

CONSOLE ADMIN > COMPTE RENDU

Panther SIEM

Panther SIEM

Panther est une plateforme de gestion des informations et des événements de sécurité (SIEM) qui peut être utilisée avec les organisations Bitwarden. Les utilisateurs de l'organisation peuvent surveiller l'[activité événementielle](#) avec l'application Bitwarden sur leur système de surveillance Panther.

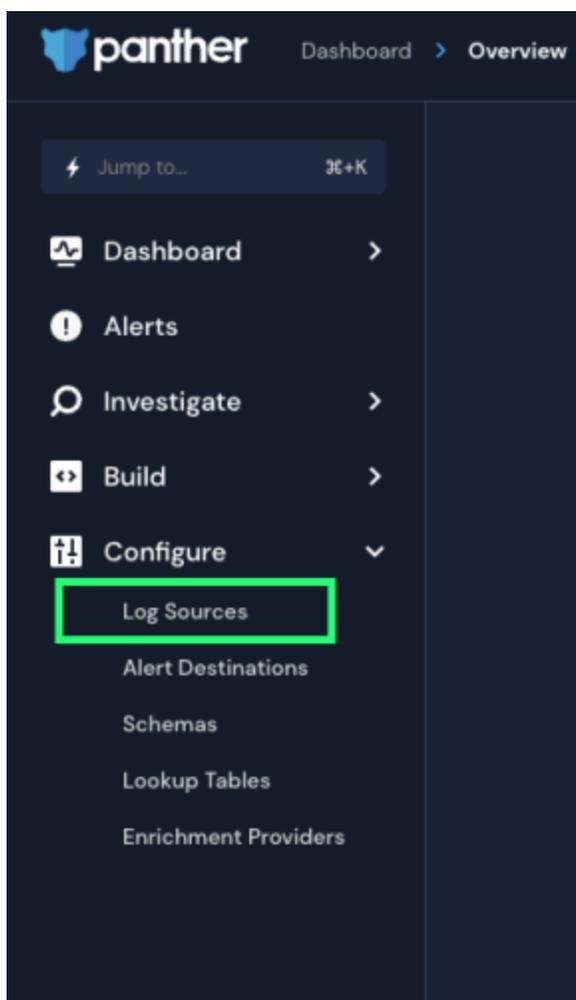
Configuration

Créez un compte Panther

Pour commencer, vous aurez besoin d'un compte Panther et d'un tableau de bord. Créez un compte Panther sur leur [site web](#).

Initialiser la source de journal Bitwarden Panther

1. Accédez au tableau de bord Panther.
2. Dans le menu, ouvrez le menu déroulant **Configurer** et sélectionnez **Sources de journal**.



Panther Log Sources

3. Sélectionnez **Embarquez vos journaux**.

Log Sources

Onboard logs for detection and investigation.



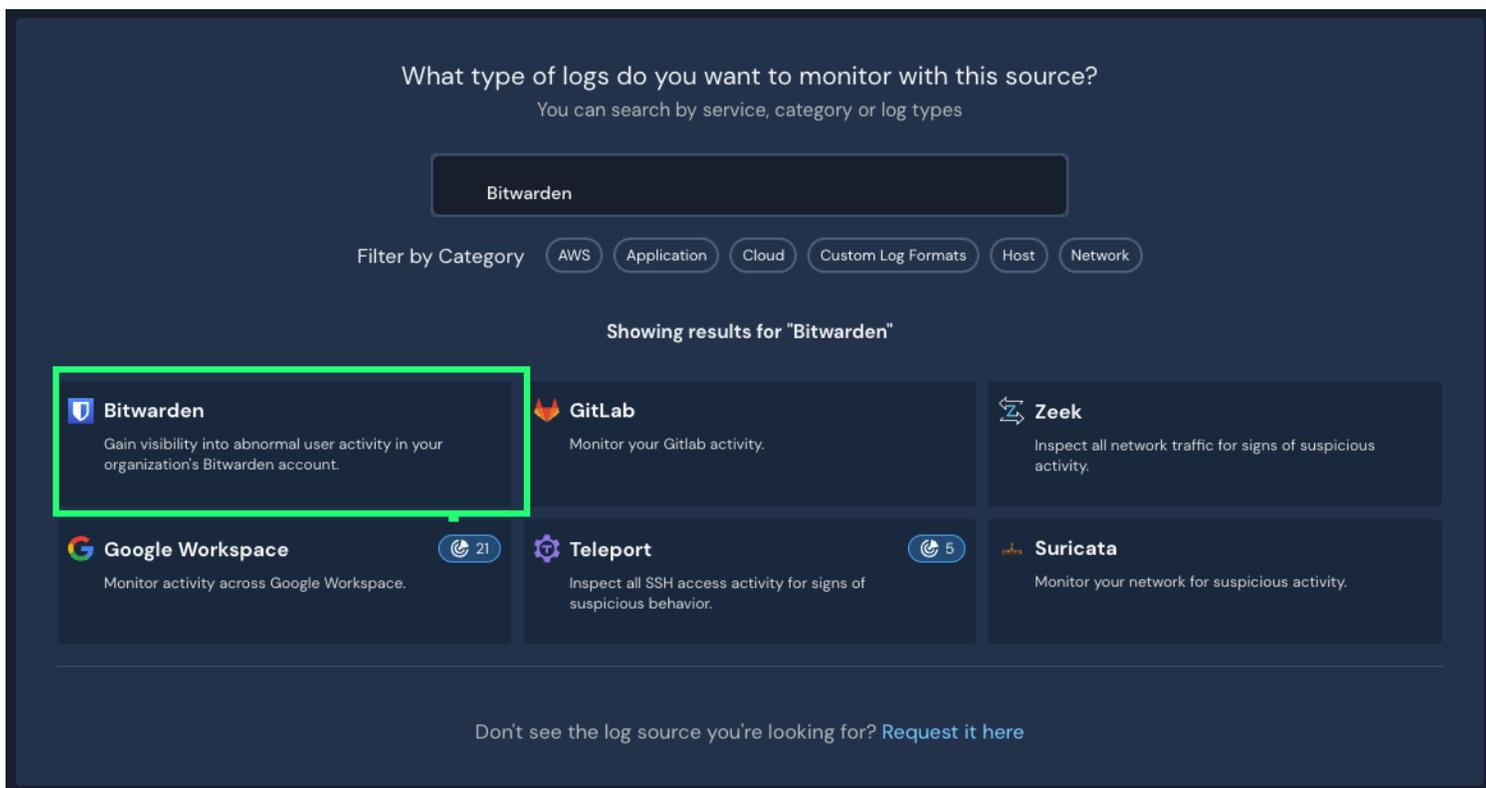
It's empty in here

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

[Onboard your logs](#)

Panther Onboard logs

4. Recherchez **Bitwarden** dans le catalogue.



Elastic Bitwarden integration

5. Cliquez sur l'intégration **Bitwarden** et sélectionnez **Commencer l'installation**.

Connectez votre organisation Bitwarden

Après avoir sélectionné **Démarrer l'installation**, vous serez dirigé vers l'écran de configuration.

Note

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

1. Entrez un nom pour l'intégration puis sélectionnez **Configuration**.
2. Ensuite, vous devrez accéder à votre **ID de client** et **Secret de client** de votre organisation Bitwarden. Gardez cet écran ouvert, sur un autre onglet, connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit ():

Password Manager

- Vaults
- Send
- Tools
- Reports
- Settings

All vaults

FILTERS

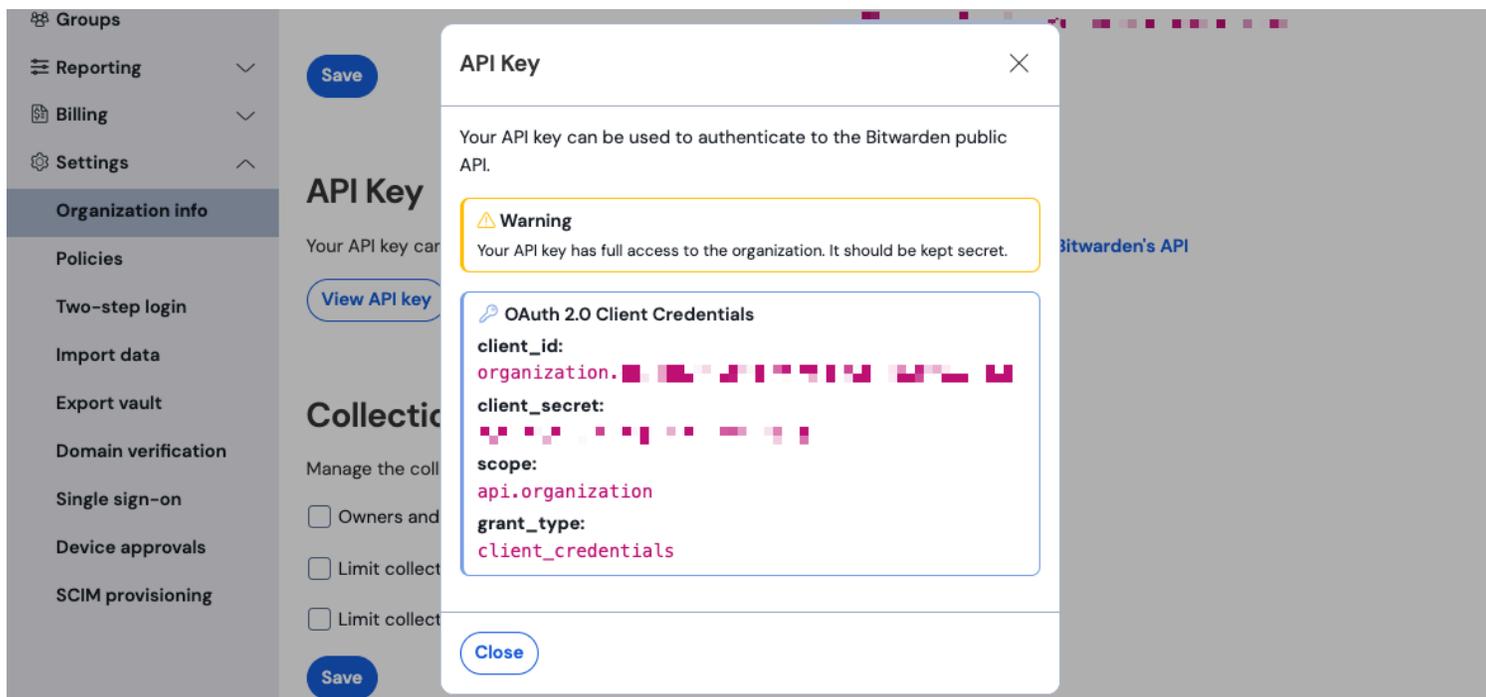
Search vau

- 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 shareusername	My Organiz...	⋮

commutateur-de-produit

3. Naviguez vers l'écran d'informations de votre **Paramètres** → Organisation de votre organisation et sélectionnez le bouton **Afficher la clé API**. On vous demandera de ressaisir votre mot de passe principal afin d'accéder à vos informations de clé API.



Informations sur l'API de l'organisation

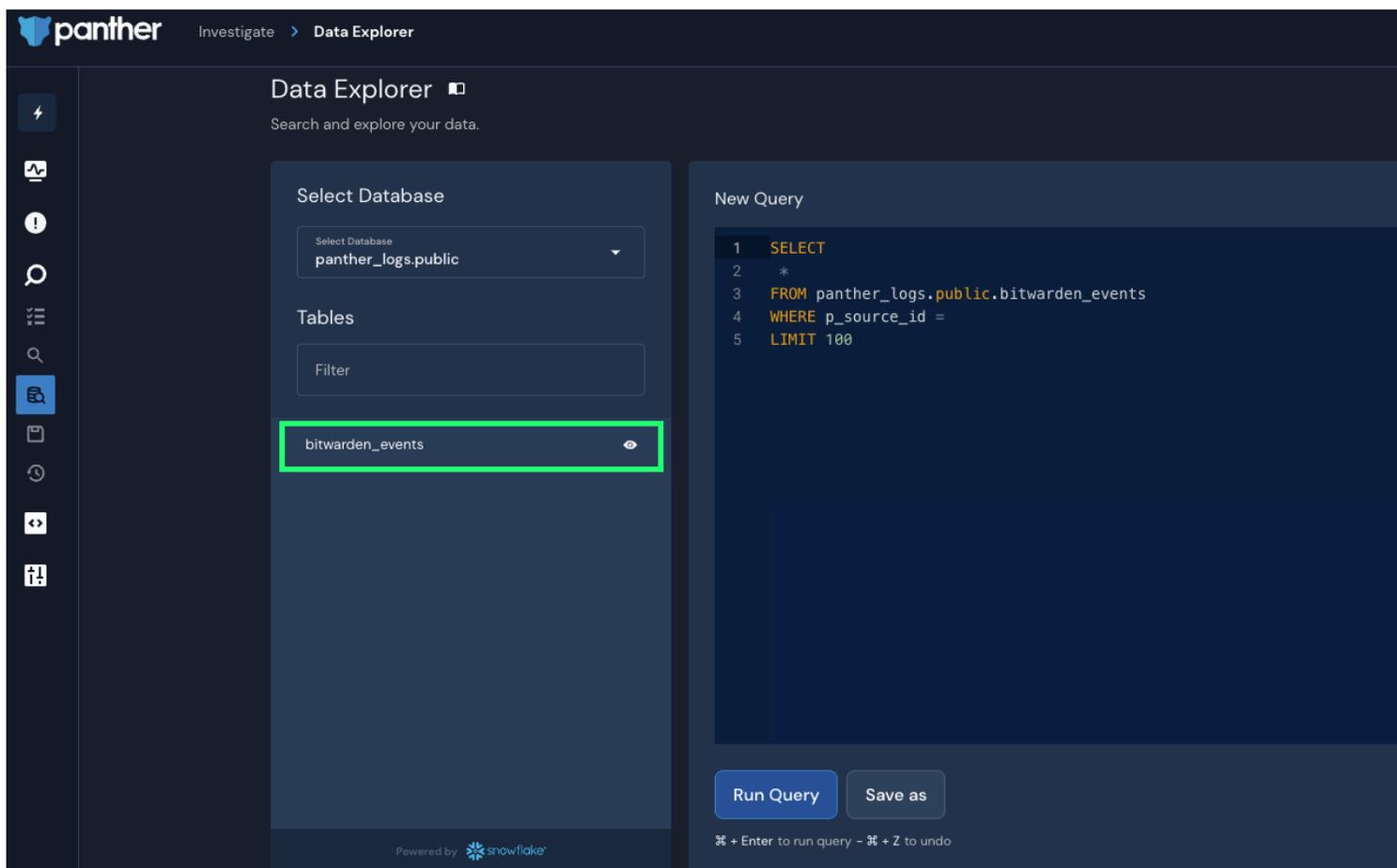
4. Copiez et collez les valeurs `client_id` et `client_secret` dans leurs emplacements respectifs sur la page de configuration de l'application Bitwarden. Une fois que vous avez entré les informations, continuez en sélectionnant à nouveau **Configuration**.
5. La panthère effectuera un test sur l'intégration. Une fois qu'un test réussi a été effectué, vous aurez la possibilité d'ajuster vos préférences. Terminez l'installation en appuyant sur **Afficher la source du journal**.

Note

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

Commencez à surveiller les données

1. Pour commencer à surveiller les données, rendez-vous sur le tableau de bord principal et sélectionnez **Enquêteur** et **Explorateur de Données**.
2. Sur la page Explorateur de Données, sélectionnez la base de données `panther_logs_public` dans le menu déroulant. Assurez-vous que `bitwarden_events` est également affiché.



Panther Data Explorer

3. Une fois que vous avez effectué toutes vos sélections requises, sélectionnez **Exécuter la requête**. Vous pouvez également **Enregistrer sous** pour utiliser la requête à un autre moment.
4. Une liste des événements Bitwarden sera produite au bas de l'écran.

	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. Les événements peuvent être développés et affichés en JSON en sélectionnant **Afficher JSON**.

```
{
  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: 0
  p_source_id:
  p_source_label:
  type: 1000
}
```

Panther JSON Object

Pour plus d'informations concernant les événements de l'organisation Bitwarden, voir [ici](#). Des options supplémentaires pour des requêtes spécifiques sont disponibles, consultez la documentation de l'[Explorateur de Données Panther](#) pour plus d'informations.