ThreatQuotient

BitSight CDF

Version 1.2.0

February 25, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

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

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.2.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The BitSight CDF ingests threat intelligence information such as security change alerts, leaks, and rating reports from the BitSight vendor.

The integration provides the following feeds:

- **BitSight Rating Alerts** - ingests alerts that are generated when a company's security rating changes
- **BitSight Leaks** - ingests credential leaks that may affect your organization.
- **BitSight Rating Reports** - ingests the security rating PDF reports for the selected companies/countries in your portfolio.

The integration ingests the following system object types:

- Events
- Files
- Identities
- Incidents

Prerequisites

The following is required to install and run the integration:

- A BitSight License.
- A BitSight API token.

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
6. Select the individual feeds to install, when prompted, and click **Install**.

   > 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.

   The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(s).

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).

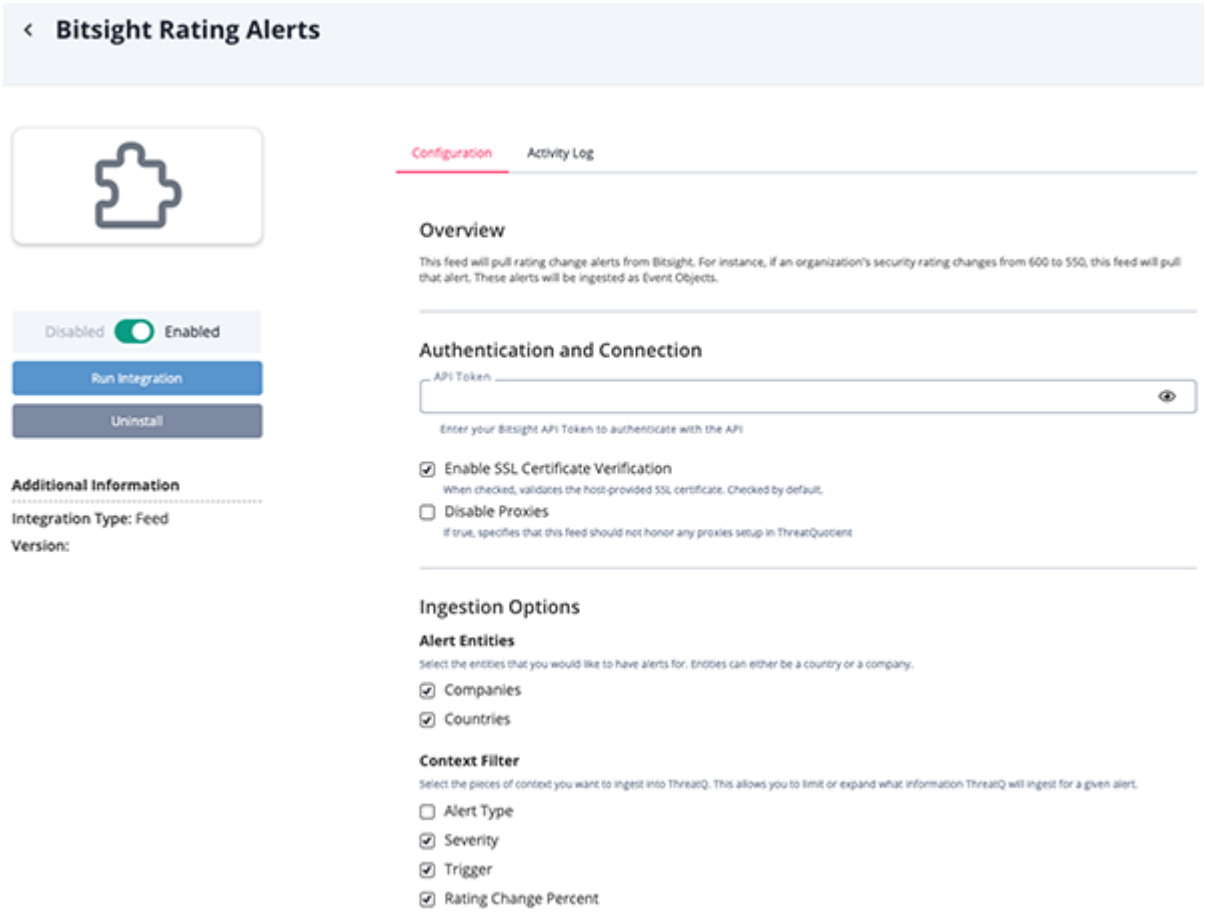
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

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

BitSight Rating Alerts Parameters

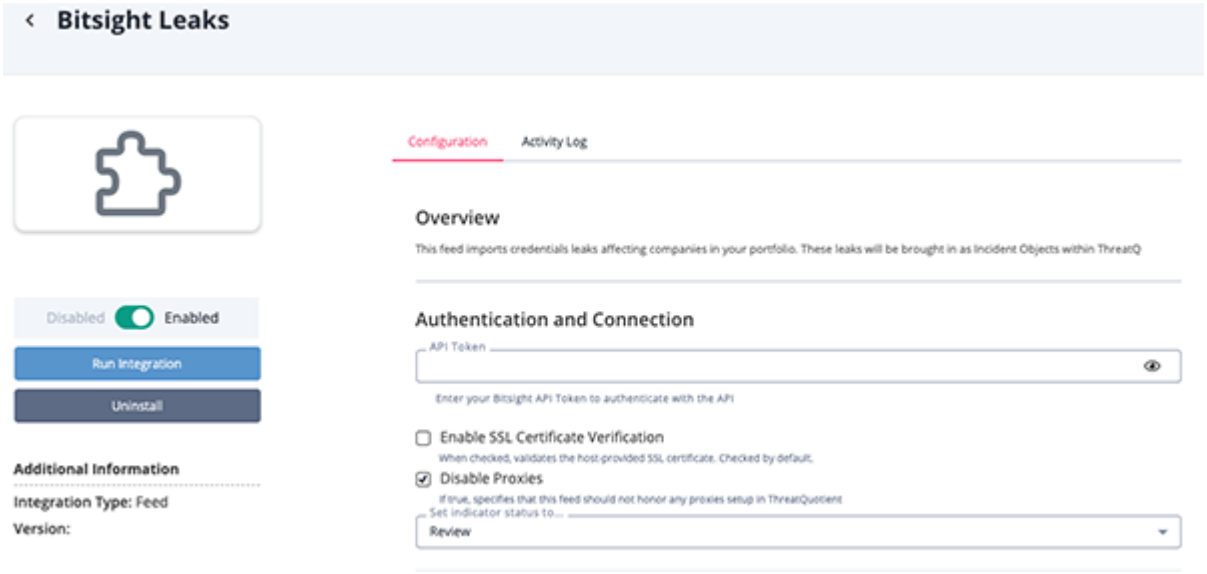
PARAMETER	DESCRIPTION
API Key	Your BitSight API Key.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Alert Entities	Select the entities to ingest alerts for on the ThreatQ platform. Options include: ◦ Companies ◦ Countries
Context Filter	Select the pieces of context for an alert to ingest into ThreatQ. This parameter allows you to limit or expand what information ThreatQ will ingest for a given alert. Options include: ◦ Alert Type ◦ Vulnerability

- Severity
- Trigger
- Rating Change Percent
- Rating Threshold
- Start Rating
- End Rating
- Risk Category
- Info Category
- NIST Category
- Folder Name
- Entity Type



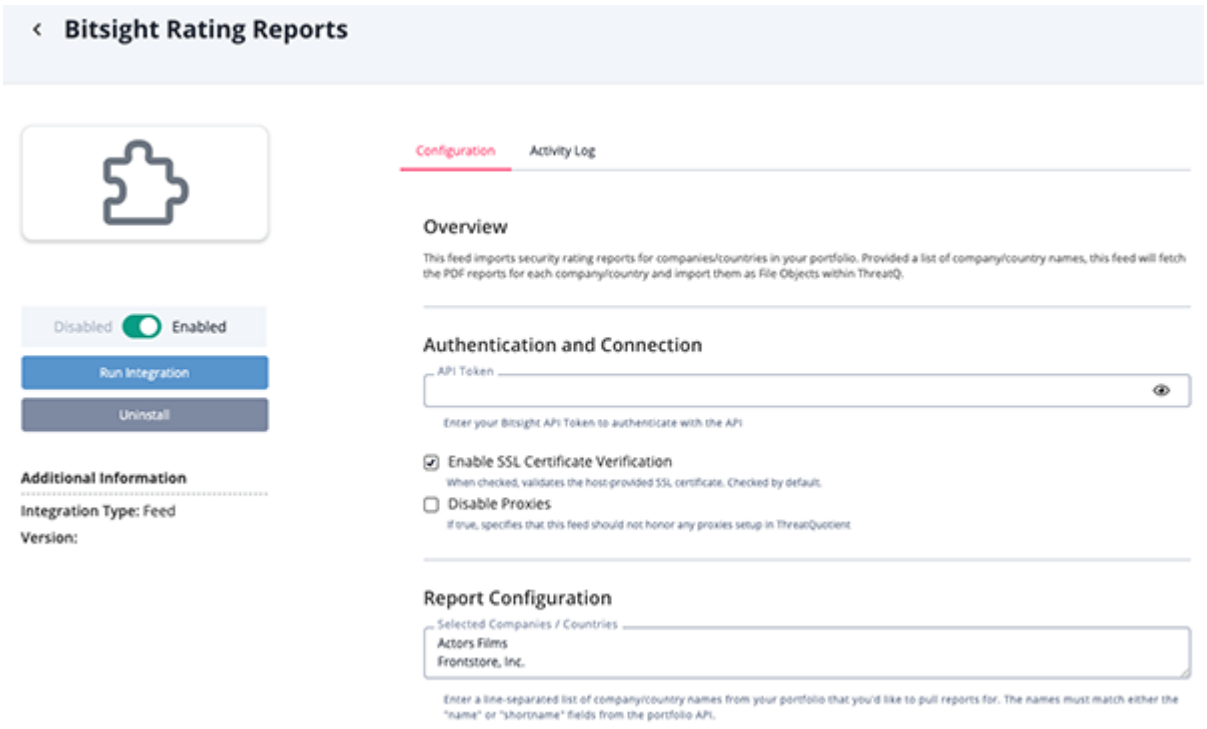
BitSight Leaks Parameters

PARAMETER	DESCRIPTION
API Key	Your BitSight API Key.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



BitSight Rating Reports Parameters

PARAMETER	DESCRIPTION
API Key	Your BitSight API Key.
Enable SSL Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Selected Companies / Countries	Enter a line-separated list of company/country names from your portfolio that you'd like to pull reports for. The names must match either the "name" or "shortname" fields from the portfolio API.



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 Rating Alerts

The BitSight Rating Alerts feed ingests alerts that are generated when a company's security rating changes, allowing you to track changes in your organization's security rating within ThreatQ.

`GET https://api.bitsighttech.com/ratings/v2/alerts/latest`

Sample Response:


```
{
  "links": {
    "next": null,
    "previous": null
  },
  "count": 3,
  "results": [
    {
      "guid": 399820624,
      "alert_type": "RATING_THRESHOLD",
      "alert_date": "2023-12-11",
      "start_date": "2023-12-10",
      "company_name": "Alabama (United States) - Food Production",
      "company_guid": "04ae83b6-4335-46ef-bed6-4529723a9f35",
      "company_url": "/app/sovereign-dashboard/?country=Alabama+
%28United+States%2industry=Food+Production",
      "folder_guid": "14a64fd5-5540-41e7-b71a-8c7002c49d31",
      "folder_name": "Territory Benchmark",
      "severity": "CRITICAL",
      "trigger": "Threshold",
      "details": {
        "rating_threshold": 640,
        "start_rating": 650,
        "end_rating": 640
      }
    },
    {
      "guid": 399820670,
      "alert_type": "VULNERABILITY",
      "alert_date": "2023-12-11",
      "start_date": "2023-12-10",
      "company_name": "Acme Corp",
      "company_guid": "a397fd67-c85e-4ee8-a152-2f384aff918f",
      "company_url": "/company/a397fd67-c85e-4ee8-a152-2f384aff918f/",
      "folder_guid": "e24beb6b-8a72-413e-8299-c5c96e0646db",
      "folder_name": "All Companies",
      "severity": "INFORMATIONAL",
```

```
      "trigger": "Infection",
      "details": {
        "id": 351,
        "message": "InstallBrain"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on the item the `results` list from the API response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.alert_type`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title
`.company_name`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title
`.severity`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title
`.details.message`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `Vulnerability`
`.details.rating_change_pct`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `Percent Change`
`.details.end_rating`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `Percent Change` or `Rating Threshold`
`.details.start_rating`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `Rating Threshold`
`.details.risk_category`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `Risk Category`
`.details.nist_category_name`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `NIST Category`
`.details.nist_category`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `NIST Category`
`.details.info_category`	Event Title	Alert	`.alert_date`	N/A	Field concatenated to form event title for alert type `Informational`
*	Event Description	N/A	`.alert_date`	N/A	All fields in JSON format.
`.alert_type`	Event Attribute	Event Type	`.alert_date`	`Percent Change`	Title-cased; User-configurable
`.severity`	Event Attribute	Severity	`.alert_date`	`Critical`	Title-cased; User-configurable; Updatable
`.trigger`	Event Attribute	Trigger	`.alert_date`	`Infection`	User-configurable
`.details.rating_change_pct`	Event Attribute	Rating Change Percent	`.alert_date`	`-1`	User-configurable. Updatable
`.details.rating_threshold`	Event Attribute	Rating Threshold	`.alert_date`	`640`	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.details.start_rating`	Event Attribute	Start Rating	`.alert_date`	`650`	User-configurable. Updatable
`.details.end_rating`	Event Attribute	End Rating	`.alert_date`	`640`	User-configurable. Updatable
`.details.message`	Event Attribute	Vulnerability	`.alert_date`	`InstallBrain`	When Alert Type == `Vulnerability`; User-configurable
`.details.risk_category`	Event Attribute	Risk Category	`.alert_date`	N/A	When Alert Type == `Risk Category`; User-configurable
`.details.info_category`	Event Attribute	Info Category	`.alert_date`	N/A	When Alert Type == `Informational`; User-configurable
`.details.nist_category`	Event Attribute	NIST Category	`.alert_date`	N/A	When Alert Type == `NIST Category`; User-configurable
`.folder_name`	Event Attribute	Folder Name	`.alert_date`	`My Territories`	User-configurable
`.company_name`	Event Attribute	Entity	`.alert_date`	`Acme Corp`	N/A
N/A	Event Attribute	Entity Type	`.alert_date`	`Country`	Can be `Country` or `Company`; User-configurable

BitSight Leaks

The BitSight Leaks feed ingests credential leaks from BitSight, allowing you to more closely track leaks that may directly affect your organization.

```
GET https://api.bitsighttech.com/ratings/v1/exposed-credentials/leaks
```

Sample Response:


```
{
  "links": {
    "next": null,
    "previous": null
  },
  "count": 16,
  "results": [
    {
      "guid": "04109a90-ba9f-4c40-b3c3-9929613fd4a7",
      "name": "Apollo",
      "leak_date": "2018-07-23",
      "date_added": "2018-10-12T04:04:18.952625Z",
      "description": "In July 2018, the sales engagement startup <a
href=\"https://www.wired.com/story/apollo-breach-linkedin-salesforce-data/\"
rel=\"noopener\" target=\"_blank\">Apollo left a database containing billions
of data points publicly exposed without a password</a>. The data was discovered
by security researcher <a href=\"http://www.vinnytroia.com/\" rel=\"noopener\"
target=\"_blank\">Vinny Troia</a> who subsequently sent a subset of the data
containing 126 million unique email addresses to Have I Been Pwned. The data
left exposed by Apollo was used in their \"revenue acceleration platform\" and
included personal information such as names and email addresses as well as
professional information including places of employment, the roles people hold
and where they're located. Apollo stressed that the exposed data did not
include sensitive information such as passwords, social security numbers or
financial data.",
      "data_types_leaked": [
        {
          "name": "Email Addresses",
          "description": "Any email addresses associated with the information
in a disclosed user account, typically used for signup or notifications."
        },
        {
          "name": "Name",
          "description": "Typically the real-world name of the owner of the
disclosed account"
        },
        {
          "name": "Phone numbers",
          "description": "Contact information for the owner of the disclosed
account."
        }
```

```
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each item with the `results` list from the API response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.name`	Incident Value	N/A	`.leak_date`	N/A	N/A
`.description`	Incident Description	N/A	N/A	In July 2018, the...	N/A
`.leak_date`	Incident Attribute	Leak Date	`.leak_date`	`2023-05-01`	Updatable
`.data_types_leaked[].name`	Incident Attribute	Leaked Data	`.leak_date`	`Name`	N/A
`.data_types_leaked[].name`	Incident Description	N/A	N/A	`Name`	Concatenated with other keys
`.data_types_leaked[].description`	Incident Description	N/A	N/A	`Typically the ...s`	Concatenated with other keys

BitSight Rating Reports

The BitSight Rating Reports feed ingests the security rating PDF reports for the selected companies/countries in your portfolio, allowing your analysts in ThreatQ to have visibility into your organization's attack surface.

`GET https://api.bitsighttech.com/ratings/v2/portfolio`

Sample Response:


```
{
  "links": {
    "next": null,
    "previous": null
  },
  "count": 8,
  "results": [
    {
      "guid": "6d9cad45-6a91-4523-b51e-c11365fddfb0",
      "custom_id": null,
      "name": "Acme Corp",
      "shortname": "ACME",
      "network_size_v4": 45429,
      "rating": 500,
      "rating_date": "2023-12-11",
      "added_date": "2023-11-27",
      "industry": {
        "name": "Utilities",
        "slug": "utilities"
      },
      "sub_industry": {
        "name": "Utilities",
        "slug": "utilities"
      },
      "type": ["CURATED"],
      "logo": "https://api.bitsighttech.com/ratings/v1/companies/
6d9cad45-6a91-4523-b51e-c11365fddfb0/logo-image",
      "sparkline": "https://api.bitsighttech.com/ratings/v1/companies/
6d9cad45-6a91-4523-b51e-c11365fddfb0/sparkline?size=small",
      "subscription_type": {
        "name": "Total Risk Monitoring",
        "slug": "continuous_monitoring"
      },
      "primary_domain": "acme.com",
      "display_url": "https://service.bitsighttech.com/app/tprm/company/
6d9cad45-6a91-4523-b51e-c11365fddfb0/overview/",
      "tier": null,
      "tier_name": null,
      "life_cycle": null,
      "relationship": null,
```

```
      "details": {
        "is_primary": false,
        "primary_company": null
      }
    },
    {
      "guid": "1e6661d7-2512-41c6-a6a6-4158835fff1a",
      "custom_id": null,
      "name": "United States of America",
      "shortname": "US",
      "network_size_v4": 0,
      "rating": 620,
      "rating_date": "2023-12-11",
      "added_date": "2023-11-20",
      "industry": null,
      "sub_industry": null,
      "type": ["COUNTRY"],
      "logo": "https://api.bitsighttech.com/ratings/v1/companies/
1e6661d7-2512-41c6-a6a6-4158835fff1a/logo-image",
      "sparkline": "https://api.bitsighttech.com/ratings/v1/companies/
1e6661d7-2512-41c6-a6a6-4158835fff1a/sparkline?size=small",
      "subscription_type": {
        "name": "Territory Benchmark",
        "slug": "countries"
      },
      "primary_domain": null,
      "display_url": null,
      "tier": null,
      "tier_name": null,
      "life_cycle": null,
      "relationship": null,
      "details": {
        "is_primary": false,
        "primary_company": null
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each item within the `results` list from the API response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.name`	File Title	PDF	N/A	N/A	Field is concatenated within a string to form the title
`.name`	Identity Value	N/A	N/A	`Acme Corp`	N/A
`.rating`	File Attribute	Security Rating	N/A	`600`	N/A
`.name`	Identity Attribute	Name	N/A	`Acme Corp`	N/A
`.shortname`	Identity Attribute	Short Name	N/A	`ACME`	N/A
`.industry.name`	Identity Attribute	Industry	N/A	`Utilities`	N/A
`.sub_industry.name`	Identity Attribute	Sub Industry	N/A	N/A	N/A
`.type`	Identity Attribute	Type	N/A	`COMPANY`	N/A
`.primary_domain`	Identity Attribute	Primary Domain	N/A	`acme.com`	N/A
`.tier_name`	Identity Attribute	Tier	N/A	N/A	N/A
`.subscription_type.name`	Identity Attribute	Subscription Type	N/A	`Territory Benchmark`	N/A
`.life_cycle.name`	Identity Attribute	Lifecycle	N/A	N/A	N/A
`.relationship.name`	Identity Attribute	Relationship	N/A	N/A	N/A

Average Feed Run

Object counts and Feed runtime are 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.

BitSight Rating Alerts

METRIC	RESULT
Run Time	1 minute
Events	80
Event Attributes	478

BitSight Leaks

METRIC	RESULT
Run Time	1 minute
Incidents	16
Incident Attributes	79

BitSight Rating Reports

METRIC	RESULT
Run Time	1 minute
Files	2
Identities	2
Identity Attributes	11

Change Log

- **Version 1.2.0**
  - BitSight feed updates:
    - Updated the name of the feed from BitSight to **BitSight Rating Alerts**.
    - The feed now uses the new version 2 alerts endpoint.
    - Events titles are now more descriptive.
    - Event descriptions now include raw alert data.
    - Added the following new configuration parameters:
      - **Enable SSL Certificate Verification** - determine if the feed will validate the host-provided SSL certificate.
      - **Disable Proxies** - determine if the feed should honor proxies set in the ThreatQ UI.
      - **Alert Entities** - select the entities to ingest alerts for on the ThreatQ platform.
      - **Context Filter** - select the pieces of context for an alert to ingest into ThreatQ.
  - Added two new feeds:
    - **BitSight Leaks** - ingests credential leaks from BitSight.
    - **BitSight Rating Reports** - ingests the security rating PDF reports for the selected companies/countries in your portfolio.
  - Updated the minimum ThreatQ version to 5.12.1.
- **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