ThreatQuotient

AlienVault OTX CDF User Guide

Version 2.0.1

January 16, 2024

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	2.0.1
Compatible with ThreatQ Versions	>= 4.4.0
Support Tier	ThreatQ Supported

Introduction

AlienVault OTX is the world’s largest open threat intelligence community, enabling collaborative defense with actionable, community-powered threat data. These feed ingests data from AlienVault's Open Threat Exchange.

The CDF provides the following feed:

- **AlienVault OTX -** returns responses is a plain text list of CSV-like values, using `#`'s as separators.

The integration ingests indicators 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. The feed will be added to the integrations page. You will still need to configure and then enable the feed.

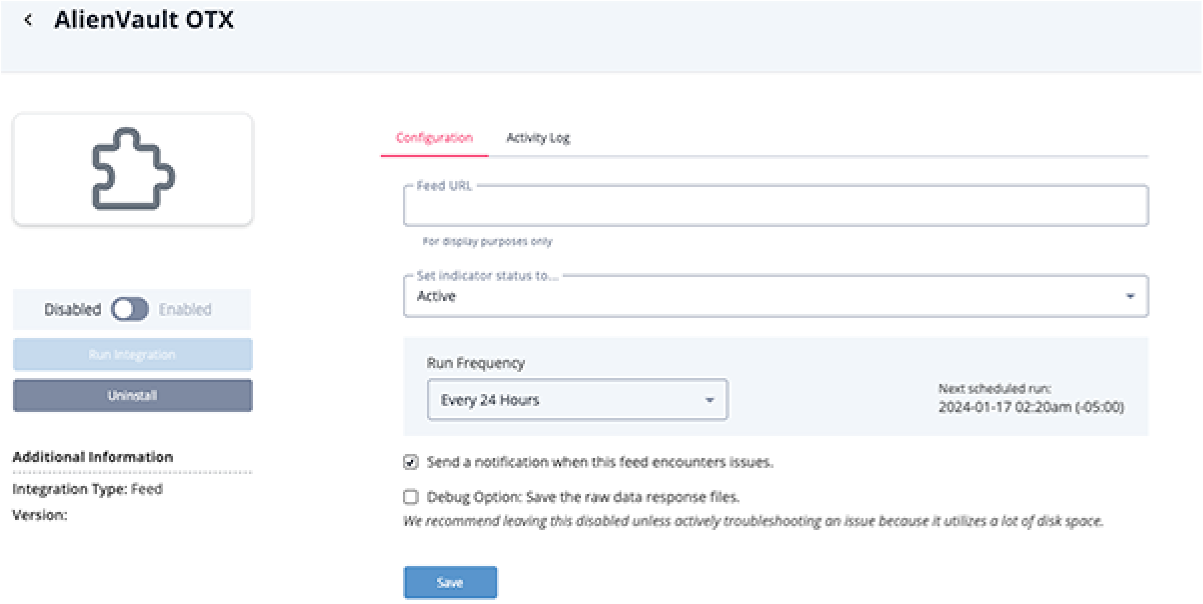
Configuration

> 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 **OSINT** option from the *Category* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Feed URL	Displays the endpoint polled by this feed. This field is for display purposes only.



AlienVault OTX

Configuration | Activity Log

Feed URL

For display purposes only

Set indicator status to...: Active

Run Frequency: Every 24 Hours

Next scheduled run: 2024-01-17 02:20am (-05:00)

☑ 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.

Additional Information

Integration Type: Feed

Version:

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

AlienVault OTX

`GET https://reputation.alienvault.com/reputation.data`

The response is a plain text list of CSV-like values, using `#`'s as separators:

```
46.4.123.15#4#2#Malicious Host#DE##51.2993011475,9.49100017548#3
49.143.32.6#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
45.248.192.48#4#3#Malicious Host#IN#Sikar#27.6166992188,75.1500015259#3
100.27.42.243#4#2#Malicious Host#US#Ashburn#39.0480995178,-77.4728012085#3
36.27.208.157#4#2#Malicious Host#CN##30.2936000824,120.161399841#3
106.13.17.16#4#2#Malicious Host#CN##39.9289016724,116.388298035#3
118.89.65.15#4#2#Malicious Host#CN#Beijing#39.9287986755,116.388900757#3
...
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
0 (first token)	Indicator.Value	IP Address	46.4.123.15	N/A
1 (second token)	Indicator.Attribute	AlienVault Reliability	4	N/A
2 (third token)	Indicator.Attribute	AlienVault Threat Level	2	Updates at ingestion.
3 (fourth token)	Indicator.Attribute	Description	Malicious Host	Split on `;`
4 (fifth token)	Indicator.Attribute	Country	CN	N/A
5 (sixth token)	Indicator.Attribute	City	Beijing	N/A
7 (eighth token)	Indicator.Attribute	AlienVault Revision	3	Split on `;`

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.

AlienVault OTX

METRIC	RESULT
Run Time	2 minutes
Indicator	1,595
Indicator Attributes	8,903

Change Log

- **Version 2.0.1**
  - Added ingest rules to the `AlienVault Threat Level` attribute. This attribute value will now be updated upon ingestion instead of duplicated.
- **Version 2.0.0**
  - Removed API Key usage.
- **Version 1.0.0**
  - Initial release