ThreatQuotient

Check Point Reputation Operation Guide

Version 1.0.0 rev-a

February 14, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.34.0`

Introduction

The Check Point Reputation Operation enriches ThreatQ indicators with context obtained from the Check Point Reputation API.

The operation enriches ThreatQ objects through the following actions:

- IP Reputation
- URL Reputation
- Hash Reputation

See the Actions chapter for further information on these actions.

The operation is compatible with ThreatQ indicators.

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 feed 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.
6. 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).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Client Key	Your Check Point Reputation Client Key.
Automatically Add Indicators	If checked, related indicators together with their attributes are added automatically. If not checked, the user can select which indicators to be added (without their attributes). This option only applies to the `URL Reputation` action.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

ACTION	DESCRIPTION	OBJECT TYPES
IP Reputation	Enriches ThreatQ objects	IP Address Indicators
URL Reputation	Enriches ThreatQ objects	URL and FQDN Indicators
Hash Reputation	Enriches ThreatQ objects	SHA-1, MD5, and SHA-256 Indicators

IP Reputation

The IP Reputation action enriches ThreatQ objects using the returned JSON response.

`POST https://rep.checkpoint.com/ip-rep/service/v2.0/query?resource={ip-address}`

Sample Response:


```
{
   "response":[
      {
         "status":{
            "code":2001,
            "label":"SUCCESS",
            "message":"Succeeded to generate reputation"
         },
         "resource":"109.127.8.242",
         "reputation":{
            "classification":"Unclassified",
            "severity":"N/A",
            "confidence":"N/A"
         },
         "risk":34,
         "context":{
            "location":{
               "countryCode":"AZ",
               "countryName":"Azerbaijan",
               "region":null,
               "city":null,
               "postalCode":null,
               "latitude":40.5,
               "longitude":47.5,
               "dma_code":0,
               "area_code":0,
               "metro_code":0
            },
            "asn":50274,
            "as_owner":"Alfanet LLC"
         }
      }
   ]
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH .RESPONSE[0]	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.risk	Indicator.Attribute	Risk	34	N/A
.reputation.classification	Indicator.Attribute	Classification	Unclassified	N/A
.reputation.severity	Indicator.Attribute	Severity	N/A	N/A
.reputation.confidence	Indicator.Attribute	Confidence	N/A	N/A
.context.asn	Indicator.Attribute	ASN	50274	N/A
.context.as_owner	Indicator.Attribute	AS Owner	Alfanet LLC	N/A
.context.location.countryCode	Indicator.Attribute	Country Code	AZ	N/A
.context.location.countryName	Indicator.Attribute	Country Name	Azerbaijan	N/A
.context.location.region	Indicator.Attribute	Region	N/A	N/A
.context.location.city	Indicator.Attribute	City	N/A	N/A
.context.location.postalCode	Indicator.Attribute	Postal Code	6600	N/A
.context.location.dma_code	Indicator.Attribute	DMA Code	N/A	N/A
.context.location.area_code	Indicator.Attribute	Area Code	N/A	N/A
.context.location.metro_code	Indicator.Attribute	Metro Code	N/A	N/A

URL Reputation

The URL Reputation action enriches ThreatQ objects using the returned JSON response.

`POST https://rep.checkpoint.com/url-rep/service/v2.0/query?resource={url/fqdn}`

Sample Response:


```
{
   "response":[
      {
         "status":{
            "code":2001,
            "label":"SUCCESS",
            "message":"Succeeded to generate reputation"
         },
         "resource":"adsports.in",
         "reputation":{
            "classification":"Infecting Website",
            "severity":"High",
            "confidence":"Medium"
         },
         "risk":88,
         "context":{
            "categories":[
               {
                  "id":51,
                  "name":"Business / Economy"
               }
            ],
            "indications":[
               "Known malicious domain"
            ],
            "vt_positives":7,
            "registrant":"vikram.kakkar@live.in",
            "creation_date":"2011:04:27 00:00:00",
            "related_ips":[
               {
                  "ip":"34.102.136.180",
                  "classification":"Benign",
                  "confidence":"Low"
               }
            ]
         }
      }
   ]
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH .RESPONSE[0]	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.risk	Indicator.Attribute	Risk	88	N/A
.reputation.classification	Indicator.Attribute	Classification	Infecting Website	N/A
.reputation.severity	Indicator.Attribute	Severity	High	N/A
.reputation.confidence	Indicator.Attribute	Condidence	High	N/A
.context.categories[].name	Indicator.Attribute	Category	Business / Economy	N/A
.context.indications[]	Indicator.Attribute	Indication	Known malicious domain	N/A
.context.vt_positives	Indicator.Attribute	VT Positives	7	N/A
.context.registrant	Indicator.Attribute	Registrant	vikram.kakkar@live.in	N/A
.context.creation_date	Indicator.Attribute	Creation Date	2011:04:27 00:00:00	N/A
.context.related_ips[].ip	Related Indicator.Value	IP Address	34.102.136.180	Status Active
.context.related_ips[].classification	Related Indicator.Attribute	Classification	Benign	N/A
.context.related_ips[].confidence	Related Indicator.Attribute	Confidence	Low	N/A

Hash Reputation

The Hash Reputation action enriches ThreatQ objects using the returned JSON response.

`POST https://rep.checkpoint.com/file-rep/service/v2.0/query?resource={sha-256/sha-1/md5}`

Sample Response:


```
{
   "response":[
      {
         "status":{
            "code":2001,
            "label":"SUCCESS",
            "message":"Succeeded to generate reputation"
         },
         "resource":"9498FF82A64FF445398C8426ED63EA5B",
         "reputation":{
            "classification":"Malware",
            "severity":"High",
            "confidence":"High"
         },
         "risk":100,
         "context":{
            "malware_family":"Zbot",
            "protection_name":"Trojan-Spy.Win32.Zbot.ufyx.TC.a",
            "malware_types":[
               "Bot",
               "Trojan"
            ],
            "metadata":{
               "company_name":"MySQL, AB",
               "product_name":"ShellExtension",
               "copyright":"Copyright 2003-2013",
               "original_name":"ShellExtension"
            }
         }
      }
   ]
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH .RESPONSE[0]	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.risk	Indicator.Attribute	Risk	100	N/A
.reputation.classification	Indicator.Attribute	Classification	Malware	N/A
.reputation.severity	Indicator.Attribute	Severity	High	N/A
.reputation.confidence	Indicator.Attribute	Confidence	High	N/A
.context.malware_family	Indicator.Attribute	Malware Family	Zbot	N/A
.context.protection_name	Indicator.Attribute	Protection Name	Trojan-Spy.Win32.Zbot.ufyx.TC.a	N/A
.context.malware_types[]	Indicator.Attribute	Malware Type	Trojan	N/A
.context.metadata.company_name	Indicator.Attribute	Company Name	MySQL, AB	N/A
.context.metadata.product_name	Indicator.Attribute	Product Name	ShellExtension	N/A
.context.metadata.original_name	Indicator.Attribute	Original Name	ShellExtension	N/A

Change Log

- **Version 1.0.0 rev-a**
  - Updated vendor name in this user guide.
- **Version 1.0.0**
  - Initial Release