

ThreatQuotient



AlienVault OTX Pulse Connector Guide

Version 1.1.0

Friday, June 26, 2020

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.

Copyright © 2020 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.

Last Updated: Friday, June 26, 2020

Contents

AlienVault OTX Pulse Connector Guide	1
Warning and Disclaimer	2
Contents	3
Versioning	4
Introduction	5
Installation	6
Configuration	7
ThreatQ Mapping	8
Indicator Types Mapping	13
Changelog	14

Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions: 4.17.0 or higher

Introduction

AlienVault Open Threat Exchange is a Threat Intelligence sharing community, provided at no cost to users. Users 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 AlienVault OTX Pulse connector retrieves pulses from `https://otx.alienvault.com/api/v1/pulses/subscribed`.

Installation

Perform the following steps to install the connector:



The same steps can be used to upgrade the connector to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the **AlienVault OTX Pulse** integration file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the feed 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.

The feed will be added to the **OSINT** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API Key	The AlienVault account API key.
Ingest Related Pulses	When checked, ingests related pulses. <div> This option is not checked by default.</div>

5. Click on **Save Changes**.
6. Click on the toggle switch next to the feed name to enable it.

ThreatQ Mapping

The request will contain a parameter called `modified_since` in iso format datetime (UTC) that will cause the api to only include pulses whose modified time is greater than the specified parameter. This value will be automatically set to the datetime of the last feed run. The default frequency of this feed is 24 hours, so the value supplied to the api will be the time at which the feed begins execution minus 24 hours.

The response is in json format and contains a list of pulses. For each pulse, an api call occurs to load the related pulses (https://otx.alienvault.com/api/v1/{pulse_id}/related). The response has the same format as the initial call. See the example below:

```
{
  "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/PwC-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
    }
}
```

ThreatQ provides the following default mapping for the connector:

AlienVault Pulse Key	ThreatQ Entity	ThreatQ Name
Event		
name	event.title	
event.type	Pulse	
tlp	event.tlp	TLP
description	event.description	
created	event.published_at	
created	event.happened_at	
id	event.attribute	Pulse URL
modified	event.attribute	Modified Time
author_name	event.attribute	Author
public	event.attribute	Public
revision	event.attribute	Revision
industries	event.attribute	Target Industry
targeted_countries	event.attribute	Target Country
references	event.attribute	Reference
tags	event.attribute	Tag
adversary	adversary.name	Adversary
indicator		
indicators[].value	indicator.value	

AlienVault Pulse Key	ThreatQ Entity	ThreatQ Name
indicators[].type	indicator.type	
event.tlp	indicator.tlp	
indicators[].indicator	indicator.published_at	
indicators[].title	indicator.attribute	Title
indicators[].description	indicator.attribute	Description
indicators[].is_active	indicator.attribute	Is Active
indicators[].access_type	indicator.attribute	Access Type
indicators[].content	indicator.attribute	Content
indicators[].role	indicator.attribute	Role
indicators[].expiration	indicator.attribute	Expiration
Related Pulses		

Indicator Types Mapping

The mapping between the indicator types in AlienVault and ThreatQ are displayed below:

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

Changelog

- **Version 1.1.0**
 - Added a Ingest Related Pulses checkbox option to feed configuration page that provides the option of preventing related pulses (events) ingestion.
- **Version 1.0.0**
 - Initial release