ThreatQuotient

abuse.ch ThreatFox CDF User Guide

Version 1.0.1

November 20, 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	1.0.1
Compatible with ThreatQ Versions	>= 4.50.0
Support Tier	ThreatQ Supported

Introduction

ThreatFox is a project of **abuse.ch** with the goal of sharing indicators of compromise (IOCs) associated with malware with the infosec community, AV vendors and threat intelligence providers.

The integration provides the following feed:

- **abuse.ch ThreatFox** - retrieves a copy of the current IOC dataset from ThreatFox.

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

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

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 **OSINT** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Review all settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

abuse.ch ThreatFox

The abuse.ch ThreatFox feed retrieves a copy of the current IOC dataset from ThreatFox.

`POST https://threatfox-api.abuse.ch/api/v1/`

Sample Request:

```
{
    "query": "get_iocs",
    "days": 1
}
```

Sample Response:


```
{
   "data":[
      {
         "id":"1020675",
         "ioc":"http://116.202.5.101/1679",
         "threat_type":"botnet_cc",
         "threat_type_desc":"Indicator that identifies a botnet command&control
server (C&C)",
         "ioc_type":"url",
         "ioc_type_desc":"URL that is used for botnet Command&control (C&C)",
         "malware":"win.vidar",
         "malware_printable":"Vidar",
         "malware_alias":null,
         "malware_malpedia":"https://malpedia.caad.fkie.fraunhofer.de/details/
win.vidar",
         "confidence_level":100,
         "first_seen":"2022-11-18 07:48:30 UTC",
         "last_seen":null,
         "reference":null,
         "reporter":"crep1x",
         "tags":[
            "Vidar"
         ]
      },
      {
         "id":"1020674",
         "ioc":"185.132.53.205:1312",
         "threat_type":"botnet_cc",
         "threat_type_desc":"Indicator that identifies a botnet command&control
server (C&C)",
         "ioc_type":"ip:port",
         "ioc_type_desc":"ip:port combination that is used for botnet
```

```
Command&control (C&C)",
         "malware":"elf.mirai",
         "malware_printable":"Mirai",
         "malware_alias":"Katana",
         "malware_malpedia":"https://malpedia.caad.fkie.fraunhofer.de/details/
elf.mirai",
         "confidence_level":75,
         "first_seen":"2022-11-18 06:50:05 UTC",
         "last_seen":null,
         "reference":"https://bazaar.abuse.ch/sample/
b0aed60367755280b88f0efd6d64083ac5d29ac095851ab0f013a6397ec5bcad/",
         "reporter":"abuse_ch",
         "tags":[
            "Mirai"
         ]
      }
   ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].ioc	Indicator	Value	`.data[].first_seen`	185.132.53.205	IOC value depends on type. Check Indicator Type Map
.data[].tags	Indicator Tag	N/A	N/A	"dll", "QakBot", "qbot", "SilentBuilder", "TR"	Related Malware Tags
.data[].reporter	Indicator Attribute	Reporter	`.data[].first_seen`	abuse_ch	Strings_seperated
.data[].threat_type_desc	Indicator Attribute	Description	`.data[].first_seen`	Indicator that identifies a malware distribution server (payload delivery)	Describes Indicator
.data[].confidence_level	Indicator Attribute	Confidence	`.data[].first_seen`	100	Value between 0-100
.data[].id	Indicator Attribute	ThreatFox Link	`.data[].first_seen`	https://threatfox.abuse.ch/ioc/1000/	Format to URL data.id is platform specific primary key for the indicator.
.data[].ioc	Indicator Attribute	Port	`.data[].first_seen`	4003	If IOC type is `ip:port`. Indicates port for server payload. Split ip and port on condition ioc_type is "ip:port".
.data[].threat_type	Indicator Attribute	Threat Type	`.data[].first_seen`	payload_delivery	describes the delievery method of the threat
.data[].reference	Indicator Attribute	Reference	`.data[].first_seen`	https:\/\/twitter.com\/JAMESWT_MHT\/status\/1336229725082177536	reference for the threat
.data[].malware_malpedia	Indicator Attribute	Malware Malpedia	`.data[].first_seen`	https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot	Link to malpedia reference material for malware sample

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].malware_printable	Indicator Attribute	Malware Family	`.data[].first_seen`	QakBot	Malware Name
.data[].malware_alias	Indicator Attribute	Malware Alias	`.data[].first_seen`	Katana	Malware Alias

Indicator Type Mapping

The following table shows abuse.ch to ThreatQ indicator mapping:

ABUSE.CH VALUE	THREATQ VALUE
URL	URL
ip:port	IP Address
domain	URL
sha1_hash	SHA-1
sha3_384_hash	SHA-384
sha256_hash	SHA-256
sha512_hash	SHA-512
md5_hash	MD5
envelope_from	Email Address
body_from	Email Address

Average Feed Run

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

METRIC	RESULT
Run Time	3 min
Indicators	2,275
Indicator Attributes	20,521

Known Issues / Limitations

- API data fetching is restricted from 1 to 7 days with the time unit of 1 day.

Change Log

- **Version 1.0.1**
  - The Attribute Confidence is now updated when a new value is ingested.
- **Version 1.0.0**
  - Initial release