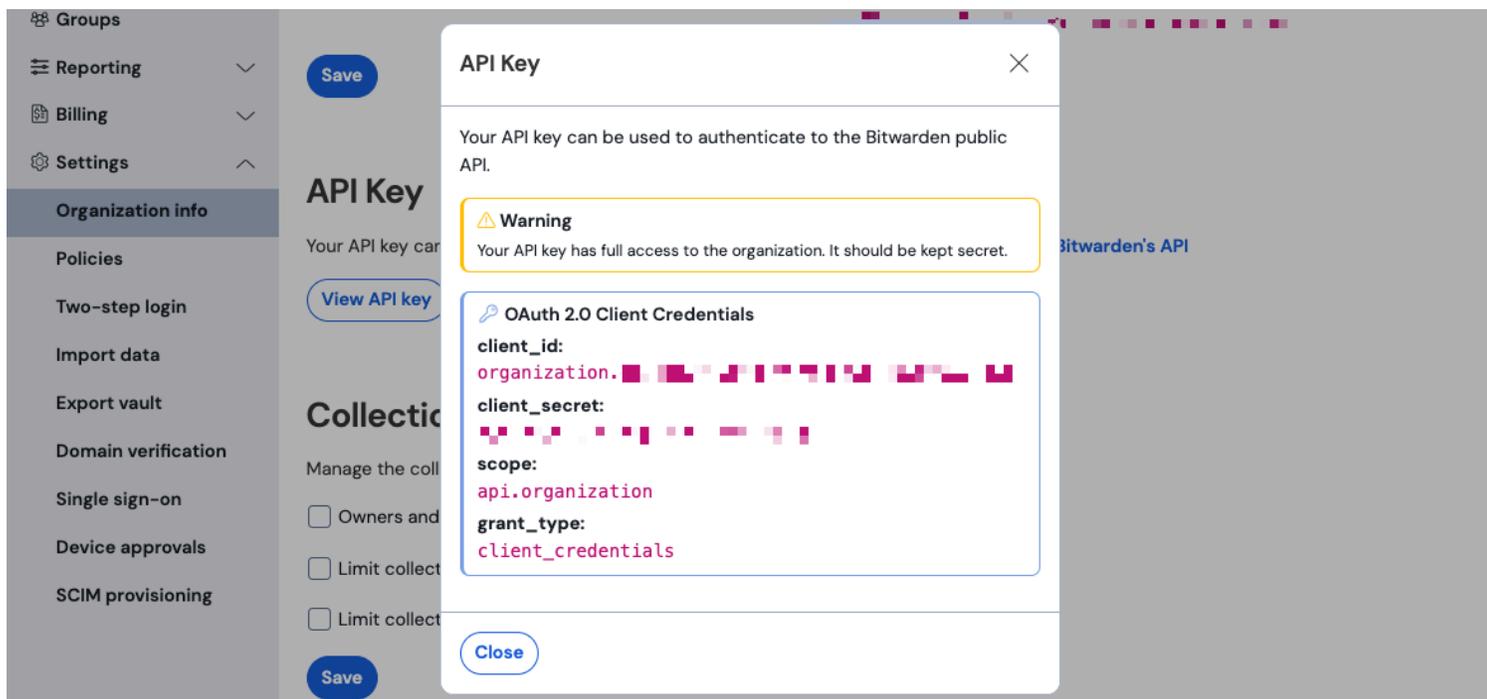
Panther SIEM services are only available for Bitwarden cloud hosted organizations.

1. 統合の名前を入力し、次に**設定**を選択します。
2. 次に、あなたのBitwarden組織の**クライアントID**と**クライアントシークレット**にアクセスする必要があります。この画面を開いたまま、別のタブでBitwardenウェブアプリにログインし、製品スイッチャー (🔗) を使用して**管理者コンソール**を開きます。



製品-スイッチャー

3. あなたの組織の**設定** → 組織情報画面に移動し、**APIキーを表示**ボタンを選択してください。あなたのAPIキー情報にアクセスするために、マスターパスワードを再入力するように求められます。



組織API情報

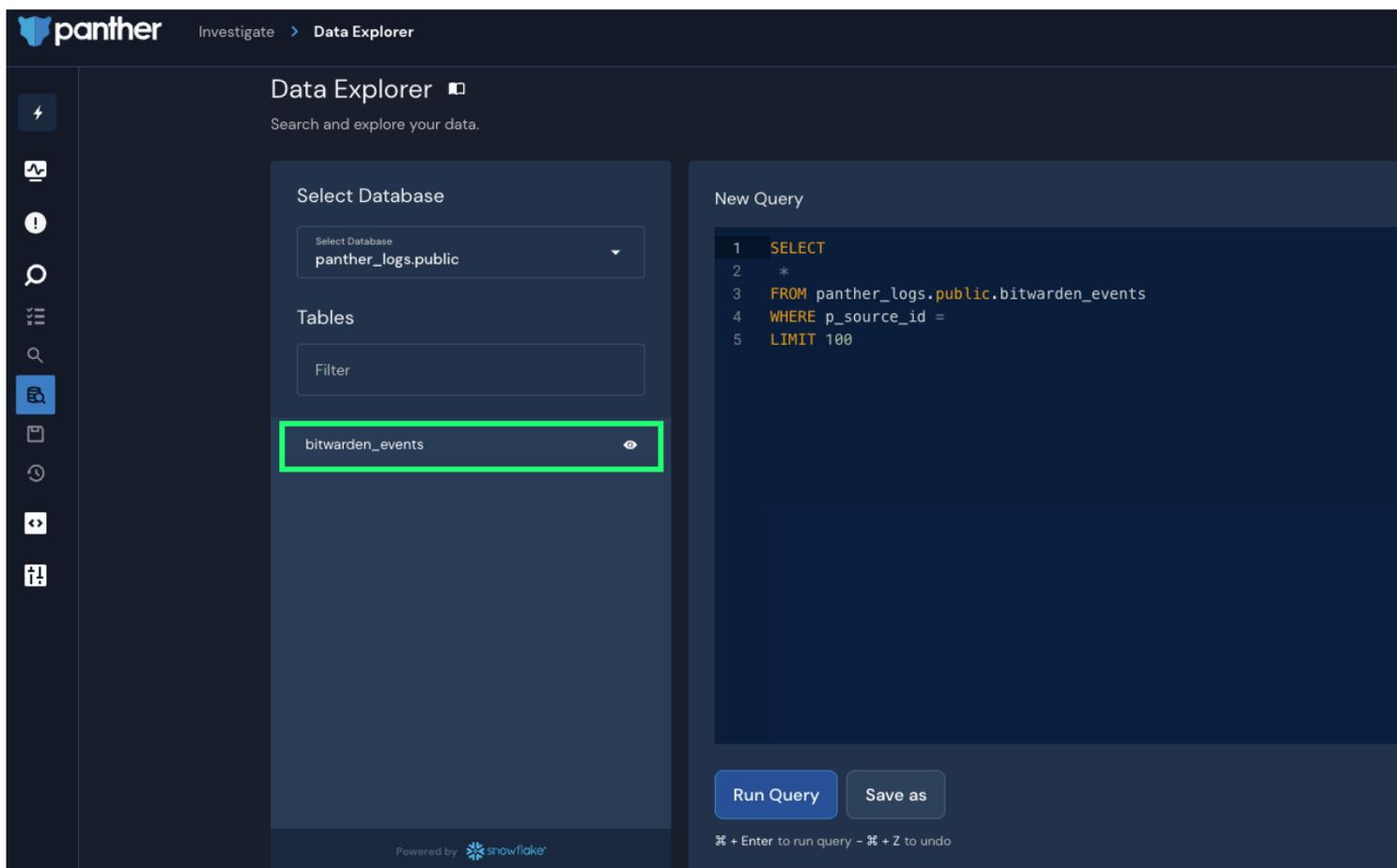
4. `client_id`と`client_secret`の値をコピーして、それぞれをBitwardenアプリの設定ページの対応する場所に貼り付けてください。情報を入力したら、**設定**を再度選択して続けてください。
5. パンサーは統合についてのテストを実行します。成功したテストが完了したら、設定を調整するオプションが与えられます。設定を完了するには、**ログソースを表示**を押してください。

Note

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

データの監視を開始します

1. データの監視を開始するには、プライマリダッシュボードに移動し、**調査**と**データエクスプローラ**を選択してください。
2. データエクスプローラーページで、ドロップダウンメニューから`panther_logs.public`データベースを選択してください。`bitwarden_events` も表示されていることを確認してください。



The screenshot shows the Panther Data Explorer interface. On the left is a navigation sidebar with various icons. 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 table named "bitwarden_events" 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 right, there are "Run Query" and "Save as" buttons, and a keyboard shortcut提示: ⌘ + Enter to run query - ⌘ + Z to undo. The interface is powered by Snowflake.

Panther Data Explorer

3. 必要なすべての選択を行ったら、**クエリを実行**を選択してください。
また、別の時間でクエリを使用するために**名前を付けて保存**することもできます。
4. 画面の下部にBitwardenのイベントリストが表示されます。

	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. イベントは、**JSONを表示**を選択することでJSONで拡張して表示することができます。☹.

```
{
  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

Bitwarden組織のイベントに関する追加情報については、[ここ](#)をご覧ください。特定のクエリに対する追加のオプションが利用可能です、[パンサーデータエクスプローラーのドキュメンテーション](#)を参照してください。詳細情報はそちらでご確認いただけます。