ThreatQuotient

Cuckoo Sandbox Operation User Guide

Version 1.0.0

October 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	>= 3.6.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQuotient for Cuckoo Operation allows a ThreatQ user to submit files and FQDNs/URLs to their Cuckoo Sandbox instance. The file will be sandboxed by executing one action, and the report for the sandboxing will be downloaded by executing another action.

The operation provides the following action:

- **Submit** - submits the selected file to your Cuckoo Sandbox instance to be sandboxed.
- **Get Reports** - downloads the sandbox report on the object.

The operation is compatible with Attachments as well as FQDN and URL Indicator types.

This operation supports the following fields/reports:

- JSON Report parsing
- HTML Report download/upload
- General Information
- Target Information
- Network Information
- Signatures (as attributes)
- Dropped Files

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
Host URL	The Host or IP of your Cuckoo Sandbox instance.
Api URL	The Host or IP of your Cuckoo Sandbox API instance.
API Key	Your API token from Cuckoo Sandbox (if Bearer token is enabled).

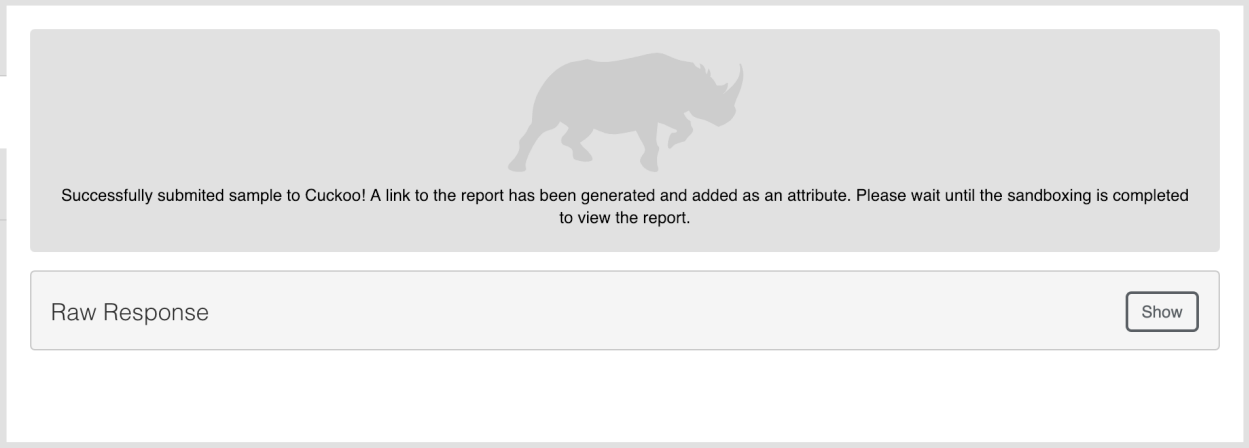
5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Usage

This operation applies to attachments/files, FQDNs, and URLs within ThreatQ. You will not be able to scan any other object type.

1. Find a Malware Sample or FQDN/URL in ThreatQ that you want scanned
2. Navigate to its' `Operations` section
   - You should see a `Cuckoo Sandbox` entry
3. When you run the `Submit` operation, you will get a popup window asking you if you want to re-submit the file. If this is your first run on the current ThreatQ object, ignore it and run it. If you have already ran the `Submit` operation on the ThreatQ object, then you will choose whether you want to resubmit the file, or not. Selecting no will abort the submission.

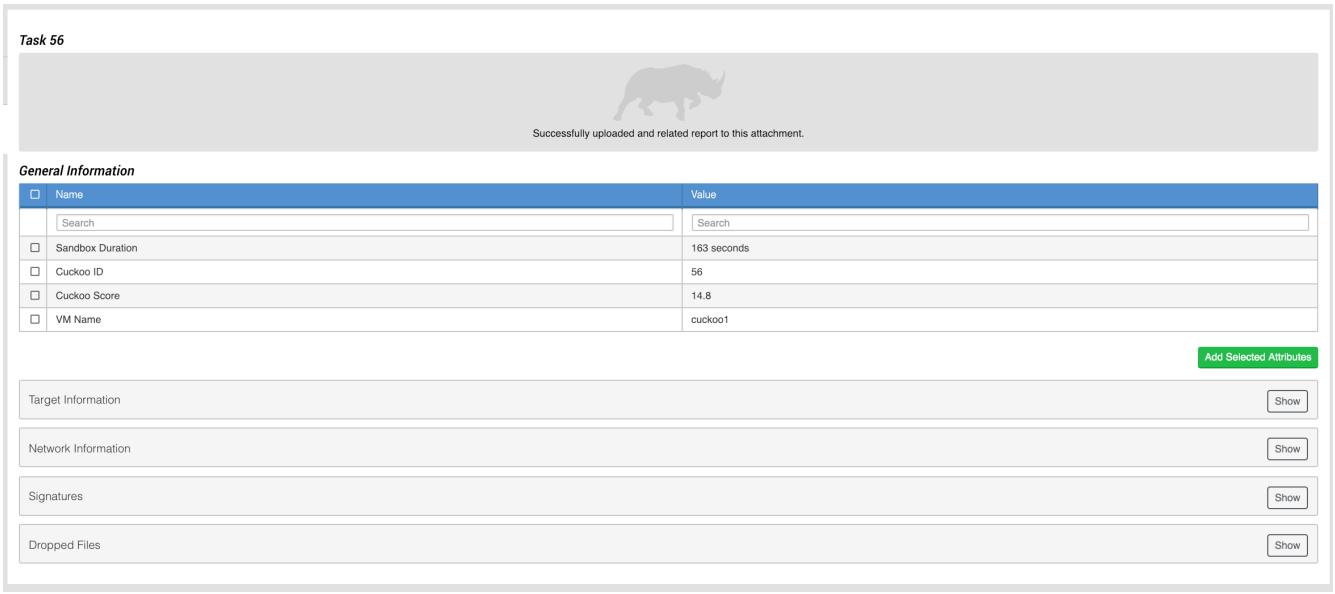
   Once the file is ran, the result should be similar to this:

   You must run the `Submit` operation before running the `Get Reports` operation. However, if you have a report you want in ThreatQ but do not want to rescan it, you can add an attribute to the ThreatQ object to have it fetch the report.

   - **Attribute Name**: Cuckoo Report Link
   - **Attribute Value**: http://<cuckoo-host>/analysis/<scan-id>/summary
4. When you run the `Get Reports` operation, the plugin will look for any `Cuckoo Task Summary Links` in the ThreatQ object's attributes. If it finds one, it will use that link to get the reports associated with it. It will download the report, upload it to ThreatQ, and then relate it to the current ThreatQ object.

Once the operation is ran, this should be the result:



Reports will automatically be downloaded and related to the ThreatQ object. Refresh the page to see the relationship

If you get an error saying there is no HTML report, or you get an empty response back, it probably means the sandboxing is not finished.

Known Issues / Limitations

- By default, the JSON report is enabled. The HTML report will only be downloaded if you have enabled HTML reporting in Cuckoo. This operation does not support the PDF reporting because the formatting in it is not handled as well as it is in the HTML report.
- You must run the `Submit` operation before running the `Get Reports` operation. However, if you have a report you want in ThreatQ but do not want to rescan it, you can add an attribute to the ThreatQ object to have it fetch the report.
  - **Attribute Name**: Cuckoo Report Link
  - **Attribute Value**: http:///analysis//summary
- Reports will automatically be downloaded and related to the ThreatQ object. Refresh the page to see the relationship
- If you get an error saying there is no HTML report, or you get an empty response back, it probably means the sandboxing is not finished.

Change Log

- **Version 1.0.0**
  - Initial release