# ThreatQuotient

## ANY.RUN Operation Guide

**Version 1.0.0**

October 04, 2022

**ThreatQuotient**
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

**Not Actively Supported**

# 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 **Not Actively Supported**.

Integrations, apps, and add-ons designated as **Not Actively Supported** are not supported by ThreatQuotient's Customer Support team.

While you can report issues to ThreatQ's Customer Support team regarding the integration/app/add-on, you are solely responsible for ensuring proper functionality and version compatibility of Not Supported designations with the applicable ThreatQuotient software.

If unresolvable functional or compatibility issues are encountered, you may be required to uninstall the integration/app/add-on from your ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

> ⚠ For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply to issues caused by Not Actively Supported integrations/apps/add-ons.

# Integration Details

ThreatQuotient provides the following details for this integration:

| | |
|---|---|
| **Current Integration Version** | 1.0.0 |
| **Compatible with ThreatQ Versions** | >= 4.0.0 |
| **Support Tier** | Not Actively Supported |
| **ThreatQ Marketplace** | https://marketplace.threatq.com/details/any-run-operation |

# Introduction

The ANY.RUN Operation for ThreatQuotient enables a ThreatQ user to interact with ANY.RUN by submitting files and URLs to analyze and retrieve report data.

The operation provides the following actions:

- **Analyze** - sends a FQDN, URL or File to ANY.RUN to be analyzed in a sandbox.
- **Get Report** - fetches from ANY.RUN the reports for the analysis tasks that have been submitted from ThreatQ.

The operation is compatible with the following system objects:

- FQDN
- URL
- Attachment

# 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 parameters under the **Configuration** tab:

| PARAMETER | DESCRIPTION |
|---|---|
| **API Key** | Your ANY.RUN API Key. |
| **Automatically Add MITRE Techniques** | Enable this option to automatically upload MITRE Techniques filtered by threat level (Unknown, Suspicious, Malicious, Unsafe). |

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 actions:

| ACTION | DESCRIPTION | OBJECT TYPE | OBJECT SUBTYPE |
|---|---|---|---|
| Analyze | Sends a FQDN, URL or File to ANY.RUN to be analyzed in a sandbox. | Indicator, File | URL, FQDN |
| Get Reports | Fetches the reports for the analysis tasks that have been submitted from ThreatQ. | Indicator, File | URL, FQDN |

# Analyze

The Analyze action sends a URL or File to ANY.RUN to be analyzed in their sandbox, in an environment An attribute linking to the ANY.RUN applicator will be automatically added to the indicator/file.

`POST https://api.any.run/v1/analysis`

### Sample Response:

```
{
    "error": false,
    "data": {
        "taskid": "fa3d833e-97e5-40bf-a833-58b42f118612"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| data.taskid | Indicator.Attribute | Analysis Link | N/A | fa3d833e-97e5-40bf-a833-58b42f118612 | Formatted as `https://app.any.run/tasks/fa3d833e-97e5-40bf-a833-58b42f118612` |

# Action Parameters

The Analyze action provides the following parameters:

| PARAMETER | DESCRIPTION |
|---|---|
| **Environment** | The environment in which the indicator / file should be analyzed.<br><br>Options include:<br><br>• Windows 10 64 bit (default)<br>• Windows 8.1 64 bit<br>• Windows 8.1 32 bit<br>• Windows 7 64 bit<br>• Windows 7 32 bit<br>• Windows Vista 64 bit<br>• Windows Vista 32 bit |
| **Offline Analysis** | Whether the analysis should be run online. |
| **Network Location** | Geo location option.<br><br>Options include:<br><br>• Fastest (default)<br>• Australia<br>• Brazil<br>• France<br>• Germany<br>• Italy<br>• Russia<br>• South Korea<br>• Switzerland<br>• United Kingdom |

| PARAMETER | DESCRIPTION |
| --- | --- |
| | • United States |

# Get Reports

The Get Reports action fetches the reports for the analysis tasks that have been submitted from ThreatQ, via the operation.

```
GET https://api.any.run/v1/analysis/{taskID}
```

### Sample Response:

```
{
    "error": false,
    "data": {
        "analysis": {
            "uuid": "1e9a91bc-10d6-4b1f-b9a5-42718c0b87c8",
            "permanentUrl": "https://app.any.run/tasks/1e9a91bc-10d6-4b1f-
b9a5-42718c0b87c8",
            "reports": {
                "IOC": "https://api.any.run/report/1e9a91bc-10d6-4b1f-b9a5-42718c0b87c8/
ioc/json",
                "MISP": "https://api.any.run/report/1e9a91bc-10d6-4b1f-b9a5-42718c0b87c8/
summary/misp",
                "HTML": "https://api.any.run/report/1e9a91bc-10d6-4b1f-b9a5-42718c0b87c8/
summary/html",
                "graph": "https://content.any.run/tasks/1e9a91bc-10d6-4b1f-
b9a5-42718c0b87c8/graph"
            },
            "sandbox": {
                "name": "ANY.RUN - Interactive Sandbox",
                "plan": {
                    "name": "Tester"
                }
            },
            "duration": 60,
            "creation": 1663679409953,
            "creationText": "2022-09-20T13:10:09.953Z",
            "tags": [],
            "options": {
                "timeout": 60,
                "additionalTime": 0,
                "fakeNet": false,
                "heavyEvasion": false,
                "mitm": false,
                "tor": {
                    "used": false,
                    "geo": null
                },
                "presentation": false,
                "video": true,
                "hideSource": false,
```

```
                "network": false,
                "privacy": "bylink",
                "privateSample": false,
                "automatization": {
                    "uac": false
                }
            },
            "scores": {
                "verdict": {
                    "score": 30,
                    "threatLevel": 0,
                    "threatLevelText": "No threats detected"
                },
                "specs": {
                    "injects": false,
                    "autoStart": false,
                    "cpuOverrun": false,
                    "crashedApps": false,
                    "crashedTask": false,
                    "debugOutput": false,
                    "executableDropped": false,
                    "exploitable": false,
                    "lowAccess": false,
                    "memOverrun": false,
                    "multiprocessing": true,
                    "networkLoader": false,
                    "networkThreats": false,
                    "rebooted": false,
                    "serviceLauncher": false,
                    "spam": false,
                    "staticDetections": false,
                    "stealing": false,
                    "suspStruct": false,
                    "torUsed": false,
                    "privEscalation": false,
                    "notStarted": false,
                    "malwareConfig": false,
                    "knownThreat": false
                }
            },
            "content": {
                "mainObject": {
                    "type": "url",
                    "url": "http://rigpriv.com",
                    "hashes": {
                        "md5": "105ef5bef0041559a6bb087796af694e",
                        "sha1": "3043dd1bc9f2b2c5aca5742aa12bcece40e4910e",
                        "sha256":
"77e5b3abf9b6f2a24a1c2a0b7075e9b5e913a5b9793a166912dba824e232427a",
                        "ssdeep": "3:N1KMZ4dI:CMuK"
                    }
                },
                "video": {
                    "present": true,
                    "permanentUrl": "https://content.any.run/tasks/1e9a91bc-10d6-4b1f-
b9a5-42718c0b87c8/download/mp4"
                },
                "pcap": {
                    "present": false
                },
                "sslkeys": {
                    "present": false
```

```
                },
                "screenshots": [
                    {
                        "uuid": "79e1ba99-a1d1-4467-9a0d-f798293c4381",
                        "time": 47378,
                        "permanentUrl": "https://content.any.run/tasks/1e9a91bc-10d6-4b1f-
b9a5-42718c0b87c8..",
                        "thumbnailUrl": "https://content.any.run/tasks/1e9a91bc-10d6-4b1f-
b9a5-42718c0b87c8.."
                    },
                    {
                        "uuid": "81f18319-7f5c-4976-b01e-793992b40cc0",
                        "time": 21951,
                        "permanentUrl": "https://content.any.run/tasks/1e9a91bc-10d6-4b1f-
b9a5-42718c0b87c8/..",
                        "thumbnailUrl": "https://content.any.run/tasks/1e9a91bc-10d6-4b1f-
b9a5-42718c0b87c8/.."
                    }
                ]
            }
        },
        "environments": {
            "os": {
                "title": "Windows 7 Professional Service Pack 1 (build: 7601, 64 bit)",
                "build": 7601,
                "product": "Windows",
                "variant": "Professional",
                "productType": "Client",
                "major": "7",
                "servicePack": "1",
                "softSet": "complete",
                "bitness": 64
            },
            "internetExplorer": {
                "version": "11.0.9600.18860",
                "kbnum": "KB4052978"
            },
            "software": [
                {
                    "title": "Microsoft Visual C++ 2015-2019 Redistributable (x64) -
14.21.27702",
                    "version": "14.21.27702.2"
                },
                {
                    "title": "Adobe Acrobat Reader DC MUI",
                    "version": "15.007.20033"
                }
            ],
            "hotfixes": [
                {
                    "title": "WUClient SelfUpdate Core TopLevel"
                },
                {
                    "title": "KB3156016"
                }
            ]
        },
        "counters": {},
        "processes": [],
        "malconf": [],
        "network": {},
        "modified": {},
```

```
        "incidents": [],
        "debugStrings": [],
        "mitre": [
            {
                "id": "T1012",
                "phases": [
                    "discovery"
                ],
                "name": "Query Registry"
            }
        ],
        "status": "done"
    }
}
```

ThreatQuotient provides the following default mapping for this action:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .data.analysis.permanentUrl | Indicator.Attribute, File.Attribute | Analysis Link | N/A | https://app.any.run/tasks/1e9a91bc-10d6-4b1f-b9a5-42718c0b87c8 | N/A |
| .data.analysis.duration | Indicator.Attribute, File.Attribute | Analysis Duration | N/A | 60 | N/A |
| .data.analysis.tags[].tag | Indicator.Attribute, File.Attribute | Tag | N/A | N/A | N/A |
| .data.analysis.scores.verdict.score | Indicator.Attribute, File.Attribute | ANY.RUN Score | N/A | 30 | N/A |
| .data.analysis.scores.verdict.threatLevel | Indicator.Attribute, File.Attribute | Threat Level Code | N/A | 0 | N/A |
| .data.analysis.scores.verdict.threatLevelText | Indicator.Attribute, File.Attribute | Threat Level | N/A | No threats detected | N/A |
| .data.analysis.content.pcap.permanentUrl | Indicator.Attribute, File.Attribute | PCAP Link | N/A | https://content.any.run/tasks/cb81908f-f6b0-4bf4-bac0-a3b05ee0adaf/download/pcap | N/A |
| .data.environments.os.title | Indicator.Attribute, File.Attribute | Analysis Environment | N/A | Windows 7 Professional Service Pack 1 (build: 7601, 64 bit) | N/A |
| .data.mitre[].id - .data.mitre[].name | Related Attack Pattern.Value | N/A | N/A | T1012 - Query Registry | If `.data.analysis.scores.verdict.threatLevel` is selected in the `Auto Add Context Threat Levels` user configuration |
| .data.mitre[].phases[] | Related Attack Pattern.Attribute | Tactic | N/A | N/A | N/A |

# Associated Indicators

The indicators associated with reports will be loaded using this endpoint:

```
GET https://api.any.run/report/{taskID}/ioc/json
```

### Sample Response:

```
[
    {
        "category": "DNS requests",
        "type": "domain",
        "ioc": "r3.o.lencr.org",
        "reputation": 4
    },
    {
        "category": "Connections",
        "type": "ip",
        "ioc": "52.152.108.96",
        "reputation": 1
    }
]
```

ThreatQuotient provides the following default mapping for indicators of compromise:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| data[].ioc | Related Indicator.Value | Related Indicator.Type | N/A | r3.o.lencr.org | The type of the indicator is `.data[].type` |
| .data[].reputation | Related Indicator.Attribute | Reputation | N/A | 1 | Mapped using the `Reputation Mapping table` |
| .data[].category | Related Indicator.Attribute | Category | N/A | Connections | N/A |

## Reputation Mapping

ThreatQuotient provides the following ANY.RUN to ThreatQ reputation mapping:

| FEED DATA PATH | THREATQ ENTITY |
|---|---|
| 0 | Unknown |
| 1 | Suspicious |
| 2 | Malicious |
| 3 | Unsafe |

# Known Issues / Limitations

- You can only get reports for samples that you have submitted from ThreatQ. This is due to the fact that you can only get samples via a task ID, and not a hash value. The sample must have at least one attribute, "Analysis Link", with a value that links to the task.
- After running the **Analyze** action it might take some time for the report to be visible by the **Get Report** action. In the meantime, the message `Analysis task [taskID] is still in progress. Please try again later.` will be displayed when running **Get Reports**.

# Change Log

- **Version 1.0.0**
  - Initial release