ThreatQuotient

ThreatQuotient for Bulk CSV Exporter Connector

Version 1.0.0

August 21, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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.

Last Updated: Wednesday, August 21, 2019

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for Bulk CSV Exporter Connector allows a ThreatQ user to export a saved search from their Threat Library as CSV files, one per object.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient Bulk CSV Exporter Connector. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

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

1.4 Scope

This document covers the implementation of the ThreatQuotient for Bulk CSV Exporter Connector only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Bulk CSV Exporter Connector	1.0.0	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for Bulk CSV Exporter Connector into the managed estate:

- All ThreatQuotient equipment is online and in service.
- All required firewall ports have been opened.

2 Implementation Overview

This document explains how to install and execute the ThreatQuotient for Bulk CSV Exporter Connector.

2.1 Prerequisites

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change, depending 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
```

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

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

2.2 Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required or applicable.

All engineers are reminded that all data belonging and pertaining to the business is confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

3 ThreatQuotient for Bulk CSV Exporter Connector Installation

3.1 Setting up the Integration

From the ThreatQuotient Repository

To install this ThreatQuotient for Bulk CSV Exporter Connector from the ThreatQuotient repository with YUM credentials.

1. Install the ThreatQuotient for Bulk CSV Exporter Connector by using the following commands.

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

```
$> pip install tq-conn-bulk-csv-exporter
Collecting tq-conn-bulk-csv-exporter
  Downloading https://extensions.threatq.com/threatq/integrations-
dev/+f/e7b/7112897638161/ tq-conn-bulk-csv-exporter-1.0.0-py2-none-any.whl
Requirement already satisfied: jinja2==2.8 in /usr/lib/python2.7/site-packages
(from threatqcc>=1.3.0-> tq-conn-bulk-csv-exporter) (2.8)
Collecting pyasn1>=0.3.7 (from python-ldap==3.2.0-> tq-conn-bulk-csv-exporter)
  Downloading https://extensions.threatq.com/root/pypi/+f/da6/b43a8c9ae93bc/pyasn1-
0.4.5-py2.py3-none-any.whl (73kB)
    100% |████████████████████████████████| 81kB 1.0MB/s
Collecting pyasn1_modules>=0.1.5 (from python-ldap==3.2.0-> tq-conn-bulk-csv-
exporter)
  Downloading
  Running setup.py install for python-ldap ... done
Successfully installed pyasn1-0.4.5 pyasn1-modules-0.2.5 python-ldap-3.2.0 tq-conn-
bulk-csv-exporter-1.0.0
```

Offline from the .whl File

To install this ThreatQuotient for Bulk CSV Exporter Connector from a wheel file, the wheel file (.whl) file `tq-conn-bulk-csv-exporter-<version>-py2-none-any.whl` will need to be copied via SCP into your ThreatQ instance.

1. Install the .whl file using the following command.

Figure 4: Installing .whl File (Inc Example Output)

```
$> sudo pip install /file/path/to/app/tq-conn-bulk-csv-exporter-<version>-py2-none-
any.whl
Requirement already satisfied (use --upgrade to upgrade): urllib3<1.25,>=1.21.1 in
/usr/lib/python2.7/site-packages (from requests>=2.9.1->threatqsdk>=1.6.7-> tq-conn-
bulk-csv-exporter)
Requirement already satisfied (use --upgrade to upgrade): chardet<3.1.0,>=3.0.2 in
/usr/lib/python2.7/site-packages (from requests>=2.9.1->threatqsdk>=1.6.7-> tq-
conn-bulk-csv-exporter)
Requirement already satisfied (use --upgrade to upgrade): idna<2.9,>=2.5 in
/usr/lib/python2.7/site-packages (from requests>=2.9.1->threatqsdk>=1.6.7-> tq-
conn-bulk-csv-exporter)
Installing collected packages: tq-conn-bulk-csv-exporter
Successfully installed tq-conn-bulk-csv-exporter-1.0.0
```

Once the application has been installed, you must create a directory structure for all configuration, logs and files, using the `mkdir -p` command. See the example below:

Figure 5: Creating Integration Directories (Example)

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

A driver called **`tq-conn-bulk-csv-exporter`** is installed.

2. 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 refers to the API credentials that can be found at the **User icon > My Account**.
   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 status.

Figure 6: Running the Integration

```
$> tq-conn-bulk-csv-exporter -v 3 -ll /path/to/log/dir -c
/path/to/config/dir
ThreatQ Host: <ThreatQ Host IP or Hostnme >
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 ThreatQ instance and install the user interface component of the connector.

```
Connector configured.  Set information in UI
```

3.2 Configuring the connector

To configure the application, navigate in the ThreatQ user interface to the **Settings icon** > **Incoming Feeds** > **Labs** and find the Bulk CSV Exporter feed.

1. Expand the Feed Settings for the **Bulk CSV Exporter** section.
   - **Saved Search Name (Threat Library):** The name of the saved search from the Threat Library
   - **Output Directory:** The directory that will receive the output of the CSV files**.**

     Note: This directory must be accessible from whereever you are running the connector (typically on the ThreatQ server).

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

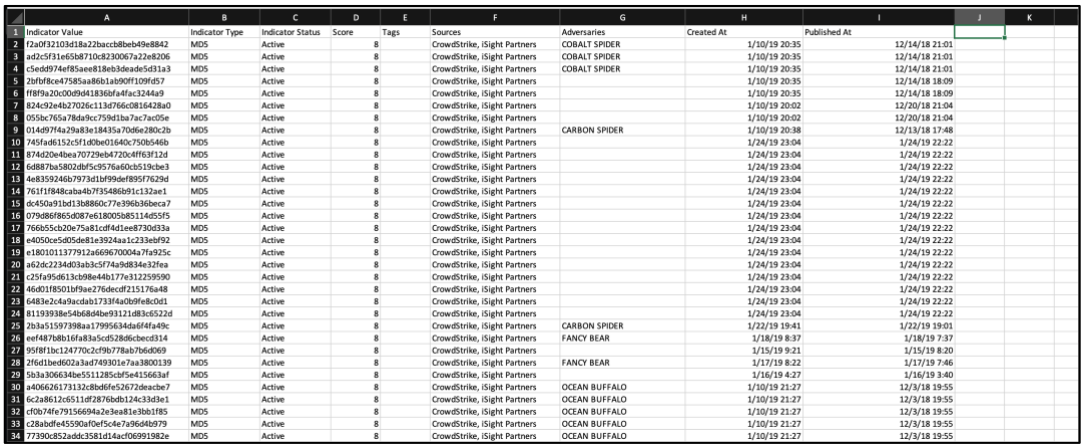
2. Ensure to enable the feed toggle.

Figure 7: UI Configuration

Once completed, the integration is now ready for operation.

3.2.1.1 Example Output

Figure 8: Example Output



Indicator Value	Indicator Type	Indicator Status	Score	Tags	Sources	Adversaries	Created At	Published At
f2a0f32103d18a22baccb8beb49e8842	MD5	Active	8		CrowdStrike, iSight Partners	COBALT SPIDER	1/10/19 20:35	12/14/18 21:01
ad2c5f31e65b8710c8230067a22e8206	MD5	Active	8		CrowdStrike, iSight Partners	COBALT SPIDER	1/10/19 20:35	12/14/18 21:01
c5edd974ef85aee818eb3deade5d31a3	MD5	Active	8		CrowdStrike, iSight Partners	COBALT SPIDER	1/10/19 20:35	12/14/18 21:01
2bfbf8ce47585aa86b1ab90ff109fd57	MD5	Active	8		CrowdStrike, iSight Partners		1/10/19 20:35	12/14/18 18:09
ff8f9a20c00d9d41836bfa4fac3244a9	MD5	Active	8		CrowdStrike, iSight Partners		1/10/19 20:35	12/14/18 18:09
824c92e4b27026c113d766c0816428a0	MD5	Active	8		CrowdStrike, iSight Partners		1/10/19 20:02	12/20/18 21:04
055bc765a78da9cc759d1ba7ac7ac05e	MD5	Active	8		CrowdStrike, iSight Partners		1/10/19 20:02	12/20/18 21:04
014d97f4a29a83e18435a70d6e280c2b	MD5	Active	8		CrowdStrike, iSight Partners	CARBON SPIDER	1/10/19 20:38	12/13/18 17:48
745fad6152c5f1d0be01640c750b546b	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
874d20e4bea70729eb4720c4ff63f12d	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
6d887ba5802dbf5c9576a60cb519cbe3	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
4e8359246b7973d1bf99def895f7629d	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
761f1f848caba4b7f35486b91c132ae1	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
dc450a91bd13b8860c77e396b36beca7	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
079d86f865d087e618005b85114d55f5	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
766b55cb20e75a81cdf4d1ee8730d33a	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
e4050ce5d05de81e3924aa1c233ebf92	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
e1801011377912a669670004a7fa925c	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
a62dc2234d03abb3c5f74a9d834e32fea	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
c25fa95d613cb98e44b177e312259590	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
46d01f8501bf9ae276decdf215176a48	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
6483e2c4a9acdab1733f4a0b9fe8c0d1	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
81193938e54b68d4be93121d83c6522d	MD5	Active	8		CrowdStrike, iSight Partners		1/24/19 23:04	1/24/19 22:22
2b3a51597398aa17995634da6f4fa49c	MD5	Active	8		CrowdStrike, iSight Partners	CARBON SPIDER	1/22/19 19:41	1/22/19 19:01
eef487b8b16fa83a5cd528d6cbecd314	MD5	Active	8		CrowdStrike, iSight Partners	FANCY BEAR	1/18/19 8:37	1/18/19 7:37
95f8f1bc124770c2cf9b778ab7b6d069	MD5	Active	8		CrowdStrike, iSight Partners		1/15/19 9:21	1/15/19 8:20
2f6d1bed602a3ad749301e7aa3800139	MD5	Active	8		CrowdStrike, iSight Partners	FANCY BEAR	1/17/19 8:22	1/17/19 7:46
5b3a3066345be5511285cbf5e415663af	MD5	Active	8		CrowdStrike, iSight Partners		1/16/19 4:27	1/16/19 3:40
a406626173132c8bd6fe52672deacbe7	MD5	Active	8		CrowdStrike, iSight Partners	OCEAN BUFFALO	1/10/19 21:27	12/3/18 19:55
6c2a8612c6511df2876bdb124c33d3e1	MD5	Active	8		CrowdStrike, iSight Partners	OCEAN BUFFALO	1/10/19 21:27	12/3/18 19:55
cf0b74fe79156694a2e3ea81e3bb1f85	MD5	Active	8		CrowdStrike, iSight Partners	OCEAN BUFFALO	1/10/19 21:27	12/3/18 19:55
c28abdfe45590af0ef5c4e7a96d4b979	MD5	Active	8		CrowdStrike, iSight Partners	OCEAN BUFFALO	1/10/19 21:27	12/3/18 19:55
77390c852addc3581d14acf06991982e	MD5	Active	8		CrowdStrike, iSight Partners	OCEAN BUFFALO	1/10/19 21:27	12/3/18 19:55

Supported Fields:

- Value
- Title
- Name
- Type
- Status
- Score
- Tags
- Sources
- Adversaries
- Created At
- Published At (First Seen)

3.3 CRON

To run this script on a reoccurring basis use CRON or some other system schedule. The argument in the cron script ***must*** specify the config and log locations.

This can be run multiple times a day and can be run as often as required.

3.3.1 Setting up the CRONJOB

1. Login via a CLI terminal session to your ThreatQ host.
2. Input the commands below.

Figure 9: Command Line Crontab 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. Input the commands below – this example shows every **4 Hours.**

Figure 10: Command Line Crontab Command

```
0 */4 * * * tq-conn-bulk-csv-exporter -v 3 -ll /path/to/log/dir -c
/path/to/config/dir --cache /path/to/cache/dir
```

Figure 11: Command Line Crontab Command (Bespoke Name)

```
0 */4 * * * tq-conn-bulk-csv-exporter -n <Bespoke_Name> -v 3 -ll
/path/to/log/dir -c /path/to/config/dir --cache /path/to/cache/dir
```

To run this script on a re-occurring basis, use CRON or some other on system schedule. CRON is displayed here.

The argument in the cron script ***must*** specify the config and log locations.

For further reference, see the ThreatQ Help Center.

Appendix A: Supplementary Information

Uninstalling the Connector

```
sudo pip uninstall tq-conn-bulk-csv-exporter
```

Driver command line options

The **tq-conn-bulk-csv-exporter** driver has several command line arguments that will help you and your customers execute it. They are listed below. You can view these arguments by executing: `/usr/bin/tq-conn-bulk-csv-exporter --help.`

```
usage: tq-conn-bulk-csv-exporter [-h] [-ll LOGLOCATION][-c CONFIG] [-v VERBOSITY]
```

optional arguments:

```
  -h, --help
```

Shows the help message and exit

```
  -ll LOGLOCATION, --loglocation LOGLOCATION
```

This sets the logging location for this connector. The location should exist and be writable by the current user. 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 have read and write permissions for the current user. If no config file is given, the current directory will be used. This file is also where some information from each run of the connector may be stored (e.g. last run time, private OAuth, etc).

```
  -cache, --cache
```

(required): The path to the directory where you want to store your cache.

```
  -v {1,2,3}, --verbosity {1,2,3}
```

This is the logging verbosity level. The Default is 1 (Warning).

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE TERMS AND CONDITIONS WHEN PURCHASED. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.