

ThreatQuotient



ThreatQ Functions App for IBM Security QRadar SOAR

Version 2.0.0

October 02, 2024

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details.....	5
Introduction	6
Prerequisites	7
Generating ThreatQ OAuth Client ID and Client Secret	7
ThreatQ v6 OAuth Registration Steps	7
ThreatQ v5 OAuth Registration Steps	8
Installation.....	9
Configuration	13
Customizations	15
Playbooks	15
Functions.....	16
Rules	17
Usage.....	18
Migrating from V1 to V2.....	20
Removing the v1 App Customizations	20
Removing Action Fields - Optional	21
Uninstall Python Packages.....	21
Uninstall the ThreatQ Threat Source	22
Install V2	22
Important Notes.....	22
Troubleshooting	24
Connection Error when Testing Configuration	24
Certificate Error	24
Change Log	26

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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com

Support Web: <https://support.threatq.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.0.0
Compatible with ThreatQ Versions	>= 5.6.0
Recommended QRadar SOAR Versions	>=51.0.0.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Functions App for IBM Security SOAR gives IR teams the ability to leverage ThreatQ to enrich incidents and artifacts with your curated and prioritized threat intelligence data.

The app provides a set of functions that allow users to interact with ThreatQ including, but not limited to:

- searching for indicators
- adding attributes
- exporting incidents

The app also includes a set of playbooks that demonstrate how to use these functions to get your IR team the information they need to make efficient decisions

Prerequisites

The following is required to utilize the app:

- ThreatQ Username, Pass and API Credential (CID)



You can also use your OAuth Client ID and Client Secret.

- IBM Security QRadar SOAR Administrator Privileges
- IBM Security App Host

Generating ThreatQ OAuth Client ID and Client Secret

Use the following steps to generate an OAuth Client ID and Client Secret IF you elect not authenticate via your ThreatQ username and password.

ThreatQ v6 OAuth Registration Steps

1. SSH to your ThreatQ installation.
2. Create a new client id and client secret password using the following command:

```
kubectl exec --namespace threatq --stdin --tty deployment/api-  
schedule-run -- ./artisan threatq:oauth2-client --name="IBM QRadar  
SOAR"
```

The Client ID and Secret will be included in the command output as demonstrated in the example below.

```
session_timeout_minutes: 1440  
name: IBM QRADAR SOAR  
type: private  
client_id: ntdjzwe3mduyyjqxyjdiyza5mzyxmtkx  
client_secret:  
YThlOTBlZjM0YTYxNWM1YjVkdDdmMTdjNGY5MzZkYTg4M2RmYmRiZGJmNjk1OTRm  
updated_at: 2020-01-14 14:03:27  
created_at: 2020-01-14 14:03:27
```

3. Copy and save the **client_id** and **client_secret** in a secure location.

ThreatQ v5 OAuth Registration Steps

1. SSH to your ThreatQ installation.
2. Navigate to the api directory using the following command:

```
cd /var/www/api
```

3. Create a new client id and client secret password using the following command:

```
php artisan threatq:oauth2-client --name="IBM QRadar SOAR"
```

The Client ID and Secret will be included in the command output as demonstrated in the example below.

```
session_timeout_minutes: 1440
name: IBM QRADAR SOAR
type: private
client_id: ntdjzwe3mduyyjqxyjdiyza5mzyxmtkx
client_secret:
YThlOTBlZjM0YTlYxNWM1YjVkdDdmMTdjNGY5MzZkYTg4M2RmYmRiZGJmNjk1OTRm
updated_at: 2020-01-14 14:03:27
created_at: 2020-01-14 14:03:27
```

4. Copy and save the **client_id** and **client_secret** in a secure location.

Installation

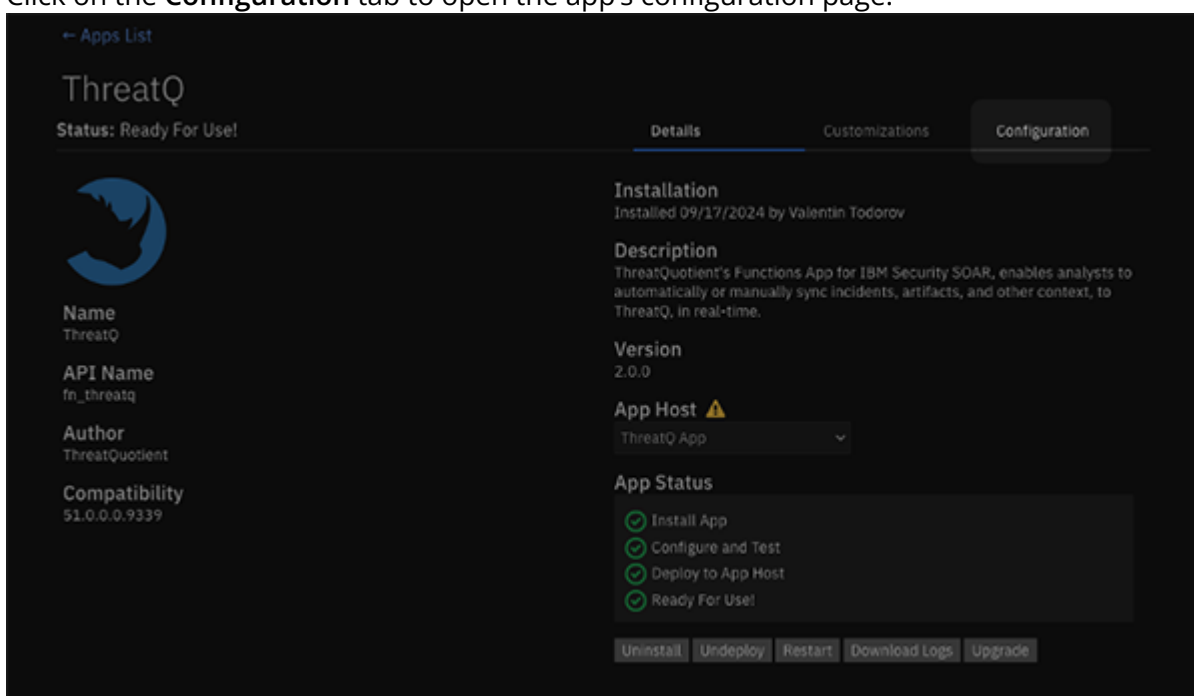
Perform the following steps to install the app:

1. Download the **ThreatQ Functions App** from the **IBM X-Force App Exchange**.
2. Log into your IBM Security QRadar SOAR (Resilient) instance.
3. Navigate to **User Profile > Administrator Settings > Apps**.
4. Install the ThreatQ Functions App

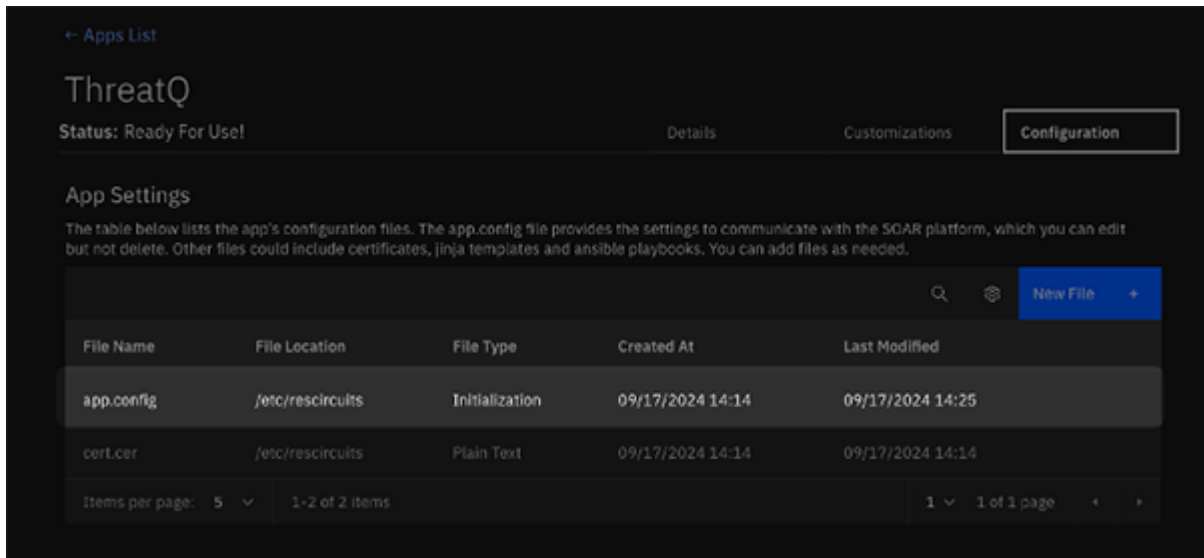


You must allow the installation of the app's customization settings to use the app.




5. Click on the **Configuration** tab to open the app's configuration page.





- Click on the **app.config** entry within the *App Settings* table. This will display two new sections: **File Content** and **Secrets**.



- Click on the **Add Secret** button, located in the *Secrets* section, to enter in the fields you see in the *File Content* section:

FIELD	DESCRIPTION
TQ_HOST	Your ThreatQ Hostname.
TQ_USER	Your ThreatQ username. <div>  This is required if you are not using OAuth authentication. </div>
TQ_PASSWORD	The password associated with your ThreatQ username. This field is encrypted. <div>  This is required if you are not using OAuth authentication. </div>
TQ_CID	Your ThreatQ API Credential. <div>  This is required if you are not using OAuth authentication. </div>

FIELD	DESCRIPTION
TQ_CLIENT_ID	<p>The Client ID for the app.</p> <div>  <p>This is required if you are not using the user-authentication. Steps for generating the Client ID can be found under the Prerequisite chapter.</p> </div>
TQ_CLIENT_SECRET	<p>The Client Secret for the App. This field is encrypted.</p> <div>  <p>This is required if you are not using the user-authentication. Steps for generating the Client ID can be found under the Prerequisite chapter.</p> </div>

File Content

Text or code as appropriate.

File Type Initialization












```

1- [fn_threatq]
2- # ThreatQ Connection Information
3- host = $TQ_HOST
4- verify_ssl = False
5- # ThreatQ User-Authentication Information
6- username = $TQ_USER
7- password = $TQ_PASSWORD
8- cid = $TQ_CID
9- # ThreatQ OAuth-Authentication Information
10- # OAuth credentials must be generated via the ThreatQ CLI.
11- # Please contact ThreatQuotient Support to generate these credential
12- client_id = $TQ_CLIENT_ID
13- client_secret = $TQ_CLIENT_SECRET
14- # Set a custom source name for anything synced with ThreatQ
15- custom_source = IBM QRadar SOAR
16- # Custom Field Handling
17- # Map Resilient Custom Fields to ThreatQ attributes using a comma-se
18- custom_attributes =
19- # Map Resilient Custom Fields to ThreatQ custom objects using a comm
20- custom_objects =
21-
22- [resilient]
23- api_key_id = c07629f2-2d6b-4904-89ed-46407c0a4512
24- api_key_secret = $API_KEY_SECRET
25- cafile = False
26- host = 10.114.0.210
27- port = 443
28-


```

Secrets


Filter Add Secret +

Secret Name	
API_KEY_SECRET	 
TQ_CID	 
TQ_HOST	 
 TQ_PASSWORD	 
TQ_USER	 

- You can also manually modify the File Contents for fields such as “custom_source” and “custom_attributes,”



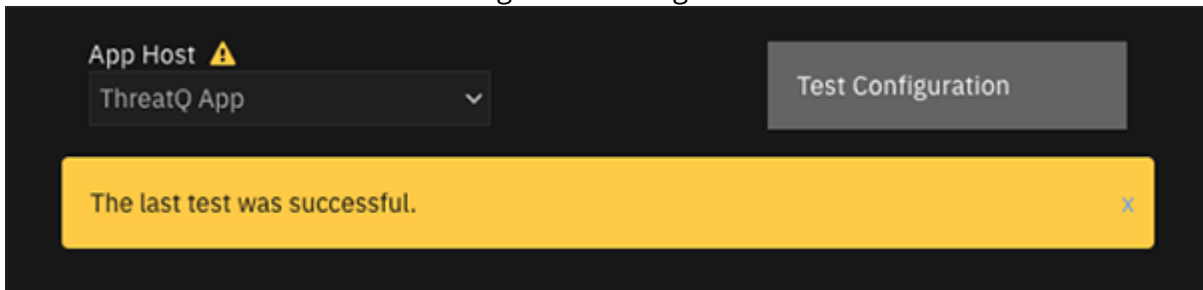
If your IBM Security QRadar SOAR instance is using a self-signed certificate, set the “cafile” field to “False” under the “resilient” section




If your ThreatQ instance is using a self-signed certificate, set the “verify_ssl” field to “False” under the “fn_threatq” section.

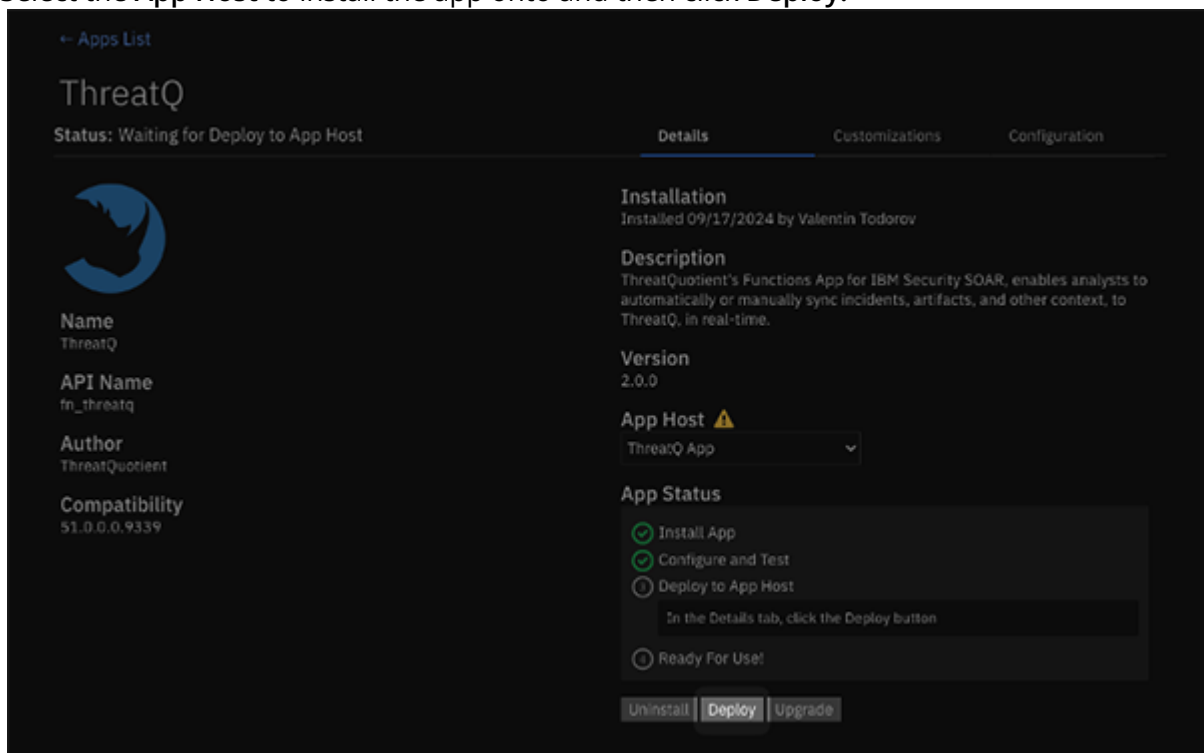
- Click on the **Save and Push Changes** button to save your configurations.


10. Click on the Test Configuration button to ensure everything is working properly. You will receive a "The last test was successful" message if the configuration is correct.



 Any errors will be displayed in a red error message with error details.

11. Navigate back to the **Details** page for your app. You should now be allowed to deploy your app.
12. Select the **App Host** to install the app onto and then click **Deploy**.



 The installation process may take up to a few minutes • In the event that an error occurs, download the app logs and share them with the ThreatQuotient Support Team.

Configuration

The table below contains the specifications for the app.config file.

PARAMETER	>DESCRIPTION
host	Required. Enter the hostname or IP address to your ThreatQ server. Do not include a scheme or a URL path.
verify_ssl	True/False. Disabling this option will allow the app to skip SSL verification when connecting to your ThreatQ server.
username	Required if using user-authentication. Enter the username for a local ThreatQ account with at least Primary Contributor permissions.
password	Required if using user-authentication. Enter the password associated with the provided ThreatQ username.
cid	Required if using user-authentication. Enter your API Credential, found in your ThreatQ user profile.
client_id	Required if using Client Credentials to authenticate. Enter your OAuth Client ID. Obtain these credentials by contacting the ThreatQ Support Team.
client_secret	Required if using Client Credentials to authenticate. Enter your OAuth Client Secret. Obtain these credentials by contacting the ThreatQ Support Team.
custom_source	Required. Enter the source name to apply to all intelligence added to ThreatQ from IBM Security QRadar SOAR.
custom_attributes	Enter a comma-separated list of key/value pairs where the key is the Resilient Field's API name and the value is the ThreatQ Attribute Name. Each key value pair should be separated by an equals (=) character. Example: target_country=Target Country, target_sector=Target Sector

PARAMETER	>DESCRIPTION
custom_objects	Enter a comma-separated list of key/value pairs where the key is the Resilient Field's API name and the value is the ThreatQ Object Type. Each key value pair should be separated by an equals (=) character. Example: threat_actor=adversaries, malware_family=malware

Customizations

The ThreatQ Functions App for IBM Security QRadar SOAR comes with various Functions, Rules, and Playbooks to seamlessly integrate with ThreatQ.

Playbooks

* Disabled by default

NAME	DESCRIPTION
ThreatQ: Add Attribute to Artifact	A menu item allowing you to add an attribute directly to an artifact in ThreatQ.
ThreatQ: Add Tags to Artifact	A menu item allowing you to add a tags directory to an artifact in ThreatQ.
ThreatQ: Automatically Export Artifact *	An automated playbook to automatically export artifacts to ThreatQ.
ThreatQ: Automatically Export Incident *	An automated playbook to automatically export incidents to ThreatQ.
ThreatQ: Automatically Find Artifact Hits	An automated playbook to automatically perform artifact lookups against ThreatQ, returning hits back to IBM Security QRadar SOAR.
ThreatQ: Export Artifact	A menu item to export an artifact to ThreatQ, manually.
ThreatQ: Export Incident	A menu item to export an incident to ThreatQ, manually.
ThreatQ: Find Artifact Hits	A menu item to perform an artifact lookup against ThreatQ, manually. Hits will be returned back to IBM Security QRadar SOAR.

NAME	DESCRIPTION
ThreatQ: Find Related Artifacts	A menu item to perform a lookup for all related indicators to a given artifact in ThreatQ. Related indicators will be added as artifacts to the corresponding incident.
ThreatQ: Find Related Malware (Example)	An example playbook for a menu item that will perform a lookup in ThreatQ for malware related to the given artifact.

Functions

NAME	DESCRIPTION
ThreatQ: Add Artifact Attribute	A function to add an attribute to an artifact in ThreatQ.
ThreatQ: Add Artifact Tags	A function to add tags to the corresponding artifact in ThreatQ.
ThreatQ: Export Artifact	A function to export an artifact to ThreatQ.
ThreatQ: Export Incident	A function to export an incident to ThreatQ.
ThreatQ: Find Artifact Hits	A function to perform an artifact lookup in ThreatQ.
ThreatQ: Find Related Artifacts	A function to find indicators (artifacts) from ThreatQ that are related to an input artifact from IBM Security QRadar SOAR.
ThreatQ: Search Threat Library	A function to search your ThreatQ Threat Library.
ThreatQ: Set Artifact Status	A function to set the status of an artifact in ThreatQ.

Rules

* Disabled by default

NAME	DESCRIPTION
ThreatQ: Import Attachment	A menu item to import an incident attachment into ThreatQ.
ThreatQ: Set Task Status *	A menu item to manually set a task's status in ThreatQ.
ThreatQ: Sync Tasks *	An automated rule to automatically export tasks to ThreatQ.

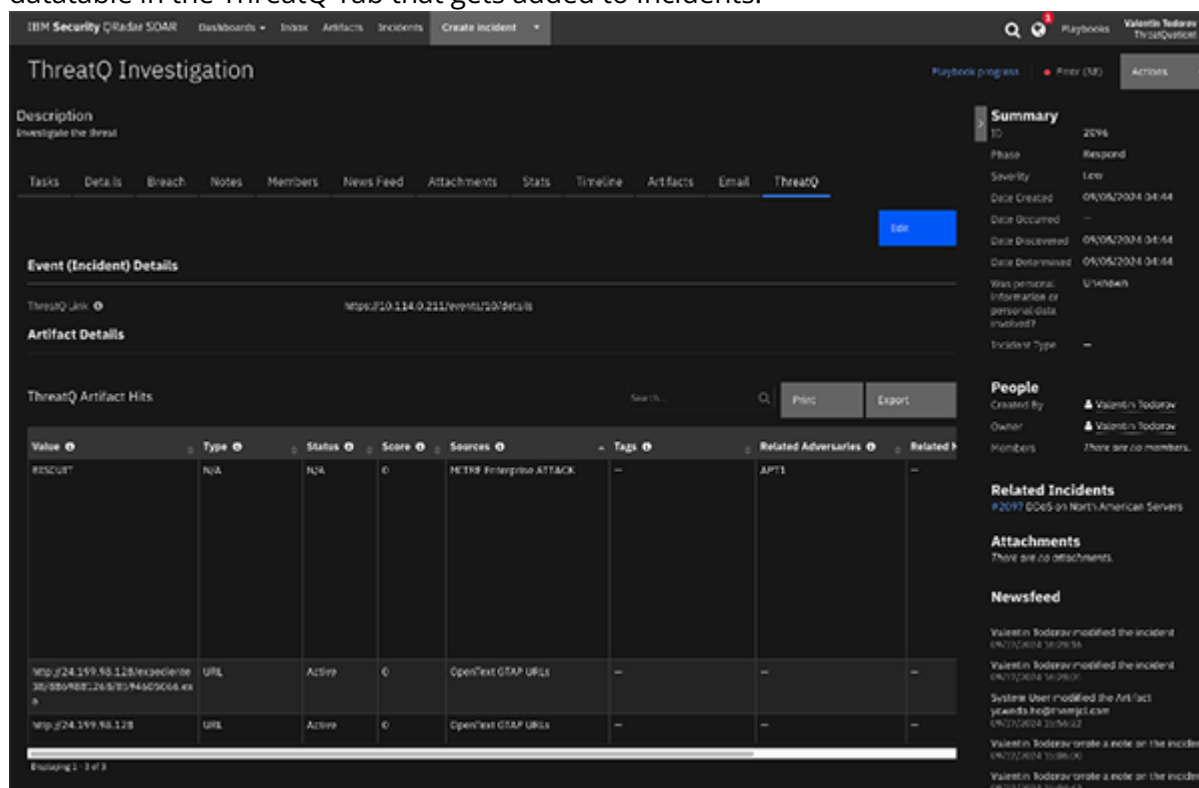
Usage

By default, all menu item Playbooks are enabled, however, nearly all automated Playbooks are disabled.

If you would like incidents and artifacts to automatically sync to your connected ThreatQ instance, enable the following Playbooks:

- ThreatQ: Automatically Export Incidents
- ThreatQ: Automatically Export Artifacts

The only automated Playbook that is enabled by default is the **ThreatQ: Automatically Find Artifact Hits** playbook. This Playbook replicates the functionality that was previously part of the ThreatQ CTS App for IBM Security QRadar SOAR. This Playbook will automatically perform lookups of supported artifacts, returning the results to the hits section for the artifact. It will also populate the Artifact Hits datatable in the ThreatQ Tab that gets added to Incidents.



ThreatQ Investigation

Description: Investigate the threat

Summary:

- ID: 2096
- Phase: Respond
- Severity: Low
- Date Created: 04/04/2024 04:44
- Date Occurred: --
- Date Discovered: 04/04/2024 04:44
- Date Determined: 04/04/2024 04:44
- Was personal information or personal data involved?: Unknown
- Incident Type: --

People:

- Created By: Valentin Rodraz
- Owner: Valentin Rodraz
- Members: There are no members.

Related Incidents: #2097 DDOS on North American Servers

Attachments: There are no attachments.

Newsfeed:

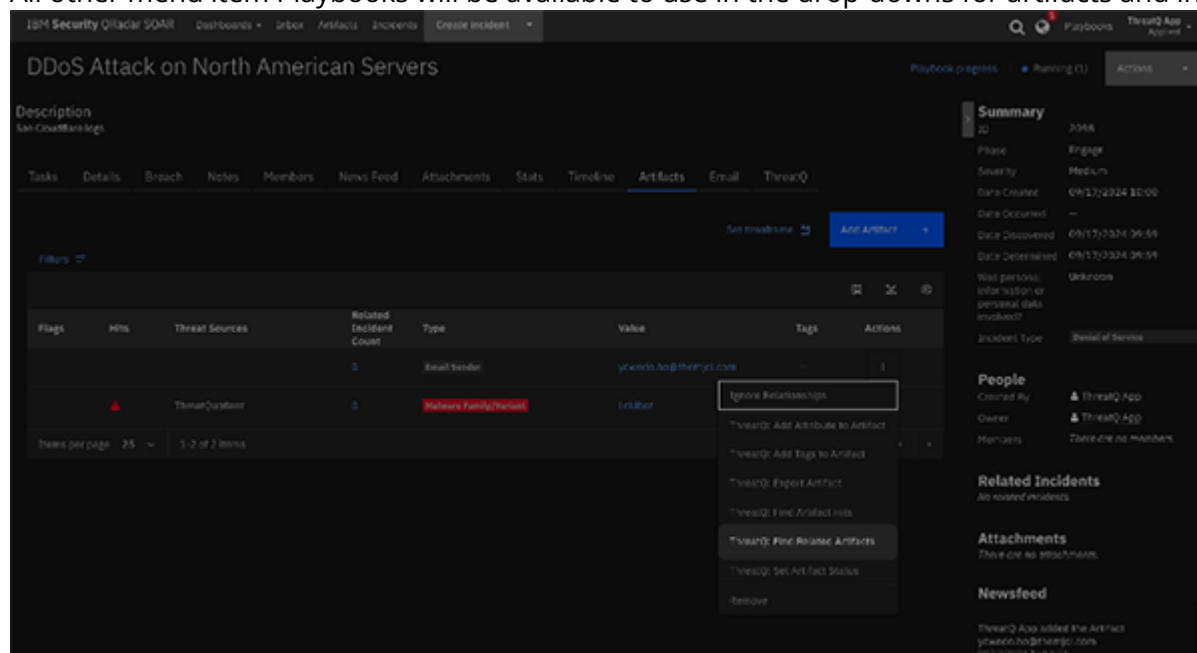
- Valentin Rodraz modified the incident: 04/04/2024 04:44
- Valentin Rodraz modified the incident: 04/04/2024 04:44
- System User modified the artifact: yawsda-hdgr-weged.com: 04/04/2024 03:50:23
- Valentin Rodraz create a note on the incident: 04/04/2024 03:50:23
- Valentin Rodraz create a note on the incident: 04/04/2024 03:50:23

ThreatQ Artifact Hits

Value	Type	Status	Score	Sources	Tags	Related Adversaries	Related Incidents
RCSCUT	N/A	N/A	0	HEX8 Enterprise ATTACK	--	APT1	--
http://24.199.98.128/exceciencie35/8849881245/515443C56444x	URL	Active	0	OpenText OTAP URLs	--	--	--
http://24.199.98.128	URL	Active	0	OpenText OTAP URLs	--	--	--

Showing 1 of 3

All other menu item Playbooks will be available to use in the drop-downs for artifacts and incidents.



DDoS Attack on North American Servers

Description: [See Description](#)

Task Details: [Details](#) [Breach](#) [Notes](#) [Members](#) [News Feed](#) [Attachments](#) [Stats](#) [Timeline](#) [Artifacts](#) [Email](#) [ThreatQ](#)

Filters: 17

Flags	Items	Threat Sources	Related Incident Count	Type	Value	Tags	Actions
			0	Email Sender	youw@h@thre@q.com		
		ThreatQ:Source	0	Malware Family/Variant	LinkBot		

ThreatQ: Add Attribute to Artifact
ThreatQ: Add Tags to Artifact
ThreatQ: Export Artifact
ThreatQ: Find Artifact Info
ThreatQ: Find Related Artifacts
ThreatQ: Set Artifact Status
Remove

Summary

ID: 2096
Phase: Engage
Severity: Medium
Data Created: 09/13/2024 10:00
Data Occurred: --
Data Discovered: 09/13/2024 09:59
Data Determined: 09/13/2024 09:59
Was person, information or personal data involved? Unknown
Incident Type: Denial of Service

People

Created By: ThreatQ App
Owner: ThreatQ App
Members: [View all members](#)

Related Incidents

No related incidents

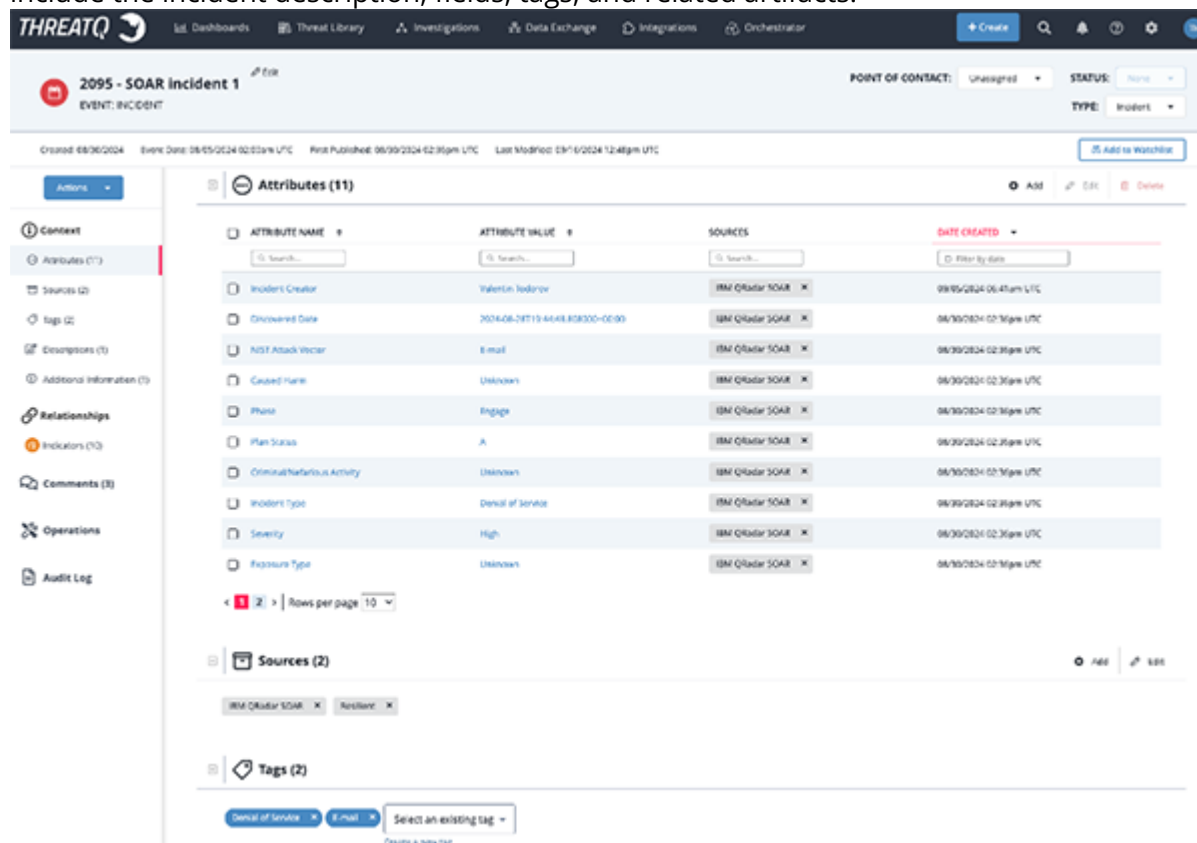
Attachments

There are no attachments

Newsfeed

ThreatQ App added the Artifact youw@h@thre@q.com on 09/13/2024 10:00

Exported incidents will appear in ThreatQ as Event Objects with the type, Incident. Each event will include the incident description, fields, tags, and related artifacts.



2095 - SOAR incident 1

EVENT: INCIDENT

POINT OF CONTACT: Unassigned STATUS: None TYPE: Incident

Created: 08/30/2024 Event Date: 08/05/2024 02:00am UTC First Published: 08/30/2024 02:35pm UTC Last Modified: 09/10/2024 12:48pm UTC

Attributes (11)

ATTRIBUTE NAME	ATTRIBUTE VALUE	SOURCES	DATE CREATED
Incident Creator	Valentin Iodora	IBM QRadar SOAR	08/30/2024 02:41pm UTC
Discovered Date	2024-08-28T19:44:48.808000-05:00	IBM QRadar SOAR	08/30/2024 02:36pm UTC
NOT Attack Vector	Email	IBM QRadar SOAR	08/30/2024 02:36pm UTC
Created Name	Unknown	IBM QRadar SOAR	08/30/2024 02:36pm UTC
Phase	Engage	IBM QRadar SOAR	08/30/2024 02:36pm UTC
IPan Status	A	IBM QRadar SOAR	08/30/2024 02:36pm UTC
Criminal/Paratious Activity	Unknown	IBM QRadar SOAR	08/30/2024 02:36pm UTC
Incident Type	Denial of Service	IBM QRadar SOAR	08/30/2024 02:36pm UTC
Severity	High	IBM QRadar SOAR	08/30/2024 02:36pm UTC
Exposure Type	Unknown	IBM QRadar SOAR	08/30/2024 02:36pm UTC

Sources (2)


IBM QRadar SOAR Incident


Tags (2)

Denial of Service Email Select an existing tag Create a new tag

Migrating from V1 to V2

The v2 release of the ThreatQ App for IBM Security QRadar SOAR introduces a number of changes to the app. These changes were implemented to not only improve the overall user experience, but also to provide a more robust and feature-rich integration with ThreatQ. The ThreatQuotient team has migrated most of the functionality away from using Rules & Workflows to using Functions & Playbooks. This change gives you more functionality and more control over the integration. It will also allow you to combine the integration's functionality with existing Workflows and Playbooks.

 Before performing the upgrade steps, ensure that you have alerted the proper teams of the upcoming downtime and changes.

 While this app supports installation onto an App Host, Edge Gateway, or Integration Server, it is highly recommended to install it onto an App Host.

Removing the v1 App Customizations

The following steps need to be taken to migrate from v1 to v2 by removing the v1 app customizations:

1. Login to your IBM Security QRadar SOAR instance as an administrator.
2. Open your **Administrator Settings** and navigate to the **Threat Sources** tab.
3. Turn off the ThreatQ entry.
4. Open your **Customization Settings** and navigate to the **Rules** tab.
5. Delete the following rules:
 - ThreatQ: Find Related Indicators
 - ThreatQ: Historical Sync
 - ThreatQ: Mark as False Positive
 - ThreatQ: Mark as True Positive
 - ThreatQ: Sync Comment
 - ThreatQ: Sync Incident
 - ThreatQ: Sync Incident Now
 - ThreatQ: Sync Indicator
 - ThreatQ: Sync Indicator Now
6. Navigate to the **Functions** tab.
7. Delete the following functions:
 - threatq_add_indicator
 - threatq_find_related_indicators
 - threatq_mark_as_false_positive
 - threatq_mark_as_true_positive
8. Navigate to the **Destinations** tab.
9. Delete the following message destinations (if they exist):
 - fn_threatq
 - ThreatQ

Removing Action Fields - Optional

You can optionally remove the "action fields" that were used in the v1 app. These fields were used when invoking the Rules. To remove these fields, follow these steps:

1. Login to your IBM Security QRadar SOAR instance as an administrator.
2. Open your Administrator Settings and navigate to the Rules tab.
3. Select ThreatQ: Import Attachment to open its configuration.
4. At the bottom of the Activities section, expand the Show Activity Fields section.
5. On the right hand side of the page, you will see a list of existing fields. Edit & delete the following fields:
 - ThreatQ: Created After Date
 - ThreatQ: Historically Sync Tasks
 - ThreatQ: Parse Indicators
 - ThreatQ: Remove Artifact After Marking

Uninstall Python Packages

If you are using the v1 app, you are more than likely running it on a Resilient Integration Server. This is a linux-based server that runs all of your QRadar SOAR apps.

To uninstall the v1 Python packages for both the ThreatQ CTS App and ThreatQ Functions App, follow these steps:

1. SSH into your Resilient Integration Server.
2. Gain root privileges by running `sudo su` and entering your password.
3. Locate your `.resilient` directory in your home directory and `cd` into it.
4. Run `ls` to list the contents of the directory.



If you do not see a `functions-env` or `cts-env` directory, either the ThreatQ App (v1) was not installed, or it was installed in a different location. Once you locate the directory, `cd` into it and continue the steps.

5. Run the following to view your current app configuration file.

```
cat app.config
```



It is highly recommend copying this configuration to a safe location for reference later when configuring the v2 app.

6. Run the following command to remove the ThreatQ Functions App (if installed):

```
rm -rf functions-env
```

7. Run the following command to remove the ThreatQ CTS App (if installed):

```
rm -rf cts-env
```

8. Run the following command to remove the ThreatQ Functions App service (if installed):

```
rm -rf /etc/systemd/system/resilient_circuits_functions.service
```

9. Run the following command to remove the ThreatQ CTS App service (if installed):

```
rm -rf /etc/systemd/system/resilient_circuits_cts.service
```

10. Run the following command to reload the systemd daemon:

```
systemctl daemon-reload
```

11. If you are not using the Integration Server for any other apps, you can decommission it.

Uninstall the ThreatQ Threat Source

Previously, ThreatQ offered an App specifically for use as a Custom Threat Service (CTS). This app is no longer necessary with the v2 app. The v2 app achieves the same result, without the need for a second app. To remove the ThreatQ CTS App, follow these steps:

1. SSH into your Resilient Server as `resadmin`.
2. Run the following command with root privileges:

```
sudo resutil threat servicedel -name "ThreatQ"
```

3. The ThreatQ entry in the Administrator Settings -> Threat Sources tab should now be removed.

Install V2

To install the v2 app, follow the steps in the [Installation](#) chapter of this document.

The v2 app will automatically install any necessary customizations into the QRadar SOAR platform. Once installed, you will need to configure & deploy the app to an App Host. For additional documentation, please refer to ThreatQ's official Help Center.

Important Notes

The following are notes about the v2 app's functionality:

- By default, the ThreatQ: Find Artifact Hits playbook is enabled and will automatically run when a new artifact is added to an incident. This playbook will enrich the artifact with hits from ThreatQ and populate the ThreatQ Artifact Hits data table in the ThreatQ incident tab.
- By default, the ThreatQ: Automatically Export Incident and ThreatQ: Automatically Export Artifact playbooks are disabled. If you would like all new incidents & artifacts to be synced to your ThreatQ instance, you can enable these playbooks. If you would like to sync incidents & artifacts on an ad-hoc basis, use the ThreatQ: Export Incident and ThreatQ: Export Artifact playbooks, which are enabled by default (as menu items).

- The app includes a sample playbook called, ThreatQ: Find Related Malware (Example). This playbook demonstrates how to execute a Threat Library search in ThreatQ. This example executes a Threat Library search looking for malware related to a given indicator (artifact). Findings will be added as artifacts to the incident. This playbook is disabled by default.

Troubleshooting

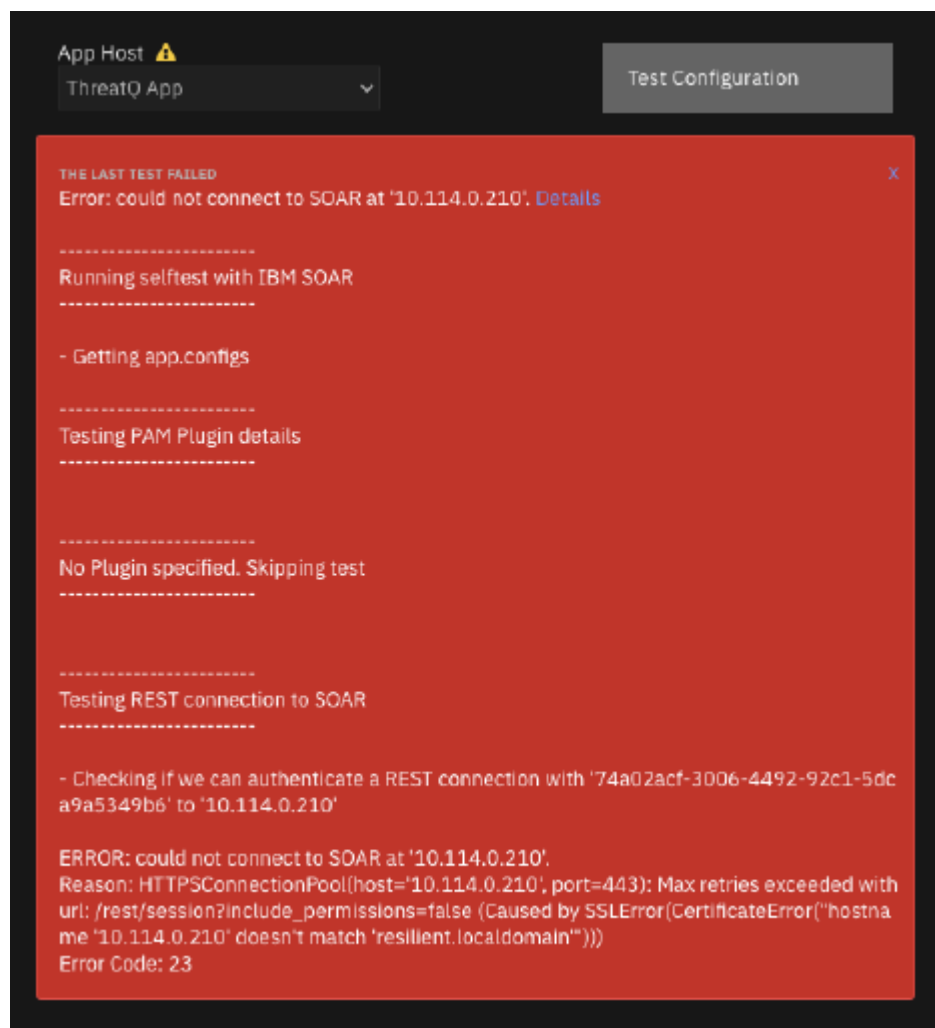
Connection Error when Testing Configuration

If you successfully deploy the App to the App Host, but the Test Configuration button/action is failing, the first thing to do is read the error message and see what the issue is.

Certificate Error

If you are receiving a certificate error when running the configuration test, you may need to temporarily disable SSL verification.

Here is a sample of the error you may be receiving:



In this case, it's erroring out because the certificate for our IBM SOAR instance is misconfigured. For one, we are using a self-signed certificate. Second, our configuration (app.config) uses the IP to

connect to our IBM SOAR instance. However, our self-signed certificate is configured with `resilient.localdomain` as the CN (hostname). This causes the error above.

The fix is simply to remove the `cafile` from the `app.config` file, setting it to `False` instead. Then, saving and pushing the changes to the App Host.

Open your `app.config` file via the UI of your IBM QRadar SOAR instance, from within your App's settings. Then, modify the file content so that `cafile = False`:

```
19 custom_objects =
20
21 [resilient]
22 api_key_id = 74a02acf-3006-4492-92c1-5dca9a5349b6
23 api_key_secret = $API_KEY_SECRET
24 cafile = False
25 host = 10.114.0.210
26 port = 443
27 org = ThreatQuotient
28
```

Change Log

- **Version 2.0.0**
 - Merged functionality of the CTS App into this App (Functions App).
 - Converted App functionality to use Playbooks instead of Rules/Workflows for many of the functions.
 - Added new Functions:
 - Add Artifact Attribute
 - Add Artifact Tag
 - Set Artifact Status
 - Export Incident
 - Export Artifact
 - Find Artifact Hits
 - Find Related Artifacts
 - Search Threat Library
 - Added new Playbooks:
 - ThreatQ: Automatically Export Incident
 - ThreatQ: Automatically Export Artifact
 - ThreatQ: Automatically Find Artifact Hits
 - ThreatQ: Find Related Artifacts
 - ThreatQ: Export Incident
 - ThreatQ: Export Artifact
 - ThreatQ: Find Artifact Hits
 - ThreatQ: Add Attribute to Artifact
 - ThreatQ: Add Tags to Artifact
 - ThreatQ: Set Artifact Status
 - ThreatQ: Find Related Malware (Example)
 - Added a new Incident Tab: ThreatQ. This displays the ThreatQ Link field, ThreatQ Artifact Hits datatable, and other ThreatQ-related fields.
 - Added a new datatable: ThreatQ Artifact Hits. This displays immediate information about artifacts with ThreatQ hits.
 - Added a new field: ThreatQ Link. This provides a link back to ThreatQ from IBM QRadar SOAR.
 - Added support for authenticating using OAuth Client ID and Secret.
 - Added support for controlling the SSL verification toggle when connecting to ThreatQ.
 - Added support for App Host deployments.
 - Updated the minimum IBM Resilient version to v51.0.0.
- **Version 1.1.1**
 - Threat Library SDK migration.
- **Version 1.0.0**
 - Initial release