ThreatQuotient

CIRCL Action

Version 1.0.0

September 16, 2024

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

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	1.0.0
Compatible with ThreatQ Versions	>= 5.26.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The CIRCL Action allows ThreatQ users to enrich hashes by checking them against CIRCL's hash lookup service, seeing if a hash is part of a known public distribution system. You'll be able to identify if a hash can be trusted or not.

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to gather, review, report and respond to computer security threats and incidents. CIRCL provides free services to to check URLs, documents, and hashes.

The integration provides the following action:

- **CIRCL - Hash Lookup** - checks hashes to see if they are part of a known public distribution system.

The action is compatible and enriches with the following system indicator types:

- MD5
- SHA-1
- SHA-256

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The action requires the following:

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
    - MD5
    - SHA-1
    - SHA-256

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

Configuration

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

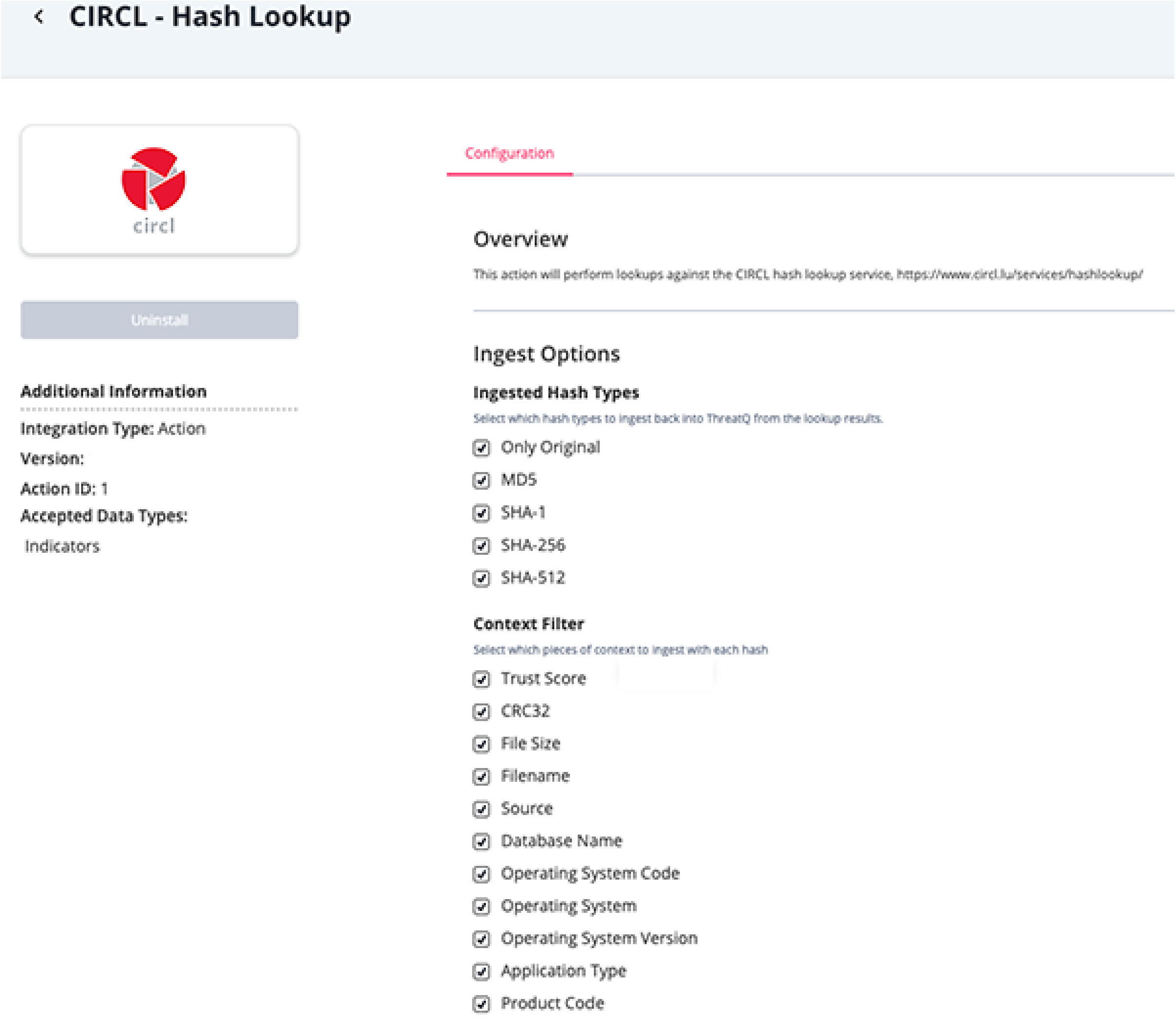
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Ingested Hash Types	Select which hash types to ingest back into ThreatQ from the lookup results. Options include: ◦ Only Original ◦ MD5 (default) ◦ SHA-1 ◦ SHA-256 (default) ◦ SHA-512
Context Filter	Select which pieces of context to ingest with each hash. Options include: ◦ Trust Score (default) ◦ CRC32 ◦ File Size ◦ Filename ◦ Source ◦ Database Name (default) ◦ Operating System Code ◦ Operating System ◦ Application Type (default) ◦ Product Code ◦ Product Name (default) ◦ Product Version ◦ Product Language ◦ Special Code ◦ Source URL ◦ MIME Type

PARAMETER	DESCRIPTION
	◦ Operating System Version
Snap Context Filter	Select which pieces of snap context to ingest with each hash. Options include: ◦ Snap Authority ◦ Snap Trust Score
Normalize Trust Score	Normalize the trust score to a standard value of Less Trusted (0-49), Neutral (50), or Trusted (50+). When enabled, this will ingest a new attribute called Trust Level.
Apply Indicator Status	The status to apply to the indicators created/enriched by this action. Options include: ◦ Review ◦ Active ◦ Whitelisted ◦ Indirect
Whitelist Trusted Hashes	By enabling this, hashes that are trusted (score > 50) will be automatically be ingested with the Whitelisted status. This option is enabled by default.
Verify SSL	Enable this option if the action should verify the SSL certificate.
Disable Proxies	Enable this option to have the action ignore proxies set in the ThreatQ UI.
Objects Per Run	The number of objects to process per run of the workflow. The default value is 1000.



‹ CIRCL - Hash Lookup

Additional Information

Integration Type: Action

Version:

Action ID: 1

Accepted Data Types:

Indicators

Overview

This action will perform lookups against the CIRCL hash lookup service, https://www.circl.lu/services/hashlookup/

Ingest Options

Ingested Hash Types

Select which hash types to ingest back into ThreatQ from the lookup results.

☑ Only Original
☑ MD5
☑ SHA-1
☑ SHA-256
☑ SHA-512

Context Filter

Select which pieces of context to ingest with each hash

☑ Trust Score
☑ CRC32
☑ File Size
☑ Filename
☑ Source
☑ Database Name
☑ Operating System Code
☑ Operating System
☑ Operating System Version
☑ Application Type
☑ Product Code

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
CIRCL - Hash Lookup	Performs lookups against CIRCL's Hash Lookup Service	Indicators	MD5, SHA-1, SHA-256

CIRCL - Hash Lookup

The CIRCL - Hash Lookup action will perform lookups against the CIRCL hash lookup service, https://www.circl.lu/services/hashlookup/ CIRCL will return information such as a trust score, filename, product code, and more. You'll also be able to whitelist hashes based on the trust score to prevent false positives.

`GET https://hashlookup.circl.lu/lookup/{{ type }}/{{ value }}`

Sample Response:

```
{
  "FileName": "snap-hashlookup-import/usr/bin/openssl",
  "FileSize": "723944",
  "MD5": "34D827A288FA51B93297EF2A8A43B769",
  "SHA-1": "72F104BF11A12511154267328F069FE0541E841E",
  "SHA-256":
"301C9EC7A9AADEE4D745E8FD4FA659DAFBBCC6B75B9FF491D14CBBDD840814E9",
  "SHA-512":
"2533D682DB224F0D3BEA043A8A986DC1D341FBEFFD158CB97CD360190BE091F43CC6DBF07E6E98
5CC0DCE17ADC207A61AC9831BE91099202093ACFED584602D1",
  "SSDEEP": "12288:g7LKf6QceJ83r69SOPdxouwUnSysbLY+YR2L7b+3l7E71rb/
t:gsceJ83rESOlxJwUZsbLY+YR2Xa3l7E7",
  "TLSH":
"T150F4281AE64719BDC8B2C230455B50327A31B945F332BF6B26C196311E42B1EA73FBE5",
  "insert-timestamp": "1706630082.5099204",
  "mimetype": "application/x-sharedlib",
  "source": "snap:pNRZCT8s1Ykp2251ycre2Q1qbzeLeBH2_325",
  "hashlookup:parent-total": 156,
  "parents": [],
  "hashlookup:trust": 100
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.MD5`	Indicator.Value	MD5	`.insert-timestamp`	N/A	N/A
`.SHA-1`	Indicator.Value	SHA-1	`.insert-timestamp`	N/A	N/A
`.SHA-256`	Indicator.Value	SHA-256	`.insert-timestamp`	N/A	N/A
`.SHA-512`	Indicator.Value	SHA-512	`.insert-timestamp`	N/A	N/A
`.CRC32`	Indicator.Attribute	CRC32	`.insert-timestamp`	`050F6055`	Optional
`.FileSize`	Indicator.Attribute	File Size	`.insert-timestamp`	`723944`	Optional
`.FileName`	Indicator.Attribute	Filename	`.insert-timestamp`	`snap-hashlookup-import/usr/bin/openssl`	Optional
`.Source`	Indicator.Attribute	Source	`.insert-timestamp`	`snap:pNRZCT8s1Ykp2251ycre2Q1qbzeLeBH2_325`	Optional
`.db`	Indicator.Attribute	Database Name	`.insert-timestamp`	`nsrl_modern_rds`	Optional
`.OpSystemCode.OpSystemCode`	Indicator.Attribute	Operating System Code	`.insert-timestamp`	`362`	Optional
`.OpSystemCode.OpSystemName`	Indicator.Attribute	Operating System	`.insert-timestamp`	N/A	Optional
`.OpSystemCode.OpSystemVersion`	Indicator.Attribute	Operating System Version	`.insert-timestamp`	N/A	Optional
`.ProductCode.ApplicationType`	Indicator.Attribute	Application Type	`.insert-timestamp`	N/A	Optional
`.ProductCode.ProductCode`	Indicator.Attribute	Product Code	`.insert-timestamp`	`217853`	Optional
`.ProductCode.ProductName`	Indicator.Attribute	Product Name	`.insert-timestamp`	N/A	Optional
`.ProductCode.ProductVersion`	Indicator.Attribute	Product Version	`.insert-timestamp`	N/A	Optional
`.ProductCode.Language`	Indicator.Attribute	Product Language	`.insert-timestamp`	N/A	Optional

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.SpecialCode.SpecialCode`	Indicator.Attribute	Special Code	`.insert-timestamp`	N/A	Optional
`.source-url`	Indicator.Attribute	Source URL	`.insert-timestamp`	N/A	Optional
`.mimetype`	Indicator.Attribute	MIME Type	`.insert-timestamp`	`application/x-sharedlib`	Optional
`.hashlookup:trust`	Indicator.Attribute	Trust Score	`.insert-timestamp`	`100`	Optional
N/A	Indicator.Attribute	Trust Level	`.insert-timestamp`	`Trusted`	Normalized from the trust score
`.snap-authority`	Indicator.Attribute	Snap Authority	`.insert-timestamp`	`canonical`	Optional
`.snap-name`	Indicator.Attribute	Snap Package Name	`.insert-timestamp`	`bytecode-viewer`	Optional

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	24 minutes
Indicators	500
Indicator Attributes	2,500

Use Case Example

I have a list of hashes coming in from my feeds and have the Review status. I want these indicators to go through an enrichment process where we want to find out if a hash is a known good hash or a malicious one, before sending it downstream to be blocked or monitored. Using this action, I can figure out if a hash is known good, to prevent it from accidentally being blocked.

Change Log

- **Version 1.0.0**
    - Initial release