ThreatQuotient

AlienVault OTX Pulse Operation Guide

Version 1.0.2

April 03, 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.

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	1.0.2
Compatible with ThreatQ Versions	>= 4.20.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/alienvault-otx-pulse-operation

Introduction

TheThreatQuotient forAlienVault OTXPulse Operation allows a ThreatQ user to query AlienVault for any indicator matches. If matches are found, related indicators will be returned, as well as any related pulses.

The operation provides the following action:

- **Query** - queries AlienVault OTX for any metadata, related indicators, and related pulses.

The operation is compatible with the following indicator types:

- CVE
- FQDN
- IP Address
- MD5
- SHA-1
- SHA-256
- URL

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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

PARAMETER	DESCRIPTION
Token	Your AlienVault OTX Pulse API Key.

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.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Queries AlienVault OTX for any metadata, related indicators, and related pulses.	Indicator	CVE, FQDN, IP Address, MD5, SHA-1, SHA-256, URL

Query

The Query action queries AlienVault OTX for any metadata, related indicators, and related pulses.

```
GET https://otx.alienvault.com/api/v1/indicators/{{TYPE_MAP[indicator_type]}}/{{indicator}}/{{section}}
```

Sample Response:

```
{
"sections": [
    "general",
    "nids_list",
    "malware"
],
"mitre_url": "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39129",
"nvd_url": "https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-39129",
"indicator": "CVE-2022-39129",
"type_title": "CVE",
"base_indicator": {},
"pulse_info": {
    "count": 0,
    "pulses": [],
    "references": [],
    "related": {
        "alienvault": {
            "adversary": [],
            "malware_families": [],
            "industries": []
        },
        "other": {
            "adversary": [],
            "malware_families": [],
            "industries": []
        }
    }
},
"false_positive": [],
"cve": "CVE-2022-39129",
"cvss": {},
"cvssv2": {},
"cvssv3": {
    "cvssV3": {
        "attackComplexity": "LOW",
        "attackVector": "LOCAL",
        "availabilityImpact": "HIGH",
        "baseScore": 5.5,
        "baseSeverity": "MEDIUM",
        "confidentialityImpact": "NONE",
        "integrityImpact": "NONE",
        "privilegesRequired": "LOW",
        "scope": "UNCHANGED",
        "userInteraction": "NONE",
        "vectorString": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H",
            "version": "3.1"
        },
        "exploitabilityScore": 1.8,
        "impactScore": 3.6
    },
    "configurations": {
        "CVE_data_version": "4.0",
        "nodes": [
            {
                "children": [
                    {
                        "children": [],
                        "cpe_match": [
                            {
                                "cpe23Uri": "cpe:2.3:o:google:android:10.0:*:*:*:*:*:*:*",
                                "cpe_name": [],
                                "vulnerable": true
                            }
                        ],
                        "operator": "OR"
                    }
                ],
                "cpe_match": [],
                "operator": "AND"
            }
        ]
    },
    "cwe": "CWE-787",
    "products": [],
    "seen_wild": false,
    "references": [
        {
            "external_source": "MISC",
            "href": "https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006",
            "type": null,
            "tags": [
                "Vendor Advisory"
            ],
            "name": "https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006"
        }
    ],
    "description": "In face detect driver, there is a possible out of bounds write due to a missing bounds check.
This could lead to local denial of service in kernel.",
    "date_modified": "2022-12-07T15:57:00",
    "date_created": "2022-12-06T07:15:00",
    "exploits": [],
    "epss": null
}
```

ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.references[].href`	Indicator Attribute	Reference	N/A	https://www.unisoc.com/en_us/secy/announcementDetail/1599588060988411006	N/A
`.nvd_url`	Indicator Attribute	NVD Reference	N/A	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-39129	N/A
`.mitre_url`	Indicator Attribute	Mitre Reference	N/A	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39129	N/A
`.country_name`	Indicator Attribute	Country	N/A	N/A	N/A
`.city`	Indicator Attribute	City	N/A	N/A	N/A
`.asn`	Indicator Attribute	ASN	N/A	N/A	N/A
`.cvss.score`	Indicator Attribute	CVSS Score	N/A	N/A	N/A
`.cvssv3.exploitabilityScore`	Indicator Attribute	CVSSv3 Exploitability Score	N/A	1.8	N/A
`.cvssv3.impactScore`	Indicator Attribute	CVSSv3 Impact Score	N/A	3.6	N/A
`.groups[].name`	Indicator Attribute	Group	N/A	N/A	N/A
`.targeted_countries[]`	Indicator Attribute	Targeted Country	N/A	N/A	N/A
`.industry[]`	Indicator Attribute	Industry	N/A	N/A	N/A
`.tag[]`	Indicator Attribute	Tag	N/A	N/A	N/A
`.products[]`	Indicator Attribute	Exploited Product	N/A	N/A	N/A
`.passive_dns[].hostname`	Related Indicator	FQDN	N/A	N/A	N/A
`.url_list[].url`	Related Indicator	URL	N/A	N/A	N/A
`.analysis.plugins.metaextract.results.urls[]`	Related Indicator	URL	N/A	N/A	N/A

Type Mapping

The following table provides threat intelligence type mapping for the integration.

KEY	VALUE
IP Address	IPv4
FQDN	domain
URL	url
MD5	file
SHA-1	file
SHA-256	file
CVE	cve

Change Log

- **Version 1.0.2**
    - Updated dependencies required by the operation.
- **Version 1.0.1**
    - Added improved Proxy support.
- **Version 1.0.0**
    - Initial release