Non-native SIEM

Non-native SIEM

Bitwarden provides comprehensive event logging capabilities that enable integration with Security Information and Event Management (SIEM) platforms beyond the solutions for which official integrations are offered. This article provides guidance for integrating Bitwarden with those SIEM solutions, such as popular platforms like Datadog, etc. etc.

Requirements

To integrate Bitwarden with your SIEM platform, you will need:

- A Bitwarden Teams or Enterprise plan (required for event logging and API access).
- Administrative access to your Bitwarden organization via the admin, owner, or custom role.
- Understanding of your SIEM platform's available data ingestion methods.

Data access

Bitwarden provides multiple methods for accessing data that may be relevant to your SIEM monitoring, allowing flexibility in how your platform ingests information:

Public API access

(**Recommended**) The Bitwarden Public API provides programmatic access to event logs through the `/events` endpoint. The API returns JSON-formatted event data that can be consumed by most modern SIEM platforms, and can be used to access more organization data than just events, including member information through the `/members` endpoint, group data through the `/groups` endpoint, and collection data through the `/collections` endpoint. Learn more about the API.

CLI data extraction

The Password Manager CLI can be used to extract additional data that may provide useful context to API-provided event analysis, for example using the `list` command to retrieve item data correlated to a member, group, or collection ID accessed from the API. Learn more about the Password Manager CLI.

Event exports

For SIEM platforms that prefer file-based ingestion, Bitwarden allows manual exporting of event logs in .csv format. This method works well for batch processing scenarios and historical data analysis. Learn more about exporting event logs.