

# <sup>管理者コンソール > レポート</sup> パンサー SIEM

ヘルプセンターで表示: https://bitwarden.com/help/panther-siem/

# **U bit**warden

## 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。

# **D** bit warden



Panther Onboard logs

4. カタログでBitwardenを検索してください。

## **D** bit warden

What ty Filter by Cate	/pe of logs do you want to monitor You can search by service, category or lo Bitwarden Gory AWS Application Cloud Custom Lo	bg Formats Host Network
Bitwarden Gain visibility into abnormal user activity in your organization's Bitwarden account.	Showing results for "Bitwarden" GitLab Monitor your Gitlab activity.	Zeek           Inspect all network traffic for signs of suspicious activity.
Google Workspace (C 2 Monitor activity across Google Workspace.	Teleport Inspect all SSH access activity for signs of suspicious behavior.	6 5 Suricata Monitor your network for suspicious activity.
	on't see the log source you're looking for? R	Request it here

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。

### (i) 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(謡)を使用して管理者コンソールを開きます。

## **D** bitwarden

D Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS ⑦		Name	Owner	:
🖉 Send					
$\ll$ Tools $\qquad \qquad \bigvee$	Q Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
₩ Reports	✓ All vaults				
🕸 Settings 🛛 🗸 🗸	<ul> <li>My vault</li> <li>My Organiz :</li> <li>Toomo Org</li> </ul>		Personal Login myusername	Me	÷
	<ul> <li>Hearns org :</li> <li>+ New organization</li> </ul>		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>④ Login</li> <li>⊡ Card</li> <li>Identity</li> <li>↓ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	:
<ul> <li>Password Manager</li> <li>Secrets Manager</li> <li> <i>∰</i> Admin Console <i>∰</i> Toggle Width         </li> </ul>	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Default colle</li> <li>Default colle</li> <li>Trash</li> </ul>				

*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。

#### Secure and trusted open source password manager for business

## **D** bit warden



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、Q. 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。

#### Secure and trusted open source password manager for business

## **D** bit warden

<b>\</b>	anther Investigate > Data Explorer	
4	Data Explorer Search and explore your data.	
<u>₹</u>	Select Database	New Query
Q ∰ α 🖬	Select Database panther_logs.public	<pre>1 SELECT 2 * 3 FROM panther_logs.public.bitwarden_events 4 WHERE p_source_id = 5 LIMIT 100</pre>
৩ ↔	Ditwarden_events •	
		Run Query Save as # + Enter to run guery - # + Z to undo
	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。

# **D** bit warden

Q	) Res	ults	🗄 Sumn	narize											
	5 Res	ults								Data Scanned <mark>O</mark> B	Filter C	Columns (O)		Download	ICSV
			object ~	type ~	itemld ~	collectionId ~	groupId ~			policyld ~	memberld ~	actingUserld v			installat
	Vie JSC	ew on →	event	1700	null	null	null				null				null
	Vie JSC	ew →	event	1700	null	null	null				null				null
	Vie JSC	ew on →	event	1700	null	null	null			-	 null				null
	Vie JSC	ew →	event	1400	null	null	I	-	•	null	null		_		null
	Vie JSC	w →	event	1000	null	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:
	date:
	device: 9
	ipAddress:
	object: event
►	p_any_ip_addresses: [] 1 item
	p_event_time:
	p_log_type: Bitwarden.Events
	p_parse_time:
	p_row_id:
	p_schema_version: <b>O</b>
	p_source_id:
	p_source_label:
}	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。