ThreatQuotient

PolySwarm Action Bundle User Guide

Version 1.0.0

July 24, 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	>= 5.14.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The PolySwarm Action Bundle for ThreatQ enables analysts to interact with PolySwarm by performing scans on files/URLs, enriching indicators, submitting YARA rules, and more.

The bundle provides the following actions:

- **PolySwarm - Lookup** - performs a lookup on a hash or URL to find context from PolySwarm.
- **PolySwarm - Rescan** - performs a Rescan for a particular hash.
- **PolySwarm - Metadata Search** - searches for scans using the metadata search.
- **PolySwarm - Live Hunt** - starts a live hunt in PolySwarm using a YARA Signature.
- **PolySwarm - Historical Hunt** - starts a historical hunt in PolySwarm using a YARA Signature.
- **PolySwarm - Add Rule** - creates a Ruleset to PolySwarm using YARA Signature.
- **PolySwarm** - Scan - scans a file or URL using PolySwarm.

The action is compatible with the following system object types:

- Indicators
  - MD5
  - SHA-1
  - SHA-256
  - URL
  - FQDN
  - IP Address
  - IPv6 Address
- Files
- Signatures
  - YARA

The action returns the following enriched system objects:

- Indicators
  - MD5
  - SHA-1
  - SHA-256
  - URL
  - FQDN
  - IP Address
  - IPv6 Address
- Files
- Signatures
  - YARA

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

Prerequisites

- A PolySwarm API key.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following objects types:
  - Indicators
    - MD5
    - SHA-1
    - SHA-256
    - URL
    - FQDN
    - IP Address
    - IPv6 Address
  - Files
  - Signatures
    - YARA

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 action 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

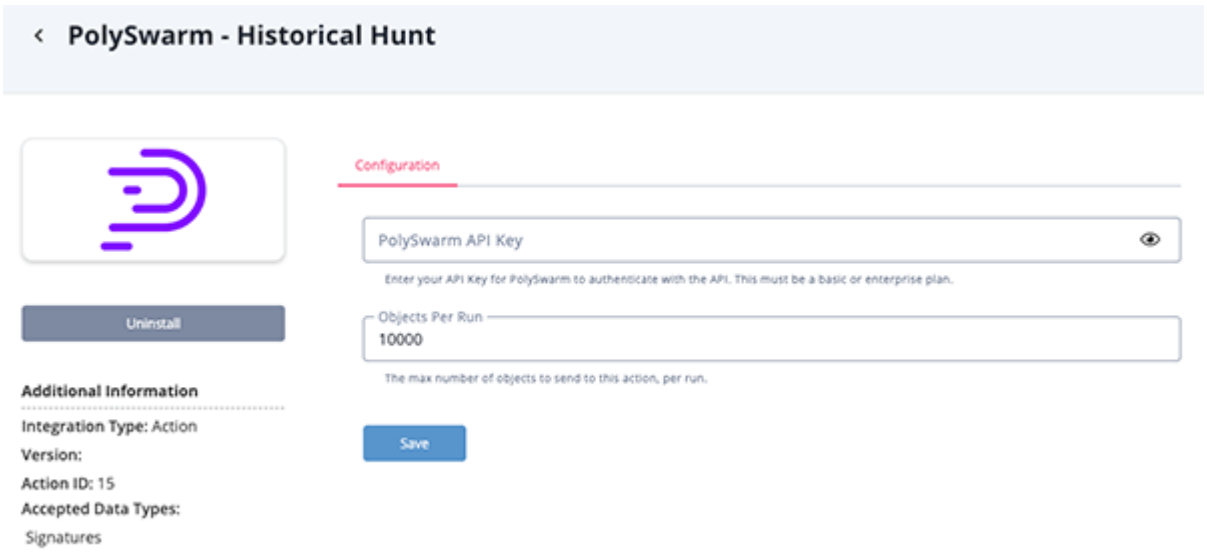
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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
PolySwarm API Key	Your PolySwarm API Key to authenticate.
Objects Per Run	The max number of objects per run to send to this action (default: 1000)



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

Actions

The action bundle provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
PolySwarm - Lookup	Perform a lookup on a hash or URL to find context from PolySwarm	Indicator	MD5, SHA-1, SHA-256, URL, FQDN
PolySwarm - Rescan	Perform a Rescan for a particular hash	Indicator	MD5, SHA-1, SHA-256
PolySwarm - Metadata Search	Search for scans using the metadata search	Indicator	IP Address, IPv6 Address, FQDN, URL
PolySwarm - Live Hunt	Start a live hunt in PolySwarm using a YARA Signature	Signature	YARA
PolySwarm - Historical Hunt	Start a historical hunt in PolySwarm using a YARA Signature	Signature	YARA
PolySwarm - Add Rule	Create a Ruleset to PolySwarm using YARA Signature	Signature	YARA
PolySwarm - Scan	Scan a file or URL using PolySwarm	Indicator, File	URL, FQDN

PolySwarm - Lookup

The Lookup action performs a lookup on a hash or URL to find context from PolySwarm

`GET https://api.polyswarm.network/v3/search/hash/{hash_type}?hash={hash}` `GET https://api.polyswarm.network/v3/search/url?url={url/fqdn}`

Sample Response:


```
{
    "has_more": false,
    "limit": 50,
    "result": [
        {
            "artifact_id": "62579306490581341",
            "assertions": [
                {
                    "author": "45003009427661603",
                    "author_name": "Qihoo 360",
                    "bid": "15000000000000000",
                    "engine": {
                        "description": "Qihoo 360 is the largest provider of
antivirus, Internet and mobile security products in China. QVM (Qihoo Support
Vector Machine) is used as a basis for a detection algorithm which is
automatically enhanced and updated with new malware samples submitted by users
to servers. Program files that do not appear on our blacklist and whitelist are
scanned using QVM, and any â€œhitsâ€ presumed to be malicious would be removed
or quarantined.",
                        "name": "Qihoo 360"
                    },
                    "mask": true,
                    "metadata": {
                        "product": "Qihoo",
                        "scanner": {
                            "signatures_version": "2022-10-04 10:25"
                        }
                    },
                    "verdict": false
                }
            ],
            "community": "mainnet1",
            "country": "US",
            "created": "2022-12-21T09:21:32.093969",
            "detections": {
                "benign": 10,
                "malicious": 0,
                "total": 10
            },
            "extended_type": "ELF 64-bit LSB pie executable, x86-64, version 1
(SYSV), dynamically linked, stripped",
```

```
            "failed": false,
            "filename":
"0184e3d3dd8f4778d192d07e2caf44211141a570d45bb47a87894c68ebebeabb",
            "first_seen": "2022-12-21T09:21:32.093969",
            "id": "62579306490581341",
            "last_scanned": "2022-12-21T09:21:32.093969",
            "last_seen": "2022-12-21T09:21:32.093969",
            "md5": "3191cb2e06e9a30792309813793f78b6",
            "metadata": [
                {
                    "created": "2022-12-21T09:31:47.609013",
                    "tool": "polyunite",
                    "tool_metadata": {
                        "labels": [],
                        "malware_family": null,
                        "operating_system": [],
                        "detection": null
                    },
                    "updated": "2022-12-21T09:31:47.609013"
                },
                {
                    "created": "2022-12-21T09:21:37.957783",
                    "tool": "hash",
                    "tool_metadata": {
                        "md5": "3191cb2e06e9a30792309813793f78b6",
                        "sha1": "b311d43144076b1268381cec3ce2f00920416d34",
                        "sha256":
"0184e3d3dd8f4778d192d07e2caf44211141a570d45bb47a87894c68ebebeabb",
                        "sha3_256":
"4c6184099c535dafb51f27dbd82b100e6f38eb53fbd810c6b51beb432188b902",
                        "sha3_512":
"95a4fef5920a9e30473505a97d5461b6b5ce1c6130a2d1c28f6415b817662e1373f48090b58bc6
d92c0394d56c2e965b194d5eec3a86841ced5622a013142ec2",
                        "sha512":
"d643ee45bda671191bfc515ee2b6b80467c7311de3442746caecf46da09d44ef6eac6e5bdc15a6
ad06208fe7fe65a788f4d90c4f75a2b8a00cebccfb60f93aa6",
                        "ssdeep":
"6144:XQ5RZYLIUIAaSsZcg6ZRAabmtXbwGRFOlgIwg:A5RmLwANgEtbMrdox",
                        "tlsh":
"6c546c02f6e048bac4a6c870875fd213ea76b4893121b57b329a5f517f27e30af4e751"
                    },
                    "updated": "2022-12-21T09:21:37.957783"
                }
            ],
            "mimetype": "application/x-pie-executable",
            "polyscore": 0.23213458159978606,
            "result": false,
            "sha1": "b311d43144076b1268381cec3ce2f00920416d34",
            "sha256":
"0184e3d3dd8f4778d192d07e2caf44211141a570d45bb47a87894c68ebebeabb",
```

```
            "size": 292632,
            "type": "FILE",
            "upload_url": "https://s3.us-east-2.amazonaws.com/ps-storage-
prodv2-instances/93/b6/57/93b657be-5461-4b63-acea-b3ea12dd9e68?X-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIARD7S6WCVBXF6ZSO5%2F20221221%2Fus-east-2%2Fs3%2Faws4_request&X-
Amz-Date=20221221T092132Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-
Signature=3b23e794b2cd1cea13ed6d6c4704fa2ebd67177db0f6bc3a0c4a8ec6f49660c9",
            "votes": [
                {
                    "arbiter": "17591329907863069",
                    "arbiter_name": "Kaspersky Arbiter",
                    "engine": {
                        "description": "Kasperskyâ€™s scanning engine, renowned
for unequalled detection rates and near-zero false positives. Backed by
superior threat intelligence and in-house expertise, fed by a decade-and-a-
halfâ€™s work with ML-based threat discovery.",
                        "name": "Kaspersky Arbiter"
                    },
                    "metadata": {
                        "product": "kaspersky",
                        "scanner": {
                            "environment": {
                                "architecture": "x86_64",
                                "operating_system": "Linux"
                            },
                            "vendor_version": "21.0.1.45",
                            "version": "0.0.1"
                        }
                    },
                    "vote": false
                },
                {
                    "arbiter": "72439373973467971",
                    "arbiter_name": "ClamAV-Arbiter",
                    "engine": {
                        "description": "ClamAV is an open source, signature-
based, anti-virus engine capable of scanning a wide variety of common file
types.",
                        "name": "ClamAV-Arbiter"
                    },
                    "metadata": {
                        "product": "clamav",
                        "scanner": {
                            "environment": {
                                "architecture": "x86_64",
                                "operating_system": "Linux"
                            },
                            "vendor_version": "ClamAV 0.105.1/26644/Wed Aug 31
07:53:02 2022",
```

```
                        "version": "0.0.1"
                    }
                },
                "vote": false
            }
        ],
        "window_closed": true
    }
  ],
  "status": "OK"
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result[].metadata[].tool_metadata[].malware_family	Indicator.Attribute	Malware Family	result[].created	N/A	N/A
result[].metadata[].tool_metadata[].operating_system	Indicator.Attribute	Operating System	result[].created	N/A	N/A
result[].metadata[].tool_metadata[].labels	Indicator.Attribute	Label	result[].created	N/A	N/A
result[].metadata[].tool_metadata[].detections	Indicator.Attribute	Detection	result[].created	N/A	N/A
result[].size	Indicator.Attribute	File Size	result[].created	292632	N/A
result[].type	Indicator.Attribute	PolySwarm Type	result[].created	FILE	N/A
result[].extended_type	Indicator.Attribute	PolySwarm Extended Type	result[].created	ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, stripped	N/A
result[].community	Indicator.Attribute	PolySwarm Community	result[].created	mainnet1	N/A
result[].mimetype	Indicator.Attribute	MIME Type	result[].created	application/x-pie-executable	N/A
result[].polyscore	Indicator.Attribute	Polyscore	result[].created	0.23213458159978606	N/A
result[].country	Indicator.Attribute	Country Code	result[].created	US	N/A
result[].last_scanned	Indicator.Attribute	Last Scanned	result[].created	2022-12-21T09:21:32.093969	N/A
result[].last_seen	Indicator.Attribute	Last Seen	result[].created	2022-12-21T09:21:32.093969	N/A
result[].detections	Indicator.Attribute	Detection Rate	result[].created	0.0%	result[].detections.malicious / result[].detections.total %
result[].detections	Indicator.Attribute	Detections	result[].created	0/10	result[].detections.malicious / result[].detections.total
result[].metadata[].tool_metadata[].network.domains.ip	Related Indicator Value	IP Address	result[].created	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result[].metadata[].tool_metadata[].network.domains.domains	Related Indicator Value	FQDN	result[].created	N/A	N/A
result[].metadata[].tool_metadata[].cape_config.c2_url	Related Indicator Value	URL	result[].created	N/A	N/A
result[].metadata[].tool_metadata[].signatures.name	Related Indicator Value	TTP	result[].created	N/A	N/A
result[].metadata[].tool_metadata[].sha256	Related Indicator Value	SHA-256	result[].created	N/A	N/A
result[].sha1	Related Indicator Value	SHA-1	result[].created	b311d43144076b1268381cec3ce2f00920416d34	N/A
result[].sha256	Related Indicator Value	SHA-256	result[].created	0184e3d3dd8f4778d192d07e2caf44211141a570d45bb47a87894c68ebebeabb	N/A
result[].md5	Related Indicator Value	MD5	result[].created	3191cb2e06e9a30792309813793f78b6	N/A
result[].filename	Related Indicator Value	Filename	result[].created	0184e3d3dd8f4778d192d07e2caf44211141a570d45bb47a87894c68ebebeabb	N/A

PolySwarm - Rescan

The Rescan action performs a Rescan for a particular hash.

`POST https://api.polyswarm.network/v3/consumer/submission/default/rescan/{hash_type}/{hash_value}`

Sample Response:


```
{
    "result": {
        "artifact_id": "43187070513778065",
        "assertions": [],
        "community": "mainnet1",
        "country": "RO",
        "created": "2023-07-10T11:03:28.999834",
        "detections": null,
        "extended_type": "ELF 64-bit LSB pie executable, x86-64, version 1
(SYSV), dynamically linked, stripped",
        "failed": false,
        "filename":
"0184e3d3dd8f4778d192d07e2caf44211141a570d45bb47a87894c68ebebeabb",
        "first_seen": "2022-12-21T09:21:32.093969",
        "id": "43187070513778065",
        "last_scanned": null,
        "last_seen": null,
        "md5": "3191cb2e06e9a30792309813793f78b6",
        "metadata": [],
        "mimetype": "application/x-pie-executable",
        "polyscore": null,
        "result": null,
        "sha1": "b311d43144076b1268381cec3ce2f00920416d34",
        "sha256":
"0184e3d3dd8f4778d192d07e2caf44211141a570d45bb47a87894c68ebebeabb",
        "size": 292632,
        "type": "FILE",
        "upload_url": null,
        "votes": [],
        "window_closed": false
    },
    "status": "OK"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result.country	Indicator.Attribute	Country Code	result.created	RO	N/A
result.community	Indicator.Attribute	PolySwarm Community	result.created	mainnet1	N/A
result.extended_type	Indicator.Attribute	Extended Type	result.created	ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, stripped	N/A
result.first_seen	Indicator.Attribute	First Seen	result.created	2022-12-21T09:21:32.093969	N/A
result.size	Indicator.Attribute	File Size	result.created	292632	N/A
result.type	Indicator.Attribute	PolySwarm Type	result.created	FILE	N/A
result.sha1	Related Indicator Value	SHA-1	result.created	b311d43144076b12 68381cec3ce2f00920 416d34	N/A
result.sha256	Related Indicator Value	SHA-256	result.created	0184e3d3dd8f4778d1 92d07e2caf44211141a 570d45bb47a87894c68 ebebeabb	N/A
result.md5	Related Indicator Value	MD5	result.created	3191cb2e06e9a307923 09813793f78b6	N/A
result.filename	Related Indicator Value	Filename	result.created	0184e3d3dd8f4778d19 2d07e2caf44211141a57 0d45bb47a87894c68eb ebeabb	N/A

PolySwarm - Metadata Search

The Metadata Search action searches for scans using the metadata search.

`POST https://api.polyswarm.network/v3/search/metadata/query?query=strings.{object_type}:{object_value}`

Sample Response:


```
{
    "has_more": false,
    "limit": 50,
    "result": [
        {
            "artifact": {
                "created": "2022-11-16T15:25:16.577496+00:00",
                "id": "85705858721751216",
                "md5": "20faa364159d2319181411a3a04f2c2f",
                "sha1": "47b68cf582499ca588d17d03ca01e67b0a91877a",
                "sha256":
"065d53198a86c52985798e724ed4743fcdd18e7cb20a0064c1fdc0c526c2f892"
            },
            "exiftool": {
                "contenttype": "text/html; charset=UTF-8",
                "description": "Izvorul Tamaduirii este o sarbatoare religioasa
celebrata anual in religia ortodoxa de catre Biserica Ortodoxa Romana.
Sarbatoarea Izvorul tÄƒmÄƒduirii pica in fiecare an in SÄƒptÄƒmÃ¢na LuminatÄƒ,
Ã®n prima vineri de dupÄƒ PaÈ™ti. In 2018, \"Izvorul tÄƒmÄƒduirii\" cade in
ziua de vineri",
                "filesize": "324 KiB",
                "filetype": "HTML",
                "filetypeextension": "html",
                "mimetype": "text/html",
                "title": " Cand cade si ce este <b>Izvorul tÄƒmÄƒduirii</b> -
Calendar 2021 È™i 2022 romÃ¢nesc Calendar ortodox si catolic PDF "
            },
            "hash": {
                "md5": "20faa364159d2319181411a3a04f2c2f",
                "sha1": "47b68cf582499ca588d17d03ca01e67b0a91877a",
                "sha256":
"065d53198a86c52985798e724ed4743fcdd18e7cb20a0064c1fdc0c526c2f892",
                "sha3_256":
"4c9714025fad8e15ad49a6128a78c02fb4694aa3b33f87e6d0df9c9cd1bc3e36",
                "sha3_512":
"069fa9874b939070c62ada9d0e4bd7fa32922e5eb5b861b5ac5c8a8702f811afc14f9212b25afc
5dfa4deca7e31519806f88f3db2b95832e0a3044baf8a56b47",
                "sha512":
"17e1c133f63ebddac7a37e7e515a181e68fbe76ba35bbb9b4f0dc8e7836087e69234adb3cfeee5
70861c60220cf6af06e88153796afdb8e993e9cde04afd4a23",
                "ssdeep": "6144:tjmhHsNW0/
```

```
SF9ALaN8QnKnkzuBJtI+U3xWPPsnL:t6hHsNWCSLALaN80uxI+UBWq",
                "tlsh":
"0e6462b23553120bd63e4492eed53ba452fcb55381c2289bf2f8398f07896cf41796da"
            },
            "modified": "2022-11-16T15:35:26.831519",
            "polyunite": {
                "labels": [],
                "operating_system": []
            },
            "scan": {
                "countries": [
                    "US"
                ],
                "detections": {
                    "benign": 12,
                    "malicious": 0,
                    "total": 12
                },
                "filename": [

"065d53198a86c52985798e724ed4743fcdd18e7cb20a0064c1fdc0c526c2f892"
                ],
                "first_scan": {
                    "Alibaba": {
                        "assertion": "unknown",
                        "metadata": {}
                    },
                    "ClamAV": {
                        "assertion": "benign",
                        "metadata": {}
                    }
                },
                "first_seen": "2022-11-16T15:25:16.577496+00:00",
                "last_seen": "2022-11-16T15:25:16.577496+00:00",
                "latest_scan": {
                    "Alibaba": {
                        "assertion": "unknown",
                        "metadata": {}
                    },
                    "ClamAV": {
                        "assertion": "benign",
                        "metadata": {}
                    }
                },
                "mimetype": {
                    "extended": "HTML document, UTF-8 Unicode text, with very
long lines",
                    "mime": "text/html"
                }
            },
            "strings": {
```

```
                "domains": [
                    "github.com",
                    "click.owl.video",
                    "e.target",
                    "www.linkedin.com",
                    "www.w3.org",
                    "vdw.staytuned.gr"
                ],
                "ipv4": [],
                "ipv6": [
                    "::bef"
                ],
                "urls": [
                    "https://calendar2018.robloguri.info/feeds/
1231490553393889070/comments/default",
                    "https://calendar2018.robloguri.info/2018/",
                    "http://calendar2018.robloguri.info/2018/02/calendar-2018-
format-printabil-pdf-imagini-caini.html"
                ]
            },
            "updated": {
                "exiftool": "2022-11-16T15:25:22.350451",
                "hash": "2022-11-16T15:25:21.773482",
                "polyunite": "2022-11-16T15:35:26.831519",
                "strings": "2022-11-16T15:25:29.864545"
            }
        }
    ],
    "status": "OK"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result[].scan.countries	Indicator.Attribute	Country Code	N/A	US	N/A
result[].scan.mimetype.mime	Indicator.Attribute	MIME Type	N/A	text/html	N/A
result[].scan.mimetype.extended	Indicator.Attribute	Extended Type	N/A	HTML document, UTF-8 Unicode text, with very long lines	N/A
result[].scan.first_seen	Indicator.Attribute	First Seen	N/A	2022-11-16T15:25:16.577496+00:00	N/A
result[].scan.last_seen	Indicator.Attribute	Last Seen	N/A	2022-11-16T15:25:16.577496+00:00	N/A
result[].scan.latest_scan.detections.malicious	Indicator.Attribute	Detection Rate	N/A	0.0%	result[].detections.malicious / result[].detections.total %
result[].scan.latest_scan.detections.malicious	Indicator.Attribute	Detection	N/A	0/12	result[].detections.malicious / result[].detections.total
result[].id	Indicator.Attribute	Scan Link	N/A	N/A	N/A
result[].artifact.sha1	Related Indicator Value	SHA-1	N/A	47b68cf582499ca588d17d03ca01e67b0a91877a	N/A
result[].artifact.sha256	Related Indicator Value	SHA-256	N/A	065d53198a86c52985798e724ed4743fcdd18e7cb20a0064c1fdc0c526c2f892	N/A
result[].artifact.md5	Related Indicator Value	MD5	N/A	20faa364159d2319181411a3a04f2c2f	N/A
result[].scan.filename	Related Indicator Value	Filename	N/A	065d53198a86c52985798e724ed4743fcdd18e7cb20a0064c1fdc0c526c2f892	N/A
result[].strings.urls	Related Indicator Value	URL	N/A	https://calendar2018.robloguri.info/2018/	N/A
result[].strings.domains	Related Indicator Value	FQDN	N/A	github.com	N/A
result[].strings.ipv4	Related Indicator Value	IP Address	N/A	N/A	N/A
result[].strings.ipv6	Related Indicator Value	IPv6 Address	N/A	::bef	N/A

PolySwarm - Live Hunt

Live Hunt action starts a live hunt in PolySwarm using a YARA Signature.

`POST https://api.polyswarm.network/v3/hunt/rule/live`

Sample Response:


```
{
  "result": {
    "created": "2023-07-10T13:00:06.739851",
    "deleted": false,
    "description": null,
    "id": "38370801958626706",
    "livescan_created": "2023-07-10T13:01:14.176047",
    "livescan_id": 82000514997528973,
    "modified": "2023-07-10T13:01:13.912525",
    "name": "banbra",
    "yara": "rule banbra : banker {\n\tstrings: \n        $a = \"senha\"
fullword nocase\n        $b = \"cartao\" fullword nocase\n        $c =
\"caixa\" \n        $d = \"login\" fullword nocase\n        $e =
\".com.br\"\n\n     condition:\n        #a > 3 and #b > 3 and #c > 3 and #d > 3
and #e > 3              \n}\n"
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result.livescan_id	Signature.Attribute	PolySwarm Live Hunt Scan ID	N/A	82000514997528973	N/A

PolySwarm - Historical Hunt

The Historical Hunt action start a historical hunt in PolySwarm using a YARA Signature.

`POST https://api.polyswarm.network/v3/hunt/historical`

Sample Response:


```
{
  "result": {
        "created": "2023-07-10T13:10:18.035352",
        "id": "49081175099213384",
        "progress": null,
        "results_csv_uri": null,
        "ruleset_name": "banbra",
        "status": "PENDING",
        "summary": null,
        "yara": "rule banbra : banker {\n\tstrings: \n        $a = \"senha\"
fullword nocase\n        $b = \"cartao\" fullword nocase\n        $c =
\"caixa\" \n        $d = \"login\" fullword nocase\n        $e =
\".com.br\"\n\n     condition:\n        #a > 3 and #b > 3 and #c > 3 and #d > 3
and #e > 3              \n}\n"
    }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result.id	Signature.Attribute	PolySwarm Historical Hunt ID	N/A	49081175099213384	N/A

PolySwarm - Add Rule

The Add Rule action starts a live hunt in PolySwarm using a YARA Signature.

`POST https://api.polyswarm.network/v3/hunt/rule`

Sample Response:


```
{
  "result": {
    "created": "2023-07-10T12:54:26.643961",
    "deleted": false,
    "description": null,
    "id": "29974659155558474",
    "livescan_created": null,
    "livescan_id": null,
    "modified": "2023-07-10T12:54:26.643961",
    "name": "banbra",
    "yara": "rule banbra : banker {\n\tstrings: \n        $a = \"senha\"
fullword nocase\n        $b = \"cartao\" fullword nocase\n        $c =
\"caixa\" \n        $d = \"login\" fullword nocase\n        $e =
\".com.br\"\n\n     condition:\n        #a > 3 and #b > 3 and #c > 3 and #d > 3
and #e > 3              \n}\n"
    }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
result.id	Signature.Attribute	PolySwarm Rule ID	N/A	29974659155558474	N/A

PolySwarm - Scan

Scan a file or URL using PolySwarm

`POST https://api.polyswarm.network/v3/instance`

Sample Response:


```
{
  "result": {
    "artifact_id":"19327280013263178",
    "assertions":[],
    "community":"mainnet1",
    "country":"RO",
    "created":"2023-07-10T11:01:24.825922",
    "detections":null,
    "extended_type":null,
    "failed":false,
    "filename":"ad452d161782290ad5004b2c9497074f",
    "first_seen":"2023-07-10T11:01:24.825922",
    "id":"19327280013263178",
    "last_scanned":null,
    "last_seen":null,
    "md5":null,
    "metadata":[],
    "mimetype":null,
    "polyscore":null,
    "result":null,
    "sha1":null,
    "sha256":null,
    "size":null,
    "type":"FILE",
    "upload_url":"https://s3.us-east-2.amazonaws.com/ps-storage-prodv2-
instances/3e/62/9c/3e629ccf-9c60-47f3-9a33-6581c8232d17?X-Amz-Algorithm=AWS4-
HMAC-SHA256&X-Amz-Credential=AKIARD7S6WCVBXF6ZSO5%2F20230710%2Fus-
east-2%2Fs3%2Faws4_request&X-Amz-Date=20230710T110124Z&X-Amz-Expires=300&X-Amz-
SignedHeaders=host&X-Amz-
Signature=d4b461a8ac8b5356dcef0a6947750a3a1bdf95408ba969dd46ca8b8776b22bad",
    "votes":[],
    "window_closed":false
  }
}
```

Change Log

- **Version 1.0.0**
  - Initial release