

ThreatQuotient



MWDB Cert Polska CDF Guide

Version 1.0.1

October 18, 2021

ThreatQuotient

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

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Support 4

Versioning..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping 9

Average Feed Run..... 13

Change Log..... 14

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 © 2021 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.

Versioning

- Current integration version 1.0.1
- Supported on ThreatQ versions $\geq$ 4.49.0

Introduction

The MWDB CERT Polska CDF ingests malware information, such as hashes and related IoCs, from CERT Polska's MWDB.

Malware families are ingested as malware objects and related to corresponding hash IoCs. You also have the option to ingest/download the corresponding files.

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Username	Your MWDB CERT Polska username.
Password	Your MWDB CERT Polska password.
Download Files	Select this option to download related malware files.
Verify SSL	Select this option to verify the SSL certificate for the server.  This option should not be selected, in most cases, when using self-signed.

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

GET <https://mwdb.cert.pl/api/file>

Creates ThreatQ indicators and malware objects, with the option to also create ThreatQ files.

Sample response data in JSON formatting:

```
{
  "files": [
    {
      "file_size": 129899,
      "md5": "3449523cdf7ef61bfa8e86eac05ad27b",
      "sha256": "1cc82190c83e90deb60128588e0f8e02ef603586aaea3d4cc11a032132b005de",
      "upload_time": "2021-08-06T09:49:06.333018+00:00",
      "type": "file",
      "tags": [
        {"tag": "urlhaus:elf"},
        {"tag": "urlhaus:gafgyt"},
        {"tag": "feed:urlhaus"},
        {"tag": "runnable:linux"}
      ],
      "file_name": "armv4l",
      "id": "1cc82190c83e90deb60128588e0f8e02ef603586aaea3d4cc11a032132b005de",
      "file_type": "ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, with debug_info, not stripped"
    },
    {
      "file_size": 129857,
      "md5": "94e794c8b269dbccab50ccf989243181",
      "sha256": "17992e45bb24c8f0c2b19f1ac7c9f90a07b6f48e87bbd1c4e05e7c2f9732fe6a",
      "upload_time": "2021-08-06T09:36:09.546226+00:00",
      "type": "file",
      "tags": [
        {"tag": "urlhaus:elf"},
        {"tag": "feed:urlhaus"},
        {"tag": "runnable:linux"},
        {"tag": "urlhaus:gafgyt"}
      ],
      "file_name": "sparc",
      "id": "17992e45bb24c8f0c2b19f1ac7c9f90a07b6f48e87bbd1c4e05e7c2f9732fe6a",
      "file_type": "ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, with debug_info, not stripped"
    },
    {
      "file_size": 155429,
      "md5": "33cb976e962930398427e7b03e5258c5",
      "sha256": "6662b1d99e7cad6f799602dcb4e4ef54d1ed46404f28c7f160fee8d1a3e64e39",
      "upload_time": "2021-08-06T09:36:07.922018+00:00",
      "type": "file",
      "tags": [
        {"tag": "feed:urlhaus"},
        {"tag": "urlhaus:gafgyt"},
        {"tag": "runnable:linux"}
      ]
    }
  ]
}
```

```
    {"tag": "urlhaus:elf"}
  ],
  "file_name": "mips",
  "id": "6662b1d99e7cad6f799602dcb4e4ef54d1ed46404f28c7f160fee8d1a3e64e39",
  "file_type": "ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, not stripped"
},
{
  "file_size": 118091,
  "md5": "63bb652dc7e6d51abf5c96bab358d64e",
  "sha256": "4dc09a5006cf6d659ca9474f8cca6dbf00fde3a842a7dd485b37c6eb4680bc71",
  "upload_time": "2021-08-06T09:36:06.330160+00:00",
  "type": "file",
  "tags": [
    {"tag": "urlhaus:gafgyt"},
    {"tag": "feed:urlhaus"},
    {"tag": "urlhaus:elf"},
    {"tag": "runnable:linux"}
  ],
  "file_name": "m68k",
  "id": "4dc09a5006cf6d659ca9474f8cca6dbf00fde3a842a7dd485b37c6eb4680bc71",
  "file_type": "ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, not stripped"
},
{
  "file_size": 104139,
  "md5": "df1fd232f63302bfb5bc72c9617b03da",
  "sha256": "8937e4b91d5248b9b46d70d8aa4286d36f35198e7f26d7ed9b643ecc106e7e3d",
  "upload_time": "2021-08-06T09:36:04.741609+00:00",
  "type": "file",
  "tags": [
    {"tag": "urlhaus:gafgyt"},
    {"tag": "feed:urlhaus"},
    {"tag": "runnable:linux"},
    {"tag": "urlhaus:elf"}
  ],
  "file_name": "i686",
  "id": "8937e4b91d5248b9b46d70d8aa4286d36f35198e7f26d7ed9b643ecc106e7e3d",
  "file_type": "ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, not stripped"
},
{
  "file_size": 100043,
  "md5": "7553d65b0b499aa639eb5d3cf618612a",
  "sha256": "4a8f0e4a6118533b5b3465901bd6bace1bcb4b2291e29b52de4edda4b3554e84",
  "upload_time": "2021-08-06T09:36:03.151971+00:00",
  "type": "file",
  "tags": [
    {"tag": "urlhaus:gafgyt"},
    {"tag": "feed:urlhaus"},
    {"tag": "runnable:linux"},
    {"tag": "urlhaus:elf"}
  ],
  "file_name": "i586",
  "id": "4a8f0e4a6118533b5b3465901bd6bace1bcb4b2291e29b52de4edda4b3554e84",
  "file_type": "ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, not stripped"
},
{
  "file_size": 112634,
  "md5": "54cce3900a37f6a135bfbad5fcd3890d",
  "sha256": "08f511a97848ad5e4cb04b96451d71162ebf33f758a560813e2ebe22e96b3425",
  "upload_time": "2021-08-06T09:36:01.546801+00:00",
```

```
"type": "file",
"tags": [
  {"tag": "runnable:linux"},
  {"tag": "urlhaus:elf"},
  {"tag": "feed:urlhaus"},
  {"tag": "urlhaus:gafgyt"}
],
"file_name": "sh4",
"id": "08f511a97848ad5e4cb04b96451d71162ebf33f758a560813e2ebe22e96b3425",
"file_type": "ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, not stripped"
},
{
  "file_size": 116787,
  "md5": "f5a73cf73038bd244be050f23304ae12",
  "sha256": "0e8a8ed8330b1e6dd7c1177f7e604e89716b0c2c34bc00cb20c0c9f87bd65ccf",
  "upload_time": "2021-08-06T09:36:00.015167+00:00",
  "type": "file",
  "tags": [
    {"tag": "feed:urlhaus"},
    {"tag": "urlhaus:elf"},
    {"tag": "runnable:linux"},
    {"tag": "urlhaus:gafgyt"}
  ],
  "file_name": "powerpc",
  "id": "0e8a8ed8330b1e6dd7c1177f7e604e89716b0c2c34bc00cb20c0c9f87bd65ccf",
  "file_type": "ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, not
stripped"
},
{
  "file_size": 155477,
  "md5": "abc3af6dca227c37fbaf27c10756a7eb",
  "sha256": "c99e64f6b6383792ab96694d374cf63dd368fd8dec5d41ac3a866459d6492f8f",
  "upload_time": "2021-08-06T09:35:58.572290+00:00",
  "type": "file",
  "tags": [
    {"tag": "runnable:linux"},
    {"tag": "feed:urlhaus"},
    {"tag": "urlhaus:gafgyt"},
    {"tag": "urlhaus:elf"}
  ],
  "file_name": "mipsel",
  "id": "c99e64f6b6383792ab96694d374cf63dd368fd8dec5d41ac3a866459d6492f8f",
  "file_type": "ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, not stripped"
},
{
  "file_size": 143020,
  "md5": "5c8c61e90480836135cc020154269ebe",
  "sha256": "0d3465d3c8f49d16feac675a07fa2d44872d546b9917b23560d646385aceb1a1",
  "upload_time": "2021-08-06T09:35:56.930006+00:00",
  "type": "file",
  "tags": [
    {"tag": "urlhaus:elf"},
    {"tag": "feed:urlhaus"},
    {"tag": "urlhaus:gafgyt"},
    {"tag": "runnable:linux"}
  ],
  "file_name": "armv6l",
  "id": "0d3465d3c8f49d16feac675a07fa2d44872d546b9917b23560d646385aceb1a1",
  "file_type": "ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, with debug_info, not
stripped"
}
```

```
}  
]  
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.files[].md5	Indicator.Value	MD5	N/A	3449523cdf7ef61bfa8e86eac05ad27b	N/A
.files[].sha256	Indicator.Value	SHA-256	N/A	1cc82190c83e90deb60128588e0f8e02ef603586aaea3d4cc11a032132b005de	N/A
.files[].file_name	Indicator.Value	Filename	N/A	armv4l	N/A
.files[].file_type	Indicator.Attribute	Malware Type	N/A	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, with debug_info, not stripped	N/A
.files[].tags[].tag	Related Malware.Value	N/A	N/A	glupteba	Only ingest tags not-containing a colon (:)
/api/file/{.files[].id}.sha1	Indicator.Value	SHA-1	N/A	6ff6c7eb2d5d52a24b9cc8a5c0f68c39ac989a86	Using separate api endpoint
/api/file/{.files[].id}.sha512	Indicator.Value	SHA-512	N/A	827e4ba7de2b18d2a5a2ae0b03fd3933bf1fd0557b2de8a6a36d0f54c96c645fbec9bbcae18804bc619d537363d297415797cdaac7727e81e5035c5fb58ee9c4	Using separate api endpoint (same as above/ SHA-1)
/api/file/{.files[].id}/download .	File.Content	N/A	N/A	N/A	Using separate api endpoint; user optional

Average Feed Run

The following metrics are from 24 hours worth of data from MWDB CERT Polska - from October 11, 2021 at 3:02pm to October 12, 2021 at 3:02pm.

METRIC	RESULT
Run Time	20 minutes
Indicators	3,236
Indicator Attributes	3,240
Malware	12
Files	585



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.

Change Log

- **Version 1.0.1**
 - Fixed an issue with the time range query.
- **Version 1.0.0**
 - Initial release