ThreatQuotient

Hatching Triage Operation Guide

Version 1.0.0

November 09, 2021

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`

Introduction

The Hatching Triage Operation submits URL Indicators and Files object types to the Hatching Triage API for context enrichment.

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
Hostname	Your Triage instance hostname. Use `https://api.tria.ge/v0/` for public cloud API and `https://private.tria.ge/api/v0/` for private cloud API. You can also use your own if using an on-prem machine.
API Key	Your Triage instance API Key.

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

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPES	OBJECT SUB-TYPE
Submit URL	Submits a URL for analysis.	Indicators (URL)	URL
Submit File	Submits a File for analysis.	Files	N/A
Get Report	Retrieves the report and enriches the threat object.	Indicators, Files	URL (Indicators)

Submit URL & Submit File

The Submit action is used to submit a URL or File to Hatching Triage API for Analysis.

`POST https://<triage-host>/samples`

Sample Response:

```
{
    "submitted": "2021-11-02T12:33:44Z",
    "private": false,
    "status": "pending",
    "kind": "url",
    "id": "211102-prkjxacee7",
    "url": "https://github.com/ytisf/theZoo/raw/master/malware/Binaries/All.ElectroRAT/All.ElectroRAT.zip"
}
```

The **Submit URL Action** has the following configuration option: Submission Type.

OPTION	DESCRIPTION
Submission Type	Indicates how the submission will be handled by the analyzer. Options include: • Submit URL • Submit fetched sample form URL

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.submitted	Indicator.Attribute	Hatching Triage Submission Date	2021-11-02 12:33:44-00:00	Automatically added
.id	Indicator.Attribute	Hatching Triage Submission ID	211102-prkjxacee7	Automatically added

Get Report

The Get Report action is used to retrieve the submission summary for the submitted threat object.

`GET https://<triage-host>/samples/<submission_id>/summary`

Sample Response:

```
{
    "target": "https://github.com/ytisf/theZoo/raw/master/malware/Binaries/All.ElectroRAT/All.ElectroRAT.zip",
    "created": "2021-11-02T12:33:44Z",
    "owner": "shark2.ams5.hatching.dev",
    "completed": "2021-11-02T12:36:18Z",
    "tasks": {
        "211102-prkjxacee7-static1": {
            "kind": "static",
            "status": "reported"
        },
        "211102-prkjxacee7-behavioral1": {
            "target": "https://github.com/ytisf/theZoo/raw/master/malware/Binaries/All.ElectroRAT/
All.ElectroRAT.zip",
            "resource": "win10-en-20211014",
            "queue_id": 139808,
            "kind": "behavioral",
            "status": "reported",
            "score": 1,
            "backend": "horse2",
            "platform": "windows10_x64"
        },
        "211102-prkjxacee7-urlscan1": {
            "target": "https://github.com/ytisf/theZoo/raw/master/malware/Binaries/All.ElectroRAT/
All.ElectroRAT.zip",
            "failure": "400: Scan prevented ...: The submitted domain is on our blacklist, we will not scan it.",
            "kind": "urlscan",
            "status": "failed"
        }
    },
    "custom": "frontend:66ca4d10-0e04-4f87-8c90-022bd1d64937",
    "sample": "211102-prkjxacee7",
    "score": 1,
    "status": "reported",
    "sha256": {}
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.score	Indicator.Attribute	Triage Score	1	n/a
.sha256	Indicator.Value	SHA-256	9db4c2b2fca0039c97522753964...	n/a

Change Log

- **Version 1.0.0**
    - Initial release