ThreatQuotient

Recorded Future Action Guide

Version 1.0.0

May 22, 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

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	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Recorded Future Action submits any supported object types from a Data Collection to the Recorded Future API. Recorded Future returns a risk score and associated rule for each Indicator of Compromise, if found.

The integration provides the following action:

- **Recorded Future** - retrieves the risk score of an IP address, domain or URL, hash, vulnerability as well as the rules and values of the provided IP address, domain, URL, hash, vulnerability which tells how critical the object is.

The action is compatible with the following indicator types:

- MD5
- SHA-1
- SHA-256
- SHA-512
- IP Address
- Domain
- CVE
- URL

The action returns the following enriched data:

- Indicators
  - Indicator Attributes
  - Indicator Tags

> 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.
- Recorded Future API key.
- A data collection containing at least one of the following indicator types:
    - IP Address
    - Domains
    - URLs
    - Hashes

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

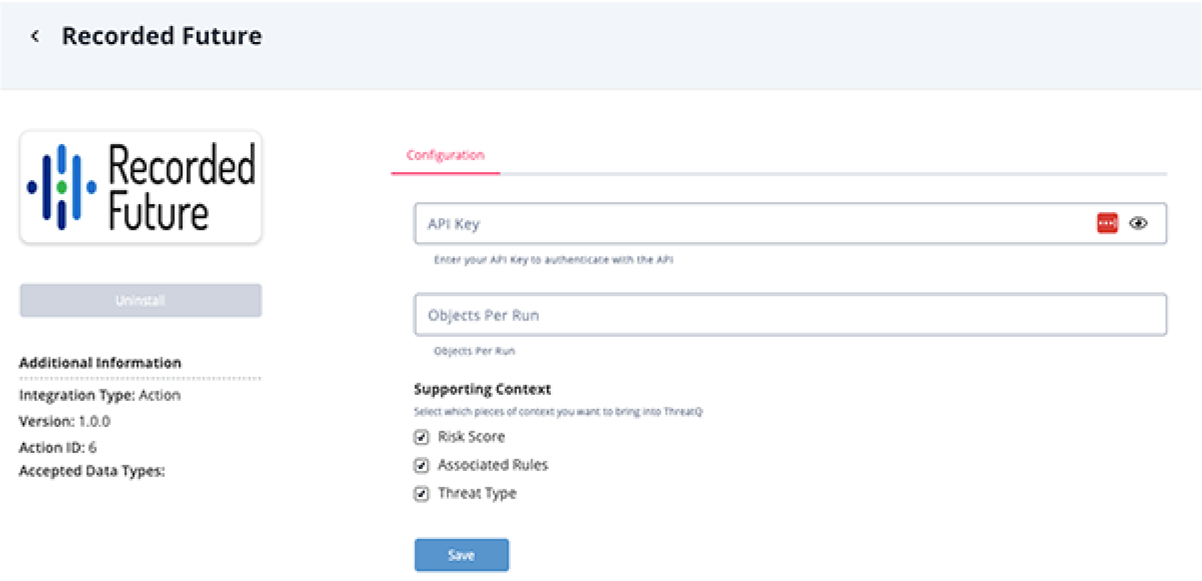
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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	Your Recorded Future API Key.
Objects Per Run	The number of object to return with each run.
Supporting Context	Select the context for the action to return. Options include: ◦ Risk Score ◦ Associated Rules ◦ Threat Type



Additional Information

Integration Type: Action

Version: 1.0.0

Action ID: 6

Accepted Data Types:

API Key

Enter your API Key to authenticate with the API

Objects Per Run

Objects Per Run

Supporting Context

Select which pieces of context you want to bring into ThreatQ

☑ Risk Score

☑ Associated Rules

☑ Threat Type

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

Actions Functions

The following action is available with the integration:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Recorded Future	Submits the data to the SOAR Enrichment API and gets the IOC related data	Indicator	MD5, SHA-1, SHA-256, SHA-512, IP, Domain, URL, CVE

Recorded Future

The Recorded Future action collects the user data fields and submits it to the Recorded Future API via POST call. The API analyzes the IP Address or url or domain which we have passed as run_params, sends the risk score, rule associated to it and even the threat type of the object.

`POST https://api.recordedfuture.com:443/v2/soar/enrichment`

Sample Response:

```
[
    {
        "Recorded_Future_action": {
            "results": [
                {
                    "entity": {
                        "id": "ip:5.39.93.43",
                        "name": "5.39.93.43",
                        "type": "IpAddress"
                    },
                    "risk": {
                        "context": {
                            "c2": {
                                "rule": {
                                    "count": 0,
                                    "maxCount": 2
                                },
                                "score": 0.0
                            },
                            "phishing": {
                                "rule": {
                                    "count": 0,
                                    "maxCount": 3
                                },
                                "score": 0.0
                            },
                            "public": {
                                "mostCriticalRule": "Historical Positive Malware Verdict",
                                "rule": {
                                    "maxCount": 63
                                },
                                "score": 24.0,
                                "summary": [
                                    {
                                        "count": 6.0,
                                        "level": 1.0
                                    }
                                ]
                            }
                        },
                        "level": 1.0,
                        "rule": {
                            "count": 6,
                            "evidence": {
                                "analystNote": {
                                    "count": 1,
                                    "description": "1 sighting on 1 source: <e id=VKz42X>Insikt Group</e>. 1 report:
Recorded Future-analyzed sample communicates with <e id=ip:5.39.93.43>5[.]39[.]93[.]43</e>, historical <e
id=LPc838>C&C server</e>. Most recent link (Jul 30, 2018): https://app.recordedfuture.com/live/sc/5UVpLbAD91Ga",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historically Reported by Insikt Group",
                                    "sightings": 1,
                                    "timestamp": "2018-07-30T00:00:00.000Z"
                                },
                                "cncServer": {
                                    "count": 2,
                                    "description": "3 sightings on 2 sources: <e id=RqhhKn>BroadAnalysis</e>, <e
id=VKz42X>Insikt Group</e>.",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historical C&C Server",
                                    "sightings": 3,
                                    "timestamp": "2022-09-08T07:45:46.296Z"
                                },
                                "historicalThreatListMembership": {
                                    "count": 1,
                                    "description": "Previous sightings on 1 source: <e id=report:Tluf00>Recorded
Future Analyst Community Trending Indicators</e>. Observed between Aug 13, 2018, and Aug 21, 2018.",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historically Reported in Threat List",
                                    "sightings": -1,
                                    "timestamp": "2022-09-08T07:45:46.296Z"
                                },
                                "linkedIntrusion": {
                                    "count": 2,
                                    "description": "3 sightings on 2 sources: <e id=LErKlJ>Malware-Traffic-
Analysis.net - Blog Entries</e>, <e id=TbciDE>ReversingLabs</e>. 5 related intrusion methods: <e id=JVTS__>Exploit
Kit</e>, <e id=QhiNin>CryptMix</e>, <e id=LFGSHZ>RIG Exploit Kit</e>, <e id=J0Nl-p>Ransomware</e>, <e
id=ctmpMt>Trojan.Hydracrypt</e>. Most recent link (Oct 19, 2016): https://a1000.reversinglabs.com/accounts/login/?
next=/%3Fq%3D573c68bd0951e81e24d4fc5ca8fb9756866e53aefa8ea085a0d5aa31f28dbf08",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historically Linked to Intrusion Method",
                                    "sightings": 3,
                                    "timestamp": "2016-10-19T12:26:00.000Z"
                                },
                                "positiveMalwareVerdict": {
                                    "count": 2,
                                    "description": "3 sightings on 2 sources: <e id=LErKlJ>Malware-Traffic-
Analysis.net - Blog Entries</e>, <e id=TbciDE>ReversingLabs</e>. Most recent link (Oct 17, 2016): http://malware-
traffic-analysis.net/2016/10/17/index.html",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historical Positive Malware Verdict",
                                    "sightings": 3,
                                    "timestamp": "2016-10-19T00:00:00.000Z"
                                },
                                "threatResearcher": {
                                    "count": 1,
                                    "description": "2 sightings on 1 source: <e id=RqhhKn>BroadAnalysis</e>. Most
recent link (Oct 17, 2016): http://www.broadanalysis.com/2016/10/17/rig-exploit-kit-via-eitest-delivers-crypt2-
ransomware-c2-5-39-93-43/",
                                    "level": 1,
                                    "mitigation": "",
                                    "rule": "Historical Threat Researcher",
                                    "sightings": 2,
                                    "timestamp": "2016-10-17T18:27:32.000Z"
                                }
                            },
                            "maxCount": 64,
                            "mostCritical": "Historical Positive Malware Verdict",
                            "summary": [
                                {
                                    "count": 6.0,
                                    "level": 1.0
                                }
                            ]
                        },
                        "score": 24
                    }
                }
            ]
        }
    }
]
```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.tags`	Indicator.Tag	Tag	N/A	`Emotet`	
`.attributes`	Indicator.Attribute	Attribute	N/A	`Emotet`	
`.md5_hash`	Indicator.Value	MD5	N/A	N/A	
`.sha1_hash`	Indicator.Value	SHA-1	N/A	N/A	
`.sha256_hash`	Indicator.Value	SHA-256	N/A	N/A	
`.sha512_hash`	Indicator.Value	SHA-512	N/A	N/A	
`.c2`	Indicator.Value	IP ADDRESS	N/A	`5.39.93.43`	
`.c2`	Indicator.Value	URL	N/A	`https://www.gmail.com/malware.php`	
`.c2`	Indicator.Value	Domain	N/A	`google.com`	

Use Case Example

1. A user submits IP Address `5.39.93.43` data using the Recorded Future action to the Recorded Future Enrichment SOAR API.
2. The Recorded Future API queries to submitted data for IP Address type data.
3. The action returns a list of dictionary type data from the provider which contains details like Risk score, Associated Rule, Threat Type etc.

Known Issues / Limitations

- This enrichment action utilizes Recorded Future's "SOAR Enrichment" API, which only returns a subset of everything Recorded Future knows about a given IOC.

Change Log

- **Version 1.0.0**
    - Initial release