

ThreatQuotient

A Securonix Company



Recorded Future Operation

Version 1.5.0

March 30, 2026

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details	5
Introduction.....	6
Prerequisites	7
Installation.....	8
Configuration.....	9
Actions.....	11
Enrich.....	12
Find Entity Links	15
Run Configuration Options	18
Entity IOC Type Mapping.....	20
Entity Object Type Mapping	21
Intel Card Link	22
Update Playbook Alert.....	23
Run Configuration Options	23
Update Alert.....	26
Run Configuration Options	26
Change Log	28

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.

Copyright © 2026 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.


Support Email: tq-support@securonix.com

Support Web: <https://ts.securonix.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 1.5.0

Compatible with ThreatQ Versions $\geq 5.0.0$

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.
- **Update Playbook Alert** - updates a Recorded Future Playbook Alert associated with an event.
- **Update Alert** - updates a Recorded Future Alert associated with an event.

The operation is compatible with the following object types:

- Adversaries
- Attack Patterns
- Events
- Indicators



See the [Actions table](#) for specific compatible indicator types.

- Malware

Prerequisites

The following is required in order to install and run the integration:

- A Recorded Future 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 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.

< Recorded Future



Disabled Enabled

Uninstall

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: Enrichment data plugin for Recorded Future.

Configuration

Hostname

Enter the hostname for the Recorded Future API (Do not change the default value unless you have received a different host)

Port

Enter the port for the Recorded Future host

API Key [Redacted]
Enter the API key provided by Recorded Future

Automatically create related objects
Check this to automatically create related objects during operation run

Bypass system proxy configuration for this operation

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	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	IP Address, FQDN, CVE, MD5, SHA-1, SHA-256, SHA-384, SHA-512
Update Playbook Alert	Update a Recorded Future Playbook Alert linked to an event	Event	Recorded Future Playbook Alert
Update Alert	Update a Recorded Future Alert linked to an event	Event	N/A

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,timesta
mps
```

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 action:

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.relatedEntities[].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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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 action:

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

Run Configuration Options



These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this action:

PARAMETER	DESCRIPTION
Metadata Sections	<p>Select which metadata sections to fetch from the Recorded Future Links API. Options include:</p> <ul style="list-style-type: none"> • Actors, Tools & TTPs • Indicators & Detection Rules • Victims & Exploit Targets
IOC Types	<p>Select which IOC types to fetch from the Recorded Future Links API. Options include:</p> <ul style="list-style-type: none"> • IP Addresses • FQDNs • Hashes • CVEs • Usernames
Entity Types	<p>Select which entity types to fetch from the Recorded Future Links API. Options include:</p> <ul style="list-style-type: none"> • Malware • Actors • MITRE Techniques / Tactics • Attack Vectors
Sources	<p>Select which sources to use for fetching entity info from the Recorded Future Links API. Options include:</p> <ul style="list-style-type: none"> • Technical

PARAMETER

DESCRIPTION

- 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"  
  }  
}
```

Update Playbook Alert

The Update Playbook Alert action enables you to update the corresponding Playbook Alert in Recorded Future.

PUT `https://api.recordedfuture.com/playbook-alert/common/{alertId}`

Sample Request:

```
{
  "status": "Resolved",
  "priority": "Moderate",
  "reopen": "Never",
  "added_actions_taken": ["cyber_vulnerability.patched"]
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Event.Attribute	Status	N/A	Resolved	Updatable. Based on user-field selection for the Operation
N/A	Event.Attribute	Priority	N/A	Moderate	Updatable. Based on user-field selection for the Operation
N/A	Event.Attribute	Log Entry	N/A	N/A	Updatable. Based on user-field selection for the Operation

Run Configuration Options



These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this action:

PARAMETER	DESCRIPTION
Priority	Select the priority of the alert. Options include: <ul style="list-style-type: none"> • Do Not Change • High • Moderate • Informational

PARAMETER

DESCRIPTION

Status

Select the status of the alert. Options include:

- Do Not Change
- New
- In Progress
- Resolved
- Dismissed

Never Reopen

Enable this option to never reopen the alert. This option is disabled by default.

Added Actions

Select the actions taken on the alert. Options include:

- Vulnerability Patched
- Keys Rotated
- Takedown Requested
- Vendor Mitigated Findings
- Enforce Password Reset

Remove Actions

Select the actions taken on the alert. Options include:

- Vulnerability Patched
- Keys Rotated
- Takedown Requested
- Vendor Mitigated Findings
- Enforce Password Reset

Log Entry

Enter a log entry to be added to the alert.

Phishing Email scam [Edit](#)

EVENT: INCIDENT

Created: 03/30/2026 Event Date: 03/30/2026 07:28pm First Published: 03/30/2026 07:28pm Last Modified: 03/30/2026 07:28pm

- Actions
- Context
 - Attributes (0)
 - Sources (1)
 - Tags (0)
 - Descriptions (0)
 - Additional Information (1)
- Relationships
- Comments (0)
- Operations**
- Orchestrator
- Audit Log

Operations

Select An Operation

Recorded Future: Update Playbook Alert

Configuration Parameters

Priority
Do Not Change
Set the priority of the alert

Status
Do Not Change
Set the status of the alert

Never Reopen
Check this to never reopen the alert

Added Actions

Actions taken on the alert

- Vulnerability Patched
- Keys Rotated
- Takedown Requested
- Vendor Mitigated Findings
- Enforced Password Reset

Removed Actions

Actions removed from the alert

- Vulnerability Patched
- Keys Rotated
- Takedown Requested
- Vendor Mitigated Findings
- Enforced Password Reset

Log Entry
Add a log entry to the alert

Update Alert

The Update Alert action enables you to update the corresponding Alert in Recorded Future.

POST <https://api.recordedfuture.com/v2/alert/update>

Sample Request:

```
[
  {
    "statusInPortal": "Resolved",
    "note": "This is a test note"
  }
]
```

Run Configuration Options



These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration options are available for this action:

PARAMETER	DESCRIPTION
Status	Select the status of the alert. Options include: <ul style="list-style-type: none"> • Do Not Change • New • Resolved • Pending • Dismissed
Note	Enter a note to be added to the alert.

 **Operations**

Select An Operation
 **Recorded Future: Update Alert**

Configuration Parameters

Status
Do Not Change

Set the status of the alert

Note

Set a note for the alert

Run

Change Log

- **Version 1.5.0**
 - Added two new operation actions:
 - **Update Playbook Alert** - updates a Recorded Future Playbook Alert associated with an event.
 - **Update Alert** - updates a Recorded Future Alert associated with an event.
 - Updated the minimum ThreatQ version to 5.0.0.
- **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