ThreatQuotient



Silobreaker Operation User Guide

Version 1.0.0

November 03, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400 Ashburn, VA 20147





Contents

Varning and Disclaimer	3
upport	4
ntegration Details	5
ntroduction	
nstallation	
onfiguration	8
ctions	
In Focus	10
Heat	11
Action Parameters	11
hange Log	13



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 **Not Actively Supported**.

Integrations, apps, and add-ons designated as Not Actively Supported are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/addon, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.



For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Actively Supported integrations/apps/add-ons.



Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version 1.0.0

Compatible with ThreatQ >= 4.0.0

Versions

Support Tier Not Actively Supported



Introduction

The Silobreaker Operation for ThreatQ enables a user to query Silobreaker for any reputation context for a given indicator of compromise.

The operation provides the following actions:

- In Focus queries Silobreaker for the top 'x' related entities for a given entity.
- **Heat** queries Silobreaker for the most recent documents pertaining to an entity and its' related entities

The operation is compatible with the following system objects:

- Adversaries
- Identities
- Indicators
 - URL
 - FQDN
 - IP Address
 - CVE
 - ° MD5
 - ° SHA-1
 - · SHA-256
 - Username
 - ASN
- Malware
- TTPs
- Vulnerabilities



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:

PARAMETER

- 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:

API Key	Your Silobreaker API Key.
Shared Key	Your Silobreaker Shared Key.
Count Per Entity Type	The number of each entity type you'd like returned. The default setting is 10.

DESCRIPTION

- 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:

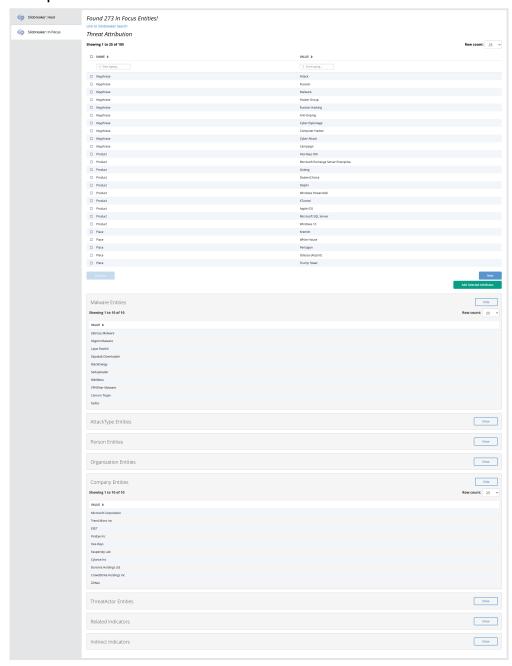
ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
In Focus	Queries Silobreaker for the top 'x' related entities for a given entity such as a Threat Actor or Malware.	Adversaries, Identities, Indicators, Malware, TTPs, Vulnerabilities	Indicators - URL, FQDN, IP Address, CVE, MD5, SHA-1, SHA-256, Username, ASN
Heat	Queries Silobreaker for the most recent documents pertaining to an entity and its' related entities.	Adversaries, Identities, Indicators, Malware, TTPs, Vulnerabilities	Indicators - URL, FQDN, IP Address, CVE, MD5, SHA-1, SHA-256, Username, ASN



In Focus

The In Focus action queries Silobreaker for the top 'x' related entities for a given entity such as a Threat Actor or Malware.

Example Result





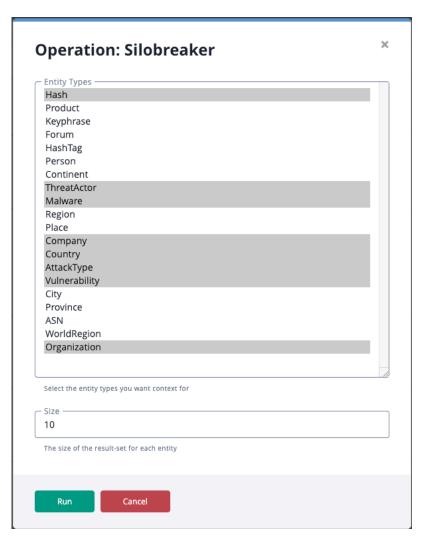
Heat

The In Focus action queries Silobreaker for the top 'x' related entities for a given entity such as a Threat Actor or Malware.

Action Parameters

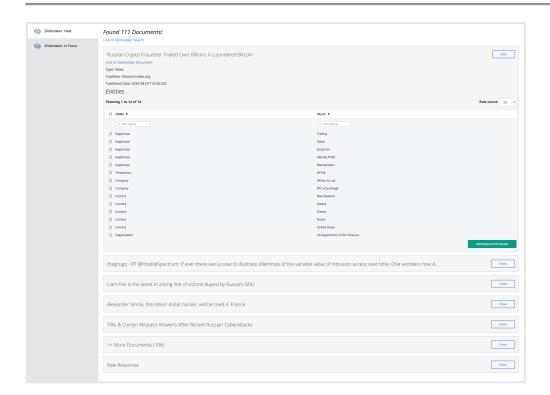
Running the Heat action requires you to enter/confirm the following options:

PARAMETER	DESCRIPTION
Entity Types	Select which entity types you want to query.
Size	Enter how many, of each entity, to return.



Example Result







Change Log

- Version 1.0.0
 - Initial release