

ThreatQuotient



abuse.ch ThreatFox Action User Guide

Version 1.0.1

July 10, 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 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation..... 8

Configuration 9

Action Functions 11

 abuse_ch ThreatFox..... 11

Enriched Data..... 14

Use Case Example..... 15

Change Log 16

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.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	1.0.1
-----------------------------	-------

Compatible with ThreatQ Versions	>= 5.14.1
-------------------------------------	-----------

ThreatQ TQO License Required	Yes
---------------------------------	-----

Support Tier	ThreatQ Supported
--------------	-------------------

Introduction

The abuse.ch ThreatFox Action submits a collection of indicators to the abuse.ch ThreatFox API in the form of individual HTTP requests. The returning response will provide additional contextual information for every indicator submitted.

The action can perform the following function:

- **abuse.ch ThreatFox** - enriches supported objects with attributes and related objects describing the IOC.

The action is compatible with the following indicator types:

- MD5
- SHA-1
- SHA-256
- FQDN
- IP
- URL
- Email Address

The action returns the following enriched system objects:

- Indicators
- Malware



This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
 - MD5
 - SHA-1
 - SHA-256
 - FQDN
 - IP
 - URL
 - Email Address

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
 - Drag and drop the zip file into the dialog box
 - Select **Click to Browse** to locate the zip file on your local machine



ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to [configure](#) the action.

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:

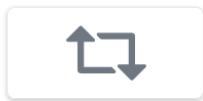
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:



The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Supporting Context	Select the context you want to ingest into ThreatQ. Options include: • Threat Type (default) • Threat Type Description • Related Malware (default) • Related Malware (default) Samples (Hashes) • Malware Aliases (default) • Malware Identifier (i.e. "win.asynchr") • Malware Malpedia Reference (External Reference) • abuse.ch Reference (External Reference) • Confidence Level (default) • First Seen • Last Seen • Reporter • Tags (default)
Objects Per Run	The maximum number of objects to send to this action, per run. The maximum value for this parameter is 50,000.

< abuse_ch ThreatFox



Uninstall

Additional Information

Integration Type: Action

Version: 1.0.0

Action ID: 5

Accepted Data Types:

Configuration

Context Filter

Select which pieces of context you want to bring into ThreatQ

- ☒ Threat Type
- ☐ Threat Type Description
- ☒ Related Malware
- ☒ Related Malware Samples (Hashes)
- ☒ Malware Aliases
- ☐ Malware Identifier (i.e. "win.asyncrat")
- ☐ Malware Malpedia Reference (External Reference)
- ☐ abuse.ch Reference (External Reference)
- ☒ Confidence Level
- ☐ First Seen
- ☐ Last Seen
- ☐ Reporter
- ☒ Tags

Objects Per Run

5000

The max number of objects to send to this action, per run.

Save

5. Review any additional settings, make any changes if needed, and click on **Save**.

Action Functions

The action provides the following function:

FUNCTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
abuse_ch ThreatFox	Queries ThreatFox API for context	Indicators	MD5, SHA-1, SHA-256, FQDN, IP, URL, Email Address

abuse_ch ThreatFox

The abuse_ch ThreatFox function enriches supported indicators by using the ThreatFox API.

POST <https://threatfox-api.abuse.ch/api/v1/>

Sample Body:

```
{
  "query": "search_ioc",
  "search_term": "<ioc_value>"
}
```

Sample Response:

```
{
  "query_status": "ok",
  "data": [
    {
      "id": "1035527",
      "ioc": "https://xoopscube.xyz/vema/index.php?QB0T.zip",
      "threat_type": "payload_delivery",
      "threat_type_desc": "Indicator that identifies a malware distribution server (payload delivery)",
      "ioc_type": "url",
      "ioc_type_desc": "URL that delivers a malware payload",
      "malware": "win.qakbot",
      "malware_printable": "QakBot",
      "malware_alias": "Oakboat,Pinkslipbot,Qbot,Quakbot",
      "malware_malpedia": "https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot",
      "confidence_level": 100,
      "first_seen": "2022-12-07 18:58:08 UTC",
      "last_seen": null,
      "reference": null,
      "reporter": "Cryptolaemus1",
      "tags": [
```

```

        "BB09",
        "QakBot",
        "qbot",
        "Quakbot",
        "TR",
        "U12",
        "vhd",
        "zip"
    ],
    "malware_samples": []
}
]
}

```

ThreatQuotient provides the following default mapping for this function:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].malware_printable	malware.value	n/a	.data[].first_seen	QakBot	If enabled
.data[].malware_alias	malware.attribute	Alias	.data[].first_seen	[Oakboat, Pinkslipbot, Qbot, Quakbot]	If enabled
.data[].malware_malpedia	malware.attribute	External Reference	.data[].first_seen	https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot	If enabled
.data[].malware	malware.attribute	Malware Identifier	.data[].first_seen	win.qakbot	If enabled
.data[].malware_samples[].md5_hash	indicator.value	MD5	.data[].malware_samples[].time_stamp	n/a	If enabled
.data[].malware_samples[].sha256_hash	indicator.value	SHA-256	.data[].malware_samples[].time_stamp	n/a	If enabled
.data[].first_seen	indicator.attribute	First Seen	.data[].first_seen	2022-12-07 18:58:08 UTC	If enabled
.data[].last_seen	indicator.attribute	Last Seen	.data[].first_seen	n/a	If enabled
.data[].reporter	indicator.attribute	Reporter	.data[].first_seen	Cryptolaemus1	If enabled
.data[].reference	indicator.attribute	External Reference	.data[].first_seen	n/a	If enabled
.data[].confidence_level	indicator.attribute	Confidence Level	.data[].first_seen	100	If enabled
.data[].threat_type_description	indicator.attribute	Threat Type Description	.data[].first_seen	Indicator that identifies a malware distribution server (payload delivery)	If enabled
.data[].threat_type	indicator.attribute	Threat Type	.data[].first_seen	payload_delivery	If enabled
.data[].ioc	indicator.attribute	n/a	.data[].first_seen	n/a	n/a

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.data[].tags</code>	Indicator.tag	N/A	<code>.data[].first_seen</code>	<code>['BB09', 'QakBot', 'qbot', 'Quakbot', 'TR', 'U12', 'vhd', 'zip']</code>	If enabled

Enriched Data



Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Indicators	4
Indicator Attributes	25
Malware	3
Malware Attributes	11

Use Case Example

1. A Threat Analyst identifies a collection of supported objects they would like to enrich.
2. The Threat Analyst adds the abuse.ch ThreatFox Action to a workflow.
3. The Threat Analyst configures the action with the desired parameters and enables the workflow.
4. The workflow executes all actions in the graph, including the abuse.ch ThreatFox action.
5. The action returns the documented objects from the provider, ingesting them into the ThreatQ platform.

Change Log

- **Version 1.0.1**
 - The action is now capable of parsing the entire data from the response.
 - Updated action standards.
 - Updated minimum ThreatQ version to 5.14.1.
- **Version 1.0.0**
 - Initial release