

# ThreatQuotient



## Intel 471 Indicators - Malware Intelligence CDF Guide

Version 1.2.0

August 08, 2022

**ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

**Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](http://support.threatq.com)

Phone: 703.574.9893

# Contents

Integration Details.....	5
Introduction .....	6
Installation.....	7
Configuration .....	8
ThreatQ Mapping .....	9
Intel 471 Indicators - Malware Intelligence .....	9
Average Feed Run.....	12
Change Log.....	13

# 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 © 2022 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](mailto: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:

<b>Current Integration Version</b>	1.2.0
<b>Compatible with ThreatQ Versions</b>	>= 4.41.0
<b>Support Tier</b>	ThreatQ Supported
<b>ThreatQ Marketplace</b>	<a href="https://marketplace.threatq.com/details/intel471-indicators-malware-intelligence">https:// marketplace.threatq.com/ details/intel471-indicators- malware-intelligence</a>

---

# Introduction

The Intel 471 Indicators - Malware Intelligence integration returns a list of indicators that match filter criteria from the following endpoint:

- **Intel 471 Indicator - Malware Intelligence** - <https://api.intel471.com/v1/indicators/stream>

The integration ingests indicator and indicator attributes.

# 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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
<b>Email Address</b>	Your Intel 471 account email address.
<b>API Key</b>	Your Intel 471 account API key.
<b>Indicator Type</b>	Search indicators by type (file, ipv4, url).  If no option is selected, all indicator types are queried.

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

## Intel 471 Indicators - Malware Intelligence

GET <https://api.intel471.com/v1/indicators/stream>

### Sample Response:

```
{
  "indicatorTotalCount": 224181,
  "indicators": [
    {
      "data": {
        "indicator_id": "c8c1385ee0411410463bb39a8a944c2ec7025d09",
        "threat": {
          "type": "malware",
          "uid": "b38ef686caf0103866339452d3d1c4fb",
          "data": {
            "malware_family_profile_uid": "b38ef686caf0103866339452d3d1c4fb",
            "family": "dridex"
          }
        },
        "expiration": 1622192350000,
        "confidence": "medium",
        "context": {
          "description": "plugin downloaded by dridex malware family"
        },
        "mitre_tactics": "stage_capabilities",
        "indicator_type": "file",
        "indicator_data": {
          "file": {
            "md5": "c444f89248e673d3bc22ed125c4ed162",
            "sha1": "c652139e29b209757d497e026bfc187ef3bfadc7",
            "sha256": "cd7bc57e2d614137de1594ac0b04004b936797f0e5b402ace3e75a7138e61370",
            "type": "PEDLL_x86",
            "size": 382976,
            "download_url": "https://api.intel471.com/v1/download/malwareIntel/cd7bc57e2d614137de1594ac0b04004b936797f0e5b402ace3e75a7138e61370.zip"
          }
        },
        "intel_requirements": [
          "1.3.4",
          "1.1.4"
        ]
      },
      "meta": {
        "version": "0.1"
      },
      "last_updated": 1590656362056,
      "uid": "b366979d1abdedf51f985fe03d0fc19e",
      "activity": {
        "first": 1590503428000,
        "last": 1590656350000
      }
    }
  ]
}
```

```

    }
  ]
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].data.threat.type	Indicator.Attribute	Malware Type	.indicators[].data.activity.first	malware	
.indicators[].data.threat.uid	Indicator.Attribute	Threat UID	.indicators[].data.activity.first	b38ef686ca f010386633 9452d3d1c4 fb	
.indicators[].data.threat.data.malware_family_profile_uid	Indicator.Attribute	Malware Family Profile UID	.indicators[].data.activity.first	b38ef686caf0 10386633945 2d3d1c4fb	
.indicators[].data.threat.data.family	Indicator.Attribute	Malware Family	.indicators[].data.activity.first	dridex	
.indicators[].data.expiration	Indicator.Attribute	Expires At	.indicators[].data.activity.first	16227120150 00	
.indicators[].data.confidence	Indicator.Attribute	Confidence	.indicators[].data.activity.first	medium	
.indicators[].data.context.description	Indicator.Description	N/A	.indicators[].data.activity.first	plugin downloaded by dridex malware family	
.indicators[].data.mitre_tactics	Indicator.Attribute	MITRE Tactics	.indicators[].data.activity.first	stage_capabilities	
.indicators[].data.indicator_data.file.md5	Indicator.Value	MD5	.indicators[].data.activity.first	05f7722289b1b8a7 7b77a15ba192adb8	Indicator from type File
.indicators[].data.indicator_data.file.sha1	Indicator.Value	SHA-1	.indicators[].data.activity.first	1b38f9ae60d1cb05 9f15139c5c6919f14 503bca9	Indicator from type File
.indicators[].data.indicator_data.file.sha256	Indicator.Value	SHA-256	.indicators[].data.activity.first	3ce665e28a462697 3d252af6d1a6d969 f378e2d9aaf120c0f 862061fd6384b5e	Indicator from type File
.indicators[].data.indicator_data.url	Indicator.Value	URL	.indicators[].data.activity.first	http://mailchristen.at	Indicator from type URL
.indicators[].data.indicator_data.address	Indicator.Value	IP Address	.indicators[].data.activity.first	54.38.22.65	Indicator from type IPv4
.indicators[].data.intel_requirements	Indicator.Attribute	Intelligence Requirement	.indicators[].data.activity.first	1.3.4	
.indicators[].data.meta.version	Indicator.Attribute	Document Version	.indicators[].data.activity.first	0.1	
.indicators[].data.last_updated	Indicator.Attribute	Last Updated At	.indicators[].data.activity.first	1591176018215	
.indicators[].data.uid	Indicator.Attribute	Indicator UID	.indicators[].data.activity.first	55464586356a9bde 14b86e5488673620	
.indicators[].data.activity.first	Indicator.Attribute	Active Period First	.indicators[].data.activity.first	1591172700000	
.indicators[].data.activity.last	Indicator.Attribute	Active Period Last	.indicators[].data.activity.first	1591176015000	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].data.indicator_data.file.download_url	Indicator.Attribute	Download URL	.indicators[].data.activity.first	https://api.intel471.com/v1/download/malwareIntel/3ce665e28a4626973d252af6d1a6d969f378e2d9aaf120c0f862061fd6384b5e.zip	This attribute is only for MD5, SHA-1 and SHA-256
.indicators[].data.indicator_data.file.type	Indicator.Attribute	File Type	.indicators[].data.activity.first	PEDLL_x86	This attribute is only for MD5, SHA-1 and SHA-256
.indicators[].data.indicator_data.file.size	Indicator.Attribute	File Size	.indicators[].data.activity.first	382976	This attribute is only for MD5, SHA-1 and SHA-256

# 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 minutes
Indicators	983
Indicator Attributes	16,304

# Change Log

- **Version 1.2.0**
  - Updated the endpoint to use the streaming API.
  - Removed the **Count** user configuration option.
- **Version 1.1.1**
  - Fixed feed name typo.
- **Version 1.1.0**
  - Added ability to ingest all indicator types at once.
- **Version 1.0.0**
  - Initial release.