bitwarden | Help Center Article

ADMIN CONSOLE > OVERSIGHT & VISIBILITY > EVENT LOGGING

Monitoring Event Logs

View in the help center:
https://bitwarden.com/help/monitoring-event-logs/

Monitoring Event Logs

Event monitoring with SIEM (system information and event management) integration is an important tool for monitoring your organization to maintain best security practices and ensure compliance. The following sections highlight several monitoring reference points that will provide increased observability of your Bitwarden solutions. This monitoring includes enabling insights into user actions in the vault, and providing examples of targets for automated alerting.

These events have been selected from the Bitwarden Event logs. By configuring a combination of instant alerts with alerting-over-time against the events that matter to your business, you will be able to audit your organization's use of Bitwarden in accordance with your unique security landscape.

Understanding Logs

Various SIEM platforms integrate with Bitwarden to review critical information on day to day vault usage.


```
{
  "object": "event",
  "type": 1107,
  "itemId": "d1a4f236-90f5-4a8c-90a8-b1ee009feb11",
  "collectionId": null,
  "groupId": null,
  "policyId": null,
  "memberId": null,
  "actingUserId": "75efc9f5-f405-47ad-9557-af9700df73cf",
  "installationId": null,
  "date": "2024-09-17T12:26:22.188Z",
  "device": 9,
  "ipAddress": "147.161.248.179",
  "secretId": null,
  "serviceAccountId": null
}
```


Panther JSON Object

SIEM event monitoring platforms will provide specific fields which should be monitored to maintain high security standards:

Value	Description
`actingUserEmail`	The email of the user performing the action.
`actingUserId`	Unique id of user performing action.

Value	Description
`actingUserName`	Name of the user performing an action.
`collectionId`	Organization collection id.
`device`	Numerical id of device. Exact mapping can be located here.
`ipAddress`	The ip address that performed the event.
`itemId`	Vault item (cipher, secure note, etc..) of the organization vault.
`policyId`	Organization policy update. See organization events here.

Concerning trends

Tracking Bitwarden usage trends can identify questionable activity, or potential security threats:

Abnormal Rate of failed login attempts

- Failed Login attempts
  - `1005` Login attempt failed with incorrect password
  - `1006` Login attempt failed with incorrect two step login.

Abnormal rate of viewing sensitive or hidden fields

- Viewing item
  - `1107` Viewed item `item-identifier`
  - `1108` Viewed password for item `item-identifier`
  - `1109` Viewed hidden field for item `item-identifier`
  - `1110` Viewed security code for item `item-identifier`

- Copying item fields

- `1111` Copied password for item `item-identifier`
- `1112` Copied security code for item `item-identifier`

Usage trends

Monitor usage trends to identify users engaging with Bitwarden and maintaining security practices:

Monitor user frequency

- Vault usage
  - `1000` Logged in
  - `1010` User requested device approval

Critical vault actions

Specific events may be monitored in order to track critical actions made by high-level users, or changes made to critical vault items:

Super-user activities

- Individual account activity
  - `1000` Logged in
  - `1001` Changed account password
  - `1002` Enabled/updated two-step login
  - `1003` Disabled two-step login
  - `1007` User exported their individual vault items
  - `1603` Organization vault access by a managing provider

- Organization activities
  - `1500` Invited user `user-identifier`
  - `1501` Confirmed user `user-identifier`
  - `1502` Edited user `user-identifier`
  - `1504` Edited groups for user `user-identifier`
  - `1511` Revoked organization access for user `user-identifier`
  - `1512` Restored organization access for `user-identifier`
  - `1513` Approved device for `user-identifier`

- `1600` Edited organization settings
- `1609` Modified collection management setting
- `1700` Modified policy `policy-identifier`
- `2001` Removed domain `domain-name`

- Exporting organization vault information
  - `1602` Exported organization vault

Critical item activities

- Changes made to items that have been identified to be critical
  - `1101` Edited item `item-identifier`
  - `1105` Moved item `item-identifier` to an organization
  - `1106` Edited collections for item `item-identifier`
  - `1107` Viewed item `item-identifier`
  - `1108` Viewed password for item `item-identifier`
  - `1109` Viewed hidden field for item `item-identifier`
  - `1110` Viewed security code for item `item-identifier`
  - `1111` Copied password for item `item-identifier`
  - `1112` Copied hidden field for item `item-identifier`
  - `1113` Copied security code for item `item-identifier`
  - `1114` Autofilled item `item-identifier`
  - `1117` Viewed card number for item `item-identifier`