ThreatQuotient

Silobreaker Connector for ThreatQuotient

Version 1.0.0

Wednesday, April 1, 2020

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

Introduction

The Silobreaker connector for ThreatQuotient allows a ThreatQ user to ingest reports and other context from Silobreaker, based on your custom search queries.

Preface

This guide is to provide the information necessary to implement the Silobreaker connector for ThreatQuotient. This document is not specifically intended to form a site reference guide.

It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

Audience

This document is intended for use by the following parties:

1. ThreatQ and Security engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

Scope

This document covers the implementation of the application only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	Version
ThreatQ Platform	Version 4.29 or greater
Silobreaker connector for ThreatQuotient	1.0.0

Prerequisites

Throughout this implementation document, there will be referrals to several files and directories, some of which will be symbolic, and others may change depend on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time, time zone and date, 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, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

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

To change the time zone to UTC, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

Installation

The Silobreaker connector for ThreatQuotient is installed from the ThreatQuotient repository with YUM credentials.

Install the Silobreaker Connector for ThreatQuotient by using the following commands.

Figure 3: Installing From The ThreatQuotient Repository (Example Output)

```
sudo pip install tq-conn-silobreaker
```

To install this Silobreaker from a wheel file, the wheel file (.whl) file `pip install tq_conn_silobreaker-*-py2-none-any.whl` will need to be copied via SCP into your ThreatQ instance.

1. Once the application has been installed, A directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. See example below:

Figure 4: Creating Integration Directories (Example)

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

2. A driver which will be called `tq-conn-silobreaker` is installed.
3. Issue the following commands to initialize the integration.

You will be asked the following questions:

a. **ThreatQ Host:** This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
b. **Client ID:** This is the OAuth id that can be found at **Settings Gear** → **User Management** → **API details** within A user's details
c. **E-mail Address:** This is the *User in the ThreatQ System* for integrations
d. **Password:** The password for the above ThreatQ account
e. **Status:** This is the default status for IoCs that are created by this Integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

Figure 5: Running the Integration

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

The driver will run once, where it will connect to the TQ instance and install the UI component of the Connector.

Configuration

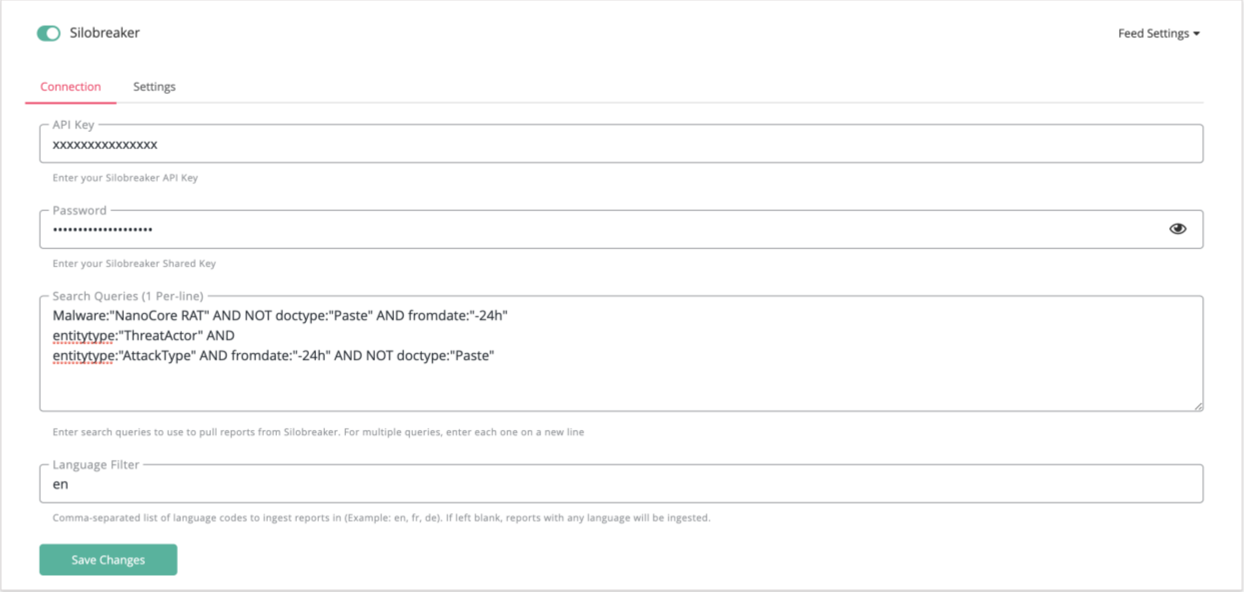
To configure the application, navigate to the ThreatQ UI via **Settings Gear** → **Incoming Feeds** → **Labs** and find the Silobreaker section.

Navigate to the custom connectors configuration page and enter the following values for the Silobreaker integration. Once completed, save the configuration by clicking on the Save Changes button:

1. **API Key**: Enter your Silobreaker API Key
2. **Shared Secret**: Enter your Silobreaker Shared Secret Key
3. **Search Queries (1 Per-line)**: Enter a line-separated list of search queries that you want to use to ingest reports from
4. **Language Filter**: Comma-separated list of language codes to ingest reports in. If left blank, reports with any language will be ingested
    a. **Example**: en, fr, de, sp.

Once all the relevant information has been entered, click **Save Changes**

Figure 6: UI Configuration



API Key: xxxxxxxxxxxxxxx

Enter your Silobreaker API Key

Password: ••••••••••••••••••••

Enter your Silobreaker Shared Key

Search Queries (1 Per-line):

```
Malware:"NanoCore RAT" AND NOT doctype:"Paste" AND fromdate:"-24h"
entitytype:"ThreatActor" AND
entitytype:"AttackType" AND fromdate:"-24h" AND NOT doctype:"Paste"
```

Enter search queries to use to pull reports from Silobreaker. For multiple queries, enter each one on a new line

Language Filter: en

Comma-separated list of language codes to ingest reports in (Example: en, fr, de). If left blank, reports with any language will be ingested.

Once completed, the integration is now ready for operation.

Usage

This connector is used just like other custom connector. However, it has one additional CLI argument that you can include for historical imports.

Basic Usage

```
?> tq-conn-silobreaker -v 3 -ll /var/log/tq_labs/ -c /etc/tq_labs/
```

Advanced Usage

If it is required to import reports in the past, you can do so via the `-hist, --historical` command line option. With this option, you can specify a date to download reports since. It must be in the `'YYYY-MM-DD'` format. The below example will import all reports since January 1st, 2019.

```
?> tq-conn-silobreaker -v 3 -ll /var/log/tq_labs/ -c /etc/tq_labs/ -hist
2020-01-01
```

Command Line Arguments

Here is a list of the command line arguments you can add

- **-v** (required): Sets the log verbosity (3 means everything)
- **-c** (required): The path to the directory where you want to store your config file
- **-ll** (required): The path to the directory where you want to store your logs
- **-n, --name**: Change the name of the connector
- **-hist, --historical**: Allows you to set a historical date to import context since
    - Example: [-hist [YYY-MM-DD]]

Document Change Log

Version	Details
1.0.0	Initial Document Release