

ThreatQuotient



Splunk Operation Guide

Version 1.1.0

October 25, 2021

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
- Actions 10
 - Example Result 10
- Change Log..... 11

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 © 2021 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: 1.1.0
- Supported on ThreatQ versions \geq 4.0.0

Introduction

The Splunk Operation performs lookups within Splunk to locate logs related to a selected indicator.

The operation works with the following indicator sub-types:

- FQDN
- IP Address
- URL

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

6. You will still need to [configure and then enable the operation](#).

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operations** option from the *Type* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Splunk IP	The IP of the server that is running Splunk.
Splunk Web Port	The port that the Splunk web app is running on. The default setting is port 8000.
Splunk API Port	The port that the Splunk API endpoints are running on. The default setting is port 8089.
Splunk Username	The username that you use to log into the Splunk web application.
Splunk Password	The password associated with the username above.
Days to Search	The historical timeframe to search through.

PARAMETER	DESCRIPTION
<hr/>	
Language Code	The language code that is being used in Splunk. The default setting is en-US.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPES
Splunk Search	Queries Splunk logs for related indicators.	Indicator	FQDN, IP Address, URL

Example Result

Splunk: Search

Found 2 results!

[Splunk Query Link](#)

Splunk Results

HOST	SOURCE	SOURCE TYPE	DATE/TIME
tis-splunk.threatq.com	/opt/splunk/var/spool/splunk/a5cd4893832f12f_events.stash_new	Splunk	2019-02-26T21:41:03.000+00:00
tis-splunk.threatq.com	/opt/splunk/var/spool/splunk/47ab70bf26138f40_events.stash_new	Splunk	2019-02-26T20:11:14.000+00:00

Raw Response

Show

Change Log

- Version 1.1.0
 - Initial release