

ThreatQuotient



Splunk SOAR App for ThreatQ Guide

Version 2.1.0

February 28, 2022

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Support	4
Versioning.....	5
Introduction	6
Installation.....	7
Configuration	8
App Actions	10
Query Indicators.....	10
Create Indicators.....	10
Create Task	11
Create Event.....	11
Create Spearphish	12
Upload File	12
Start Investigation	13
Create Adversaries.....	13
Create Custom Objects	14
Add Attribute	14
Set Indicator Status.....	15
Additional App Instructions	16
Formatting an Indicator List	16
Upgrading from 1x to 2.x	16
Change Log.....	17

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 © 2022 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.

Versioning

- Current integration version: 2.1.0
- Compatible with ThreatQ versions $\geq 4.30.0$
- Phantom App version ≥ 5.10
- Python version: 3

Introduction

The Splunk SOAR App for ThreatQ allows a user to execute a variety of actions on ThreatQ from a Phantom playbook.

 Splunk SOAR App for ThreatQ replaces the Phantom App for ThreatQ application.

With ThreatQ as a single source of truth for Threat Intelligence, you will be able to accurately triage a sighting, and ultimately, make quicker decisions. This allows you to increase your response time and improve your ROI by focusing on what's important to your organization, instead of being inundated with sightings of non-malicious indicators.

The app provides the following actions:

- **Query Indicators** - Queries a list of indicators against ThreatQ.
- **Create Indicators** - Creates indicators in ThreatQ.
- **Create Task** - Creates a task in ThreatQ.
- **Create Event** - Creates an event in ThreatQ based on the Phantom container metadata.
- **Create Spearphish** - Creates a spearphish event in ThreatQ based on a spearphish email in the Phantom vault.
- **Upload File** - Creates a file attachment in ThreatQ.
- **Start Investigation** - Creates a ThreatQ Investigation in the ThreatQ platform.
- **Create Adversaries** - Creates adversaries in ThreatQ.
- **Create Custom Objects** - Creates custom objects in ThreatQ.
- **Add Attribute** - Adds an attribute to a list of custom objects.
- **Set Indicator Status** - Sets the status of an indicator in ThreatQ.



See the [App Actions](#) chapter of this guide for more details on these actions.

Installation

This section will describe how you can install the app into your Phantom instance.



Splunk SOAR App v2.0.0 has fundamentally changed how the App operates. If you are upgrading from v1.x, please refer to the [Upgrading from 1.x to 2.x](#) section under the [Additional App Instructions](#) chapter.

1. Download the **Splunk SOAR App for ThreatQ (tar.gz)** from Splunkbase:
<https://splunkbase.splunk.com/app/6082/>
2. Log into your Phantom instance.
3. Select **Apps** from your navigation dropdown.
4. Click on the **Install App** button at the top right of your Apps page.
5. Select the **Splunk SOAR App for ThreatQ tar.gz** file.

The app will now be installed but still needs to be [configured](#).

Configuration

Once the app is installed, you will see a ThreatQ logo on your Apps page. You can also locate the app by searching for `threatq` in the search bar.

1. Click on the **Configure New Asset** button located next to the ThreatQ logo.
2. Enter following information in the *Asset Info* tab.

FIELD	VALUE
Asset Name	threatq
Asset Description	Integration with the ThreatQ Threat Intelligence Platform.
Product Vendor	ThreatQuotient
Product Name	ThreatQ

3. Click on **Save**.
4. Enter the following information in the *Asset Settings* tab.

FIELD	VALUE
Server IP/ Hostname	Enter the hostname or IP address for your ThreatQ instance.
Client ID	Enter your API Credentials found under your My Account page in ThreatQ.
Username	Enter your username to authenticate with ThreatQ.
Password	Enter your password to authenticate with ThreatQ.
Trust SSL Certificate	Check this box if you want to trust the ThreatQ certificate. This option is checked by default.

5. Click on **Save**.
6. Click the **Test Connectivity** button to test your connection information.



If this test fails, verify that your Phantom instance has access to your ThreatQ instance and confirm that your credentials are correct.

The ThreatQ App will now be configurable within a playbook.

App Actions

The following actions come out of the box with the Splunk SOAR App for ThreatQ.

Query Indicators

FIELD	DETAILS
Name	query_indicators
Description	Query a list of indicators against ThreatQ
Parameters	indicator_list: A list of indicator values to query

Create Indicators

FIELD	DETAILS
Name	create_indicators
Description	Create indicators in ThreatQ
Parameters	indicator_list: A list of indicators to add
Formatting	See the Formatting an Indicator List section.

Create Task

FIELD	DETAILS
Name	create_task
Description	Create a task in ThreatQ
Parameters	• task_name: The name of the task to create • assigned_to: The email or username of a user within ThreatQ to assign the task to • task_status: The task status in ThreatQ • task_priority: The task priority in ThreatQ • task_description: The description of the task • indicator_list: A list of indicators to relate to the task
Formatting	See the Formatting an Indicator List section.

Create Event

FIELD	DETAILS
Name	create_event
Description	Creates an event in ThreatQ, based on the container metadata in Phantom
Parameters	• event_type: The type of event to create in ThreatQ • indicator_list: A list of indicators to relate to the task
Formatting	See the Formatting an Indicator List section.

Create Spearphish

FIELD	DETAILS
Name	upload_spearphish
Description	Creates a spearphish event in ThreatQ, based on a spearphish email in the Phantom vault
Parameters	• vault_id: The ID of an email file in your Phantom vault • indicator_status: The indicator status for any parsed indicators from the spearphish

Upload File

FIELD	DETAILS
Name	upload_file
Description	Creates a file (attachment) in ThreatQ
Parameters	• vault_id: The ID of a file in your Phantom vault • parse_for_indicators: Whether or not to parse the file for indicators • default_indicator_status: The indicator status for any parsed indicators from the file

Start Investigation

FIELD	DETAILS
Name	start_investigation
Description	Creates an investigation in ThreatQ
Parameters	• investigation_name: The name of the investigation to create in ThreatQ • investigation_priority: The priority of the investigation in ThreatQ • investigation_description: The description of the investigation in ThreatQ • investigation_visibility: Whether the investigation is public or private • indicator_list: A list of indicators to relate to the task
Formatting	See the Formatting an Indicator List section.

Create Adversaries

FIELD	DETAILS
Name	create_adversaries
Description	Create adversaries in ThreatQ
Parameters	adversary_list: A list of adversary names to create in ThreatQ

Create Custom Objects

FIELD	DETAILS
Name	create_custom_objects
Description	Creates custom objects in ThreatQ
Parameters	• object_list: A list of custom object values in ThreatQ • object_type: The type of object that the object list specifies

Add Attribute

FIELD	DETAILS
Name	add_attribute
Description	Adds an attribute to a list of custom objects
Parameters	• object_list: A list of custom object values in ThreatQ • object_type: The type of object that the object list specifies • attribute_name: The name for the attribute to add • attribute_value: The value for the attribute to add

Set Indicator Status

FIELD	DETAILS
Name	set_indicator_status
Description	Sets the status of an indicator in ThreatQ
Parameters	- indicator_list: A list of indicators to relate to the task - indicator_status: The status to give to the list of indicators
Formatting	See the Formatting an Indicator List section.

Additional App Instructions

The following section contains information on formatting indicator lists and upgrading app versions.

Formatting an Indicator List

You can pass a list of indicators to an action using several different methods. While the methods for parsing may differ slightly, the outcomes will be similar.

- If only values are specified, the integration will attempt to "detect" the indicator types and upload the known values (i.e. `1.1.1.1`, `badurl.com`).
- You can specify indicator types by separating the type and value by a `:` or `=` character (i.e. `IP Address: 1.1.1.1`, `FQDN: badurl.com`).
- You can even pass the function a list of dictionaries, specifying the indicator type and value, like so:

```
[
  {
    "type": "IP Address",
    "value": "1.1.1.1"
  },
  {
    "type": "FQDN",
    "value": "badurl.com"
  }
]
```

Upgrading from 1x to 2.x

While many of the actions in v2.x of the Splunk SOAR App look very similar to the v1.x App, they operate very differently. It is recommended that you recreate and reconfigure all of the ThreatQ App actions. Review the [App Actions](#) chapter for configuration information.

Change Log

- **Version 2.1.0**

- Fixed an issue where FQDN indicators were created when parsing a URL that did not have a URL pathway.

- **Version 2.0.3**

- The app has been renamed to Splunk SOAR App for ThreatQ (previously known as Phantom App).
- Performed backend code updates to provide better input support, error handling, and overall app stability.
- Replaced all "reputation" actions with an all-in-one query action.
- Added actions to interact with custom objects.
- All response views now share the same template, including tables for attributes and related objects (including custom objects).
- Response data is now better formatted to be used within Phantom playbooks to make better decisions.
- Querying an indicator will query *all* information about that indicator, including attributes, score, status, and relationships. That information is then made accessible within the conditions block in order to make a decision.

- **Version 1.3.0**

- Indicator lookup now does an "approximate" lookup so we can find "similar" results instead of exact matches



This allows subdomains and full URLs to be returns when searching for just the host domain

- Added action to start an investigation from a Phantom Playbook
- Added action to create a task from a Phantom Playbook
- Added action to upload a spearphish email from a Phantom Playbook
- All new actions will create relationships in ThreatQ
- Fixed a bug where indicator score would be > 0
- Fixed a bug where related indicators would not be shown

- **Version 1.2.0**

- Various bug fixes.

- Version 1.0.0
 - Initial release