ThreatQuotient

Maldatabase CDF User Guide

Version 1.0.0

October 18, 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	>= 4.21.2
Support Tier	ThreatQ Supported

Introduction

Maldatabase is designed to help malware data science and threat intelligence feeds.

They collect a lot of samples reported by sandboxes and malware analysis services. Among all this data they can find both malicious software and legitimate software. For both types of data they have interesting information such as contacted domains, files written in the system or processes executed by malware sample.

They provide this data as datasets, useful for big data in graphical network visualization and machine learning. In the same way, this data can be used by companies and researchers as a threat intelligence feed.

The ThreatQ Maldatabase CDF Integration brings in all this data and all context around it.

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 **Commercial** 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. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Token	Your Maldatabase API Key.

   See the Known Issues and Limitations chapter for details regarding the default status of objects ingested by the feed.

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.

ThreatQ Mapping

Maldatabase Feed

Maldatabase provides an API that users can use to extract data in JSON format.

Sample Response:


```
{
   "sha256":"e89bc6077a352481aab03dee0d93b1c55f6f866775d67fc70e2026ef1a3be44e",
   "threat_level":"2",
   "md5":"db696e2837ec60504d5f94fc3df7dcc9",
   "sha1":"61c65d46eb23d8064692865f80e02f1b3bdac245",
   "family":"",
   "size":"145763",
   "type":"Word document",
   "domains":[
      "aesculapius.000webhostapp.com",
      "us-east-1.route-1.000webhost.awex.io",
      "block.io"
   ],
   "processes":[
      "winword.exe",
      "svchst.exe"
   ],
   "files":[
      "svchst.exe",
      "skinsoft.visualstyler.dll",
      "newtonsoft.json.dll",
      "encryptedfilelist.txt",
      "gdipfontcachev1.dat"
   ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.rss.channel.item[].sha256	indicator.value	SHA-256	e89bc6077a352481aab03dee0d93b1c55f6f866775d67fc70e2026ef1a3be44e	Has attributes: Threat Level, Malware Family, Size, File Type. Related to mapped indicator types: SHA-1, MD5, Filename.
.rss.channel.item[].threat_level	indicator.attribute	Threat Level	2	
.rss.channel.item[].md5	indicator.value	MD5	db696e2837ec60504d5f94fc3df7dcc9	Has attributes: Threat Level, Malware Family, Size, File Type. Related to mapped indicator types: SHA-1, SHA-256, Filename.
.rss.channel.item[].sha1	indicator.value	SHA-1	61c65d46eb23d8064692865f80e02f1b3bdac245	Has attributes: Threat Level, Malware Family, Size, File Type. Related to mapped indicator types: SHA-256, MD5, Filename.
.rss.channel.item[].family	indicator.attribute	Malware Family		
.rss.channel.item[].size	indicator.attribute	Size	145763	
.rss.channel.item[].type	indicator.attribute	File Type	Word document	
.rss.channel.item[].files	indicator.value	Filename	svchst.exe	Has attributes: Threat Level, Malware Family, Size, File Type. Related to mapped indicator types: SHA-256, SHA-1, MD5.
.rss.channel.item[].domains	indicator.value	FQDN	us-east-1.route-1.000webhost.awex.io	Has attributes: Threat Level, Malware Family.

Known Issues / Limitations

- The feed has a default status of **Review**, which you can change to **Active**. However, file- names and domains will still be ingested with a **Review** status in order to avoid marking non-malicious entities as malicious.

Change Log

- **Version 1.0.0**
  - Initial release