# ThreatQuotient

## Recorded Future Operation

**Version 1.4.0**

April 02, 2024

**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** | 1.4.0 |
| **Compatible with ThreatQ Versions** | >= 4.35.0 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The ThreatQuotient for Recorded Future Operation allows a ThreatQ user to submit system objects to Recorded Future for enrichment.

The operation provides the following actions:

- **Enrich** - provides enrichment of the selected object.
- **Find Entity Links** - fetches relationships for a given entity.
- **Intel Card Link** - links to the Recorded Future Intel Card.

The operation is compatible with the following object types:

- Adversaries
- Attack Patterns
- Indicators

  > See the Actions table for specific compatible indicator types.

- Malware

# 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 whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration whl file using one of the following methods:
    - Drag and drop the whl file into the dialog box
    - Select **Click to Browse** to locate the integration whl 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.

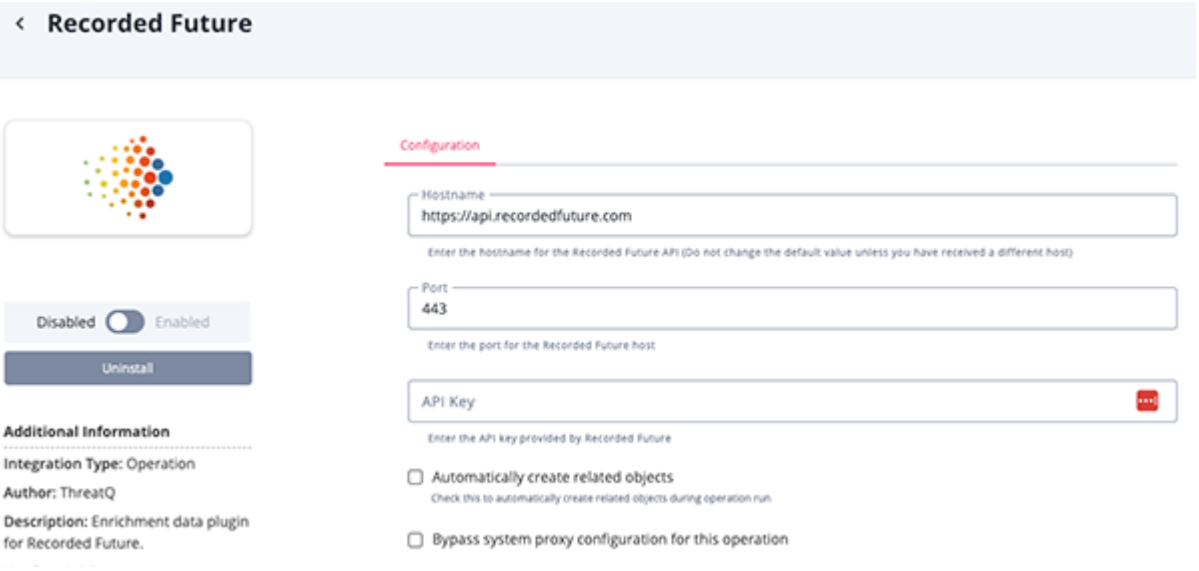
# Configuration

> 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 |
|---|---|
| **Hostname** | The hostname for the API. |
| **Port** | The port for the Recorded Future host. |
| **API Key** | The API Access Key provided by Recorded Future. |
| **Automatically Create Related Objects** | When enabled, the integration will create related objects during the operation run. |




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 |
|---|---|---|---|
| Enrich | Provides enrichment of the selected object. | Indicator | Indicator Types: IP Address, FQDN, CVE, MD5, SHA-1, SHA-256, SHA-384, SHA-512, URL |
| Find Entity Links | Fetches relationships for a given entity | Indicator, Malware, Adversary, Attack Pattern | Indicator Types: IP Address, FQDN, CVE, MD5, SHA-1, SHA-256, SHA-384, SHA-512 |
| Intel Card Link | Links to the Recorded Future Intel Card. | Indicator | Indicator Types: IP Address, FQDN, CVE, MD5, SHA-1, SHA-256, SHA-384, SHA-512 |

# Enrich

The Enrich action provides enrichment from Recorded Future on the selected object.

`GET https://api.recordedfuture.com:443/v2/ip/{indicator}?fields=risk,entity,intelCard,location,metrics,relatedEntities,timestamps`

**Sample Response:**


```
{
    "data": {
        "location": {
            "organization": "DIGITALOCEAN-ASN",
            "cidr": {
                "id": "ip:192.241.192.0/19",
                "name": "192.241.192.0/19",
                "type": "IpAddress"
            },
            "location": {
                "continent": "North America",
                "country": "United States",
                "city": "San Francisco"
            },
            "asn": "AS14061"
        },
        "timestamps": {
            "lastSeen": "2022-02-20T20:19:49.836Z",
            "firstSeen": "2020-07-09T09:24:18.846Z"
        },
        "risk": {
            "criticalityLabel": "Suspicious",
            "riskString": "9/77",
            "rules": 9,
            "criticality": 2,
            "riskSummary": "9 of 77 Risk Rules currently observed.",
            "score": 39,
            "evidenceDetails": [
                {
                    "mitigationString": "",
                    "evidenceString": "4 sightings on 1 source: AbuseIP
Database. Most recent link (Jul 9, 2020): https://www.abuseipdb.com/check/
192.241.212.32",
                    "rule": "Historical Multicategory Blocklist",
                    "criticality": 1,
                    "timestamp": "2020-07-09T09:24:09.046Z",
                    "criticalityLabel": "Unusual"
                }
            ]
        },
        "intelCard": "https://app.recordedfuture.com/live/sc/entity/
```

```
ip%3A192.241.212.32",
        "entity": {
            "id": "ip:192.241.212.32",
            "name": "192.241.212.32",
            "type": "IpAddress"
        },
        "metrics": [
            {
                "type": "unusualIPSightings",
                "value": 6
            }
        ],
        "relatedEntities": []
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .data.relatedEntities[] | Related Indicator | IP Address/FQDN/ HASH/URL | N/A | N/A | If .data.relatedEntities[].type in `RelatedIpAddress`, `RelatedInternetDomainName`, `RelatedHash`, `RelatedURL` |
| .data.relatedEntities[] | Indicator Attribute | .data.related Entities[].name | N/A | N/A | If .data.relatedEntities[].type in `RelatedMalwareCategory`, `RelatedAttackVector`, `RelatedMalware`, `RelatedProduct` |
| .data.risk.score | Indicator Attribute | Risk Score | N/A | 39 | N/A |
| .data.risk.criticalityLabel | Indicator Attribute | Criticality | N/A | Suspicious | N/A |
| .data.risk.riskSummary | Indicator Attribute | Risk Summary | N/A | 9 of 77 Risk Rules currently observed. | N/A |
| .data.risk.evidenceDetails[].rule | Indicator Attribute | Rule | N/A | Historical Multicategory Blocklist | N/A |
| .data.metrics.type/ .data.metrics.value | Indicator Attribute | Unusual IP Sightings | N/A | 6 | `.data.metric.type` is processed as title |
| .data.timestamps.firstSeen | Indicator Attribute | First Seen | N/A | 2020-07-09T09:24:18.846Z | N/A |
| .data.timestamps.lastSeen | Indicator Attribute | Last Seen | N/A | 2022-02-20T20:19:49.836Z | N/A |

# Find Entity Links

The Find Entity Links action fetches relationships for a given entity.

`POST https://api.recordedfuture.com/links/search`

**Sample Request:**

```
{"entities":["ip:192.241.212.32"],
"limits": {"search_scope": "medium", "per_entity_type": 100},
"filters": {

    "entity_types": ["type:Malware", "type:Person",
"type:MitreAttackIdentifier", "type:AttackVector", "type:Organization",
"type:IpAddress", "type:InternetDomainName", "type:Hash",
"type:CyberVulnerability", "type:Username"],
    "sources": ["technical", "insikt"],
    "sections": ["iU_ZsE", "iU_ZsG", "iU_ZsI"]
    }
}
```

**Sample Response:**

```
{
    "data": [
        {
            "entity": {
                "type": "type:IpAddress",
                "id": "ip:192.241.212.32",
                "name": "192.241.212.32"
            },
            "links": [
                {
                    "type": "type:Hash",
                    "id":
"hash:470de980ea57e5cbaaf82ffd66229a9c59fbc1ab43b41fa4ba092adcbc305dba",
                    "name":
"470de980ea57e5cbaaf82ffd66229a9c59fbc1ab43b41fa4ba092adcbc305dba",
                    "source": "technical",
                    "section": "iU_ZsG",
                    "attributes": [
                        {
                            "id": "criticality",
                            "value": "Malicious"
                        },
                        {
                            "id": "risk_score",
                            "value": 70
                        },
                        {
                            "id": "risk_level",
```

```
                        "value": 3
                    }
                ]
            },
            {
                "type": "type:Malware",
                "id": "YuDlCN",
                "name": "WARZONE RAT",
                "source": "technical",
                "section": "iU_ZsE",
                "attributes": []
            },
            {
                "type": "type:MitreAttackIdentifier",
                "id": "mitre:T1584",
                "name": "T1584",
                "source": "technical",
                "section": "iU_ZsE",
                "attributes": [
                    {
                        "id": "display_name",
                        "value": "T1584 (Compromise Infrastructure)"
                    }
                ]
            },
            {
                "type": "type:MitreAttackIdentifier",
                "id": "mitre:TA0011",
                "name": "TA0011",
                "source": "technical",
                "section": "iU_ZsE",
                "attributes": [
                    {
                        "id": "display_name",
                        "value": "TA0011 (Command and Control)"
                    }
                ]
            }
        ]
    }
]
}
```

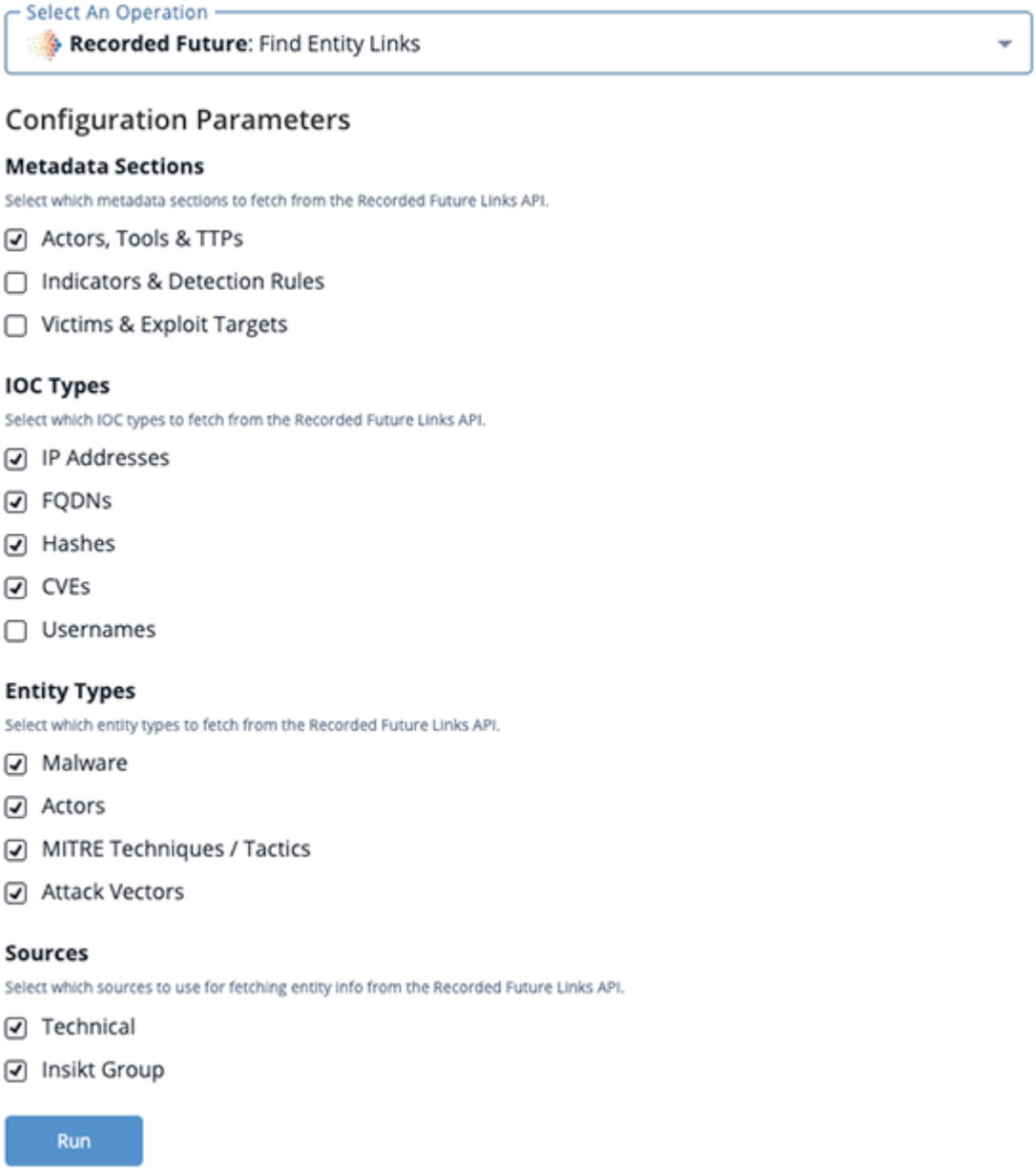
ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .data.links[].name | Related Indicator | .data.link[].type | N/A | 470de980ea57e5cb aaf82ffd66229a9c5 9fbc1ab43b41fa4ba 092adcbc305dba | If .data.links[].type in see `Entity IOC type map` table. If `Indicators & Detection Rules` is checked and if corresponding `.data.links[].type` from `Entity IOC type map` is checked |
| .data.links[].attributes[].value | Related Indicator Attribute | Criticality | N/A | Malicious | If .data.links[].attributes[].id is `criticality` |
| .data.links[].attributes[].value | Related Indicator Attribute | Risk Score | N/A | 70 | If .data.links[].attributes[].id is `risk_score` |
| .data.links[].attributes[].value | Related Indicator Attribute | Risk Level | N/A | 3 | If .data.links[].attributes[].id is `risk_level` |
| .data.links[].attributes[].value | Related Attack Pattern | N/A | N/A | T1584 (Compromise Infrastructure) | If .data.links[].type is `type:MitreAttackIdentifier` and `.data.link[].attributes[].id` is `display_name` |
| .data.links[].attributes[].value | Indicator Attribute | Tactic | N/A | Command and Control | If .data.links[].type is `type:MitreAttackIdentifier` and `.data.link[].attributes[].id` is `display_name` and `.data.link[].name` starts with `TA` |
| .data.links[].name | Related Malware | N/A | N/A | WARZONE RAT | If `.data.links[].type` is `type:Malware` and `Malware` is checked |
| .data.links[].name | Related Adversary | N/A | N/A | N/A | If `.data.links[].type` is `type:Person` or `type:Organization` and `Actors` is checked |
| .data.links[].name | Indicator Attribute | Attack Vector | N/A | N/A | If `.data.links[].type` is `type:AttackVector` and `Attack Vector` is checked |

## Find Entity Links Run Parameters

The follow run parameters are available when you select the Find Entity Links action:

| PARAMETER | DESCRIPTION |
|---|---|
| **Metadata Sections** | Select which metadata sections to fetch from the Recorded Future Links API. Options include:<br>• Actors, Tools & TTPs<br>• Indicators & Detection Rules<br>• Victims & Exploit Targets |
| **IOC Types** | Select which IOC types to fetch from the Recorded Future Links API. Options include:<br>• IP Addresses<br>• FQDNs<br>• Hashes<br>• CVEs<br>• Usernames |
| **Entity Types** | Select which entity types to fetch from the Recorded Future Links API. Options include:<br>• Malware<br>• Actors<br>• MITRE Techniques / Tactics<br>• Attack Vectors |
| **Sources** | Select which sources to use for fetching entity info from the Recorded Future Links API. Options include:<br>• Technical<br>• Insikt Group |


Select An Operation
Recorded Future: Find Entity Links
Configuration Parameters
Metadata Sections
Select which metadata sections to fetch from the Recorded Future Links API.
Actors, Tools & TTPs
Indicators & Detection Rules
Victims & Exploit Targets
IOC Types
Select which IOC types to fetch from the Recorded Future Links API.
IP Addresses
FQDNs
Hashes
CVEs
Usernames
Entity Types
Select which entity types to fetch from the Recorded Future Links API.
Malware
Actors
MITRE Techniques / Tactics
Attack Vectors
Sources
Select which sources to use for fetching entity info from the Recorded Future Links API.
Technical
Insikt Group
Run

## Entity IOC Type Mapping

The following table describes the Recorded Future to ThreatQ IOC Type mapping.

| RECORDED FUTURE VALUE | THREATQ IOC TYPE |
|---|---|
| type:IpAddress | IP Address |
| type:InternetDomainName | FQDN |
| type:Hash | MD5 |
| type:Hash | SHA-2 |
| type:Hash | SHA-256 |
| type:Hash | SHA-384 |
| type:Hash | SHA-512 |
| type:CyberVulnerability | CVE |
| type:Username | Username |

## Entity Object Type Mapping

The following table describes the Recorded Future Entity to ThreatQ Object Type mapping.

| RECORDED FUTURE VALUE | THREATQ IOC TYPE |
|---|---|
| type:Malware | Malware |
| type:Person | Adversary |
| type:Organization | Adversary |
| type:MitreAttackIdentifier | Attack Pattern-2 |

# Intel Card Link

The Intel Card Link action provides a link to the Recorded Future Intel Card.

`GET https://api.recordedfuture.com:443/v2/ip/{indicator}?fields=intelCard`

**Sample Response:**

```
{
    "data": {
        "intelCard": "https://app.recordedfuture.com/live/sc/entity/
ip%3A192.241.212.32"
    }
}
```

# Change Log

- **Version 1.4.0**
  - Added URL-type indicator support to the Enrich action.
  - Added new action: **Find Entity Links**. This action fetches relationships for a given entity.
  - Added new configuration parameter: **Automatically Create Related Objects**. This new parameter is only applicable to the **Find Entity Links** action.
- **Version 1.3.0**
  - Removed the ability to pull related vulnerabilities due to some vulnerabilities not having a proper value. This would cause an error when ThreatQ attempted to ingest the information.
- **Version 1.2.0**
  - Added enrichment of CVE objects.
  - Added the ability to pull related vulnerabilities from Recorded Future
- **Version 1.0.0**
  - Initial release