ThreatQuotient

Hybrid Analysis Operation Guide

Version 1.0.0

Monday, August 10, 2020

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

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Monday, August 10, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.30.0`

Introduction

The Hybrid Analysis Operation for ThreatQuotient enables a ThreatQ user to interact with Hybrid Analysis by fetching reports and submitting samples.

Installation

Perform the following steps to install the operation:

> The same steps can be used to upgrade the operation to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Hybrid Analysis Operation** file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Operations Management**.
5. Click on the **Install Operation** button.
6. Upload the operation file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the operation file on your local machine

> ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding.

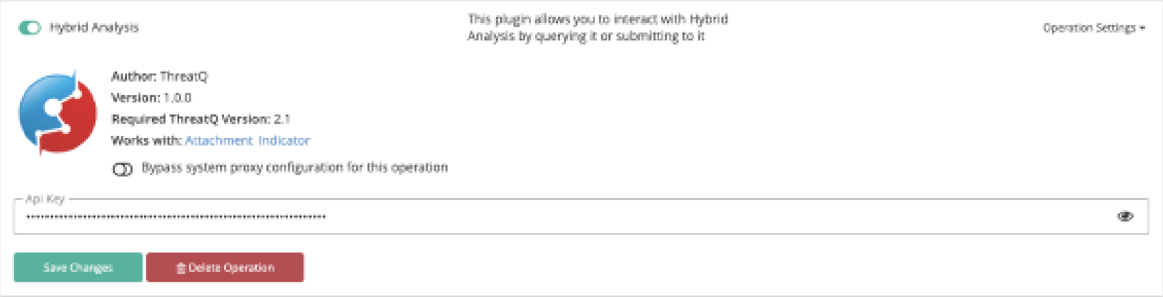
The operation will be added to your list of installed operations. You will still need to configure and then enable the operation.

Configuration

ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.

To Configure the operation:

1. Click on the **Settings** icon and select **Operations Management**
2. Locate the operation and click on **Operation Settings**.



This plugin allows you to interact with Hybrid Analysis by querying it or submitting to it

Author: ThreatQ
Version: 1.0.0
Required ThreatQ Version: 2.1
Works with: Attachment Indicator

○ Bypass system proxy configuration for this operation

Api Key: ••

3. Enter the following parameter for the operation:

Parameter	Details
API Token	Your Hybrid Analysis API Token.

4. Click on **Save Changes** then click on the toggle switch next to the operation name to enable the operation.

Actions

This operation comes with 3 actions:

- Quick Scan
- Sandbox
- Get Reports

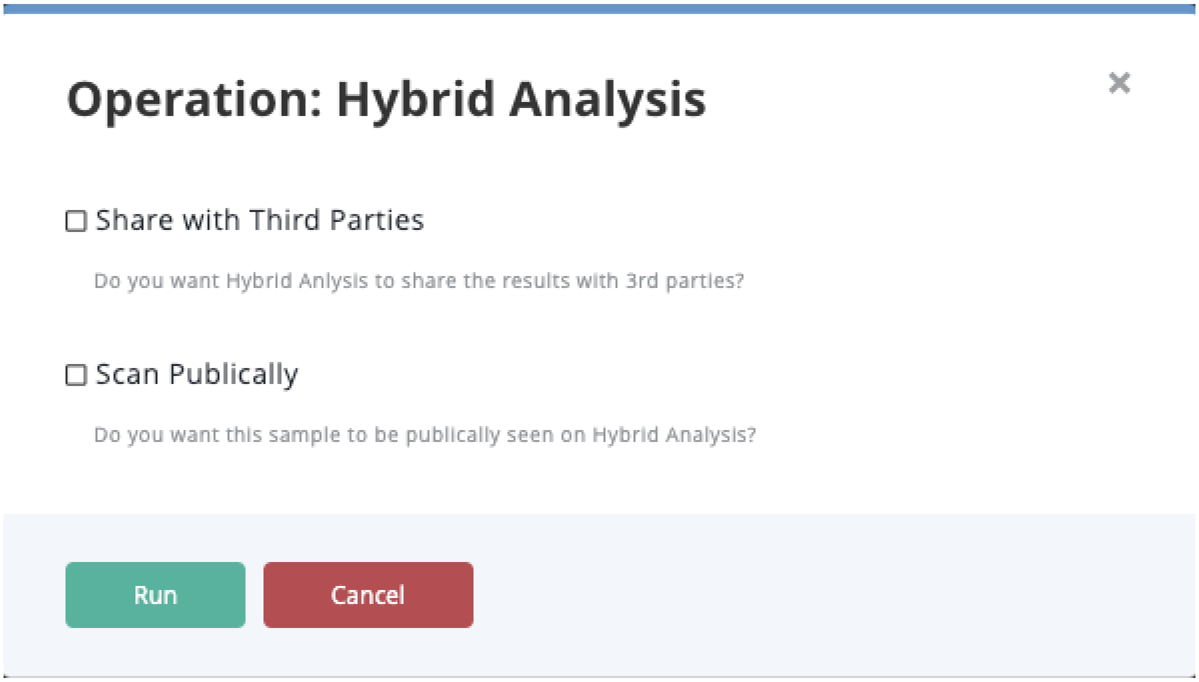
Quick Scan

This action sends an IOC or attachment to be quickly scanned by Hybrid Analysis and its' integrated scan engines

Applies to:

- Indicators (FQDN & URL)
- File / Attachment

Parameters



Operation: Hybrid Analysis

□ Share with Third Parties

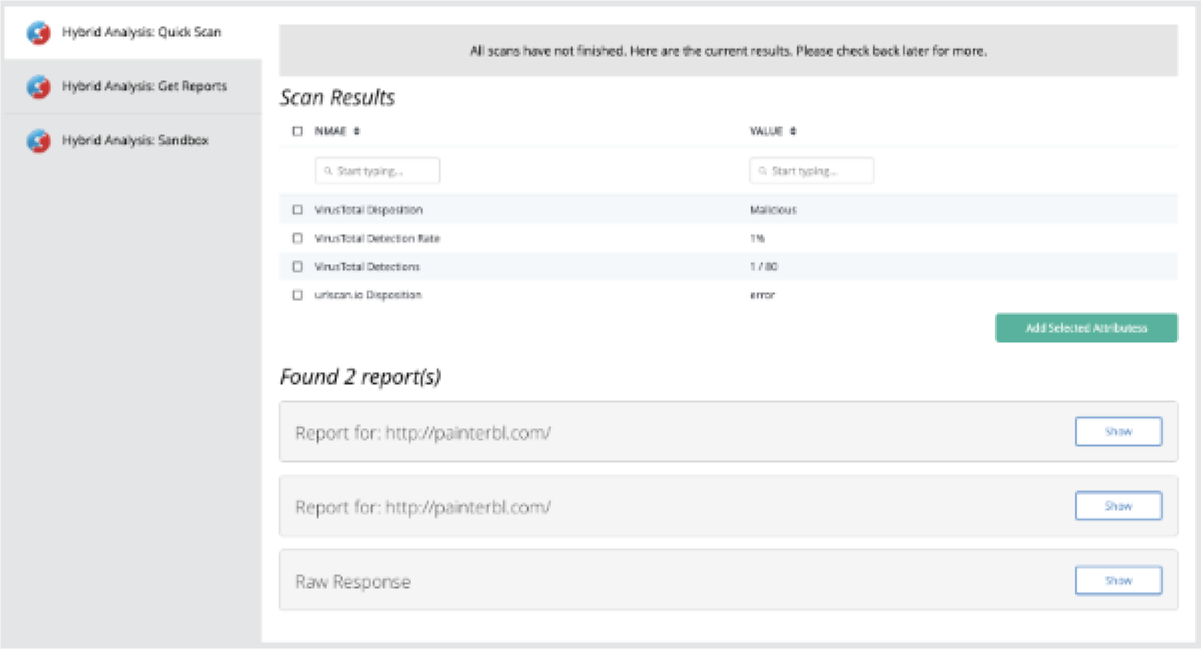
Do you want Hybrid Anlysis to share the results with 3rd parties?

□ Scan Publically

Do you want this sample to be publically seen on Hybrid Analysis?

Parameter	Description
Share with Third Parties	Enabling this will allow the sample to be shared with Hybrid Analysis' partners.
Scan Publically	Enabling this will make all your scanned samples publically viewable.

Example Result



All scans have not finished. Here are the current results. Please check back later for more.

Scan Results

□ NMAE	VALUE
□ VirusTotal Disposition	Malicious
□ VirusTotal Detection Rate	1%
□ VirusTotal Detections	1 / 80
□ urlscan.io Disposition	error

Found 2 report(s)

Report for: http://painterbl.com/

Report for: http://painterbl.com/

Raw Response

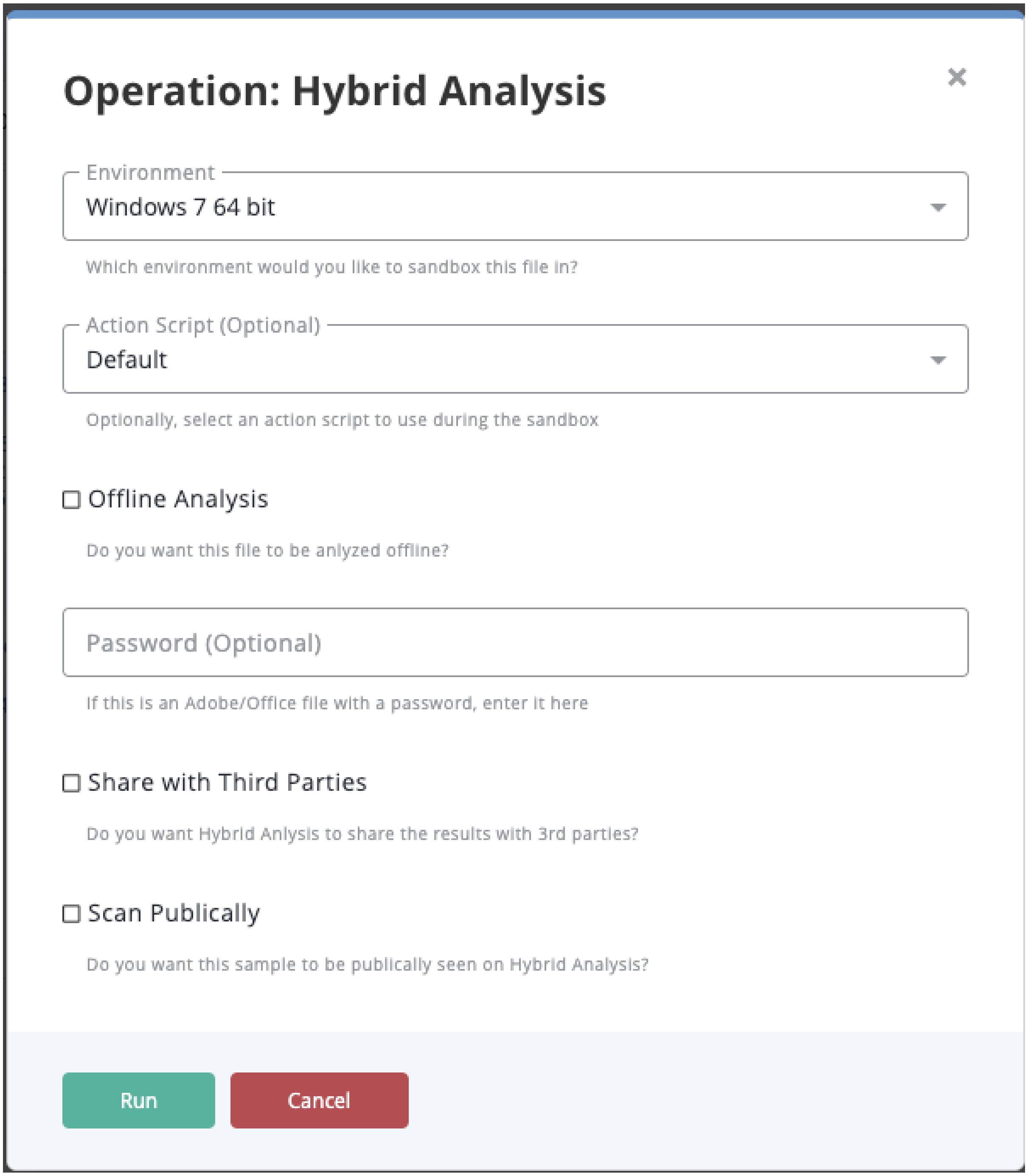
Sandbox

This action sends an IOC or attachment to the Hybrid Analysis Sandbox for a complete detonation

Applies to:

- Indicators (FQDN & URL)
- File / Attachment

Parameters



Operation: Hybrid Analysis

Environment
Windows 7 64 bit

Which environment would you like to sandbox this file in?

Action Script (Optional)
Default

Optionally, select an action script to use during the sandbox

□ Offline Analysis

Do you want this file to be anlyzed offline?

Password (Optional)

If this is an Adobe/Office file with a password, enter it here

□ Share with Third Parties

Do you want Hybrid Anlysis to share the results with 3rd parties?

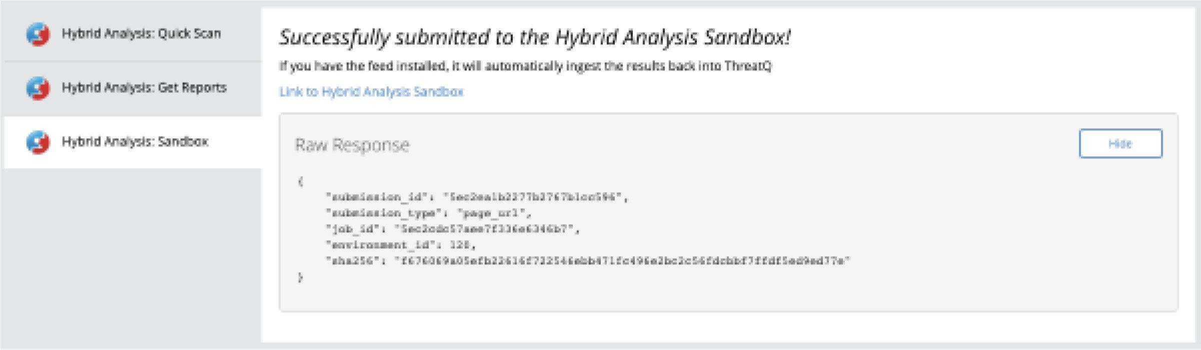
□ Scan Publically

Do you want this sample to be publically seen on Hybrid Analysis?

Parameter	Description
Environment	Select which environment you want your sample detonated in:

Parameter	Description
	• Windows 7 32 bit • Windows 7 32 bit (HWP Support) • Windows 7 64 bit (default) • Android Static Analysis • Linux (Ubuntu 16.04 64 bit)
Action Script (Optional)	Select an action script to use during the detonation: • Default • Max Anti-Evasion • Random Files • Random Theme • Open Internet Explorer
Offline Analysis	Enabling this will detonate the sample without internet access.
Password	If you are submitting an Adobe/Office file with a password, enter it here.
Share with Third Parties	Enabling this will allow the sample to be shared with Hybrid Analysis' partners.
Scan Publically	Enabling this will make all your scanned samples publically viewable.

Example Result



Successfully submitted to the Hybrid Analysis Sandbox!

If you have the feed installed, it will automatically ingest the results back into ThreatQ

Link to Hybrid Analysis Sandbox

Raw Response

```
{
    "submission_id": "5ec2ea1b2277b2767b1cc596",
    "submission_type": "page_url",
    "job_id": "5ec2cdc57aee7f336e6346b7",
    "environment_id": 120,
    "sha256": "f676069a05efb22616f722546ebb471fc496e2bc2c56fdcbbf7ffdf5ed9ed77e"
}
```

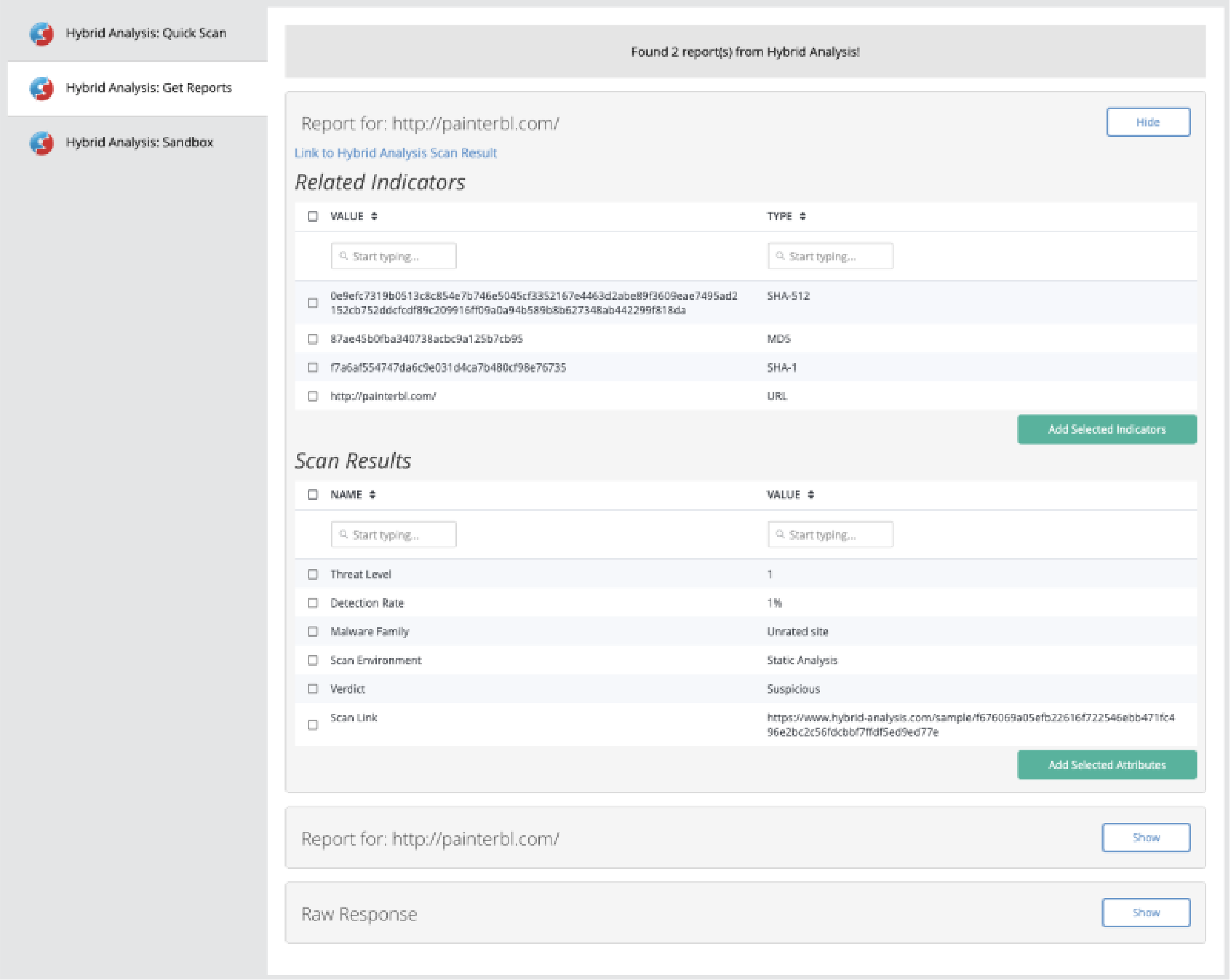
Get Reports

This action sends an IOC or attachment to the Hybrid Analysis Sandbox for a complete detonation

Applies to:

- Indicators (FQDN, URL, Filename, MD5, SHA-1, SHA-256, and IP Address)
- File / Attachment

Example Result



Found 2 report(s) from Hybrid Analysis!

Report for: http://painterbl.com/

Link to Hybrid Analysis Scan Result

Related Indicators

□	VALUE	TYPE
	Start typing...	Start typing...
□	0e9efc7319b0513c8c854e7b746e5045cf3352167e4463d2abe89f3609eae7495ad2 152cb752ddcfcdf89c209916ff09a0a94b589b8b627348ab442299f818da	SHA-512
□	87ae45b0fba340738acbc9a125b7cb95	MD5
□	f7a6af554747da6c9e031d4ca7b480cf98e76735	SHA-1
□	http://painterbl.com/	URL

Scan Results

□	NAME	VALUE
	Start typing...	Start typing...
□	Threat Level	1
□	Detection Rate	1%
□	Malware Family	Unrated site
□	Scan Environment	Static Analysis
□	Verdict	Suspicious
□	Scan Link	https://www.hybrid-analysis.com/sample/f676069a05efb22616f722546ebb471fc4 96e2bc2c56fdcbbf7ffdf5ed9ed77e

Report for: http://painterbl.com/

Raw Response

Change Log

- **Version 1.0.0**
  - Initial Release