ThreatQuotient

ThreatQuotient for Resilient (Connector)

Version 1.0.0

May 29, 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: Friday, May 29, 2019

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for Resilient (Connector) allows new context from ThreatQ to be exported to your Resilient instance. It has the ability to push new indicators and comments from updated Resilient incidents in ThreatQ to Resilient as artifacts and comments, respectively.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Resilient (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 and Security Engineers
2. ThreatQuotient Professional Services Project Team and Engineers

1.4 Scope

This document covers the implementation of the ThreatQuotient for Resilient (Connector) only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Resilient (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 Resilient (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 will show how to install the ThreatQuotient for Resilient (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
Europe/Belgrade
Europe/Berlin
```

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.

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 Resilient (Connector) Installation

3.1 Setting up the Integration

From The ThreatQuotient Repository

To install this ThreatQuotient for Resilient (Connector) from the ThreatQuotient repository with YUM credentials:

1. Install the ThreatQuotient for Resilient (Connector) by using the following commands.

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

```
> pip install tq-conn-resilient
Collecting tq-conn-resilient
  Downloading https://extensions.threatq.com/threatq/integrations-
dev/%2Bf/c5d/9cc7d14d1bc54/tq_conn_resilient-1.0.0-py2-none-any.whl
Requirement already satisfied: threatqcc>=1.3.0 in /usr/lib/python2.7/site-packages
Installing collected packages: configparser, entrypoints, secretstorage, keyring,
argparse, requests-toolbelt, requests-mock, cachetools, resilient, tq-conn-
resilient
  Running setup.py install for secretstorage ... done
  Running setup.py install for resilient ... done
Successfully installed argparse-1.4.0 cachetools-2.1.0 configparser-3.7.4
entrypoints-0.3 keyring-18.0.1 requests-mock-1.6.0 requests-toolbelt-0.9.1
resilient-32.0.140 secretstorage-2.3.1 tq-conn-resilient-1.0.0
```

Offline From the .whl File

To install this ThreatQuotient for Resilient (Connector) from a wheel file, the wheel file (.whl) file `tq_conn_resilient-<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_resilient-<version>-py2-none-any.whl
Successfully installed argparse-1.4.0 cachetools-2.1.0 configparser-3.7.4
entrypoints-0.3 keyring-18.0.1 requests-mock-1.6.0 requests-toolbelt-0.9.1
resilient-32.0.140 secretstorage-2.3.1 tq-conn-resilient-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-resilient`** 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 under **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 option.

Figure 6: Running the Integration

```
$> tq-conn-resilient -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: Active
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.

If there are multiple directories that are required or wanted for import into ThreatQ, this can be done by the use of the `-n, --name` flag to create multiple instances of the connector. These instances can be run alongside each other.

Note, if this is done, configure the 2nd instance from your ThreatQ instance will be required.

Figure 7: Running the Integration with -n flag

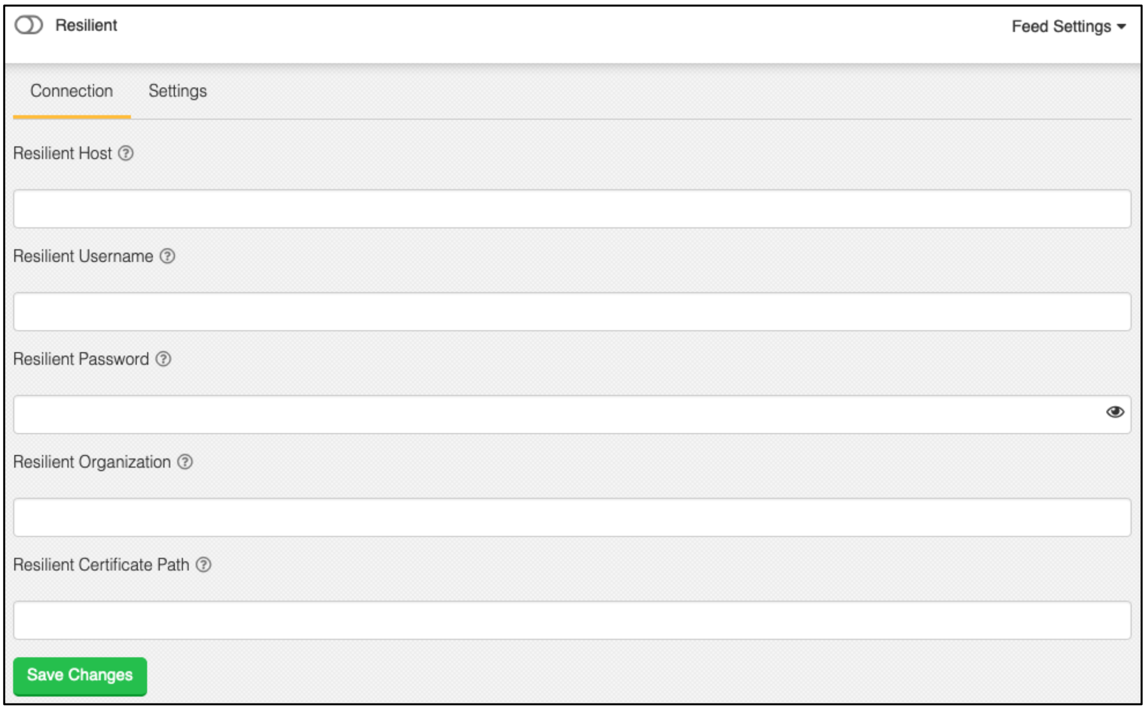
```
?> tq-conn-resilient -v 3 -ll /path/to/log/dir -c /path/to/config/dir --name
"Another Reslient Connector"
ThreatQ Host: <ThreatQ Host IP or Hostnme >
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured.  Set information in UI
```

3.2 Configuring the Connector

To configure the application, complete the following steps in the ThreatQ User Interface:

1. Choose the **Settings icon > Incoming Feeds**.
2. Click the **Labs** tab, Now expand the Feed Settings for the **Resilient** section.
   The following information will need to be entered as described below.
   a. **Resilient Host:** The hostname or IP address of the Resilient instance
   b. **Resilient Username:** The email that will be used to authenticate with the Resilient API
   c. **Resilient Password:** The password for the above account
   d. **Resilient Organization:** The organization within the Resilient instance
   e. **Resilient Certificate Path (optional):** The path to the Resilient certificate
      i. This is optional. If left blank, SSL will **not** be verified.
      ii. To generate a certificate, see the section: **Generating Certificate for Resilient**.
      iii. Ensure the certificate is accessible by the connector if used.

Figure 8: UI Configuration



Appendix A: Supplementary Information

Generating Certificate for Resilient

If it is required to use a certificate with the connector, the following command allows a user to generate one.

```
?> openssl s_client -connect <SERVER>:443 -showcerts -tls1 < /dev/null >
cacerts.pem 2> /dev/null
```

The full path of the generated **`.pem`** file should be used as the certificate path in the connector configuration.

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.