ThreatQuotient

AlienVault OTX Action Guide

Version 1.0.0

April 04, 2023

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.

Copyright © 2023 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.

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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/alienvault-otx-action

Introduction

The AlienVault OTX action enables the automatic enrichment of IOCs using AlienVault OTX.

The action can perform the following function:

- **AlienVault OTX** - Performs IOC lookups in AlienVault for enrichment and fetches file analysis context.

The action is compatible with the following indicator types:

- IP Address
- IPv6 Address
- FQDN
- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512
- URL
- CVE

The action returns the following enriched system objects:

- Indicators
  - Indicator Attributes
- Adversaries
- Tags

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following indicator objects:
  - IP Address
  - IPv6 Address
  - FQDN
  - MD5
  - SHA-1
  - SHA-256
  - SHA-384
  - SHA-512
  - URL
  - CVE

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

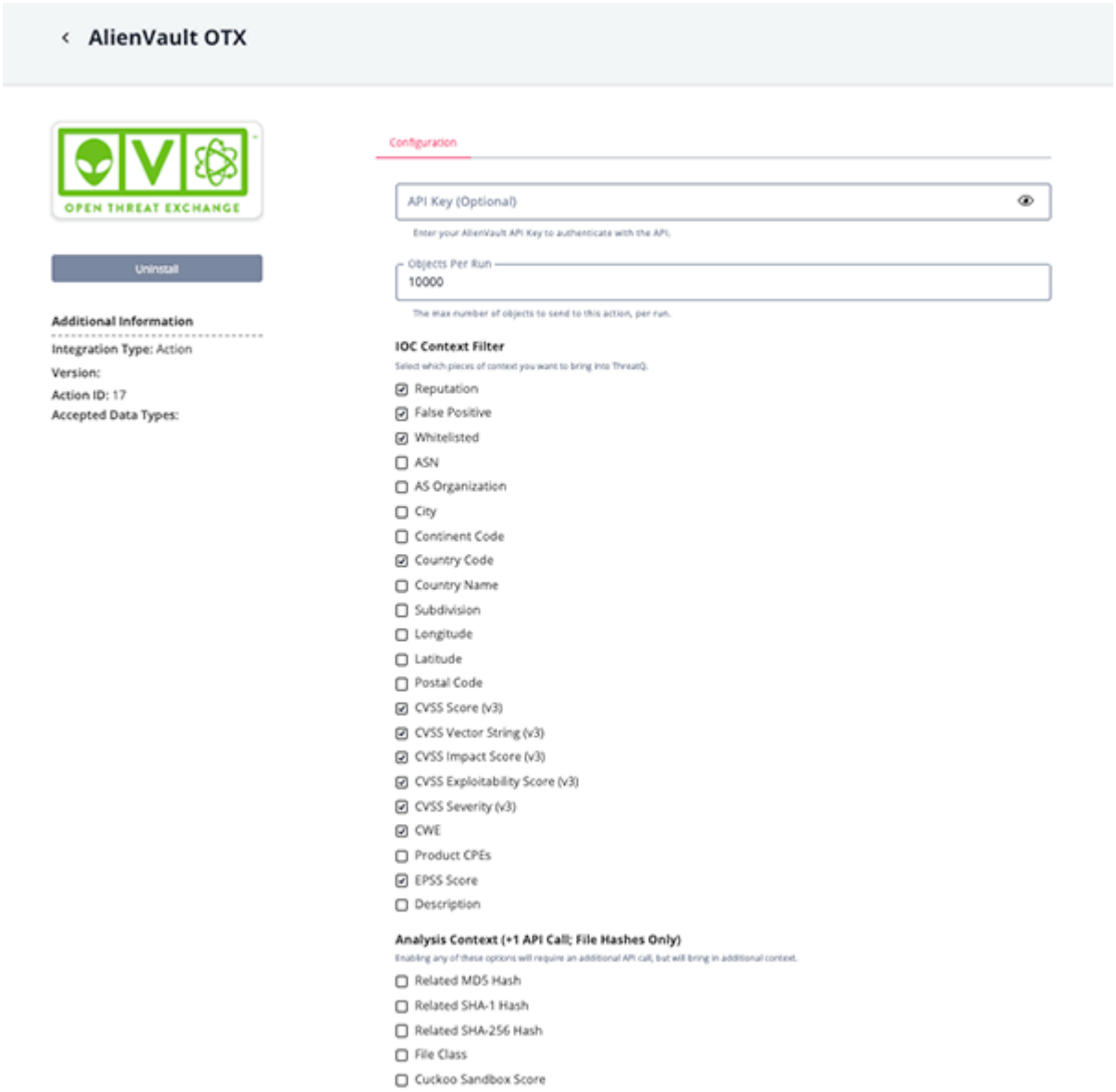
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	Enter your AlienVault API Key to authenticate with the API.
Objects Per Run	The max number of objects to send to this action, per run. (default: 10,000)
IOC Context Filter	Select which pieces of context you want to bring into ThreatQ.
Analysis Context (+1 API Call; File Hashes Only)	Enabling any of these options will require an additional API call, but will bring in additional context.
Related OTX Pulse Context Filter	Select which pieces of context you want to inherit from the related OTX Pulses.

PARAMETER	DESCRIPTION
Ingest Tags As	Select which entity type you'd like tags to be ingested as. (default: Tags)



5. Review any additional settings, make any changes if needed, and click on **Save**.

Action Functions

The action provides the following function:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
AlienVault OTX	Performs IOC lookups in AlienVault for enrichment and fetches file analysis context.	Indicators	IP Address, IPv6 Address, URL, FQDN, MD5, SHA-1, SHA-256, SHA-384, SHA-512, CVE

AlienVault OTX

The AlienVault OTX enriches an IOC using AlienVault OTX's API.

```
GET https://otx.alienvault.com/api/v1/indicators/{{ type }}/{{ value }}
```

Sample Response:


```
{
  "whois": "http://whois.domaintools.com/64.190.63.111",
  "reputation": 0,
  "indicator": "64.190.63.111",
  "type": "IPv4",
  "type_title": "IPv4",
  "base_indicator": {
    "id": 3396107990,
    "indicator": "64.190.63.111",
    "type": "IPv4",
    "title": "",
    "description": "",
    "content": "",
    "access_type": "public",
    "access_reason": ""
  },
  "pulse_info": {
    "count": 19,
    "pulses": [
      {
        "id": "6231ee27e6834a707de700ae",
        "name": "LCIA:HoneyNet:2022",
        "description": "Louisiana Cyber Investigators Alliance (LCIA): HoneyPot Suricata Log: 2022 A unified
coordinated group of federal, state, local law enforcement, as well as LA ESF-17 members, focused onsafeguarding
Louisiana's networks through collaborative vigilance and thorough investigations http://www.la-safe.org",
        "modified": "2022-10-25T16:02:05.157000",
        "created": "2022-03-16T14:03:19.241000",
        "tags": ["tsec", "tpot19", "honeypot", "la-safe.org"],
        "references": [],
        "public": 1,
        "adversary": "",
        "targeted_countries": [],
        "malware_families": [],
        "attack_ids": [],
        "industries": [],
        "TLP": "green",
        "cloned_from": null,
        "export_count": 24,
        "upvotes_count": 0,
        "downvotes_count": 0,
        "votes_count": 0,
        "locked": false,
        "pulse_source": "api",
        "validator_count": 0,
        "comment_count": 0,
        "follower_count": 0,
        "vote": 0,
        "author": {
```

```
        "username": "dm_lacia",
        "id": "132921",
        "avatar_url": "https://otx.alienvault.com/assets/images/default-avatar.png",
        "is_subscribed": false,
        "is_following": false
      },
      "indicator_type_counts": {
        "IPv4": 659879,
        "IPv6": 3
      },
      "indicator_count": 659882,
      "is_author": false,
      "is_subscribing": null,
      "subscriber_count": 202,
      "modified_text": "48 minutes ago ",
      "is_modified": true,
      "groups": [],
      "in_group": false,
      "threat_hunter_scannable": true,
      "threat_hunter_has_agents": 1,
      "related_indicator_type": "IPv4",
      "related_indicator_is_active": 0
    }
  ],
  "references": [
    "http://blog.talosintelligence.com/2022/10/threat-roundup-1007-1014.html"
  ],
  "related": {
    "alienvault": {
      "adversary": [],
      "malware_families": [],
      "industries": []
    },
    "other": {
      "adversary": [],
      "malware_families": ["Darkcomet", "Tofsee"],
      "industries": []
    }
  }
},
"false_positive": [],
"validation": [],
"asn": "AS47846 sedo",
"city_data": true,
"city": null,
"region": null,
"continent_code": "EU",
"country_code3": "DEU",
"country_code2": "DE",
"subdivision": null,
"latitude": 51.2993,
"postal_code": null,
"longitude": 9.491,
"accuracy_radius": 200,
"country_code": "DE",
"country_name": "Germany",
"dma_code": 0,
"charset": 0,
"area_code": 0,
"flag_url": "/assets/images/flags/de.png",
"flag_title": "Germany",
```

```
  "sections": [
    "general",
    "geo"
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`data.reputation`	Indicator Attribute	Reputation	N/A	`0`	N/A
`data.false_positive[]`	Indicator Attribute	False Positive	N/A	`True`	Only `True` when certain assessments are found
`data.whitelisted[]`	Indicator Attribute	Whitelisted	N/A	`True`	Only `True` when certain assessments are found
`data.asn`	Indicator Attribute	ASN	N/A	`AS01923`	Split by a space character to get the value
`data.asn`	Indicator Attribute	AS Organization	N/A	`cloudflare`	Split by a space character to get the value
`data.city`	Indicator Attribute	City	N/A	`Frankfurt`	N/A
`data.continent_code`	Indicator Attribute	Continent Code	N/A	`NA`	N/A
`data.country_code`	Indicator Attribute	Country Code	N/A	`US`	N/A
`data.country_name`	Indicator Attribute	Country	N/A	`Germany`	N/A
`data.subdivision`	Indicator Attribute	Subdivision	N/A	N/A	N/A
`data.latitude`	Indicator Attribute	Latitude	N/A	`0.12313`	N/A
`data.longitude`	Indicator Attribute	Longitude	N/A	`-9.2314`	N/A
`data.postal_code`	Indicator Attribute	Postal Code	N/A	N/A	N/A
`data.pulse_info.pulses[].tags[]`	Indicator Attribute	Tags	N/A	`lokibot`	`Tags` is checked in `Related OTX Pulse Context Filter` and `Ingested Tags As` is set to `Attributes`
`data.pulse_info.pulses[].tags[]`	Tag value	Tags	N/A	`lokibot`	`Tags` is checked in `Related OTX Pulse Context Filter` and `Ingested Tags As` is set to `Tags`
`data.pulse_info.pulses[].targeted_countries[]`	Indicator Attribute	Targeted Country	N/A	`Russia`	N/A
`data.pulse_info.pulses[].malware_families[]`	Indicator Attribute	Malware Family	N/A	`Lokibot`	N/A
`data.pulse_info.pulses[].adversary`	Adversary value	N/A	N/A	`Anonymous`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`data.pulse_info.pulses[].industries[]`	Indicator Attribute	Affected Industry	N/A	`Energy`	N/A
`data.cvssv3.cvssV3.baseScore`	Indicator Attribute	CVSS Score	N/A	`7.5`	N/A
`data.cvssv3.cvssV3.vectorString`	Indicator Attribute	CVSS Vector String	N/A	N/A	N/A
`data.cvssv3.impactScore`	Indicator Attribute	CVSS Impact Score	N/A	`2.5`	N/A
`data.cvssv3.exploitabilityScore`	Indicator Attribute	CVSS Exploitability Score	N/A	`4.5`	N/A
`data.cvssv3.cvssV3.baseSeverity`	Indicator Attribute	CVSS Severity	N/A	`HIGH`	N/A
`data.cwe`	Indicator Attribute	CWE	N/A	`CWE-123`	N/A
`data.products`	Indicator Attribute	CPE	N/A	N/A	N/A
`data.epss`	Indicator Attribute	EPSS Score	N/A	`0.9327`	N/A
`data.description`	Indicator Attribute	Description	N/A	N/A	N/A
`analysis.info.results.file_class`	Indicator Attribute	File Class	N/A	`PEXE`	N/A
`analysis.plugins.cuckoo.result.info.combined_score`	Indicator Attribute	Cuckoo Sandbox Score	N/A	`3`	N/A
`analysis.info.results.sha1`	Indicator Value	SHA-1	N/A	N/A	N/A
`analysis.info.results.md5`	Indicator Value	MD5	N/A	N/A	N/A
`analysis.info.results.sha256`	Indicator Value	SHA-256	N/A	N/A	N/A

AlienVault OTX - Get Analysis (Supplemental)

The Get Anaylsis endpoint fetches analysis information for file IOCs.

```
GET https://otx.alienvault.com/api/v1/indicators/{{ type }}/{{ value }}/analysis
```

Enriched Data

> Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

AlienVault OTX

METRIC	RESULT
Run Time	12 minutes
Indicators	973
Indicator Attributes	4,049
Adversaries	9

Known Issues / Limitations

- Not all fields are available for all IOC types. For instance, CVEs will have CVSS scores associated, but IP Address will not. Similarly, files will have analysis results while domains will not.

Change Log

- **Version 1.0.0**
  - Initial release