ThreatQuotient

Resilient Functions Guide

Version 1.1.1

July 12, 2021

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

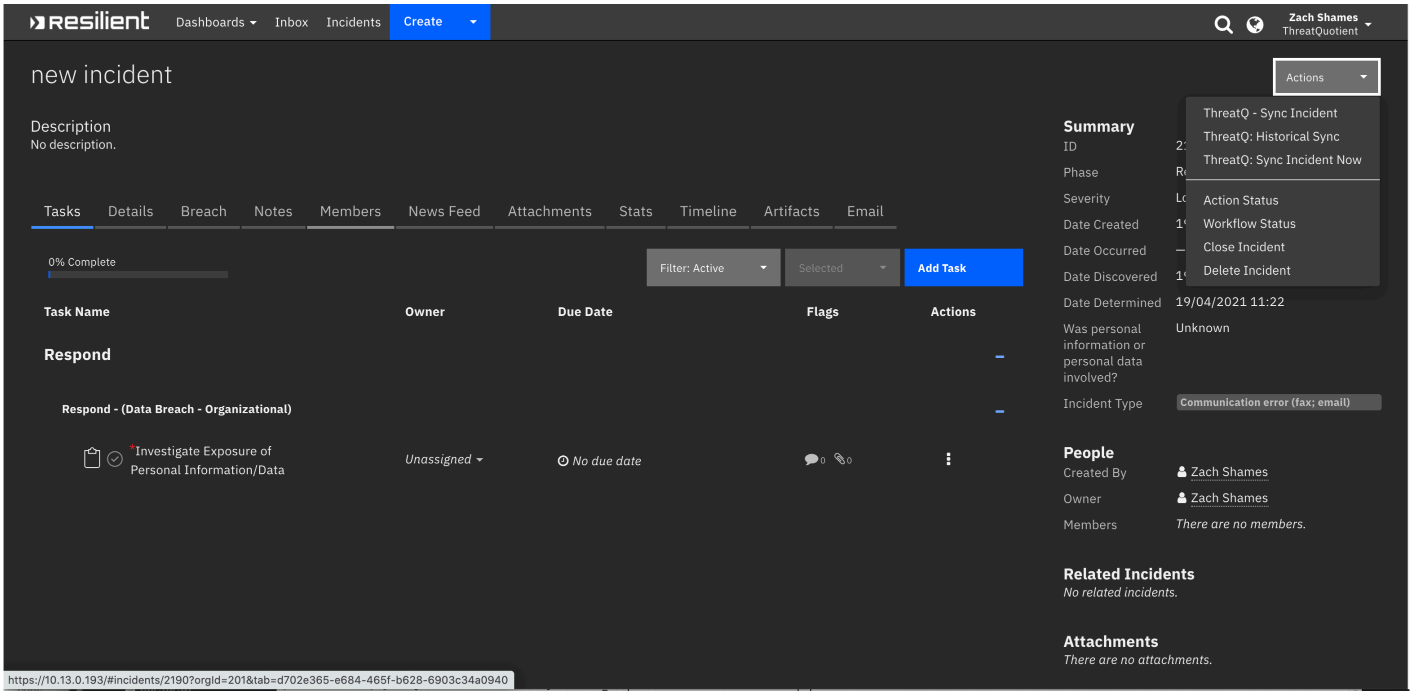
Versioning

- Current integration version `1.1.1`
- Integration Server >= `v37.0.214`
- Supported on ThreatQ versions >= `4.24.0`

Introduction

ThreatQuotient's Resilient Functions App for IBM Security SOAR, enables analysts to automatically or manually sync incidents, artifacts, and other context, to ThreatQ, in real-time.

> ⚠ This app does not support use of a proxy server.



new incident

Description
No description.

0% Complete

Task Name	Owner	Due Date	Flags	Actions
Respond				
Respond - (Data Breach - Organizational)				
*Investigate Exposure of Personal Information/Data	Unassigned	No due date	0 0	

Summary

ID	2
Phase	R
Severity	Lo
Date Created	1
Date Occurred	–
Date Discovered	1
Date Determined	19/04/2021 11:22
Was personal information or personal data involved?	Unknown
Incident Type	Communication error (fax; email)

People

Created By	Zach Shames
Owner	Zach Shames
Members	There are no members.

Related Incidents
No related incidents.

Attachments
There are no attachments.

https://10.13.0.193/#incidents/2190?orgId=201&tab=d702e365-e684-465f-b628-6903c34a0940

Prerequisites

> ⚠ This app does not support use of a proxy server.

- Python 3.x
- Resilient platform >= `v37.0.214`
- An Integration Server running `None`
  - See ibm.biz/res-int-server-guide for information on setting up an integration server.
  - If using API Keys, minimum required permissions are:
    - Org Data: Read, Edit
    - Function: Read
    - Incidents: Read
    - Incident Status: Edit
    - Incident Fields: Edit
    - Private Tasks: Read
    - Private Task Members: Edit
    - Private Task Notes: Edit
    - Public Tasks: Read
    - Public Task Members: Edit
    - Public Task Notes: Edit
    - Action Invocations: Read
    - Functions: Create, Read, Edit
    - Layouts: Read, Edit

Installation

The following links will point you to the steps required to install an app or integration on the Resilient Platform.

See the the steps found on ibm.biz/resilient-docs to install or uninstall an App or Integration on the *Resilient platform*.

See the steps under the *Orchestration and Automation* at ibm.biz/cp4s-docs to install or uninstall an App on *IBM Cloud Pak for Security*.

> ⚠ This app does not support use of a proxy server.

APP Configuration

The following table provides the settings required to configure the app. These settings are made in the `app.config` file.

See the Resilient documentation links for the steps provided in the Prerequisites section of this guide for more details.

```
| Config | Required | Example | Description |
| ------ | :------: | ------- | ----------- |
| **host** | Yes | `threatq.<org>.com` | Enter the hostname or IP for your ThreatQ instance |
| **username** | Yes | `resilient` | Enter a ThreatQ username for authentication |
| **password** | Yes | `xxxx` | Enter a ThreatQ password for authentication |
| **cid** | Yes | `xxxx` | Enter your ThreatQ CID (Client ID) found under `My Account` |
| **custom_source** | Yes | `Resilient` | Enter a source name for the data pushed to ThreatQ |
| **custom_attributes** | Yes | `mitre_tactic=MITRE Tactic` | Enter a comma-separated key/value pair, mapping the resilient field (api name) to a ThreatQ attribute |
| **custom_objects** | Yes | `mitre_technique=Attack Pattern, malware_family=Malware` | Enter a comma-separated key/value pair, mapping the resilient field (api name) to a ThreatQ object type |
```

Configuring for Reboot

This section will describe how to configure the integration (resilient-circuits) to auto-run on reboot.

1. Create a file for the new service:

```
sudo vi /etc/systemd/system/
resilient_circuits_functions.service
```

2. Paste the following into the file:

> Fill out required fields (between < >).
>
> Delete lines 4 and 5 completely (`After=...` and `Requires=...`) if you are *not* installing this directly on the Resilient Server.

```
[Unit]
Description=Resilient-Circuits Service for Functions
# Comment out these 2 lines if you are running on an integration server
After=resilient.service
Requires=resilient.service
[Service]
Type=simple
User=res-integration
WorkingDirectory=/home/<username>
ExecStart=/home/<username>/.resilient/functions-env/bin/resilient-circuits run
Restart=always
TimeoutSec=10
Environment=APP_CONFIG_FILE=/home/<username>/.resilient/app.config
Environment=APP_LOCK_FILE=/home/<username>/.resilient/functions.lock
[Install]
WantedBy=multi-user.target
```

3. Give the service file the correct privileges:

```
sudo chmod 664 /etc/systemd/system/
resilient_circuits_functions.service
```

4. Reload the system daemon and enable the functions service:

```
sudo systemctl daemon-reload

sudo systemctl enable resilient_circuits_functions.service
```

5. Start the service:

```
sudo systemctl start resilient_circuits_functions
```

6. You can view the logs for the service by running the following:

```
sudo journalctl -u resilient_circuits_functions -f
```

> This will "follow" the logs in real-time.

Customizing Functionality

By default, the integration includes the following automatic actions:

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

If you do not want those actions to be automated, you can convert them to menu item actions.

Disabling Rules (Actions)

1. Go to **Customization Settings -> Rules**.
2. Find the rule you want to disable.
3. Move the switch to the off position.

Switching to Menu Item Rules

1. Go to `Customization Settings -> Rules`
2. Choose the rule you want to switch to be a menu item

   > Make note the name. Usually `ThreatQ:`, followed by the action name - see the Features section.

3. Delete the rule
4. Create a new rule and then make it a menu item.
5. Enter the name noted in step 2.
6. Set the message destination to `fn_threatq` and then save.

Additionally, two of the actions support some custom fields. If you have converted these automatic actions to menu item actions, see the Features section to see what fields they support.

- Sync Incident

- Sync Indicator

Functions

Due to 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 work.

If you wish to use the functions in a workflow (not via an action), please submit a request to support@threatq.com

Actions

The following actions are supported by the integration.

Sync Incident

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

FIELD	DETAILS
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]

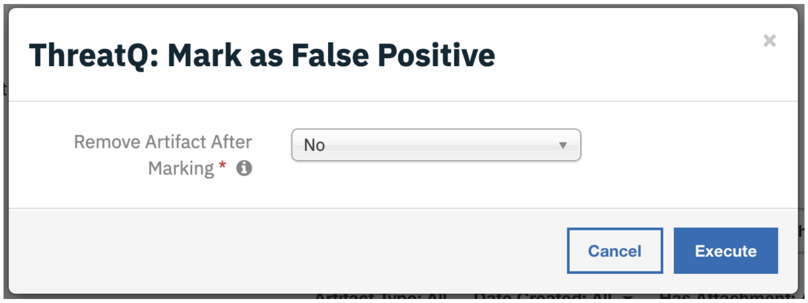
Sync Indicator

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

FIELD	DETAILS
Rule	Automatic
Type	Artifact
Supported Fields (if menu item)	• ThreatQ Indicator Status ◦ Description: The status for the indicator in ThreatQ ◦ Type: Select ◦ Options: [Active, Review, Indirect, Whitelisted, Expired] • ThreatQ Indicator Confidence ◦ Description: A confidence level for the artifact. This will get set as an attribute within ThreatQ ◦ Type: Select ◦ Options: [Low, Medium, High]

Mark as False Positive

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



ThreatQ: Mark as False Positive

Remove Artifact After Marking *: No

FIELD	DETAILS
Rule	Menu Item
Type	Artifact
Fields	ThreatQ 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]

Mark as 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**.

FIELD	DETAILS
Rule	Menu Item
Type	Artifact

Find Related Indicators

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

FIELD	DETAILS
Rule	Menu Item
Type	Artifact

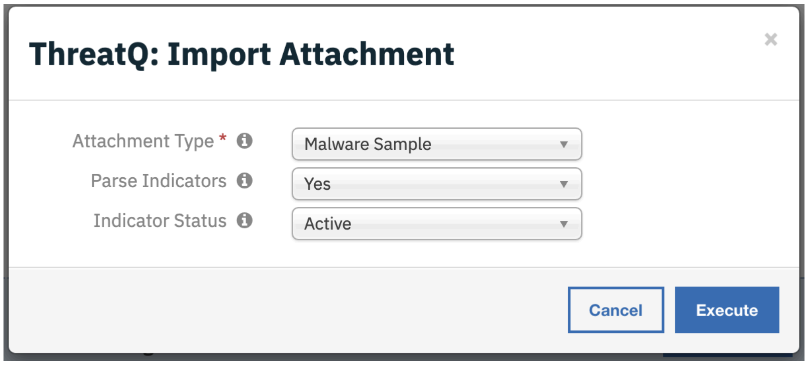
Sync Comment

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.

FIELD	DETAILS
Rule	Menu Item
Type	Artifact

Import Attachment

This action will import an attachment into ThreatQ. It gives you 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.



ThreatQ: Import Attachment

Attachment Type * : Malware Sample

Parse Indicators : Yes

Indicator Status : Active

FIELD	DETAILS
Rule	Menu Item
Type	Artifact
Fields	• ThreatQ 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] • ThreatQ Parse Indicators ◦ Description: Whether or not you want to parse indicators out of the attachment ◦ Type: Select ◦ Options: [Yes, No] • ThreatQ Indicator Status ◦ Description: The status for any parsed indicators (if enabled) ◦ Type: Select ◦ Options: [Active, Review, Indirect, Whitelisted, Expired]

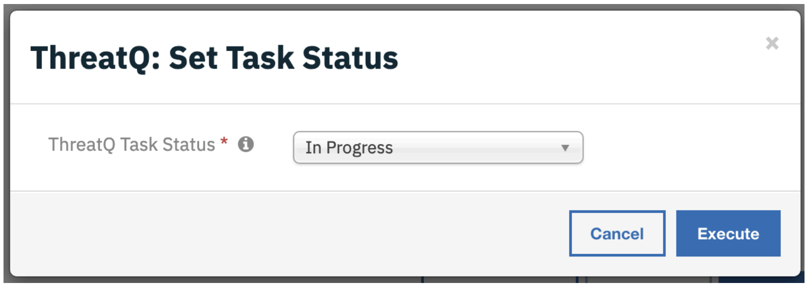
Sync Task

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

FIELD	DETAILS
Rule	Menu Item
Type	Task

Set Task Status

This actions allows you to set the task's status within ThreatQ. By default, the integration syncs tasks with the status **To Do**. If you want to mark the task as a different status, you can use this action.



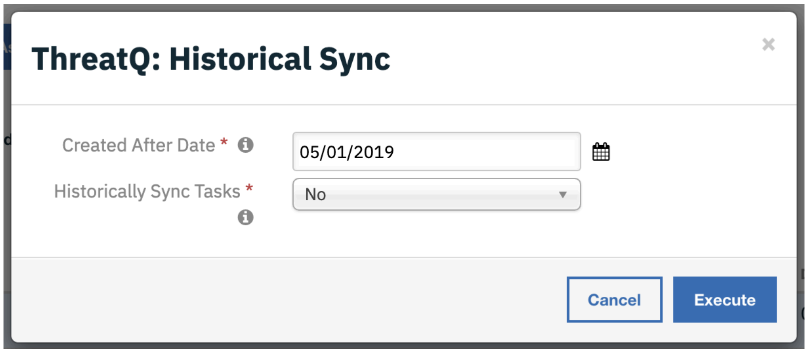
ThreatQ: Set Task Status

ThreatQ Task Status * : In Progress

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

Historical Sync

This action allows you to sync incidents historically. You will be able to customize the date to search since, as well as if you want to sync the related tasks or not.



ThreatQ: Historical Sync

Created After Date * : 05/01/2019

Historically Sync Tasks * : No

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

Updating Versions

This section describes any modifications required when upgrading.

> There are no modifications required to upgrade from version 1.1.0 to 1.1.1.

Updating from v1.0.x to v1.1.1

There are a few changes in the v1.0.1 that would call for some manual modifications.

> Some functions have been removed due to not fully supporting workflows correctly.

1. In your Customization Settings, go to the `Functions` tab and remove the following items:
    - ThreatQ: Sync Incident
    - ThreatQ: Sync Indicator
    - ThreatQ: Import Attachment
    - ThreatQ: Sync Task
    - ThreatQ: Historical Sync
    - ThreatQ: Set Task Status
    - ThreatQ: Sync Comment
    - ThreatQ: Find Related Indicators
    - ThreatQ: Mark as False Positive
    - ThreatQ: Mark as True Positive
2. The following items will be re-added back to your Functions configuration when you rerun `resilient-circuits customize`:
    - ThreatQ: Mark as False Positive
    - ThreatQ: Mark as True Positive
    - ThreatQ: Find Related Indicators

    > See Updating from v1.0.0 to v1.0.1 if you are currently on v1.0.0.

3. There are 3 new config items you can add to your `app.config` file under the `[fn_threatq]` section to support custom attribute mapping, custom object mapping, and a custom source
    - `custom_attributes=`
    - `custom_objects=`
    - `custom_source=Resilient`
    - See the *Configuration* section on how to properly set these options
4. Re-run `resilient-circuits customize` (if you did not do this in step 2).

Troubleshooting

There are several ways to verify the successful operation of a function.

Resilient Action Status

- When viewing an incident, use the Actions menu to view **Action Status**.
- By default, pending and errors are displayed.
- Modify the filter for actions to also show Completed actions.
- Clicking on an action displays additional information on the progress made or what error occurred.

Resilient Scripting Log

- A separate log file is available to review scripting errors.
- This is useful when issues occur in the pre-processing or post-processing scripts.
- The default location for this log file is: `/var/log/resilient-scripting/resilient-scripting.log`.

Resilient Logs

- By default, Resilient logs are retained at `/usr/share/co3/logs`.
- The `client.log` may contain additional information regarding the execution of functions.

Resilient-Circuits

- The log is controlled in the `.resilient/app.config` file under the section [resilient] and the property `logdir`.
- The default file name is `app.log`.
- Each function will create progress information.
- Failures will show up as errors and may contain python trace statements.

Change Log

- **Version 1.1.1**
    - Addressed an issue with the Resilient DNS Name stripping `www.` from content.
- **Version 1.1.0**
    - Added the ability to:
        - sync tasks
        - historically sync incidents (manually)
        - sync comments/notes (manually)
        - sync attachments (manually)
    - Added custom field mapping in configuration to map Resilient fields to ThreatQ objects
    - Added custom field mapping in configuration to map Resilient fields to ThreatQ attributes
- **Version 1.0.0**
    - Initial Release