ThreatQuotient

VirusTotal Retrohunt Operation Guide

Version 1.0.0

April 25, 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	>= 4.43.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/virustotal-retrohunt-operation

Introduction

The VirusTotal Retrohunt Operation submits YARA signatures to VirusTotal Retrohunt.

The operation provides the following action:

- **Submit Yara** - submits Yara signatures to VirusTotal Retrohunt to run against the goodware job.

The operation is compatible with Signature system objects.

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
API Key	Your private or public VirusTotal Retrohunt API key.
Email Address To Notify	Optional - The email address to receive notifications by email.

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 action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Submit Yara	Submits Yara signatures into VirusTotal Retrohunt	Signatures	YARA

Submit Yara

The Submit Yara action submits the Yara signature to VirusTotal Retrohunt. VirusTotal will then run the Retrohunt job against all files, or "goodware," against a set of known goodware. This is useful to know whether the YARA rules raise lots of false positives.

`POST https://www.virustotal.com/api/v3/intelligence/retrohunt_jobs`

Sample Response:

```
{
    "data": {
        "type": "retrohunt_job",
        "attributes": {
            "rules": "rule CTM_Webshell_b374k_ops {strings:\n$general1 = \"Shell\"\ncondition:\nall of ($general*) )\n}\n\n",
            "notification_email": "test@email.com",
            "corpus": "main"
        }
    }
}
```

Change Log

- **Version 1.0.0**
  - Initial release