ThreatQuotient

ZScaler Sandbox Operation Guide

Version 1.1.0

September 06, 2022

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	1.1.0
Compatible with ThreatQ Versions	>= 4.20.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/zscaler-sandbox-operation

Introduction

The ThreatQuotient for Zscaler Sandbox Operation runs and analyzes files in a virtual environment to detect malicious behaviour. It propagates a hash of malicious files to all Zscaler Enforcement Nodes (ZENs) throughout the cloud, effectively maintaining a real time blacklist so that it can prevent users anywhere in the world from downloading malicious files.

The operation provides the following actions:

- **Sandbox Report** - creates an authenticated session to Zscaler and retrieves the report for the MD5 hash.
- **Export IOC** - creates an authenticated session to Zscaler and exports the current IOC to Zscaler's blacklist.

The operation is compatible with MD5, FQDN, and URL Indicator types.

Prerequisites

Review the following requirements before attempting to install the operation.

Configure ZScaler for Malware File Submission

Perform the following steps to enable submission of files to the sandbox.

Forward Traffic

In order to be able to submit files to the sandbox, the internet traffic of the computer, from which the submission performed, needs to be forwarded to Zscaler. See the steps in the link provided below to setup traffic forwarding for MacOS or Windows.

https://help.zscaler.com/zia/documentation-knowledgebase/traffic-forwarding/zscaler-app

The following items will be needed for logging in to the Zscaler traffic forwarding app:

- **Hostname**: The hostname of the ZScaler sandbox instance.
- **Username**: The ZScaler provided username.
- **Password**: The password associated with the username listed above.
- **API key**: The API access key provided by ZScaler.

Submit Files to ZScaler

After the traffic has been forwarded to ZScaler, log into the app, and go to the following location to manually submit files for detonation: http://filecheck.zscaler.com/

There is no official documented API endpoint for detonating files in the sandbox, but it's posible to use CURL for submission. The following is an example of submitting a malware called Anti_EXE_BOOT.IMA to the sandbox using CURL:

```
curl -F "data=@/PATH/TO/MALWARE/AntiExe.A/Anti_EXE_BOOT.IMA" "http://filecheck.zscaler.com/app/upload?
timestamp_load=1554921279087&timestamp_upload=1554921285485&name=o_2d8462s6sceqndc11d811cuq7s7.IMA" -v
```

There are three parameters in the URL that are needed:

PARAMETER	DESCRIPTION
timestamp_load	Time since epoch in milliseconds (on CentOS use `date +%s%3N`).
timestamp_upload	Time since epoch in milliseconds (should be larger than timestamp_load).
name	A unique file name. It appears that the original filename name is changed to a long string which always starts with "o_" but the extension remains the same as the extension of the file in curl.

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
Hostname	The hostname of the ZScaler Sandbox instance.
Username	Your ZScaler username.
Password	The password associated with the username above.
API Key	The API access key provided by ZScaler.

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
Sandbox Report	Creates an authenticated session to Zscaler and retrieves the report for the MD5 hash.	Indicator	MD5
Export IOC	Creates an authenticated session to Zscaler and exports the current IOC to Zscaler's blacklist.	Indicator	FQDN, URL

Sandbox Report

The Zscaler sandbox service runs and analyzes files in a virtual environment to detect malicious behavior. It propagates a hash of malicious files to all Zscaler Enforcement Nodes (ZENs)throughout the cloud, effectively maintaining a real time blacklist so it can prevent users anywhere in the world from downloading malicious files.

> Currently, the malware files can only be submitted manually via the portal http://filecheck.zscaler.com/. See the Prerequisites chapter for more details.

The ThreatQ operation searches Zscaler for the MD5 of files that have already been scanned by the sandbox and brings back into ThreatQ the results of the malware analysis.

```
GET https://zsapi.zscalerbeta.net/api/v1/sandbox/report/<MD5 value>?details=summary
```

Sample Response:

```
{
    "additionalProp1": {},
    "additionalProp2": {},
    "additionalProp3": {}
}
```

Action Parameters

The Sandbox Report action has the following configuration parameter:

PARAMETER	DESCRIPTION
Sandbox Report Detail	Select if requested report is a summary or has full details.

Export IOC

The Export IOC action formats and exports the selected URL to Zscaler's URL blacklist.

```
POST https://zsapi.zscalerbeta.net/api/v1/security/advanced/blacklistUrls?
action=ADD_TO_LIST
```

Change Log

- **Version 1.1.0**
  - Added new action: **Export IOC**.
- **Version 1.0.0**
  - Initial release