ThreatQuotient

PassiveTotal CDF User Guide

Version 2.0.1

August 14, 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	2.0.1
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported

Introduction

The PassiveTotal CDF retrieves data from RiskIQ Community API using the following feeds:

- **PassiveTotal** - ingests project data from the RiskIQ Community API.
- **PassiveTotal Artifacts** - ingests related Indicator `Artifacts` for each PassiveTotal `Project`.
- **PassiveTotal Bulk Artifacts Enrichment** - retrieves enrichment data for each related Indicator `Artifact` returned by the PassiveTotal Artifacts endpoint.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes

PassiveTotal publishes information grouped as `Projects`. PassiveTotal's `Artifact` endpoint is called for each `Project`, retrieving associated indicators (called artifacts in PassiveTotal). These associated Indicators are enriched via PassiveTotal's Bulk Artifact Enrichment endpoint. ThreatQ ingests these Indicators with the `Project` context as Attributes.

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. If prompted, select the individual feeds to install and click **Install**. 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 **Commercial** 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
Username	The PassiveTotal account Username.
API Key	The PassiveTotal account 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.

ThreatQ Mapping

PassiveTotal's API endpoints use HTTP basic authentication.

PassiveTotal

The PassiveTotal feed ingests project data from the RiskIQ Community API.

`GET https://api.passivetotal.org/v2/project`

Sample Response:


```
{
    "success": true,
    "results": [
        {
            "active": true,
            "can_edit": false,
            "collaborators": [],
            "created": "2016-11-16T05:55:00.425000",
            "creator": "mike.wyatt@riskiq.net",
            "description": "Browser exploit kit used for distribution of
malware to vulnerable computers",
            "featured": true,
            "guid": "182d1a3a-5be3-dad4-76b8-67f8f79e8488",
            "link": null,
            "links": {
                "artifact": "/v2/artifact?project=182d1a3a-5be3-
dad4-76b8-67f8f79e8488",
                "self": "/v2/project?project=182d1a3a-5be3-
dad4-76b8-67f8f79e8488",
                "tag": "/v2/project/tag?project=182d1a3a-5be3-
dad4-76b8-67f8f79e8488"
            },
            "name": "RIG Exploit Kit",
            "organization": "riskiq",
            "owner": "riskiq",
            "subscribers": [
                "yonathan@riskiq.net",
                "zann@riskiq.net"
            ],
            "success": true,
            "tags": [
                "crimeware",
                "exploit kit",
                "rig"
            ],
            "visibility": "community"
```

```
        },
        ...
    ]
}
```

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[].active	Report.Attribute	Active	.results[].created	true	Formatted as a title-cased string
.results[].name / .results[].guid	Report.Value	N/A	.results[].created	RIG Exploit Kit	Formatted as `{{.results[].name}} - {{.results[].guid}}`
.results[].tags[]	Report.Attribute	Tag	.results[].created	crimeware	N/A
.results[].visibility	Report.Attribute	Visibility	.results[].created	community	N/A
.results[].organization	Report.Attribute	Organization	.results[].created	riskiq	N/A
.results[].owner	Report.Attribute	Owner	.results[].created	riskiq	N/A
.results[].featured	Report.Attribute	Featured	.results[].created	true	N/A
.results[].description	Report.Description	N/A	N/A	Browser exploit kit used for distribution of malware to vulnerable computers	N/A
.results[].guid	Report.Attribute & Indicator.Attribute	Project ID	.results[].created	83276f14-5069-8b12-11ff-2ba73f1b9c3e	N/A

PassiveTotal Artifacts

The PassiveTotal Artifacts endpoint retrieves related Indicator `Artifacts` for each PassiveTotal `Project`.

`GET https://api.passivetotal.org/v2/artifact?project=<Project-GUID>`

Sample Response:

```
{
    "artifacts": [
        {
            "created": "2017-02-15T13:31:41.256000",
            "creator": "mike.wyatt@riskiq.net",
            "enterprise": false,
            "guid": "83276f14-5069-8b12-11ff-2ba73f1b9c3e",
            "links": {
                "tag": "/v2/artifact/tag?
artifact=83276f14-5069-8b12-11ff-2ba73f1b9c3e",
                "self": "/v2/artifact?
artifact=83276f14-5069-8b12-11ff-2ba73f1b9c3e",
                "project": "/v2/project?project=182d1a3a-5be3-
dad4-76b8-67f8f79e8488"
            },
            "monitor": true,
            "monitorable": false,
            "organization": "riskiq",
            "owner": "riskiq",
            "project": "182d1a3a-5be3-dad4-76b8-67f8f79e8488",
            "query": "aavm50cc.top",
            "system_tags": [],
            "tag_meta": {},
            "tags": [],
            "type": "domain",
            "user_tags": []
        },
        ...
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.artifacts[].creator	Indicator.Attribute	Creator	.artifacts[].created	mike.wyatt@riskiq.net	N/A
.artifacts[].enterprise	Indicator.Attribute	Enterprise	.artifacts[].created	False	Formatted as a title-cased string
.artifacts[].monitor	Indicator.Attribute	Monitor	.artifacts[].created	true	Formatted as a title-cased string
.artifacts[].monitorable	Indicator.Attribute	Monitorable	.artifacts[].created	False	Formatted as a title-cased string
.artifacts[].organization	Indicator.Attribute	Organization	.artifacts[].created	riskiq	N/A
.artifacts[].owner	Indicator.Attribute	Owner	.artifacts[].owner	riskiq	N/A
.artifacts[].query	Indicator.Value	See `PassiveTotal to ThreatQ Indicator Type Mapping` below	.artifacts[].created	aavm50cc.top	Derived from `.artifacts[].type`. Only types supported via PassiveTotal to ThreatQ Indicator Type Mapping below will be ingested.

PassiveTotal Bulk Artifacts Enrichment

The PassiveTotal Bulk Artifacts Enrichment endpoint retrieves enrichment data for each related Indicator `Artifact` returned by the PassiveTotal Artifacts endpoint. This endpoint expects a JSON data body with the request containing the `Artifacts` to enrich structured - see the Sample Reponse below for an example.

`GET https://api.passivetotal.org/v2/enrichment/bulk`

Sample Response:

```
{
    "results": {
        "146.0.72.186": {
            "autonomousSystemName": "HOSTKEY B.V.",
            "autonomousSystemNumber": 57043,
            "classification": null,
            "country": "NL",
            "dynamicDns": false,
            "everCompromised": false,
            "global_tags": [
                "hostkey"
            ],
            "latitude": 52.38240051269531,
            "longitude": 4.899499893188477,
            "network": "146.0.72.0/24",
            "primaryDomain": "particulieren-bank.nl",
            "queryType": "ip",
            "queryValue": "146.0.72.186",
            "sinkhole": false,
            "subdomains": [
                "mail"
            ],
            "system_tags": [
                "routable",
                "HOSTKEY-B.V."
            ],
            "tag_meta": {},
            "tags": [],
            "tld": "net"
        },
        ...
    }
}
```

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.`artifact`.autonomousSystemName	Indicator.Attribute	Autonomous System Name	N/A	HOSTKEY B.V.	Only applies to the ASN Indicator created from `.results.`artifact`.autonomousSystemNumber`
.results.`artifact`.autonomousSystemNumber	Indicator.Value	ASN	N/A	57043	N/A
.results.`artifact`.classification	Indicator.Attribute	Classification	N/A	null	Only created if present
.results.`artifact`.country	Indicator.Attribute	Country	N/A	NZ	N/A
.results.`artifact`.dynamicDns	Indicator.Attribute	Dynamic Dns	N/A	false	Formatted as a title-cased string
.results.`artifact`.everCompromised	Indicator.Attribute	Ever Compromised	N/A	false	Formatted as a title-cased string
.results.`artifact`.global_tags	Indicator.Attribute	Global Tag	N/A	hostkey	N/A
.results.`artifact`.latitude	Indicator.Attribute	Latitude	N/A	52.38240051269531	N/A
.results.`artifact`.longitude	Indicator.Attribute	Longitude	N/A	4.899499893188477	N/A
.results.`artifact`.network	Indicator.Value	CIDR Block	N/A	146.0.72.0/24	N/A
.results.`artifact`.primaryDomain	Indicator.Attribute	Primary Domain	N/A	particulieren-bank.nl	N/A
.results.`artifact`.sinkhole	Indicator.Attribute	Sinkhole	N/A	false	Formatted as a title-cased string
.results.`artifact`.system_tags	Indicator.Attribute	System Tag	N/A	routable	N/A
.results.`artifact`.tags	Indicator.Attribute	Tag	N/A	hostkey	N/A
.results.`artifact`.tld	Indicator.Attribute	TLD	N/A	net	N/A

Indicator Type Mapping

The following table provides the PassiveTotal to ThreatQ indicator type mapping.

PASSIVETOTAL	THREATQ
domain	FQDN
Email	Email Address
ip	IP Address
MD5 Hash	MD5
autonomusSystemNumber	ASN

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.

PassiveTotal (Scheduled Run)

The following metrics is for an hourly scheduled run.

METRIC	RESULT
Run Time	2 minutes
Indicators	136
Indicator Attributes	1492
Reports	2
Report Attributes	10

PassiveTotal (Manual Run)

The following metrics is for a long Passive Total manual run - 01/01/2020 to 09/29/2020.

METRIC	RESULT
Run Time	1 hour 2 minutes
Indicators	15,311
Indicator Attributes	159,606

METRIC	RESULT
Reports	381
Report Attributes	2,166

Change Log

- **Version 2.0.1**
  - Updated the messaging used when an account rate limit has been reached.
- **Version 2.0.0**
  - Added Manual Run support
  - Added primary Report objects linking to PassiveTotal's `Projects`. These Report objects are related to their Indicator `Artifacts`.
  - Removed `subdomain` Attributes from Indicators.
  - Refactor Feed
- **Version 1.1.0**
  - Added ASN indicator ingestion
- **Version 1.0.1**
  - Initial release