ThreatQuotient

RST IoC Lookup Action User Guide

Version 1.0.0

December 10, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Developer Supported

Support
Email: support@rstcloud.net
Web: N/A
Phone: N/A

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.

Copyright © 2024 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 **Developer Supported**.

Support Email: support@rstcloud.net
Support Web: N/A
Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration's download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/ apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their 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 for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient's determination, fulfilling reasonable obligations for support and maintenance.

> EX Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	Developer Supported

Introduction

The RST IoC Lookup Action enriches indicators from different collections using workflows with data from RST Cloud. This data includes risk scores, related threat categories, threat names, CVEs, related industries, TTPs, and other useful information.

The integration provides the following action:

- **RST IoC Lookup** - enriches indicators with data from RST Cloud.

The action is compatible with the following indicator types:

- FQDN
- IP Address
- URL
- MD5
- SHA-1
- SHA-256

The action returns the following enriched system objects:

- Adversaries
- Campaigns
- Indicators
  - FQDN
  - IP Address
  - URL
  - MD5
  - SHA-1
  - SHA-256
- TTP
- Vulnerabilities

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

Prerequisites

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

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.

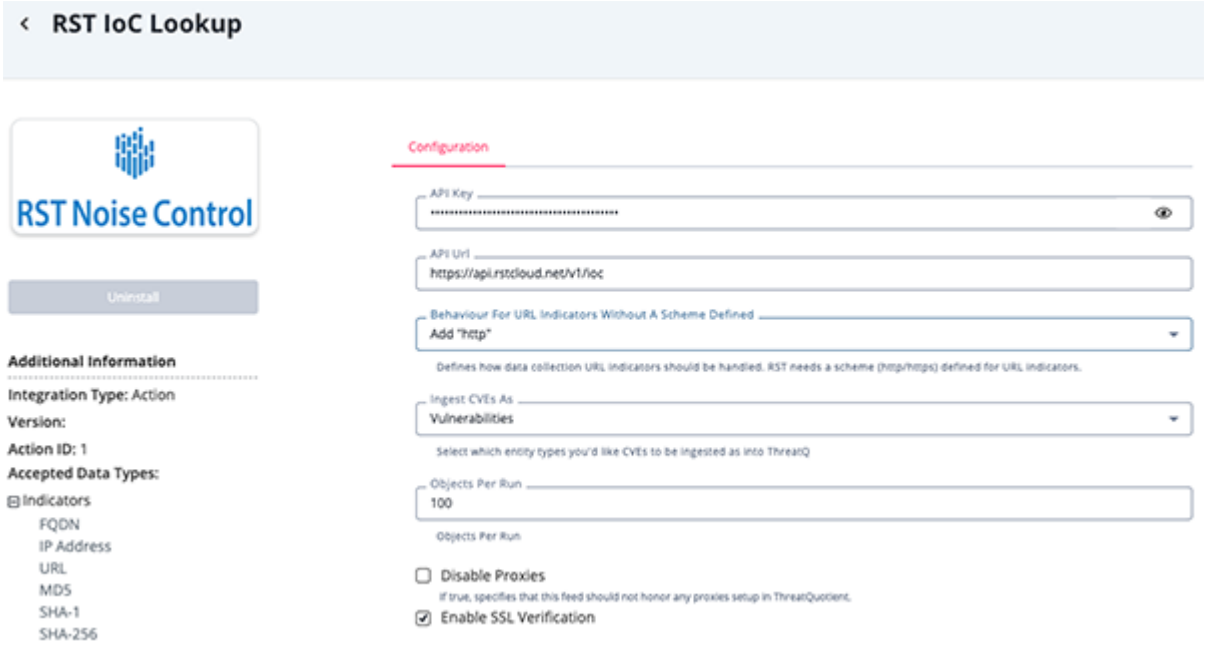
To configure the integration:

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
API Key	Enter your RST API Key.
API Url	Enter the RST API url for indicator lookup.
Behavior for URL Indicators without a Scheme Defined	Defines how data collection URL indicators without a scheme should be handled. Options include: ◦ Skip Indicators ◦ Add "http" ◦ Add "https" ⚠ RST needs a scheme (http/https) defined for URL indicators.
Ingest CVEs As	Select the entity type you'd like CVEs ingested in ThreatQ. Options include **Vulnerabilities** and **Indicators**.
Objects per run	Enter the maximum number of objects to submit per run.

PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.



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
RST IoC Lookup	Enriches indicators with data from RST Cloud	Indicator	FQDN, IP Address, URL, MD5, SHA-1, SHA-256

RST IoC Lookup

The RST IoC Lookup action enriches indicators from different collections using workflows with data from RST Cloud. This data includes risk scores, related threat categories, threat names, CVEs, related industries, TTPs, and other useful information.

`GET {api_url}?value={ioc}`

Sample Response:


```
{
  "src": {
    "name": [
      "urlhouse"
    ],
    "report": "https://urlhaus.abuse.ch/downloads/csv_online/"
  },
  "ioc_value": "https://147.45.44.104/prog/66d70e8640404_trics.exe",
  "parsed": {
    "schema": "https",
    "path": "/prog/66d70e8640404_trics.exe",
    "params": null,
    "port": "443",
    "domain": "147.45.44.104",
    "anchor": null
  },
  "industry": [],
  "fseen": "1727913600",
  "ioc_type": "url",
  "score": {
    "total": "61",
    "src": "68.79",
    "tags": "0.89",
    "frequency": "1",
    "last": "61"
  },
  "fp": {
    "alarm": "false",
    "descr": ""
  },
  "ttp": [],
  "cve": [],
  "collect": "1727913600",
  "resolved": {
    "status": "200"
  },
  "lseen": "1727913600",
  "description": "IOC with tags: malware",
  "threat": [],
  "id": "28bcb177-b57f-3a0b-82e3-3541f1b38edf",
```

```
  "tags": {
    "str": [
      "malware"
    ],
    "codes": [
      "10"
    ]
  },
  "title": "RST Threat feed. IOC: https://147.45.44.104/prog/
66d70e8640404_trics.exe"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.score.total	Indicator.Attribute	RST Score	N/A	61	Updatable
.ports[]	Indicator.Attribute	Ports	N/A	N/A	N/A
.resolved.ip.a	Related Indicator	IP Address	N/A	N/A	For FQDN indicators
.resolved.ip.alias	Related Indicator.Attribute	Related DNS Alias Records	N/A	N/A	For FQDN indicators
.resolved.ip.cname	Related Indicator.Attribute	Related DNS CNAME Records	N/A	N/A	For FQDN indicators
.resolved.whois.age	Indicator.Attribute	Whois Age when last seen	N/A	N/A	For FQDN indicators
.resolved.whois.registrant	Indicator.Attribute	Whois Registrant when last seen	N/A	N/A	For FQDN indicators
.resolved.whois.registrar	Indicator.Attribute	Whois Registrar when last seen	N/A	N/A	For FQDN indicators
.resolved.whois.expires	Indicator.Attribute	Whois Expires On when last seen	N/A	N/A	For FQDN indicators
.resolved.whois.updated	Indicator.Attribute	Whois Updated On when last seen	N/A	N/A	For FQDN indicators
.resolved.whois.created	Indicator.Attribute	Whois Created On when last seen	N/A	N/A	For FQDN indicators
.resolved.whois.havedata	Indicator.Attribute	Whois Data Available when last seen	N/A	N/A	For FQDN indicators
.resolved.status	Indicator.Attribute	HTTP Status when last seen	N/A	200	For URL indicators
.tags.str	Indicator.Attribute	Threat Categories	N/A	malware	N/A
.threat[]	Related Adversary/ Campaign	Adversary/Campaign	N/A	N/A	If `.threat` value ends in `_campaign`Campaign will be ingested, Adversary otherwise.
.cve[]	Related Vulnerability/ Indicator	CVE	N/A	N/A	User Configurable
.ttp[]	Related TTP	TTP	N/A	N/A	N/A
.src.report	Indicator.Attribute	External References	N/A	https://urlhaus.abuse.ch/downloads/csv_online/	N/A
.fseen	Indicator.Attribute	First Seen	N/A	1727913600	Timestamp value; Updatable
.lseen	Indicator.Attribute	Last Seen	N/A	1727913600	Timestamp value; Updatable
.fp.alarm	Indicator.Attribute	Is it a False Positive?	N/A	false	Updatable
.fp.descr	Indicator.Attribute	Reason for a False Positive	N/A	N/A	N/A
.filename	Indicator.Attribute	Related File Names	N/A	N/A	For "MD5","SHA-1","SHA-256" indicators

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	1 minute
Adversaries	2
Campaigns	1
Indicators	2
Indicator Attributes	23
TTPs	1
Vulnerabilities	2

Change Log

- **Version 1.0.0**
  - Initial release