ThreatQuotient

ThreatMiner Operation Guide

Version 1.0.1

August 30, 2022

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email:	support@threatq.com
Web:	support.threatq.com
Phone:	703.574.9893

Contents

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.

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 3.6.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/threatminer-operation

Introduction

The ThreatMiner operation for ThreatQ provides enrichment data for indicators.

The operation provides the following actions based on indicator type:

- **IP DNS Lookup** - returns WHOIS information for an IP or FQDN including related name servers, network CIDR Blocks, registrant, ASN, Emails and more.
- **Hash Lookup** - returns WHOIS information, emails, related network traffic, domains, hosts, mutants, registry keys and anti-virus Detections.
- **Email Lookup** - returns related domains associated with emails.
- **Samples Lookup** - returns related APT notes and samples.

The operation is compatible with the following indicator types:

- Email Address
- Filename
- FQDN
- IP Address
- MD5
- Mutex
- Registry Key
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- User-Agent
- URL Path

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 operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
IP DNS Lookup	WHOIS information for an IP or FQDN including related name servers, network CIDR Blocks, registrant, ASN, Emails and more.	Indicators	IP Address, FQDN
Hash Lookup	WHOIS information, emails, related network traffic, domains, hosts, mutants, registry keys and anti-virus Detections.	Indicators	MD5, SHA-1, SHA-256, SHA-384, SHA-512
Email Lookup	Related domains associated with emails.	Indicators	Email Address
Sample Lookup	Related APT notes and samples.	Indicators	Filename, Mutex, Registry Key, URL Path, User-agent

Change Log

- **Version 1.0.1**
  - N/A
- **Version 1.0.0**
  - Initial release