ThreatQuotient

AlienVault OTX Pulse CDF

Version 1.2.0

June 17, 2025

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	1.2.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

AlienVault Open Threat Exchange is a Threat Intelligence sharing community provided at no cost to users, who are encouraged (but not required to share) intel information with other members. Users can subscribe to certain members to consume the intel that they publish.

The integration provides the following feed:

- **AlienVault OTX Pulse -** ingests indicators from user-subscribed pulses.

The integration ingests the following object types:

- Adversaries
- Attack Patterns
- Events
    - Event Attributes
- Indicators
    - Indicator Attributes

Prerequisites

The following is required to run the integration:

- AlienVault API Key
- MITRE ATT&CK Attack Patterns must have already been ingested by a previous run of the feeds included with the MITRE ATT&CK CDF integration in order for the MITRE TIDs to be extracted and mapped to the corresponding MITRE ATT&CK attack patterns. The individual feeds included with the MITRE ATT&CK CDF are:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE ICS ATT&CK

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:

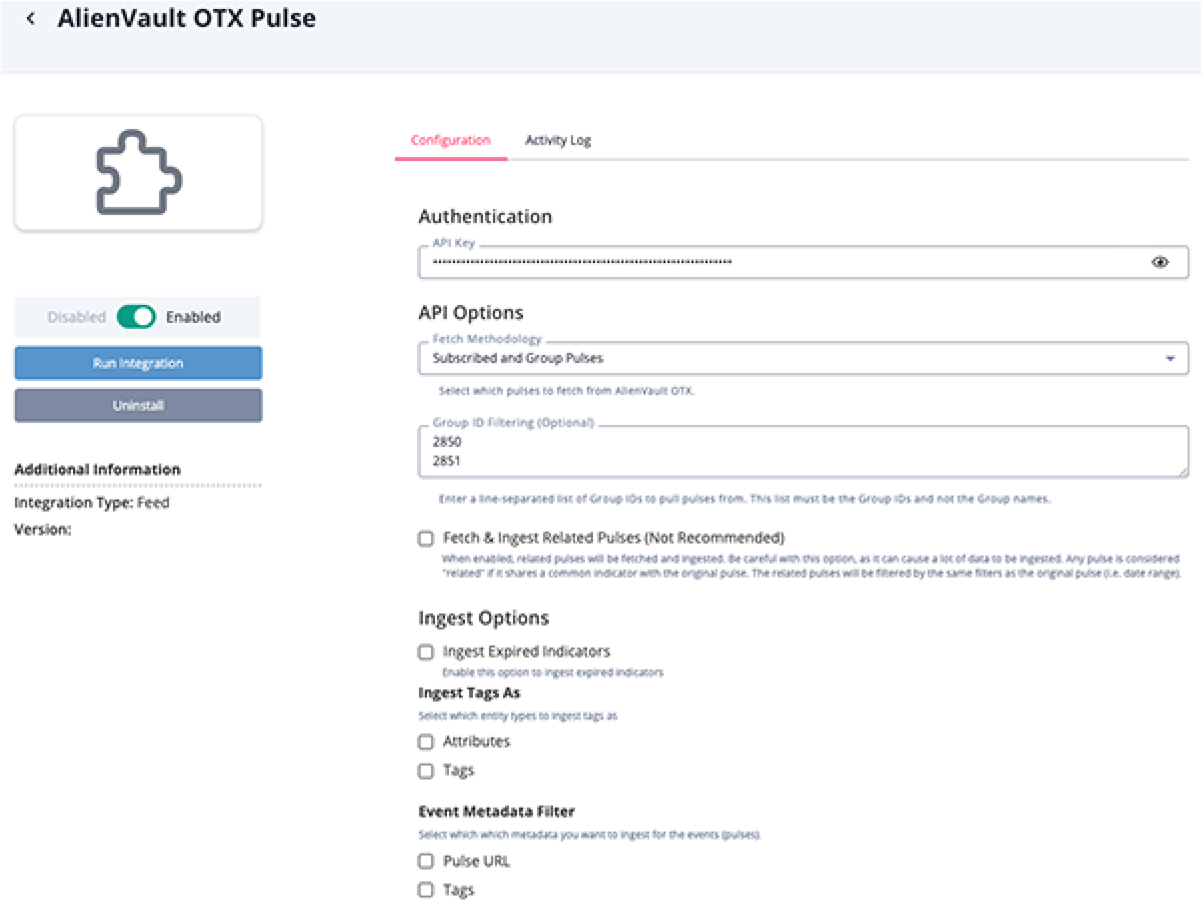
1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).

   > 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	Your AlienVault account API Key.
Fetch Methodology	Select which pulses to fetch from AlienVault OTX. Options include: ◦ Both Subscribed and Group Pulses (default) ◦ Only Group Pulses
Group ID Filtering	Enter a line-separated list of Group IDs to pull pulses from. This list must be the Group IDs and not the Group names.
Fetch & Ingest Related Pulses	Enable this option to fetch and ingest related pulses. ⚠ ThreatQuotient does not recommend enabling this parameter as it can result in ingestion of a large amount of data. Any pulse is considered "related" if it shares a common indicator with the original pulse. The related pulses will be filtered by the same filters as the original pulse (i.e. date range).
Ingest Expired Indicators	Enable this parameter to ingest expired indicators. This parameter is disabled by default.

PARAMETER	DESCRIPTION
Ingest Tags as	Select which entity types to ingest tags as in ThreatQ platform. Options include: ◦ Attributes *(default)* ◦ Tags
Event Metadata Filter	Select which metadata to ingest for the events (pulses). Options include: ◦ Pulse URL *(default)* ◦ Tags *(default)* ◦ Related Attack Patterns *(default)* ◦ Author *(default)* ◦ Public *(default)* ◦ Target Industry *(default)* ◦ Target Country *(default)* ◦ Reference *(default)* ◦ Revision ◦ Modified At
Indicator Metadata Filter	Select which metadata to ingest for the related Indicators. Options include: ◦ Title *(default)* ◦ Description *(default)* ◦ Is Active *(default)* ◦ Access Type *(default)* ◦ Content *(default)* ◦ Role *(default)* ◦ Expiration *(default)*
Inherit Event Metadata to Indicators	Select which pieces of metadata to inherit to indicators. Options include: ◦ Tags ◦ Target Industry ◦ Target Country



‹ AlienVault OTX Pulse

Disabled ● Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration | Activity Log

Authentication

API Key: ••

API Options

Fetch Methodology: Subscribed and Group Pulses

Select which pulses to fetch from AlienVault OTX.

Group ID Filtering (Optional):
2850
2851

Enter a line-separated list of Group IDs to pull pulses from. This list must be the Group IDs and not the Group names.

□ Fetch & Ingest Related Pulses (Not Recommended)

When enabled, related pulses will be fetched and ingested. Be careful with this option, as it can cause a lot of data to be ingested. Any pulse is considered "related" if it shares a common indicator with the original pulse. The related pulses will be filtered by the same filters as the original pulse (i.e. date range).

Ingest Options

□ Ingest Expired Indicators

Enable this option to ingest expired indicators

Ingest Tags As

Select which entity types to ingest tags as

□ Attributes

□ Tags

Event Metadata Filter

Select which which metadata you want to ingest for the events (pulses).

□ Pulse URL

□ Tags

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 Pulse

The AlienVault OTX Pulse feed will fetch and ingest indicators from pulses that the authenticated user is subscribed to, whether that's a user, group, or specific pulse. The feed will ingest context such as tags, related adversaries, attack patterns, target countries, target industries, and more. This context can also be inherited to the underlying indicators within the pulse, when enabled by the user.

AlienVault OTX Pulse - `GET https://otx.alienvault.com/api/v1/pulses/subscribed`

Related Pulses (supplemental) - `GET https://otx.alienvault.com/api/v1/pulses/{{pulse_id}}/related` . The Related Pulses supplemental feed retrieves Related Pulses that have the same format as events.

Sample Response:

```
{
   "count":1734,
   "next":"https://otx.alienvault.com/api/v1/pulses/subscribed?page=2",
   "results":[
      {
         "industries":[
            "Engineering",
            "Construction"
         ],
         "tlp":"white",
         "description":"PwC\u2019s cyber security practice has worked
closely...",
         "created":"2017-04-10T16:08:17.604000",
         "tags": ["ransomware"],
         "modified":"2019-03-08T12:37:08.057000",
         "author_name":"AlienVault",
         "public":1,
         "extract_source":[
         ],
         "references":[
            "https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/
operation-cloud-hopper.html",
            "https://raw.githubusercontent.com/PwCUK-CTO/OperationCloudHopper/
master/cloud-hopper-indicators-of-compromise-v3.csv"
         ],
         "targeted_countries":[
            "Canada",
            "United States"
         ],
         "indicators":[
            {
               "indicator":"2a0da563f5b88c4d630aefbcd212a35e",
               "description":"",
               "title":"",
               "created":"2017-04-10T16:08:19",
               "content":"",
               "type":"FileHash-MD5",
               "id":18061,
                                  "is_active":1,
                                  "access_type": "public"
            },
            {
               "indicator":"uu.logon-live.com",
               "description":"",
               "title":"",
               "created":"2017-04-10T16:08:19",
               "content":"",
               "type":"hostname",
               "id":18071,
               "is_active":1,
                                  "access_type": "public"

            }
         ],
         "more_indicators":false,
         "revision":3,
         "adversary":"Stone Panda",
         "id":"58ebadf17c71a907e4d4b067",
         "name":"Updated Cloud Hopper Indicators of Compromise"
      }
   ],
   "previous": null
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].name	event.title	Event	results[].created	Updated Cloud Hopper Indicators of Compromise	N/A
N/A	event.type	Pulse	results[].created	Pulse	N/A
results[].tlp	event.tlp	TLP	results[].created	white	N/A
results[].description	event.description	N/A	results[].created	`PwC\u2019s cyber security practice has worked closely...`	N/A
results[].id	event.attribute	Pulse URL	results[].created	`https://otx.alienvault.com/api/v1/pulses/58ebadf17c71a907e4d4b067`	User-configurable. URL mapped using pulse id.
results[].modified	event.attribute	Modified At	results[].created	2019-03-08T12:37:08.057000	User-configurable. Updatable.
results[].author_name	event.attribute	Author	results[].created	AlienVault	User-configurable.
results[].public	event.attribute	Public	results[].created	True	User-configurable. True if value is 1 and False if value is 0.
results[].revision	event.attribute	Revision	results[].created	3	User-configurable. Updatable.
results[].industries[]	event.attribute/ indicator.attribute	Target Industry	results[].created	Engineering	User-configurable. Needs to be checked for both objects to be ingested as indicator attribute.
results[].targeted_ countries[]	event.attribute/ indicator.attribute	Target Country	results[].created	Canada	User-configurable. Needs to be checked for both objects to be ingested as indicator attribute.
results[].references[]	event.attribute	Reference	results[].created	https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html	User-configurable.
results[].tags[]	event.attribute/ event.tag	Tag/ N/A	results[].created/ N/A	ransomware	User-configurable. `Tags` checked in `Event Metadata Filter` and at least one option checked in `Ingest Tags As`.
results[].adversary	adversary.name	Adversary	N/A	Stone Panda	
results[].attack_ids[]	attack pattern.value	Attack Pattern	N/A	T1495 - Firmware Corruption	User-configurable. ID(`T1495`) mapped to an existing Attack

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					Patterns in ThreatQ(`T1495 - Firmware Corruption`).
results[].indicators[].indicator	indicator.value	Indicator	results[].indicators[].created	2a0da563f5b88c4d630aefbcd212a35e	
results[].indicators[].type	indicator.type	IOC type	results[].indicators[].created	MD5	IOC type mapped like in the mapping below. (`FileHash-MD5` - `MD5`)
results[].event.tlp	indicator.tlp	N/A	results[].indicators[].created	white	
results[].indicators[].title	indicator.attribute	Title	results[].indicators[].created	N/A	User-configurable.
results[].indicators[].description	indicator.attribute	Description	results[].indicators[].created	N/A	User-configurable.
results[].indicators[].is_active	indicator.attribute	Is Active	results[].indicators[].created	True	User-configurable. Updatable. True if value is 1 and False if value is 0.
results[].indicators[].access_type	indicator.attribute	Access Type	results[].indicators[].created	public	User-configurable.
results[].indicators[].content	indicator.attribute	Content	results[].indicators[].created	N/A	User-configurable.
results[].indicators[].role	indicator.attribute	Role	results[].indicators[].created	N/A	User-configurable.
results[].indicators[].expiration	indicator.attribute	Expiration	results[].indicators[].created	N/A	User-configurable.
results[].tags	indicator.attribute/ indicator.tag	Tag/ N/A	results[].indicators[].created/ N/A	ransomware	User-configurable. `Tags` checked in `Event Metadata Filter` and at least one option checked in `Ingest Tags As`.
Related Pulses (Supplemental)	Related Event		results[].created		User-configurable. Same format as Event.See `Related Pulses(Supplemental)` below.

AlienVault to ThreatQ Indicator Mapping

ThreatQuotient provides the following AlienVault to ThreatQ indicator mapping:

ALIENVAULT	THREATQ
CIDR	CIDR Block
CVE	CVE
domain	FQDN
email	Email Address
hostname	FQDN
IPv4	IP Address
IPv6	IPv6 Address
FileHash-IMPHASH	Fuzzy Hash
FileHash-MD5	MD5
FileHash-PEHASH	Fuzzy Hash
FileHash-SHA1	SHA-1
FileHash-SHA256	SHA-256
FilePath	File Path
Mutex	Mutex
URL	URL
URI	URL Path
YARA	yara

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	1 minute
Adversaries	3
Attack Pattern	73
Events	10
Event Attributes	160
Indicators	153
Indicator Attributes	512

Change Log

- **Version 1.2.0**
    - Added support for fetching pulses from groups.
    - Added support for parsing Attack IDs as Attack Patterns.
    - Added attribution/metadata filtering.
    - Added support to ingest tags as Tags and/or Attributes.
    - Added support for inheriting context to related indicators.
    - Added ability to skip expired indicators.
    - Added the following configuration parameters:
        - **Fetch Methodology** - select which pulses to fetch from AlienVault OTX.
        - **Group ID Filtering** - enter a line-separated list of Group IDs to pull pulses from.
        - **Ingest Expired Indicators** - determine if the feed will ingest expired indicators.
        - **Ingest Tags as** - select how to ingest Tags into the ThreatQ platform.
        - **Event Metadata Filter** - select which metadata to ingest for the events (pulses).
        - **Indicator Metadata Filter** - select which metadata you want to ingest for the related indicators.
        - **Inherit Event Metadata to Indicators** - select which pieces of metadata to inherit to indicators.
    - Updated the minimum ThreatQ version to 5.12.1.
- **Version 1.1.0**
    - Added the option to prevent ingestion of related pulses (events)
- **Version 1.0.0**
    - Initial release