

ThreatQuotient

A Securonix Company



Intel 471 Indicators - Malware Intelligence CDF

Version 2.0.0

September 22, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details	5
Introduction	6
Prerequisites	7
Installation	8
Configuration	9
ThreatQ Mapping	12
Intel 471 Indicators - Malware Intelligence	12
Direct Indicators Table Mapping	14
Common Indicator Attributes Table Mapping	15
Bulletproof Hosting Indicator Attributes Table Mapping	16
File Indicator Attributes Table Mapping	16
IPv4 Indicator Attributes Table Mapping	17
YARA Signatures Table Mapping	17
Average Feed Run	19
Change Log	20

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 © 2026 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: tq-support@securonix.com

Support Web: <https://ts.securonix.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	2.0.0
Compatible with ThreatQ Versions	>= 5.24.0
Support Tier	ThreatQ Supported

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** - retrieves indicator intelligence and YARA signatures from the Intel 471 cloud Indicators stream and ingests them into ThreatQ as Indicator and Signature objects with associated attributes.

The integration ingests the following system objects:

- Indicators
 - Indicator Attributes
- Signatures
 - Signature Attributes

Prerequisites

The following is required to run the integration:

- An Intel 471 Client ID.
- An Intel 471 Client Secret.

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
Client ID	Enter your Intel 471 Client ID.
Client Secret	Enter your Intel 471 Client Secret
Fetch GIR Names	Enable this parameter to include each GIR name with its corresponding path. Disable it to use the raw GIR paths. This parameter is enabled by default
Indicator Type	Select an indicator type to send as the type query parameter. Options include: ◦ ALL ◦ Domain ◦ Email ◦ File ◦ IPv4 (<i>default</i>) ◦ URL ◦ YARA

PARAMETER	DESCRIPTION
	 Selecting ALL omits the parameter and retrieves all available indicator types. This may produce a large result set and require thousands of paginated API requests. Select specific values whenever possible to reduce API usage.
Threat Type	Select a threat type to send as the <code>threat_type</code> query parameter. Options include: ◦ ALL ◦ Malware (<i>default</i>) ◦ Bulletproof Hosting  Selecting ALL omits the parameter and may return a large result set requiring thousands of paginated API requests. Select specific values whenever possible to reduce API usage.
Confidence	Select a confidence level to send as the <code>confidence</code> query parameter. Options include: ◦ ALL (<i>default</i>) ◦ High ◦ Medium ◦ Low  Selecting ALL omits the parameter.
Text Filter	Optional - Enter text to filter the indicators returned by the feed. Example: <code>btmob</code> .
Malware Family Name	Optional - Enter a malware family name to filter the returned indicators. Example: <code>btmob</code> .

PARAMETER	DESCRIPTION
GIRs	Optional - Enter one or more comma-separated GIR paths, or enter <code>my_girs</code> or <code>company_pirs</code> to retrieve indicators from those GIR collections. Example: <code>1.1.5,2.1.3</code> .
Page Size	Enter the number of records to request per page. Valid values range from 1 to 1000. The default value is 1000.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Intel 471 Indicators - Malware Intelligence

The Intel 471 Indicators - Malware Intelligence feed retrieves indicator intelligence and YARA signatures from the Intel 471 cloud Indicators stream and ingests them into ThreatQ as Indicator and Signature objects with associated attributes.

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



Items in `.indicators[]` where `.type` is not `yara` create one or more ThreatQ Indicator objects, while items whose `.type` is `yara` create ThreatQ Signature objects of type YARA.

Sample Response:

```
{
  "count": 1,
  "cursor_next":
  "NTg2ZDYwOWUtNzhmMS00MDY5LTg3M2QtYTI5MWRjNzBhNTYyOjE3ODY4NDI0NjA4MjA6
  ZThhZWE2NTI0ZjBhOWI2MGQ4OTUwNmNkYjc2M2ExYjg3ODg0MWJiYw",
  "indicators": [
    {
      "activity": {
        "first_seen_ts": "2026-08-11T20:28:31Z",
        "last_seen_ts": "2026-08-15T20:28:49Z"
      },
      "classification": {
        "girs": [
          {
            "path": "1.1.2",
            "name": "Mobile malware"
          },
          {
            "path": "1.1.4",
            "name": "Banking trojan malware"
          },
          {
            "path": "1.4.4",
            "name": "Android"
          }
        ]
      }
    }
  ]
}
```

```

        }
      ]
    },
    "confidence": 50,
    "data": {
      "ipv4": {
        "ip_address": "130.94.40.138",
        "geo_ip": {
          "country": "Singapore",
          "country_code": "SG",
          "city": "Singapore",
          "isp": {
            "isp": "LIGHT NODE LIMITED",
            "organization": "LIGHT NODE LIMITED",
            "autonomous_system": "AS154177 LIGHT NODE
LIMITED",
            "network": "130.94.0.0/18"
          }
        }
      }
    },
    "description": "btmob controller IPv4",
    "expiration_ts": "2026-09-11T20:28:57Z",
    "id": "malware-indicator--3f5e3ccb-76bd-53b7-
b2f0-04041045c888",
    "kill_chain_phases": [
      {
        "kill_chain_name": "mitre-attack",
        "phase_name": "command_and_control"
      }
    ],
    "pattern": "[ipv4-addr:value = '130.94.40.138']",
    "pattern_type": "stix",
    "pattern_version": "2.1",
    "threat": {
      "type": "malware",
      "data": {
        "malware": {
          "id": "malware--58bc1e16-a79e-5436-
abe8-0576d0ad354b",
          "family": "btmob",
          "version": "BT-v5.0.1"
        }
      }
    }
  }
}

```

```

        },
        "malware_family": {
            "id": "malware-family--7398e343-b9ae-56c8-
ba12-30ac9541e9cd",
            "name": "btmob"
        }
    },
    "type": "ipv4"
}
]
}

```

Direct Indicators Table Mapping

ThreatQuotient provides the following default mapping for direct indicators:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].type	Indicator.Type	N/A	.indicators[].activity.first_seen_ts	ipv4, domain, email, file, url	Drives the type-specific mapping below.
.indicators[].data.ipv4.ip_address	Indicator.Value	IP Address	.indicators[].activity.first_seen_ts	130.94.40.138	Only when .type == "ipv4".
.indicators[].data.domain	Indicator.Value	FQDN	.indicators[].activity.first_seen_ts	fdaccfl.ru	Only when .type == "domain".
.indicators[].data.email	Indicator.Value	Email Address	.indicators[].activity.first_seen_ts	mobilitylog@gthltd.buzz	Only when .type == "email".
.indicators[].data.url	Indicator.Value	URL	.indicators[].activity.first_seen_ts	tcp://103.212.136.208:9090	Only when .type == "url".
.indicators[].data.file.md5	Indicator.Value	MD5	.indicators[].activity.first_seen_ts	253f2dbdc2a9e2a0cfb8dbc8bc8f874b	File records create a separate indicator for each populated hash.
.indicators[].data.file.sha1	Indicator.Value	SHA-1	.indicators[].activity.first_seen_ts	ac206745aadf006663b22c1916703ee43c987027	File records create a separate indicator for each populated hash.
.indicators[].data.file.sha256	Indicator.Value	SHA-256	.indicators[].activity.first_seen_ts	e330752b3750a012cb4c97a9b6e2c55bfce0ad4e5ccb5c0ec4f3019b4ddf00c5	File records create a separate indicator for each populated hash.

Common Indicator Attributes Table Mapping

ThreatQuotient provides the following default mapping for common indicator attributes. These mappings are applied to every non-YARA indicator. Empty or absent values are not ingested.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.indicators[].id</code>	Indicator.Attribute	Indicator ID	<code>.indicators[].activity.first_seen_ts</code>	malware-indicator--3f5e3ccb-...	Replaces the legacy indicator UID.
<code>.indicators[].description</code>	Indicator.Attribute	Description	<code>.indicators[].activity.first_seen_ts</code>	Indicator used by btmob malware	Ingest when present.
<code>.indicators[].confidence</code>	Indicator.Attribute	Confidence	<code>.indicators[].activity.first_seen_ts</code>	50	Integer value returned by the new API.
<code>.indicators[].expiration_ts</code>	Indicator.Attribute	Expires At	<code>.indicators[].activity.first_seen_ts</code>	2026-09-11T20:28:57Z	ISO 8601 timestamp.
<code>.indicators[].activity.first_seen_ts</code>	Indicator.Attribute	First Seen	<code>.indicators[].activity.first_seen_ts</code>	2026-08-11T20:28:31Z	Also used as the indicator published date.
<code>.indicators[].activity.last_seen_ts</code>	Indicator.Attribute	Last Seen	<code>.indicators[].activity.first_seen_ts</code>	2026-08-15T20:28:49Z	ISO 8601 timestamp.
<code>.indicators[].pattern</code>	Indicator.Attribute	Pattern	<code>.indicators[].activity.first_seen_ts</code>	[ipv4-addr:value = '130.94.40.138']	STIX pattern for direct indicators.
<code>.indicators[].pattern_type</code>	Indicator.Attribute	Pattern Type	<code>.indicators[].activity.first_seen_ts</code>	stix	Ingest when present.
<code>.indicators[].pattern_version</code>	Indicator.Attribute	Pattern Version	<code>.indicators[].activity.first_seen_ts</code>	2.1	Ingest when present.
<code>.indicators[].kill_chain_phases[].phase_name</code>	Indicator.Attribute	MITRE Tactics	<code>.indicators[].activity.first_seen_ts</code>	command_and_control	Multi-valued.
<code>.indicators[].classification.girs[]</code>	Indicator.Attribute	Intelligence Requirement	<code>.indicators[].activity.first_seen_ts</code>	1.1.5 - Information-stealer malware	With Fetch GIR Names enabled, use path - name; otherwise use the raw path.
<code>.indicators[].threat.type</code>	Indicator.Attribute	Threat Type	<code>.indicators[].activity.first_seen_ts</code>	malware	Values observed include malware and bulletproof_hosting.
<code>.indicators[].threat.data.malware.id</code>	Indicator.Attribute	Malware ID	<code>.indicators[].activity.first_seen_ts</code>	malware--f12da3fa-...	Malware threats only, when present.
<code>.indicators[].threat.data.malware.family</code>	Indicator.Attribute	Malware Family	<code>.indicators[].activity.first_seen_ts</code>	btmob	Malware threats only; use this value first and fall back to <code>.threat.data.malware_family.name</code> .

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.indicators[].threat.data.malware.version</code>	Indicator.Attribute	Threat Version	<code>.indicators[].activity.first_seen_ts</code>	0.7d	Malware threats only, when present.
<code>.indicators[].threat.data.malware.variant</code>	Indicator.Attribute	Malware Variant	<code>.indicators[].activity.first_seen_ts</code>	v3_variant_a	Malware threats only, when present.
<code>.indicators[].threat.data.malware_family.id</code>	Indicator.Attribute	Malware Family ID	<code>.indicators[].activity.first_seen_ts</code>	malware-family--f12da3fa-...	Malware threats only, when present.
<code>.indicators[].threat.data.malware_family.name</code>	Indicator.Attribute	Malware Family Name	<code>.indicators[].activity.first_seen_ts</code>	btmob	Malware threats only, when present.

Bulletproof Hosting Indicator Attributes Table Mapping

ThreatQuotient provides the following default mapping for Bulletproof hosting indicator attributes.



Records with `.indicators[].threat.type = bulletproof_hosting` use the direct and IPv4 mappings.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.indicators[].data.ipv4.ip_address</code>	Indicator.Value	IP Address	<code>.indicators[].activity.first_seen_ts</code>	61.82.2.181	The supplied sample is IPv4 and applies only when type is ipv4.
<code>.indicators[].threat.type</code>	Indicator.Attribute	Threat Type	<code>.indicators[].activity.first_seen_ts</code>	bulletproof_hosting	Identifies Bulletproof Hosting records.
<code>.indicators[].threat.data.bulletproof_hosting.provider</code>	Indicator.Attribute	Bulletproof Hosting Provider	<code>.indicators[].activity.first_seen_ts</code>	ccweb	Only when threat.type is bulletproof_hosting.

File Indicator Attributes Table Mapping

ThreatQuotient provides the following default mapping for file indicator attributes. This applies to each related MD5, SHA-1, and SHA-256 indicator.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.indicators[].data.file.type</code>	Indicator.Attribute	File Type	<code>.indicators[].activity.first_seen_ts</code>	PEEXE_x86	File indicators only.
<code>.indicators[].data.file.size</code>	Indicator.Attribute	File Size	<code>.indicators[].activity.first_seen_ts</code>	221184	File indicators only.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].data.file.ssdeep	Indicator.Attribute	SSDEEP	.indicators[].activity.first_seen_ts	3072:zGWSdk...	File indicators only.

IPv4 Indicator Attributes Table Mapping

ThreatQuotient provides the following default mapping for IPv4 indicator attributes:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].data.ipv4.geo_ip.country	Indicator.Attribute	Country	.indicators[].activity.first_seen_ts	South Korea	IPv4 indicators only, when present.
.indicators[].data.ipv4.geo_ip.country_code	Indicator.Attribute	Country Code	.indicators[].activity.first_seen_ts	KR	IPv4 indicators only, when present.
.indicators[].data.ipv4.geo_ip.city	Indicator.Attribute	City	.indicators[].activity.first_seen_ts	Yeongwol-gun	IPv4 indicators only, when present.
.indicators[].data.ipv4.geo_ip.subdivision[]	Indicator.Attribute	Subdivision	.indicators[].activity.first_seen_ts	Gangwon-do	IPv4 indicators only; multi-valued.
.indicators[].data.ipv4.geo_ip.isp.isp	Indicator.Attribute	ISP	.indicators[].activity.first_seen_ts	KT	IPv4 indicators only, when present.
.indicators[].data.ipv4.geo_ip.isp.organization	Indicator.Attribute	Organization	.indicators[].activity.first_seen_ts	KT	IPv4 indicators only, when present.
.indicators[].data.ipv4.geo_ip.isp.autonomous_system	Indicator.Attribute	Autonomous System	.indicators[].activity.first_seen_ts	AS4766 Korea Telecom	IPv4 indicators only, when present.
.indicators[].data.ipv4.geo_ip.isp.network	Indicator.Attribute	Network	.indicators[].activity.first_seen_ts	61.82.0.0/18	IPv4 indicators only, when present.

YARA Signatures Table Mapping

ThreatQuotient provides the following default mapping for YARA Signatures. Each item where `.indicators[].type == "yara"` creates one ThreatQ signature of type YARA, rather than a direct indicator.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
YARA	Signature.Type	N/A	.indicators[].activity.first_seen_ts	YARA	Constant value.
.indicators[].data.yara.title	Signature.Name	N/A	.indicators[].activity.first_seen_ts	crysome	Primary signature name.
.indicators[].data.yara.signature	Signature.Value	YARA	.indicators[].activity.first_seen_ts	rule cr... { ... }	Full YARA rule text.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].id	Signature.Attribute	Signature ID	.indicators[].activity.first_seen_ts	malware-indicator--2098b5b3-...	N/A
.indicators[].type	Signature.Attribute	Indicator Type	.indicators[].activity.first_seen_ts	yara	N/A
.indicators[].confidence	Signature.Attribute	Confidence	.indicators[].activity.first_seen_ts	85	N/A
.indicators[].activity.first_seen_ts	Signature.Attribute	First Seen	.indicators[].activity.first_seen_ts	2026-08-14T11:16:22Z	Also used as the signature published date.
.indicators[].activity.last_seen_ts	Signature.Attribute	Last Seen	.indicators[].activity.first_seen_ts	2026-09-07T17:23:53Z	N/A
.indicators[].pattern	Signature.Attribute	Pattern	.indicators[].activity.first_seen_ts	rule cr... { ... }	N/A
.indicators[].pattern_type	Signature.Attribute	Pattern Type	.indicators[].activity.first_seen_ts	yara	N/A
.indicators[].pattern_version	Signature.Attribute	Pattern Version	.indicators[].activity.first_seen_ts	4	N/A
.indicators[].classification.girs[]	Signature.Attribute	Intelligence Requirement	.indicators[].activity.first_seen_ts	1.1.5 - Information-stealer malware	Apply the same Fetch GIR Names behavior as indicators.
.indicators[].threat.type	Signature.Attribute	Threat Type	.indicators[].activity.first_seen_ts	malware	N/A
.indicators[].threat.data.malware_family.id	Signature.Attribute	Malware Family ID	.indicators[].activity.first_seen_ts	malware-family--...	When present.
.indicators[].threat.data.malware_family.name	Signature.Attribute	Malware Family	.indicators[].activity.first_seen_ts	crysome	When present.

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
Signature	2
Signature Attributes	24

Change Log

- **Version 2.0.0**

- Updated the integration to use the Intel 471 cloud API and corresponding cloud schema mappings.
- Added support for client credential authentication, configurable filters, and page-size settings.
- Added Unix millisecond conversion for the `from` parameter and cursor-based pagination within each feed run.
- Removed the following configuration parameters:
 - **Email Address**
 - **API Key**
- Added the following new configuration parameters:
 - **Client ID:** Specifies the Intel 471 Client ID used as the HTTP Basic authentication username.
 - **Client Secret:** Specifies the Intel 471 Client Secret used as the HTTP Basic authentication password.
 - **Fetch GIR Names:** Controls whether GIR names are included with their corresponding paths. Enabled by default.
 - **Threat Type:** Filters indicators by threat type. Available options include `ALL`, `Malware` (default), and `Bulletproof Hosting`.
 - **Confidence:** Filters indicators by confidence level. Available options include `ALL` (default), `High`, `Medium`, and `Low`.
 - **Text Filter:** Filters returned indicators using the specified text.
 - **Malware Family Name:** Filters returned indicators by malware family name.
 - **GIRs:** Filters returned indicators using specified GIR paths or the `my_girs` or `company_pirs` collections.
 - **Page Size:** Specifies the number of records requested per page, from `1` to `1000`. The default value is `1000`.
 - **Enable SSL Verification:** Controls whether the integration verifies the endpoint's SSL certificate. Enabled by default.
 - **Disable Proxies:** Controls whether the integration bypasses proxies configured in ThreatQ. Disabled by default.

-
- Added additional options to the **Indicator Type** configuration parameter.
 - Updated the minimum ThreatQ version to 5.24.0.
 - **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.