

# ThreatQuotient



## **SITE CDF**

**Version 1.0.0**

March 19, 2024

## **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](https://support.threatq.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..... 10

    SITE Import..... 10

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 © 2024 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:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

# Introduction

The SITE CDF for ThreatQ enables the automatic ingestion of IOCs from SITE (Saudi Information Technology Company) database.

The integration provides the following feed:

- **SITE Import** - ingests IOCs from SITE exports.

The integration ingests indicator type system objects.

# Prerequisites

The following is required to run this integration:

- a SITE Custom token

# 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 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.

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
Export ID	Enter the SITE export that the integration should ingest into the ThreatQ platform.
Customer Token	Enter your SITE Customer Token.

< SITE Import



Disabled ☐ Enabled ☐

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

Export ID

Customer Token

Set indicator status to...

Active

Run Frequency

Every 24 Hours

Next scheduled run: 2024-03-15 10:05am (-04:00)

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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

## SITE Import

The SITE Import feed ingests IoCs from your specified SITE export.

GET [https://intel.site.sa/api/v1/threat-intelligence/export/{EXPORT\\_ID}/?token={CUSTOMER\\_TOKEN}](https://intel.site.sa/api/v1/threat-intelligence/export/{EXPORT_ID}/?token={CUSTOMER_TOKEN})

### Sample Response:

```
[
  {
    "Created": "2023-09-26 00:00:25-00:00",
    "ID": 1581,
    "Modified": "2023-11-26 04:34:44",
    "Severity": "High",
    "Tags": [
      {
        "name": "Associated",
        "value": "Historical Typosquat Similarity - Typo or Homograph"
      },
      {
        "name": "Threat Type",
        "value": "Banking"
      },
      {
        "name": "Description",
        "value": "Information stealer focusing on theft of stored password and cryptocurrency wallet data"
      },
      {
        "name": "Kill Chain",
        "value": "Stage1"
      },
      {
        "name": "Malware Family",
        "value": "Loki Bot"
      },
      {
        "name": "Role",
        "value": "Command and control location used by malware"
      }
    ],
    "Type": "FQDN",
    "Value": "ukchevron.com"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Value	Indicator.Value	.Type	.Created	ukchevron.com	N/A
.Tags[].Value	Indicator.Attribute	.Tags[].Name	.Created	Banking	N/A
.Severity	Indicator.Attribute	Severity	.Created	High	Updated at ingestion.

# 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	9 minutes
Indicators	15,255
Indicator Attributes	112,052

# Change Log

- Version 1.0.0
  - Initial release