Ubitwarden Hilfezentrum Artikel

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.



Panther Onboard logs

4. Suchen Sie Bitwarden im Katalog.

What typ Bit	e of logs do you want to monitor with the You can search by service, category or log types warden	his source?
Filter by Categor	y AWS Application Cloud Custom Log Formats	Host Network
	Showing results for "Bitwarden"	
Bitwarden Gain visibility into abnormal user activity in your organization's Bitwarden account.	₩ GitLab Monitor your Gitlab activity.	Z Zeek Inspect all network traffic for signs of suspicious activity.
G Google Workspace (C 21) Monitor activity across Google Workspace.	Teleport (65) Inspect all SSH access activity for signs of suspicious behavior.	مغم Suricata Monitor your network for suspicious activity.
Don	't see the log source you're looking for? Request i	t here

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.

① 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 (
):

Password Manager	All vaults			New 🗸	BW BW
🗇 Vaults	FILTERS ⊘		Name	Owner	:
🕼 Send					
🖏 Tools 🛛 🗸 🗸	🔍 Search vau	VISA	Company Credit Card Visa, *4242	My Organiz	:
፰ Reports	✓ All vaults		N N N		
🕸 Settings 🛛 🗸 🗸	 ∠ My vault ∠ My Organiz : ∠ Tooms Org 		Personal Login myusername	Me	:
	+ New organization		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ۞ Login □ Card □ Identity □ Secure note 	0 Ø	Shared Login sharedusername	My Organiz	÷
 Password Manager □ Secrets Manager ℬ Admin Console Ճ Toggle Width 	 Folders No folder Collections Default colle Default colle Trash 				

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.

Secure and trusted open source password manager for business

D bit warden



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 Q. **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.

Secure and trusted open source password manager for business

D bit warden

() () ()	anther Investigate > Data Explorer	
+	Data Explorer n Search and explore your data.	
<u>~</u>	Select Database	New Query
Q 	select Database panther_logs.public	<pre>1 SELECT 2 * 3 FROM panther_logs.public.bitwarden_events 4 WHERE p source id =</pre>
ୟ ଜ୍	Filter	5 LIMIT 100
ଅ ଓ	bitwarden_events	
↔ t		
		Run Query Save as
	Powered by 🔆 showflake	¥ + Enter to run query − ¥ + Z to undo

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.

Q	Res	ults	🗄 Sumn	narize										
	5 Res	ults							Data Scanned O B	Filter C	Columns (0)		Download	ICSV
			object ~	type ~	itemld ~	collectionId ~	groupld ~		policyld ~	memberld ~	actingUserld ~			installat
	Vie JSC	ew on →	event	1700	null	null	null			null				null
	Vie JSC	ew on →	event	1700	null	null	null			null				null
	Vie JSC	w →	event	1700	null	null	null		-	 null				null
	Vie JSC	ew →	event	1400	null	null	-		null	null		-	-	null
	Vie JSC	w on →	event	1000	null	null	null		null	null	-	• •		null

Panther Event Logs

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

{	
	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: O
	p_source_id:
	p_source_label:
}	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.