

ThreatQuotient

A Securonix Company



QAX Threat Intelligence CDF

Version 1.0.0

October 13, 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.....11

 QAX Threat Intelligence.....11

Average Feed Run.....13

Change Log14

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	1.0.0
Compatible with ThreatQ Versions	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The QAX Threat Intelligence Feed integration retrieves subscribed threat intelligence indicators from the QAX Threat Intelligence Feed API and ingests them into ThreatQ. It supports the documented compromise, malicious hash, and proxy/IP reputation feed formats, creating ThreatQ Indicators with associated contextual attributes and tags.

The integration provides the following feed:

- **QAX Threat Intelligence** - retrieves one configured QAX intelligence subcategory per feed instance.

The integration ingests indicators and indicator attributes into ThreatQ.

Prerequisites

The following is required to run the integration:

- A QAX API Key.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the 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.

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
API Key	Required. Enter the API key provided by QAX.
Enable SSL Certificate Verification	Select this option to validate the SSL certificate presented by the QAX host. Default: True .
Disable Proxies	Select this option to prevent the feed from using proxies configured in ThreatQ. Default: False .
Intelligence Subcategory	Select the QAX feed subtype to retrieve for this feed instance. Default: Malicious URL .
Language	Select the language in which to retrieve intelligence from QAX. Valid options are English and Chinese . Default: English .
Request Limit	Optional. Enter the maximum number of records to request from QAX. The API supports up to 3000 records per request. Default: 3000.

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

QAX Threat Intelligence

The QAX Threat Intelligence feed retrieves indicators from a selected QAX intelligence subcategory and ingests them into ThreatQ with associated risk, confidence, threat, campaign, and other contextual data.

GET <https://a.ti.qianxin.com/feed/v1/gain>

Sample JSON Response (synthetic values):

```
[
  {
    "id": "qax-record-example-001",
    "alert_name": "Example Command and Control Indicator",
    "risk": "high",
    "malicious_family": ["ExampleFamily"],
    "malicious_type": "BOTNET",
    "kill_chain": "c2",
    "confidence": "high",
    "campaign": "Example Campaign",
    "targeted": false,
    "tag": ["command-and-control"],
    "platform": "Windows",
    "current_status": "active",
    "ioc_category": "DOMAIN_PORT",
    "ioc": ["c2.example.test", "443", "/beacon"],
    "TTP": "Synthetic example for illustrating the response fields.",
    "etime": "2026-10-01T08:00:00.000Z",
    "insert_time": 1790841600000,
    "update_time": 1790845200000
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	NOTES
.ioc[0]	Indicator	Determined from configured sub_type or .ioc_category	Standard compromise IOC value.	
.ip_str	Indicator	IP Address	Proxy/IP reputation address.	
.md5	Indicator	MD5	Creates an MD5 Indicator when present.	
.sha1	Indicator	SHA-1	Creates a SHA-1 Indicator when present.	
.sha256	Indicator	SHA-256	Creates a SHA-256 Indicator when present.	
.id	Indicator.Attribute	QAX ID	Added when non-empty; available on compromise records.	
sub_type	Indicator.Attribute	QAX Subcategory	Identifies the selected QAX intelligence subtype.	
.risk or top-level .severity	Indicator.Attribute	Risk	N/A	
.confidence or .tag_detail_info.confidence	Indicator.Attribute	Confidence	Supports compromise and proxy response formats.	
.malicious_type	Indicator.Attribute and Indicator Tag	Malicious Type	Also added as an Indicator Tag when non-empty.	
.malicious_family	Indicator.Attribute and Indicator Tag	Malicious Family	N/A	
.campaign	Indicator.Attribute	Campaign	Added when non-empty.	
.current_status or top-level .status	Indicator.Attribute	Current Status	N/A	
.kill_chain	Indicator.Attribute	Kill Chain	Added when non-empty.	
.platform	Indicator.Attribute	Platform	Added when non-empty.	
.TTP	Indicator.Attribute	QAX TTP	Added when non-empty.	
.alert_name	Indicator Tag	Tag name	Added when non-empty.	

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	2 minute
Indicators	5
Indicator Attributes	30

Change Log

- **Version 1.0.0**
 - Initial release