1 Password Integrations

Introduction

With 1Password Business, you can send your account activity to your security information and event management (SIEM) system, using the 1Password Events API.

Get reports about 1Password activity, such as sign-in attempts and item usage, while you manage all your company's applications and services from a central location.

With 1Password Events Reporting and Elastic SIEM, you can:

- Control your 1Password data retention
- Build custom graphs and dashboards
- Set up custom alerts that trigger specific actions
- Cross-reference 1Password events with the data from other services

Events

Sign-in Attempts

Use the 1Password Events API to retrieve information about sign-in attempts. Events include the name and IP address of the user who attempted to sign in to the account, when the attempt was made, and – for failed attempts – the cause of the failure.

Item Usages

This uses the 1Password Events API to retrieve information about items in shared vaults that have been modified, accessed, or used. Events include the name and IP address of the user who accessed the item, when it was accessed, and the vault where the item is stored.

Requirements

You can set up Events Reporting if you're an owner or administrator.

Ready to get started?

- https://support.1password.com/events-reporting/

1Password Integration Procedures

Please provide the following information to CyTech:

The 1Password Events API Beat returns information from 1Password through requests to the Events REST API and sends that data securely to Elasticsearch. Requests are authenticated with a bearer token. Issue a token for each application or service you use.

To connect your 1Password account to Elastic:

1. Download and install the 1Password Events API Elastic Beat from the 1Password GitHub repository.

2. Download an example eventsapibeat.yml file .

3. Configure the YAML file for the Beat to include:

- The bearer token you saved previously in the auth_token fields for each 1Password event type you plan to monitor.
- The output for events (sent directly to Elasticsearch, or through Logstash).
- Any other configurations you want to customize.

4. Run the following command: ./eventsapibeat -c eventsapibeat.yml -e

You can now use Elasticsearch with the 1Password Events API Beat to monitor events from your 1Password account. The returned data will follow the Elastic Common Schema (ECS) specifications.

Collect events from 1Password Events API

1. URL of 1Password Events API Server - options: https://events.1password.com, https://events.1password.ca, https://events.1password.eu, https://events.ent.1password.com. path is automatic

2. 1Password Authorization Token - Bearer Token, e.g. "eyJhbGciO..."

Revision #3
Created 23 April 2024 10:07:49
Updated 19 June 2024 06:54:01