

ThreatQuotient



ArcSight SOAR App User Guide

Version 1.0.0

June 22, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



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

Installation..... 8

Actions and Enrichments 9

 Running an Action..... 10

 Running an Enrichment 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 © 2023 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	1.0.0
Compatible with ThreatQ Versions	>= 5.8.0
Support Tier	ThreatQ Supported

Introduction

The ArcSight SOAR App is a bidirectional integration designed to import cases from ArcSight SOAR as events with related indicators, and export enriched indicator data to ArcSight SOAR.

The app is installed on your instance of ArcSight SOAR, and includes several actions and an enrichment.

The provided actions include:

- Creating an Event in ThreatQ from a case in SOAR
- Adding an indicator from SOAR to a ThreatQ event
- Adding tags to an event
- Creating an attribute for an event to mark it as a false or true positive
- Marking an indicator for enrichment in ThreatQ
- Updating an indicator's status in ThreatQ.
- Enrichment will search ThreatQ for a specific indicator and provide enriched data to SOAR.




This app is designed to be installed on your ArcSight SOAR instance.

Prerequisites

The following is required in order to run the app:

- A ThreatQ instance running version 5.8.0 or greater.
- An ArcSight SOAR Instance.

Installation

 **Upgrading** - If you are upgrading from a previous version, review the Change Log to determine if there are any changes to configuration file via new or removed fields. If there are changes, you must first delete your existing configuration file before proceeding with the steps below to install the new version.

Perform the following steps to install the app:



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

1. Download the app zip file from the ThreatQ Marketplace.
2. Sign into your ArcSight SOAR instance.
3. Navigate to **Respond > Configuration** and then click on **Integrations**.
4. Click on the **Upload Plug** option in the Integrations section.
5. Attach the **threatq_arcsight.zip** file then click **Save**.
6. Enter your **ThreatQ Host Address** in the Address section when prompted by the Integration Editor Card popup.
7. Click on **Create** located next to the Credential drop-down menu.
8. Enter the name you'd like the new credentials to be saved as, then type in your login info for your ThreatQ instance.
9. Enter your **ThreatQ Client ID** in the **Private Key** field.
10. Check the **Cleartext Access** box and then click **Save**.
11. Once your credentials are created, select them in the Credential dropdown menu, then click **Save**.
12. Your ThreatQ Integration should now appear in your list of integrations.

Actions and Enrichments

ACTION/ ENRICHMENT NAME	TYPE	DESCRIPTION
Create Event	Action	Creates an Event in ThreatQ corresponding to a case in ArcSight SOAR
Add Indicator	Action	Adds an indicator from the case scope in ArcSight as a related indicator to the corresponding TQ Event
Add Tags	Action	Adds a list of tags to the ThreatQ Event
Mark as False Positive	Action	Creates an attribute in the ThreatQ event marking it as a False Positive
Mark as True Positive	Action	Creates an attribute in the ThreatQ event marking it as a True Positive
Mark For Enrichment	Action	Creates an attribute in the ThreatQ event marking it as needing enrichment
Update Indicator Status	Action	Updates the status of an indicator related to the ThreatQ event
Search ThreatQ	Enrichment	Searches ThreatQ for the selected indicator and displays enriched data in ArcSight SOAR

Running an Action

To run one of the above actions in ArcSight SOAR:

1. Navigate to **Respond > Cases**.
2. Select the case you'd like to run the action on.
3. Select the **Action** option located in the top right corner of your SOAR instance.
4. Select **ThreatQ**.
5. Select which action you'd like to run and complete out the required fields.

Running an Enrichment

To run one of the above enrichments in ArcSight SOAR:

1. Navigate to **Respond > Cases**.
2. Select the case you'd like to run the enrichment on.
3. Select the **Enrich** option located in the top right corner of your SOAR instance.
4. Select **Threat Intelligence** and then select **ThreatQ**.
5. Select the enrichment you'd like to run and complete out the required fields.

Change Log

- Version 1.0.0
 - Initial release