ThreatQuotient

Symantec Threat Intelligence Operation User Guide

Version 1.0.0

November 03, 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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Installation **7**
Configuration **8**
Actions **9**
Insight 10
Protection 11
Related 12
Change Log **14**

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	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

The Symantec Threat Intelligence operation enriches ThreatQ indicators with context obtained from the Symantec Threat Intelligence API.

The operation provides the following actions:

- **Insight**
- **Protection**
- **Related**

The operation is compatible with IP Address, FQDN, and SHA-256 Indicator types.

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:

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:

PARAMETER	DESCRIPTION
Client ID	Your Symantec Threat Intelligence Client Key.
Client Secret	Your Symantec Threat Intelligence Client Secret.
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 (indicators added without their attributes). This parameter only applies only to the `Related` action.

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
Insight	Enriches ThreatQ objects	Indicators	IP Address, FQDN, SHA-256
Protection	Enriches ThreatQ objects	Indicators	IP Address, FQDN, SHA-256
Related	Enriches ThreatQ objects	Indicators	IP Address, FQDN, SHA-256

Insight

The Insight action enriches ThreatQ objects using the returned JSON response.

`GET http://brcm-cnb-star-sia.apigee.net/v1/threat-intel/insight/file/{sha-256}`

`GET http://brcm-cnb-star-sia.apigee.net/v1/threat-intel/insight/network/{ip-address/fqdn}`

Sample Response:

```
{
    "file": "eec3f761f7eabe9ed569f39e896be24c9bbb8861b15dbde1b3d539505cd9dd8d",
    "reputation": "BAD",
    "prevalence": "Hundreds",
    "firstSeen": "2020-08-27",
    "lastSeen": "2020-08-27",
    "targetOrgs": {
        "topCountries": [
            "tr",
            "de",
            "us",
            "qa",
            "ie"
        ],
        "topIndustries": [
            "wholesale",
            "manufacturing",
            "financial services",
            "retail"
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.reputation	Indicator.Attribute	Reputation	BAD	N/A
.prevalence	Indicator.Attribute	Prevalence	Hundreds	N/A
.firstSeen	Indicator.Attribute	First Seen	2020-08-27	N/A
.targetOrgs.topCountries[]	Indicator.Attribute	Country	tr	N/A
.targetOrgs.topIndustries[]	Indicator.Attribute	Industry	wholesale	N/A

Protection

The Protection action enriches ThreatQ objects using the returned JSON response.

`GET http://brcm-cnb-star-sia.apigee.net/v1/threat-intel/protection/file/{sha-256}`

`GET http://brcm-cnb-star-sia.apigee.net/v1/threat-intel/protection/network/{ip-address/fqdn}`

Sample Response:

```
{
    "network": "google.com",
    "state": [
        {
            "technology": "AntiVirus",
            "firstDefsetVersion": "2020.07.31.004",
            "threatName": "heur.advml.b"
        },
        {
            "technology": "Intrusion Prevention System",
            "firstDefsetVersion": "20150403.001",
            "threatName": "System Infected: W32.SillyFDC Activity 3"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.state[].threatName + .state[].firstDefsetVersion	Indicator.Attribute	.state[].technology (eg. AntiVirus)	heur.advml.b - 2020.07.31.004	N/A

Related

Enriches ThreatQ objects using the returned JSON response.

`GET http://api.sep.securitycloud.symantec.com/v1/threat-intel/related/file/{sha-256}`

`GET http://api.sep.securitycloud.symantec.com/v1/threat-intel/related/network/{ip-address/fqdn}`

Sample Response:

```
{
    "network": "145.249.105.165",
    "related": [
        {
            "iocType": "Network",
            "iocValues": [
                "79.142.70.106",
                "veramebel.kz",
            ],
            "relation": "byThreatActor"
        },
        {
            "iocType": "File",
            "iocValues": [

"370b4a94d511317ad0672f030478f324abd79f2edb4d690eb41dd803a0debd36",

"022d89f8ab9a60b38684b25a1b7f3fe2dd7d8817fad5642305ec9acc004e0eff",
            ],
            "relation": "byThreatActor"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.related.[].iocValues[]	Related Indicator.Value	Parsed by using .related.[].iocType	veramebel.kz	Possible indicator types IP Address, FQDN, and SHA-256
.related.[].relation	Related Indicator.Attribute	Relation	byThreatActor	N/A

Change Log

- **Version 1.0.0**
  - Initial release