ThreatQuotient

Pulsedive Operation User Guide

Version 1.0.0

November 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	1.0.0
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

The Pulsedive operation enriches Indicators (of type FQDN, IP Address, IPv6 Address, URL and CVE), Malware objects, Intrusion Sets, Adversaries, Tools, Vulnerabilities, Events and Incidents.

The operation provides the following action:

- **Query -** queries Pulsedive for any context it has on the given object.

The operation is compatible with the following system objects:

- Adversaries
- Events
- Indicators
    - IP Address
    - IPv6 Address
    - FQDN
    - URL
    - CVE
- Malware
- Tools
- Vulnerabilities
- Incident
- Intrusion Set

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
API Key	Your Pulsedive 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 Pulsedive for any context it has on the given object.	Adversaries, Events, Indicators, Malware, Tools, Vulnerabilities, Incident, Intrusion Set	Indicators - IP Address, IPv6 Address, FQDN, URL, CVE

> The operation will utilize different endpoints based on the type of system object.

Indicators

The following endpoint is used to query Indicators (except for CVE).

`GET https://pulsedive.com/api/info.php?indicator=<indicator_value>`

ThreatQuotient provides the following default mapping for this endpoint:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.risk	Indicator.Attribute	Risk	high	N/A
.riskfactors[].description	Indicator.Attribute	Risk Factor	['registration']	N/A
.attributes.hosttype[]	Indicator.Attribute	Host Type	['Name Server']	N/A
.attributes.protocol[]	Indicator.Attribute	Protocol	['DNS', 'FTP']	N/A
.attributes.technology[]	Indicator.Attribute	Technology	['Apache']	N/A
.attributes.port[]	Indicator.Attribute	Port	['21']	N/A
.properties.geo.country	Indicator.Attribute	Country	Brazil	N/A
.properties.geo.countrycode	Indicator.Attribute	Country Code	BR	N/A
.properties.geo.org	Indicator.Attribute	Organization	Mandic	N/A
.properties.dns.ptr	Indicator.Value	FQDN	mail01.emidhost4.com.br	Applicable for `ip`, `ipv6` indicators. Added with Status `Indirect`
.properties.dns.a	Indicator.Value	IP Address	12.12.12.12	Applicable for `domain` indicator. Added with Status `Review`
.properties.dns.ns[]	Indicator.Value	FQDN	['aspx.1.google.com']	Applicable for `domain` indicator. Added with Status `Indirect`
.properties.dns.mx[]	Indicator.Value	FQDN	['aspx.1.google.com']	Applicable for `domain` indicator. Added with Status `Indirect`
.properties.geo.asn	Indicator.Value	ASN	123445	Trimmed 'AS' if present in the value. Added with Status `Review`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.threats[].name	Indicator.Attribute	Pulsedive `.threats[].category`	Pulsedive Phishing	if .threats[].category == 'vulnerability' will be ingested just as Indicator
.threats[].name	Indicator.Value	CVE	CVE-1999-123455	Only if .threats[].category == 'vulnerability'. Threat with category 'vulnerability' is ingested as Related Indicator. Status is `Review`
.feeds[].name	Indicator.Attribute	Feed Name	Zeus Bad IPs	N/A
.feeds[].category	Indicator.Attribute	Feed Category	malware	N/A
.feeds[].organisation	Indicator.Attribute	Feed Organizaton	Org	N/A
.properties.whois.registrant country	Indicator.Attribute	Registrant Country	RO	(*)
.properties.whois.registrant name	Indicator.Attribute	Registrant Name	Comp	(*)
.properties.whois.registrant phone	Indicator.Attribute	Registrant Phone	+07124827845354	(*)
.properties.whois.registrant organization	Indicator.Attribute	Registrant Organization	Org.net	(*)
.properties.whois.registrant postal code	Indicator.Attribute	Registrant Postal Code	402342	(*)
.properties.whois.registrant state/province	Indicator.Attribute	Registrant State/ Province	CA	(*)
.properties.whois.registrant street	Indicator.Attribute	Registrant Street	HighLvl N1	(*)
.properties.whois.registrant email	Indicator.Attribute	Registrant Email	dsefd@comp.org	(*)

* All `.properties.whois.registrant <name>` apply in case the API request was made for an FQDN or URL indicator type

Pulsedive to ThreatQ Indicator Mapping

FEED DATA PATH	THREATQ ENTITY
domain	FQDN
ip	IPv4 Address
ipv6	IPv6 Address
ulr	URL
vulnerability	CVE

Related Indicators

The following endpoint is used to query Related Indicators.

`GET https://pulse- dive.com/api/info.php?<indicator=ndicator_value>&get=links`

ThreatQuotient provides the following default mapping for this endpoint:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.Redirects[].indicator	Indicator.Value	.Redirects[].type mapped to `Pulsedive Indicator Types Mapping.Pulsedive Type`	alvoportas.com.br	(**)
.SSL Certificate Domains[].indicator	Indicator.Value	.SSL Certificate Domains[].type mapped to `Pulsedive Indicator Types Mapping.Pulsedive Type`	accessa.com.br	(**)
.Reverse DNS[].indicator	Indicator.Value	.Reverse DNS[].type mapped to `Pulsedive Indicator Types Mapping.Pulsedive Type`	mail01.emidhost4.com.br	(**)
.Active DNS[].indicator	Indicator.Value	.Active DNS[].indicator.type mapped to `Pulsedive Indicator Types Mapping.Pulsedive Type`	alvoportas.com.br	(**)
.Mail Server[].indicator	Indicator.Value	.Mail Server[].type mapped to `Pulsedive Indicator Types Mapping.Pulsedive Type`	mail01.emidhost4.com.br	(**)
.Sources[].indicator	Indicator.Value	.Sources[].type mapped to `Pulsedive Indicator Types Mapping.Pulsedive Type`	mail01.emidhost4.com.br	(**)
.Related URLs[].indicator	Indicator.Value	.Related URLs[].type mapped to `Pulsedive Indicator Types Mapping.Pulsedive Type`	http://pulsedive.com	(**)

> ** Indicators types are created based on the .type mapped using the Pulsedive Indicator Types Mapping. FQDN indicators are ingested with Indirect status while the rest are ingested with Review.

Other Objects & CVE Indicators

The following endpoint is used to query all other object types and CVE Indicators.

`GET https://pulse- dive.com/api/info.php?threat=<object_value>`

ThreatQuotient provides the following default mapping for this endpoint:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
threat.risk	Object.Attribute	Risk	low	N/A
.threatq.stamp_added	Object Attribute	Linked At	1999-20-20 12:12:12	N/A
.threat.wikisummary + .threat.descripton	Object.Description		some desc	The concatenated value of the two keys is appended to the object description with the header as 'Pulsedive Wiki Summary'
.threat.news[].link	Object.Attribute	News Link	http:// newslnk.com	N/A
.threat.news[].title	Object.Attribute	News Title	Malwarebytes Labs	N/A
.wikireference	Object Attribute	Reference	Reference Data	N/A

> `Object` from above table refers to current ThreatQ Object this Operation runs on. All available objects are defined in the above 'Applies To'

Related Indicators of an Object

The following endpoint is used to query Related Indicators of an Object.

`GET https://pulsedive.com/api/info.php?threat= &get=links`

ThreatQuotient provides the following default mapping for this endpoint:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.results[].indicator	Indicator.Value	.results[].type	zeus	(*)

> * All `.properties.whois.registrant <name>` apply in case the API request was made for an FQDN or URL indicator type

Change Log

- **Version 1.0.0**
  - Initial release