ThreatQuotient

AlienVault OTX CDF Guide

Version 2.0.0

March 31, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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

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.

Contents

Versioning

- Current integration version: 2.0.0
- Supported on ThreatQ versions >= 4.4.0

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.

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 **OSINT** 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 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.

5. Review the **Settings** configuration, 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
...
```

ThreatQ 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	N/A
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

AlienVault OTX

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

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.

Change Log

- **Version 2.0.0**
  - Removed API Key usage.
- **Version 1.0.0**
  - Initial release