ThreatQuotient

ThreatQuotient for Resilient Functions

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 Functions integration implements actions within Resilient, allowing it to react to Contextual and Automatic Actions.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Resilient Functions. 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 Resilient Functions only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Resilient Functions	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 Functions 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 Functions.

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 Resilient Functions Application Installation

3.1 Installation Steps

The following steps outline the installation of the ThreatQuotient for Resilient Functions application.

1. SSH into the Resilient Server or a Resilient Integration Server.
2. Ensure that Python 3.2+ is installed.
    a. If Python 3.2+ isn't installed, then please follow the link below to install it: https://phoenixnap.com/kb/how-to-install-python-3-centos-7
3. Below is an overview of the guide:

Figure 3: Set-Up of a Python3 Environment

```
# Make sure everything is updated
?> sudo yum update

# Install SCL so we can install multiple versions of the same software
?> sudo yum install centos-release-scl

# Install python 3.6
?> sudo yum install rh-python36

# Enable the pythong 3.6 SCL environment
?> scl enable rh-python36 bash

# Verify your python version. It should be 3.6 or higher
?> python --version
```

4. Transfer the Functions for ThreatQ (.whl) onto your Resilient Server (or Resilient Integration Server).
    a. Build using python setup.py bdist_wheel.
5. Install the .whl file.
    a. Ensure that the python 3.6 SCL environment is activated.

```
pip install fn_threatq-<version>-py3-none-any.whl
```

6. If a resilient configuration file has not been created, this will need to be done before continuing.
    a. The default config location is **`~/.resilient/app.config`**

```
resilient-circuits config -c
```

7. Add the new configuration to the config file by running the following:

```
resilient-circuits config -u
```

8. Edit the `app.config` file with your configuration for your Resilient instance under the `[resilient]` section.
9. Edit the `app.config` file with your configuration for the integration under the `[fn_threatq]` section.
    a. Fill out the required fields in the configuration:
        i. Resilient information
        ii. ThreatQ authentication information
    b. Save the file.
10. Install the customization features (rules, message destinations, fields, etc.).

```
resilient-circuits customize
```

11. Run resilient-circuits to execute the installed integrations.

```
resilient-circuits run
```

3.1.1 Customizing Functionality

By default, this integration includes the following automatic actions:

- Sync Incident
- Add Indicator
- Sync Task
- Add Comment

If these actions are **NOT** to be automated, they can be converted to menu item actions. Please follow the step outlined below in section 4.1.2.

3.1.2 Switching to Menu Item Rules

1. Choose **Customization Settings** > **Rules.**
2. Choose the rule to be switched to be a menu item.
    a. Note the name. Usually **“ThreatQ:”** followed by the action name (see features).
3. Delete the rule.
4. Create a new rule, and make it a menu item.
5. Input the name noted in step 2.
6. Set the message destination to `ThreatQ`.
7. Add any necessary fields (see *Section 5.1: Features*)
8. Click **Save**.

In addition, two of the actions support some custom fields.
If these automatic actions have been converted to menu item actions, please see the Features section to see which fields they support.

- Sync Incident
- Add Indicator

3.1.3 Advanced Installation/Usage

If the following is required, ThreatQuotient recommends that you refer to the following document for further instructions: IBM's Integration Server Guide:
https://github.com/ibmresilient/resilient-reference/blob/master/developer_guides/Integration%20Server%20Guide.pdf

- Automatically run Integrations on startup (or restart)
- Offline Installation
- Updating the configuration file

4 Resilient Functions

Due to the requirements from IBM Resilient, functions are required to create import definitions. However, this integration does not utilize functions, only actions. Adding functions from this integration to your workflow will not do anything. If users wish to use the functions in a workflow (not via an action), please submit a request to support@threatq.com.

4.1 Features

Below are the current features/actions this integration supports:

4.1.1 Sync Incident

This action will sync an incident with ThreatQ. If the incident is updated, it will update ThreatQ with the new/updated information.

- **Rule**: Automatic
- **Type**: Incident
- **Supported Fields (If Menu Item)**:
  - Import Artifacts into ThreatQ
    - Type: Select
    - Options: [Yes, No]
  - Import Indicators from ThreatQ
    - Type: Select
    - Options: [Yes, No]

4.1.2 Add Indicator

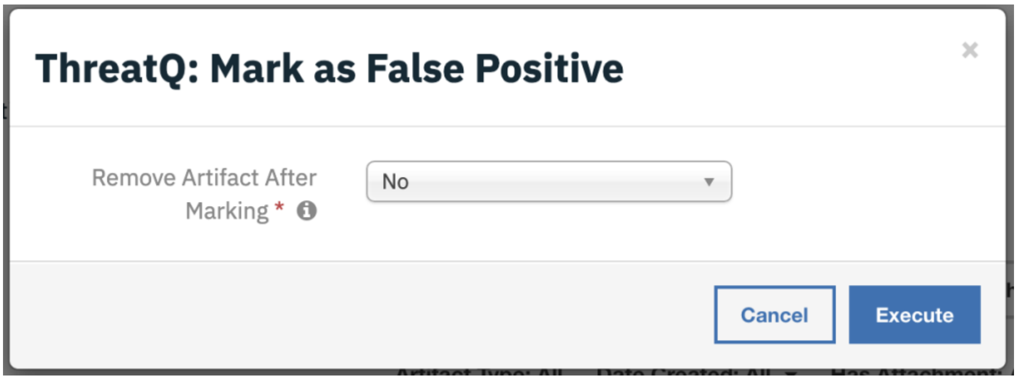
This action will add an artefact to ThreatQ as an indicator.

- **Rule**: Automatic
- **Type**: Artifact
- **Supported Fields (If Menu Item)**:
  - Indicator Status
    - Description: The status for the indicator in ThreatQ
    - Type: Select
    - Options: [Active, Review, Indirect, Whitelisted, Expired]
  - Indicator Confidence
    - Description: A confidence level for the artifact. This will get set as an attribute within ThreatQ
    - Type: Select
    - Options: [Low, Medium, High]

4.1.3 Mark as a False Positive

This action will mark the artifact selected as a false positive within ThreatQ. An attribute will be added to the indicator with the name, "False Positive" and value, "Yes".

Figure 4: Mark as False Positive



ThreatQ: Mark as False Positive

Remove Artifact After Marking * : No

- **Rule:** Menu Item
- **Type:** Artifact
- **Fields:**
  - Remove Artifact After Marking
  - Description: Setting this to 'Yes' will remove the artifact from the Artifact list in Resilient after marking
  - Type: Select
  - Options: [Yes, No]

4.1.4 Mark as a True Positive

This action will mark the artifact as a true positive within ThreatQ. An attribute will be added to the indicator with the name, "True Positive" and value, "Yes".

- **Rule:** Menu Item
- **Type:** Artifact

4.1.5 Find Related Indicators

This action will look for any related indicators to the indicator within ThreatQ. Any related indicators will be added to Resilient.

- **Rule:** Menu Item
- **Type:** Artifact

4.1.6 Add Comment

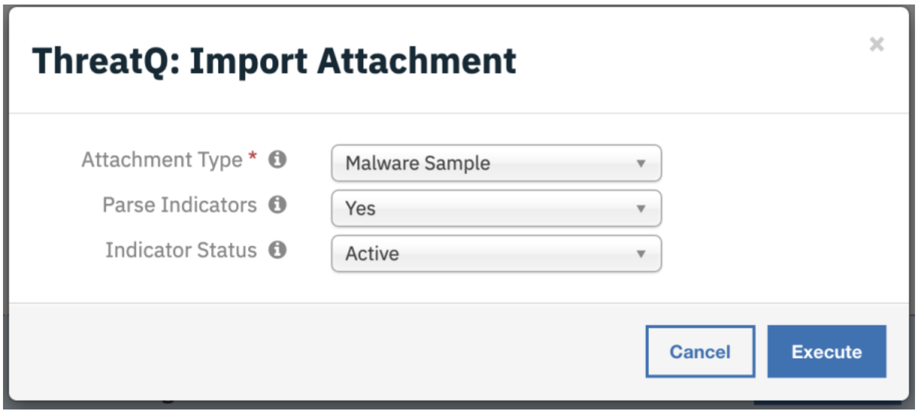
This action will add a note/comment to the associated ThreatQ Incident or Task. Comments in ThreatQ do not support markup, so the comment will not maintain the formatting from Resilient.

- **Rule:** Automatic
- **Type:** Note

4.1.7 Import Attachment

This action will import an attachment into ThreatQ. It gives a user the ability to choose what type of attachment it is, as well as the ability to choose whether or not to parse the attachment for indicators.

Figure 5: Import Attachment



ThreatQ: Import Attachment

Attachment Type * : Malware Sample

Parse Indicators: Yes

Indicator Status: Active

- **Rule:** Menu Item
- **Type:** Attachment
- **Fields:**
    - Attachment Type
        - Description: The type of attachment that the attachment will be imported as into ThreatQ
        - Type: Select
        - Options: [Malware Sample, Spearphish, PDF, Intelligence, Malware Analysis Report, Generic Text]
    - Parse Indicators
        - Description: Whether or not it is required to parse indicators out of the attachment
        - Type: Select
        - Options: [Yes, No]
    - Indicator Status
        - Description: The status for any parsed indicators (if enabled)
        - Type: Select
        - Options: [Active, Review, Indirect, Whitelisted, Expired]

4.1.8 Sync Task

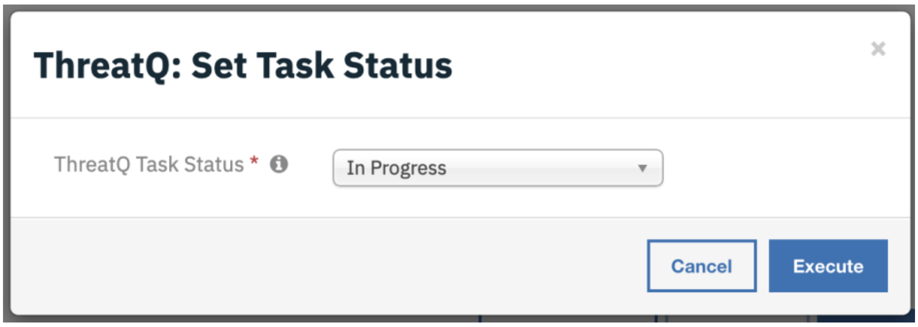
This action will sync a task to ThreatQ. Any updates made to the task will be updated within ThreatQ.

- **Rule:** Automatic
- **Type:** Task

4.1.9 Set Task Status

These actions allow a user to set the task's status within ThreatQ. By default, the integration syncs tasks with the status, "To Do". If users wish to mark the task as a different status, a user can use this action.

Figure 6: Set Task Status



ThreatQ: Set Task Status

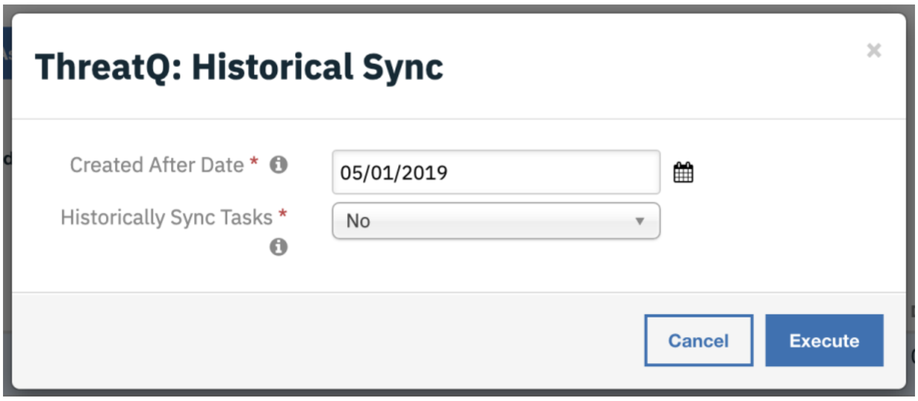
ThreatQ Task Status * : In Progress

- **Rule:** Menu Item
- **Type:** Task
- **Fields:**
    - Task Status
        - Description: The status for the task within ThreatQ
        - Type: Select
        - Options: [To Do, In Progress, Review, Done]

4.1.10 Historical Sync

This action allows users to sync incidents historically. Users will be able to customize the date to search, as well as syncing the related tasks or not.

Figure 7: Historical Sync



ThreatQ: Historical Sync

Created After Date * : 05/01/2019

Historically Sync Tasks * : No

- **Rule:** Menu Item
- **Type:** Incident
- **Fields:**
    - Created After Date
        - Description: The date to go back to sync incidents from
        - Type: Date Picker
- **Historically Sync Tasks:**
    - Description: Enabling this option will sync related tasks to a historical incident
- **Type:** Select
- **Options:** [Yes, No]

Appendix A: Supplementary Information

Generating Certificate for Resilient

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

Appendix B: Updating fields/rules/functions (customizations)

If any customization features are changed, you must recompile the definition.

1. From Resilient, go to **Administrative Settings** > **Organization** > **Export** and export your latest setup (with **all** boxes checked).
2. Come back to the development environment as described above, and run the command below. Append or remove any features as necessary.

```
resilient-circuits codegen \
--package "fn_threatq" \
--messagedestination "fn_threatq" \
--rule "ThreatQ: Sync Incident" "ThreatQ: Add Indicator" "ThreatQ: Find Related
Indicators" "ThreatQ: Mark as False Positive" "ThreatQ: Mark as True Positive"
"ThreatQ: Add Comment" "ThreatQ: Import Attachment" \
--function "threatq_sync_incident" "threatq_add_indicator"
"threatq_find_related_indicators" "threatq_mark_as_false_positive"
"threatq_mark_as_true_positive" "threatq_add_comment" "threatq_import_attachment"
```

3. This will output a new "functions package" into `./fn_threatq/fn_threatq`.
   a. the whole package is not required, but just a portion of it.
4. Copy the comment and the `ImportDefinition` code from `./fn_threatq/fn_threatq/util/customize.py` and paste it in the original, `./fn_threatq/util/customize.py`
   b. The next time resilient-circuits customize is run, this will import the new definitions.

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.