BitDefender Integrations

BitDefender GravityZone supports SIEM integration using "push notifications", which are JSON messages sent via HTTP POST to a HTTP or HTTPS endpoint, which this integration can consume.

This integration additionally provides:

1. Collection of push notification configuration via API polling, which includes the "state" of the push notification service on the BitDefender GravityZone server, e.g. indicating if it is currently enabled or disabled. This is useful as the state may change to disabled (value of 0) for unknown reasons and you may wish to alert on this event.
2. Collection of push notification statistics via API polling, which includes the number of events sent, and counters for errors of different types, which you may wish to use to troubleshoot lost push notification events and for alerting purposes.
3. Support for multiple instances of the integration, which may be needed for MSP/MSSP scenarios where multiple BitDefender GravityZone tenants exist.
4. BitDefender company ID to your own company name/description mapping, in order to determine to which tenant the event relates to in a human friendly way. This is very useful for MSP/MSSP environments or for large organizations with multiple sub-organizations.

This allows you to search, observe and visualize the BitDefender GravityZone events through Elastic, trigger alerts and monitor the BitDefender GravityZone Push Notification service for state and errors.

Data Stream

Log Stream Push Notifications

The BitDefender GravityZone events dataset provides events from BitDefender GravityZone push notifications that have been received.

All BitDefender GravityZone log events are available in the `bitdefender_gravityzone.events` field group.

Compatibility

This integration supports BitDefender GravityZone, which is the business-oriented product set sold by BitDefender.

BitDefender products for home users are not supported.

The package collects BitDefender GravityZone push notification transported events sent in `jsonrpc`, `qradar`, or `splunk` format.

The `jsonrpc` format is recommended default, but the ingest pipeline will attempt to detect if `qradar` or `splunk` format events have been received and process them accordingly.

The integration can also collect the push notification configuration and statistics by polling the BitDefender GravityZone API.

Configuration

Enabling the integration in Elastic

1. In Kibana go to **Management > Integrations**
2. In "Search for integrations" search bar type **GravityZone**
3. Click on "BitDefender GravityZone" integration from the search results.
4. Click on **Add BitDefender GravityZone** button to add BitDefender GravityZone integration.

Example Integration Configuration

Example Integration Configuration

Create a BitDefender GravityZone API key that can configure a push notification service

The API key needed to configure push notifications, and collection push notification configuration state and statistics, is typically configured within the BitDefender GravityZone cloud portal.

Bear in mind the API key will be associated to the account you create it from. A named human account may not be desirable, e.g. you may wish to (probably should) create API keys for functions such as push notifications under a non-human/software service account that will never retire or be made redundant.

Navigate to your account details within the GravityZone portal. If you have sufficient privileges, you will see the "API keys" section near the bottom of the page. Click "Add" here.

Example Configuration 1

Give the API key a description and tick the "Event Push Service API" box at minimum.

NOTE: If you intend to use the API key for other API calls you may need to tick other boxes.

Example Configuration 2

Click the Key value that is shown in blue.

Example Configuration 3

Click the clipboard icon to copy the API key to your PC's clipboard.

Example Configuration 4

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.