# ThreatQuotient

## Silobreaker Connector

**Version 1.1.1**

June 17, 2024

**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** | 1.1.1 |
| **Compatible with ThreatQ Versions** | >= 4.57.3 |
| **Python Version** | 3.6 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Silobreaker for ThreatQ integration allows a user to ingest reports and other context from Silobreaker.

# Prerequisites

Review the following requirements before attempting to install the connector.

## Third-Party Credentials

Silobreaker API key and Shared key.

## Time Zone

You should ensure all ThreatQ devices are set to the correct time, time zone, and date (UTC is recommended), and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the list-`timezones` command line option.

For example, enter the following command to list all available time zones in Europe:

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

Enter the following command, as root, to change the time zone to UTC:

```
timedatectl set-timezone UTC
```

# Integration Dependencies

The integration must be installed in a python 3.6 environment.

The following is a list of required dependencies for the integration. These dependencies are downloaded and installed during the installation process. If you are an Air Gapped Data Sync (AGDS) user, or run an instance that cannot connect to network services outside of your infrastructure, you will need to download and install these dependencies separately as the integration will not be able to download them during the install process.

Items listed in bold are pinned to a specific version. In these cases, you should download the version specified to ensure proper function of the integration.

| DEPENDENCY | VERSION | NOTES |
|---|---|---|
| threatqsdk | >=1.8.0 | N/A |
| threatqcc | >=1.4.0 | N/A |
| python-dateutil | >=2.8.1 | N/A |
| pytz | >=2023.3 | N/A |
| requests | >=2.25.1 | N/A |

# Installation

The following provides you with steps on installing a Python 3 Virtual Environment and installing the connector.

## Creating a Python 3.6 Virtual Environment

Run the following commands to create the virtual environment:

```
mkdir /opt/tqvenv/
sudo yum install -y python36 python36-libs python36-devel python36-pip
python3.6 -m venv /opt/tqvenv/<environment_name>
source /opt/tqvenv/<environment_name>/bin/activate
pip install --upgrade pip
pip install threatqsdk threatqcc setuptools==59.6.0
```

Proceed to Installing the Connector.

# Installing the Connector

**Upgrading Users** - Review the Change Log for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the install steps listed below. Failure to delete the previous configuration file will result in the connector failing.

1. Navigate to the ThreatQ Marketplace and download the .whl file for the integration.
2. Activate the virtual environment if you haven't already:

```
source /opt/tqvenv/<environment_name>/bin/activate
```

3. Transfer the whl file to the `/tmp` directory on your ThreatQ instance.
4. Install the connector on your ThreatQ instance:

```
pip install /tmp/tq_conn_silobreaker-<version>-py3-none-any.whl
```

A driver called `tq-conn-silobreaker` will be installed. After installing, a script stub will appear in `/opt/tqvenv/<environment_name>/bin/tq-conn-silobreaker`.

5. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. Use the commands below to create the required directories:

```
mkdir -p /etc/tq_labs/
mkdir -p /var/log/tq_labs/
```

6. Perform an initial run using the following command:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-silobreaker -ll /var/log/
tq_labs/ -c /etc/tq_labs/ -v3
```

7. Enter the following parameters when prompted:

| PARAMETER | DESCRIPTION |
|---|---|
| **ThreatQ Host** | This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ. |
| **ThreatQ Client ID** | This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details. |

| PARAMETER | DESCRIPTION |
|---|---|
| **ThreatQ Username** | This is the Email Address of the user in the ThreatQ System that will manage integrations. |
| **ThreatQ Password** | The password for the above ThreatQ account. |

**Example Output**

```
/opt/tqvenv/<environment_name>/bin/tq-conn-silobreaker -ll /var/log/
tq_labs/ -c /etc/tq_labs/ -v3
ThreatQ Host: <ThreatQ Host IP or Hostname>
ThreatQ Client ID: <ClientID>
ThreatQ Username: <EMAIL ADDRESS>
ThreatQ Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

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

# 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 **Labs** option from the *Category* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

| PARAMETER | DESCRIPTION |
|---|---|
| **API Key** | Your Silobreaker API Key. |
| **Shared Secret** | Your Silobreaker Shared Secret Key. |
| **Search Queries (1 Per Line)** | Enter a line-separated list of search queries that you want to use to ingest reports.<br><br>> Enter search query per line.<br><br>**Example:** `Malware:"NanoCore RAT" AND NOT doctype:"Paste" AND fromdate:"-24h" entitytype:"ThreatActor" AND entitytype:"AttackType" AND fromdate:"-24h" AND NOT doctype:"Paste"` |
| **Language Filter** | Comma-separated list of language codes to ingest reports in. If left blank, reports with any language will be ingested.<br><br>**Example**: `en, fr, de, sp` |
| **Ingest CVEs As** | Select the object type you would like CVEs to be ingested as. |

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.

# Usage

Use the following command to execute the driver:

```
/opt/tqvenv/<environment_name>/bin/tq-conn-silobreaker -v3 -ll /var/log/
tq_labs/ -c /etc/tq_labs/
```

## Command Line Arguments

This connector supports the following custom command line arguments:

| ARGUMENT | DESCRIPTION |
|---|---|
| `-h`, `--help` | Review all additional options and their descriptions. |
| `-ll LOGLOCATION`, `--loglocation LOGLOCATION` | Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default). |
| `-c CONFIG`, `--config CONFIG` | This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.) |
| `-v {1,2,3}`, `--verbosity {1,2,3}` | This is the logging verbosity level where **3** means everything. |
| `-n, --name` | Optional - Name of the connector (Option used in order to allow users to configure multiple connector instances on the same TQ box). |
| `-hist, --historical` | Allows you to set a historical date to import context since. |

# CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis, use CRON or some other jobs scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

In the example below, the command will execute the connector every two hours.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following command:

   ```
   crontab -e
   ```

   This will enable the editing of the crontab, using vi. Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.
3. Enter the commands below:

   **Every 2 Hours Example**

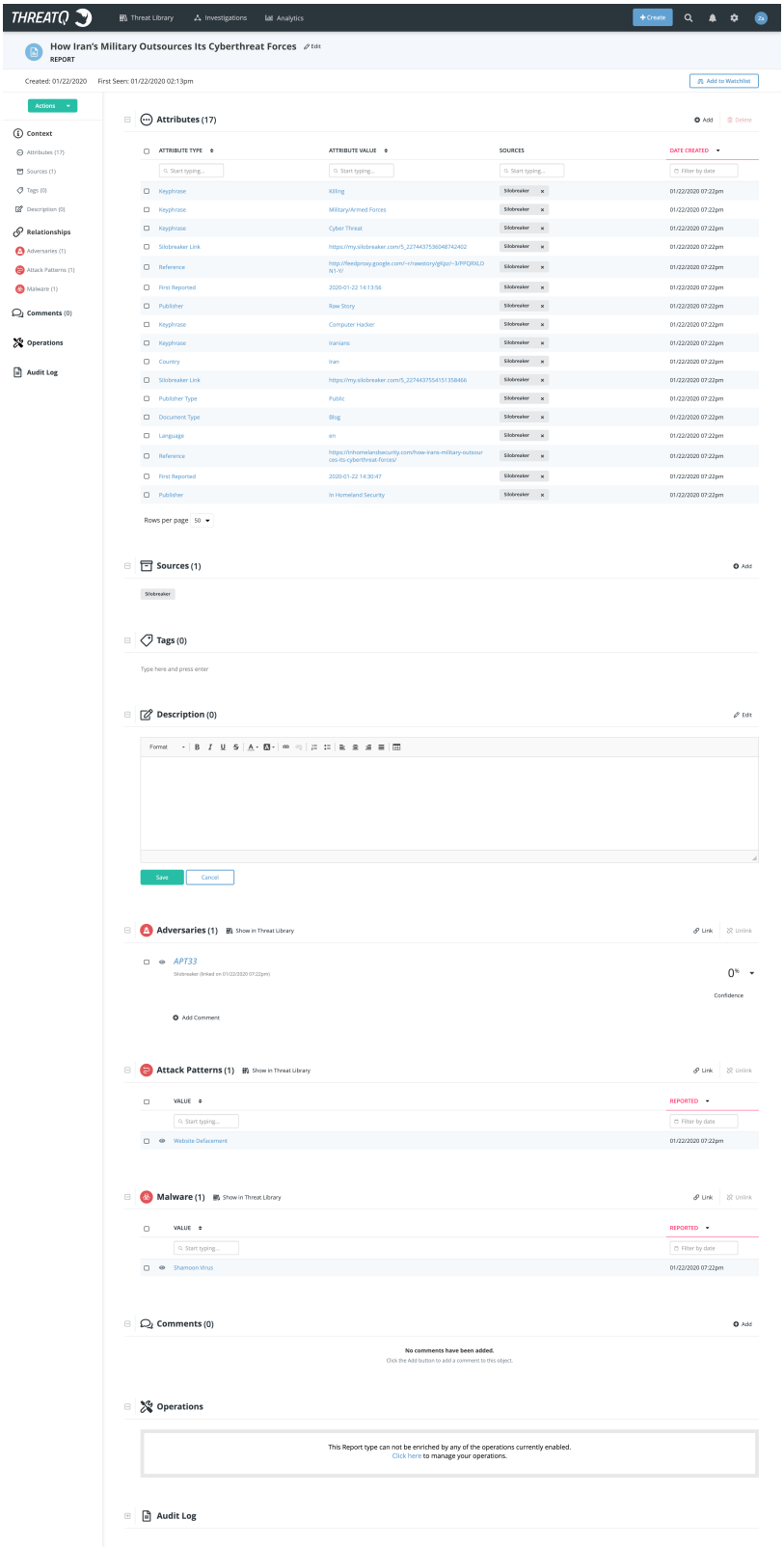
   ```
   0 */2 * * * /opt/tqvenv/<environment_name>/bin/tq-conn-silobreaker -
   c /etc/tq_labs/ -ll /var/log/tq_labs/ -v3
   ```
4. Save and exit CRON.

# Average Connector Run

| METRIC | RESULT |
|---|---|
| **Run Time** | 6 minutes |
| **Reports** | 1,575 |
| Report Attributes | 18,900 |
| Adversaries | 18 |
| Adversary Attributes | 18 |
| Attack Patterns | 74 |
| Attack Pattern Attributes | 74 |
| Identity | 350 |
| Identity Attributes | 350 |
| Indicators | 2 |
| Indicator Attributes | 2 |
| Vulnerabilities | 256 |
| Vulnerability Attributes | 256 |

# Result Example

The following example displays how the Report Details will look in ThreatQ.


THREATQ
Threat Library
Investigations
Analytics
Create
How Iran's Military Outsources Its Cyberthreat Forces
Edit
REPORT
Created: 01/22/2020
First Seen: 01/22/2020 02:13pm
Add to Watchlist
Actions
Context
Attributes (17)
Sources (1)
Tags (0)
Description (0)
Relationships
Adversaries (1)
Attack Patterns (1)
Malware (1)
Comments (0)
Operations
Audit Log
Attributes (17)
Add
Delete
ATTRIBUTE TYPE
ATTRIBUTE VALUE
SOURCES
DATE CREATED
Keyphrase
Killing
Keyphrase
Military/Armed Forces
Keyphrase
Cyber Threat
Silobreaker Link
https://my.silobreaker.com/S_2274437536048742402
Reference
http://feedproxy.google.com/~r/rnswstory/gKpz/~3/PPQ80LDN1-Y/
First Reported
2020-01-22 14:13:56
Publisher
Raw Story
Keyphrase
Computer Hacker
Keyphrase
Iranians
Country
Iran
Silobreaker Link
https://my.silobreaker.com/S_2274437554151358466
Publisher Type
Public
Document Type
Blog
Language
en
Reference
https://rnhomelandsecurity.com/how-irans-military-outsources-its-cyberthreat-forces/
First Reported
2020-01-22 14:30:47
Publisher
In Homeland Security
Rows per page 50
Sources (1)
Add
Silobreaker
Tags (0)
Type here and press enter
Description (0)
Edit
Format
Save
Cancel
Adversaries (1)
Show in Threat Library
Link
Unlink
APT33
Silobreaker (linked on 01/22/2020 07:22pm)
0%
Confidence
Add Comment
Attack Patterns (1)
Show in Threat Library
Link
Unlink
VALUE
REPORTED
Website Defacement
01/22/2020 07:22pm
Malware (1)
Show in Threat Library
Link
Unlink
VALUE
REPORTED
Shamoon Virus
01/22/2020 07:22pm
Comments (0)
Add
No comments have been added.
Click the Add button to add a comment to this object.
Operations
This Report type can not be enriched by any of the operations currently enabled.
Click here to manage your operations.
Audit Log

# Change Log

- **Version 1.1.1**
  - Updated to Python 3.
  - Removed support for Python 2.
- **Version 1.1.0**
  - Fixed an issue with date-util dependency.
  - Queries with the `fromdate` parameter ignore the last-run date.
  - Last-run date now is compared to CreatedDate instead of PublicationDate.
  - Added support for Cyber Attribution tags.
  - Added UI config option to ingest CVEs as indicators or vulnerabilities.
  - Fixed an authentication issue with API.
  - Added Python 3 support.
- **Version 1.0.0**
  - Initial release