ThreatQuotient

Splunk Phantom Operation User Guide

Version 2.1.0

November 03, 2023

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**
Installation **7**
Configuration **8**
Actions **9**
Create Container 10
Action Parameters 10
Run Playbook 11
Action Parameter 11
Get Playbook Results 13
Change Log **14**

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.

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	2.1.0
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

The Splunk Phantom Operation allows a ThreatQ user to create containers and run playbooks in Phantom.

The operation provides the following actions:

- **Create Container -** creates a container based on an event.
- **Run Playbook -** runs a playbook from a container.
- **Get Playbook Results -** fetches playbook results.

The operation is compatible with Event system objects.

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 operation 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.

The operation is now installed and will be displayed in the ThreatQ UI. 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Hostname	Your Splunk Phantom instance hostname.
Authentication Token	Your Splunk Phantom authentication token.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Create Container	Creates a container based on an event.	Events	N/A
Run Playbook	Runs a playbook from a container.	Events	N/A
Get Playbook Results	Fetches playbook results.	Events	N/A

Create Container

The Create Container action creates a container based on an event.

```
POST https://<hostname>/rest/container
```

Action Parameters

The action has the following configuration parameters:

PARAMETER	DESCRIPTION
Container Label	For example, events, generator, sample. All possible labels can be found in the Phantom UI.
Sensitivity	Container sensitivity.
Severity	Container severity.
Status	Container status.
Kill Chain	Cyber kill chain.
Artifact Label	The label to assign the artifacts.
IP Address CEF Field	The field to use for IP addresses.
FQDN CEF Field	The field to use for FQDNs.
File Hash CEF Field	The field to use for File Hashes.
Filename CEF Field	The field to use for Filenames.
File Path CEF Field	The field to use for File Paths.
Username CEF Field	The field to use for Usernames.

Run Playbook

The Run Playbook action runs a playbook from a container.

`POST https://<hostname>/rest/playbook_run`

Action Parameter

The action has the following configuration parameter:

PARAMETER	DESCRIPTION
Playbook Name	The name of the playbook to run.

Get Playbook Results

The Get Playbook Results fetches playbook results.

```
GET https://<hostname>/rest/playbook_run
```

Change Log

- **Version 2.1.0**
  - Initial release