ThreatQuotient

PolySwarm CDF User Guide

Version 1.0.0

September 19, 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	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The PolySwarm CDF for ThreatQ enables the automatic ingestion of results from the live hunt and historical hunt feeds.

The integration provides the following feeds:

- **PolySwarm Live Hunt** - periodically pulls all live results for live PolySwarm hunt, into ThreatQ.
- **PolySwarm Historical Hunt** - lists the historical hunt in the account.
- **PolySwarm Historical Details (Supplemental)** - retrieves historical hunt details for a PolySwarm hunt and ingests associated YARA rules into ThreatQ.
- **PolySwarm Historical Results List (Supplemental)** - retrieves all historical results for a PolySwarm hunt and ingests the data into ThreatQ.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
  - Indicator Tags
- Signatures

Prerequisites

The integration requires a PolySwarm Basic or Enterprise license and API key.

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:

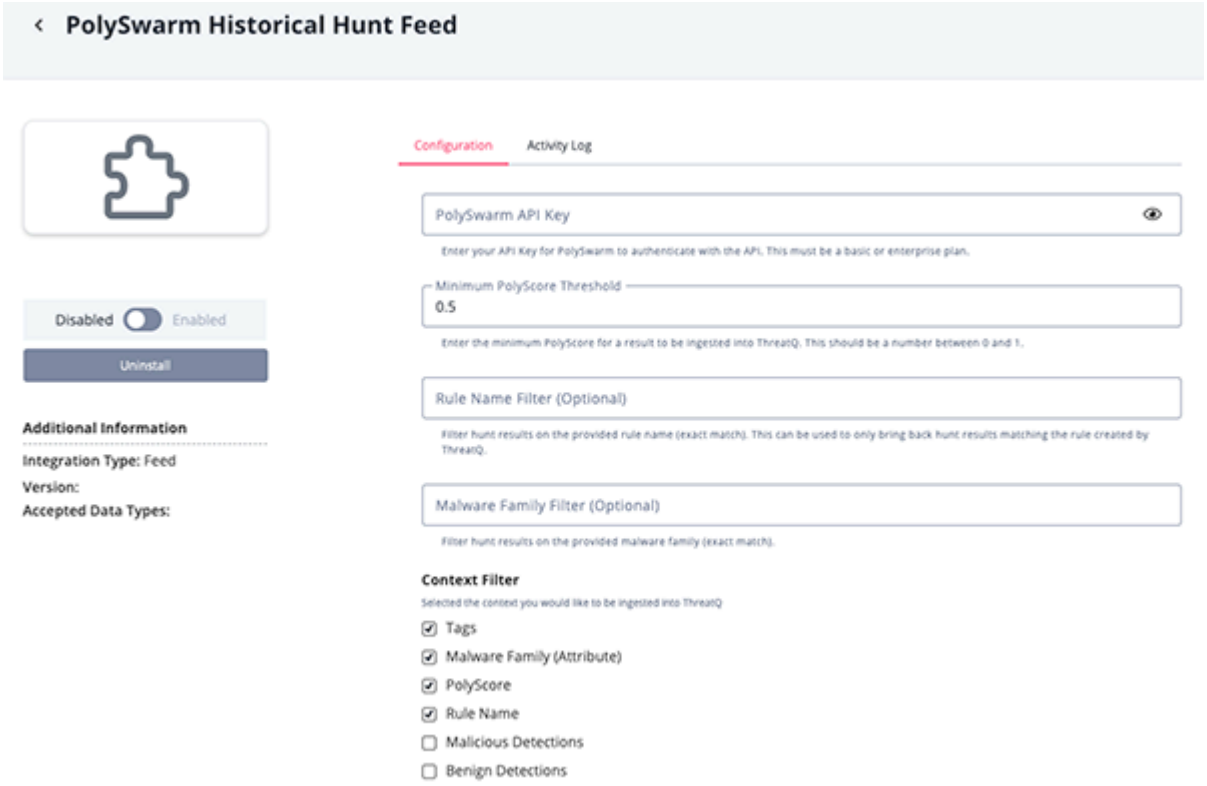
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
PolySwarm API Key	Enter your API Key for PolySwarm to authenticate with the API. > This must be a basic or enterprise plan.
Minimum PolyScore Threshold	Enter the minimum PolyScore for a result to be ingested into ThreatQ. This should be a number between 0 and 1. The default value is 0.5.
Rule Name Filter	Optional - filter hunt results on the provided rule name (exact match). > This parameter can be used to only bring back hunt results matching the rule created by ThreatQ.
Malware Family Filter	Optional - filter hunt results on the provided malware family (exact match).
Context Filter	Use the parameter provided to filter the context to be ingested into ThreatQ. Options include: ◦ Tags (default) ◦ Malware Family (Attribute) (default)

PARAMETER	DESCRIPTION
	◦ PolyScore (default) ◦ Rule Name (default) ◦ Malicious Detections ◦ Benign Detections



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

PolySwarm Live Hunt

The PolySwarm Live Hunt feed periodically pulls all live results for live PolySwarm hunt, into ThreatQ.

`GET https://api.polyswarm.network/v3/hunt/live/list`

Sample Response:


```
{
    "has_more": true,
    "limit": 100,
    "offset": "gAAAAABi1seOzAGTP13qPr5yGG9b_AZppVv1mm2gl0gPwq3AtzQ8NTMUsp1--
DS5AQJXbuYBLV6hHrXuXpNdaKWC3PSreV2IcnXqoP1SmPUzAMn4c4tr0kp8b8iXivi05zvr00pAtbss
",
    "result": [
        {
            "created": "2022-07-19T12:32:17.656340",
            "detections": {
                "benign": 6,
                "malicious": 6,
                "total": 12
            },
            "download_url": null,
            "id": "14381491890173570",
            "instance_id": "45777877121770335",
            "livescan_id": "13626756552838383",
            "malware_family": "HgIASvcA",
            "polyscore": 0.9998364323055465,
            "rule_name": "discordaio",
            "sha256":
"9fcb6558474426d1a6a6491bade5dd554fe74e23aeb514a98b969aecc9d5b54d",
            "tags": "{}",
            "yara": null
        },
        {
            "created": "2022-07-19T11:31:19.349184",
            "detections": {
                "benign": 6,
                "malicious": 7,
                "total": 13
            },
            "download_url": null,
            "id": "18281909959628115",
            "instance_id": "4518589306451487",
            "livescan_id": "13626756552838383",
            "malware_family": "HgIASvcA",
            "polyscore": 0.9999373601547417,
```

```
            "rule_name": "discordaio",
            "sha256":
"dd5f9af7752be090beb2acbaa0c8aa06c02810fa0cf2e4472dcc740fc0b6eea2",
            "tags": "{}",
            "yara": null
        },
        {
            "created": "2022-07-18T21:44:45.159177",
            "detections": {
                "benign": 7,
                "malicious": 6,
                "total": 13
            },
            "download_url": null,
            "id": "75860636920369830",
            "instance_id": "6207483134542754",
            "livescan_id": "13626756552838383",
            "malware_family": "HgIASvQA",
            "polyscore": 0.9998364323055465,
            "rule_name": "discordaio",
            "sha256":
"f177a8dcfd7c383a5ce1a4877284e67f40a1503e1ae3b801d4d9428b4ead2294",
            "tags": "{}",
            "yara": null
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.sha256`	Indicator Value	SHA-256	`.created`	'dd5f9af7752be090beb2acbaa0c8aa06c02810fa0cf2e4472dcc740fc0b6eea2'	N/A
`.malware_family`	Attribute	Malware Family	N/A	`HgIASvcA`	N/A
`.polyscore`	Attribute	PolyScore	N/A	`0.9998364323055465`	Converted to a string with 2 decimals. It gets updated at each run.
`.rule_name`	Attribute	Rule Name	N/A	`discordaio`	N/A
`.detections.benign`	Attribute	Benign Detections	N/A	`6`	Converted to a string. It gets updated at each run.
`.detections.malicious`	Attribute	Malicious Detections	N/A	`6`	Converted to a string. It gets updated at each run.
`.tags`	Tag	N/A	N/A	N/A	N/A

PolySwarm Historical Hunt

The PolySwarm Historical Hunt feed lists the historical hunt in the account.

`GET https://api.polyswarm.network/v3/hunt/historical/list`

Sample Response:


```
{
    "has_more": true,
    "limit": 10,
    "offset": "gAAAAABk7EFpa3K5tiIuX-
DaN6_B_f3J9XGNYdsNW_6oRjIQMbFh0elp8AfLcxNQhiEyqzgdEzy2GEBx090IWxSGFNrOwD2d9Eq0h
rZ3MTdxOMHK76W0JfM=",
    "result": [
        {
            "created": "2023-07-27T08:43:14.110384",
            "id": "83966264955167759",
            "progress": 100.00000000000001,
            "results_csv_uri": null,
            "ruleset_name": "university",
            "status": "COMPLETED",
            "summary": {
                "count": 4,
                "rule": {
                    "university": {
                        "count": 4
                    }
                }
            },
            "yara": null
        },
        {
            "created": "2023-07-27T08:43:13.761797",
            "id": "59018977163239070",
            "progress": 100.00000000000001,
            "results_csv_uri": null,
            "ruleset_name": "svcready_packed",
            "status": "COMPLETED",
            "summary": {
                "count": 1,
                "rule": {
                    "SVCReady_Packed": {
                        "count": 1
                    }
                }
            },
            "yara": null
        }
    ],
```

```
    "status": "OK"
}
```

This feed does not have a mapping table, the `result[].id` is used in the API of the next supplemental feeds.

PolySwarm Historical Details (Supplemental)

The PolySwarm Historical Details supplemental feed retrieves historical hunt details for a PolySwarm hunt and ingests associated YARA rules into ThreatQ.

```
GET https://api.polyswarm.network/v3/hunt/historical?id={hunt_id}
```

Sample Response:


```
{
    "result": {
        "created": "2023-07-27T08:43:14.110384",
        "id": "83966264955167759",
        "progress": 100.00000000000001,
        "results_csv_uri": "https://s3.us-east-2.amazonaws.com/ps-storage-
prodv2-historical/94/f5/
d7/94f5d75d19ff1948cc5f29375729909a423cdf36fadf98a447334d846a072d41c9f175c91275
60d08a89444f62c1f00e3394e395d9ede0e856c021f036b1c35e4984d97a?response-content-
disposition=attachment%3Bfilename%3D83966264955167759.csv&response-content-
type=application%2Foctet-stream&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIARD7S6WCVBXF6ZSO5%2F20230828%2Fus-east-2%2Fs3%2Faws4_request&X-
Amz-Date=20230828T115904Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-
Signature=0ad70519910b2b74d7f2ab348072787a728182fc1b13405f9c62c76267d57088",
        "ruleset_name": "university",
        "status": "COMPLETED",
        "summary": {
            "count": 4,
            "rule": {
                "university": {
                    "count": 4
                }
            }
        },
        "yara": "rule university\n{\n    meta:\n        author = \"Intel471\"\n
description = \"Detects unpacked university stealer samples\"\n\n    strings:\n
$y0 = \"youtube.GetYouData\" ascii\n        $y1 = \"youtube.tokenExtractor\"
ascii\n        $y2 = \"bot.GenerateToken\" ascii\n        $y3 =
\"parse.Chromium\" ascii\n        $y4 = \"parse.GeckoParse\" ascii\n        $s0
= \"University/bot\" ascii\n        $s1 = \"University/core/\" ascii\n
$s2 = \"University/core/parse\" ascii\n        $s3 = \"University/core/
cryptos\" ascii\n        $s4 = \"University/core/youtube\" ascii\n\n
condition:\n        uint16(0) == 0x5a4d and (3 of ($y*)) and (2 of ($s*))\n}"
    },
    "status": "OK"
}
```


The mapping for this feed is contained in the mapping table for the PolySwarm Historical Results Supplemental feed.

PolySwarm Historical Results List (Supplemental)

The PolySwarm Historical Results List feed retrieves all historical results for a PolySwarm hunt and ingests the data into ThreatQ.

```
GET https://api.polyswarm.network/v3/hunt/historical/results/list?id={hunt_id}
```

Sample Response:


```
{
    "has_more": false,
    "limit": 50,
    "result": [
        {
            "created": "2023-07-27T10:53:44.848800",
            "detections": {
                "benign": 5,
                "malicious": 9,
                "total": 14
            },
            "download_url": null,
            "historicalscan_id": "83966264955167759",
            "id": "77871670233119644",
            "instance_id": "76231850134176078",
            "malware_family": "Wingo",
            "polyscore": 0.9999445756446724,
            "rule_name": "university",
            "sha256":
"b4830b3135327366eef7c2fd4164c5253a34785c0e021b3fbebfb829f5efc17e",
            "tags": "{}",
            "yara": null
        },
        {
            "created": "2023-07-27T10:26:22.185699",
            "detections": {
                "benign": 5,
                "malicious": 8,
                "total": 13
            },
            "download_url": null,
            "historicalscan_id": "83966264955167759",
            "id": "94071587811020700",
            "instance_id": "96391432665847294",
            "malware_family": "WinGo",
            "polyscore": 0.9999352826306565,
            "rule_name": "university",
            "sha256":
"2b86dbdda07a91f208a278a0012a6d06175469833feee42c2ee0b41ea240c8ab",
            "tags": "{}",
            "yara": null
```

```
        }
    ],
    "status": "OK"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.result[].sha256`	Indicator Value	SHA-256	`.result[].created`	`b4830b3135327366eef7c2fd4164c5` `253a34785c0e021b3fbebfb829f5efc17e`	N/A
`.result[].malware_family`	Attribute	Malware Family	N/A	`HgIASvcA`	N/A
`.result[].polyscore`	Attribute	PolyScore	N/A	`0.9999445756446724`	Converted to a string with 2 decimals. It gets updated at each run.
`.result[].rule_name`	Attribute	Rule Name	N/A	`Wingo`	N/A
`.result[].detections.benign`	Attribute	Benign Detections	N/A	`5`	Converted to a string. It gets updated at each run.
`.result[].detections.malicious`	Attribute	Malicious Detections	N/A	`9`	Converted to a string. It gets updated at each run.
`.result[].tags[]`	Tag	N/A	N/A	N/A	N/A
`.result.yara`	Signature Value	YARA	`.result.created`	`rule university\n{\n meta:\n author = \"Intel471\"\n description = \"Detects unpacked university stealer samples\"\n\n`	N/A
`.result.ruleset_name`	Signature Name	YARA	`.result.created`	`university`	N/A

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.

PolySwarm Live Hunt

METRIC	RESULT
Run Time	5 minutes
Indicators	4,747
Indicator Attributes	26,269

PolySwarm Historical Hunt

METRIC	RESULT
Run Time	19 minutes
Indicators	19,613
Indicator Attributes	76,571
Signatures	19

Change Log

- **Version 1.0.0**
  - Initial release