ThreatQuotient

BitSight CDF Guide

Version 1.1.1

May 10, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Contents

Versioning

- Current integration version `1.1.1`
- Supported on ThreatQ versions >= `4.11.1`

Introduction

The BitSight CDF ingests threat intelligence events from the **BitSight** vendor. The CDF ingests data from the `alerts` endpoint that is mapped to specific events and their related attributes.

The BitSight feed retrieves data using the following endpoints:

- `https://api.bitsighttech.com/ratings/v1/alerts/`
- `https://api.bitsighttech.com/ratings/v1/alerts/percent/{guid}`

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your BitSight API Key.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

BitSight

`GET https://api.bitsighttech.com/ratings/v1/alerts/`


```
[
    {
        "alert_type": "PERCENT_CHANGE",
        "company_guid": "a5e23bf0-38d4-4cea-aa50-19ee75da481d",
        "href": "https://api.bitsighttech.com/ratings/v1/alerts/percent/6662353",
        "company_name": "Black Hills Technologies",
        "alert_date": "2018-08-04",
        "guid": 6662353,
        "folder_guid": "5d7bb4ba-bb2e-47ad-b6d9-a603f99fb950"
    }
]
```


The `href` field is used to make the supplemental call.

BitSight Specific Alert (Supplemental)

```
GET https://api.bitsighttech.com/ratings/v1/alerts/percent/6662353
```


```
{
    "guid": 6662353,
    "alert_date": "2018-08-04",
    "company_name": "Black Hills Technologies",
    "company_guid": "a5e23bf0-38d4-4cea-aa50-19ee75da481d",
    "start_date": "2018-07-31",
    "start_rating": 600,
    "end_rating": 560,
    "folder_guid": "5d7bb4ba-bb2e-47ad-b6d9-a603f99fb950",
    "company_url": "/company/14976400/",
    "rating_change_pct": -6,
    "alert_severity": "WARN",
    "alert_type": "PERCENT_CHANGE"
}
```


ThreatQ provides the following default mapping for the feeds. The mapping summarizes how the information from each field from the feed is converted to ThreatQ specific objects.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.alert_date	Event.Happened_at	N/A	N/A	2018-08-04	N/A
.alert_type	Event.Attribute	Alert Type	.start_date	PERCENT_CHANGE	Replaced '_' with ' ', title cased
.company_name + .alert_type	Event.Title	BitSight Alert	.start_date	Black Hills Technologies - PERCENT_CHANGE	Values are concatenated with -
.start_rating	Event.Attribute	Start Rating	.start_date	600	N/A
.end_rating	Event.Attribute	End Rating	.start_date	560	N/A
.alert_severity	Event.Attribute	Alert Severity	.start_date	WARN	Title cased
.company_name	Event.Attribute	Company	.start_date	Black Hills Technologies	N/A
.risk_category	Event.Attribute	Risk Category	.start_date	N/A	N/A
.nist_category	Event.Attribute	NIST Category	.start_date	N/A	N/A
.nist_category_name	Event.Attribute	NIST Category Name	.start_date	N/A	N/A
.start_grade	Event.attribute	Start Grade	.start_date	N/A	N/A
.end_grade	Event.Attribute	End Grade	.start_date	N/A	N/A
.grade_threshold	Event.Attribute	Grade Threshold	.start_date	N/A	N/A

Average Feed Run

Average Feed Run results for BitSight:

METRIC	RESULT
Run Time	1 minute
Events	1
Event Attributes	5

Feed runtime is supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Change Log

- **Version 1.1.1**
  - Added header to the main feed call.
  - Renamed user field to reflect the value it holds.
- **Version 1.1.0**
  - Update user field.
- **Version 1.0.0**
  - Initial release