ThreatQuotient

Recorded Future CDF

Version 2.8.7

May 14, 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	2.8.7
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Recorded Future CDF ingests threat intelligence data from the following feeds published by the *Recorded Future* vendor:

- **Recorded Future Domain Risk List** - retrieves information in the form of a CSV list where the first token is risk data and the last token containing the supporting context.
- **Recorded Future IP Risk List** - retrieves IP Addresses from the provider.
- **Recorded Future URL Risk List** - retrieves URLS from the provider.
- **Recorded Future Vulnerability Risk List** - retrieves CVEs from the provider.
- **Recorded Future Hash Risk List** - retrieves Hashes from the provider.
- **Recorded Future Analyst Note** - retrieves Reports, Indicators, and Attack Patterns from the provider.
- **Recorded Future Alerts** - retrieves Alerts from the provider.
- **Recorded Future Alerts Details (Supplemental)** - retrieves related data for each of the ingested events retrieved from the Alert endpoint.
- **Recorded Future Playbook Alerts** - retrieves a list of alerts filtered by the values provided in the configuration section.
- **Domain Abuse Playbook Alert (Supplemental)** - retrieves related data for each of the ingested events retrieved from the Alert endpoint.

The integration ingests the following system objects:

- Attack Patterns
  - Attack Pattern Attributes
- Events
  - Event Attributes
- Indicators
  - Indicator Attributes
- Malware
  - Malware Attributes
- Reports
  - Report Attributes
- Vulnerabilities
  - Vulnerability Attributes

Prerequisites

MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns ingested by the Analyst Note feed to be created. MITRE ATT&CK attack patterns are ingested from the following feeds:

- MITRE Enterprise ATT&CK
- MITRE Mobile ATT&CK
- MITRE PRE-ATT&CK

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:

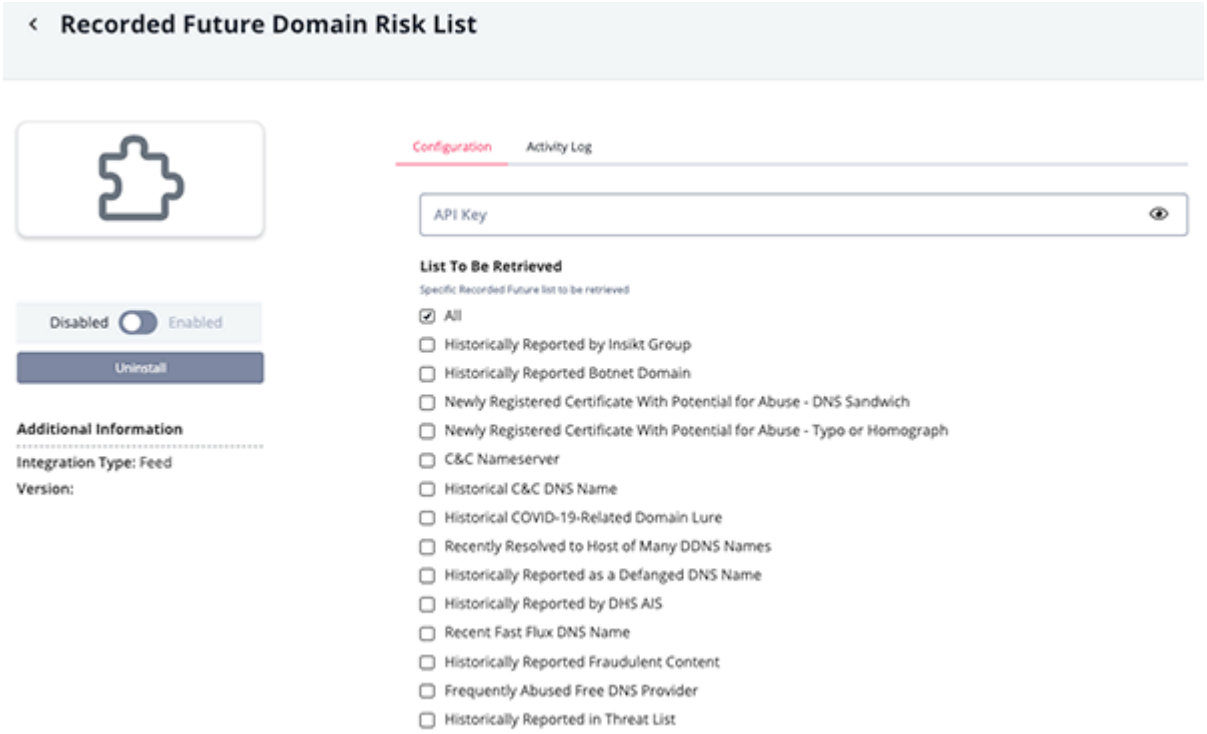
   > All Recorded Future feeds require the Recorded Future API Key. The tables below provide any additional parameters required for specific feeds included with this integration.

Recorded Future Domain Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved. It is highly recommended to use the **All** option as it will ingest the latest information from Recorded Future. If you are using the **All** option, confirm that you have unselected the other options. Running the feed with the **All** option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the **All** option.

PARAMETER	DESCRIPTION
	Options include: ◦ All (default) ◦ Historically Reported by Insikt Group ◦ Historically Reported Botnet Domain ◦ Newly Registered Certificate With Potential for Abuse - DNS Sandwich ◦ Newly Registered Certificate With Potential for Abuse - Typo or Homograph ◦ C&C Nameserver ◦ Historical C&C DNS Name ◦ Historical COVID-19-Related Domain Lure ◦ Recently Resolved to Host of Many DDNS Names ◦ Historically Reported as a Defanged DNS Name ◦ Historically Reported by DHS AIS ◦ Recent Fast Flux DNS Name ◦ Historically Reported Fraudulent Content ◦ Frequently Abused Free DNS Provider ◦ Historically Reported in Threat List ◦ Historically Linked to Cyber Attack ◦ Historically Detected Malware Operation ◦ Historically Suspected Malware Operation ◦ Historically Detected Cryptocurrency Mining Techniques ◦ Blacklisted DNS Name ◦ No Risk Observed ◦ Observed in the Wild by Recorded Future Telemetry ◦ Historical Phishing Lure ◦ Historically Detected Phishing Techniques ◦ Historically Suspected Phishing Techniques ◦ Active Phishing URL ◦ Recorded Future Predictive Risk Model ◦ Recently Reported Fraudulent Content ◦ Recently Linked to Cyber Attack ◦ Recently Detected Malware Operation ◦ Recently Suspected Malware Operation ◦ Recent Cryptocurrency Mining Pool ◦ Recently Detected Cryptocurrency Mining Techniques ◦ Recent Phishing Lure: Malicious ◦ Recent Phishing Lure: Suspicious ◦ Recently Detected Phishing Techniques ◦ Recently Suspected Phishing Techniques ◦ Recent Web Filter Avoidance Proxy Domain ◦ Recent Punycode Domain ◦ Recently Referenced by Insikt Group ◦ Recently Reported Spam or Unwanted Content ◦ Recent Suspected C&C DNS Name ◦ Recent Threat Researcher ◦ Recent Typosquat Similarity - DNS Sandwich ◦ Recent Typosquat Similarity - Typo or Homograph ◦ Recent Ukraine-Related Domain Lure: Malicious ◦ Recent Ukraine-Related Domain Lure: Suspicious ◦ Recently Active Weaponized Domain

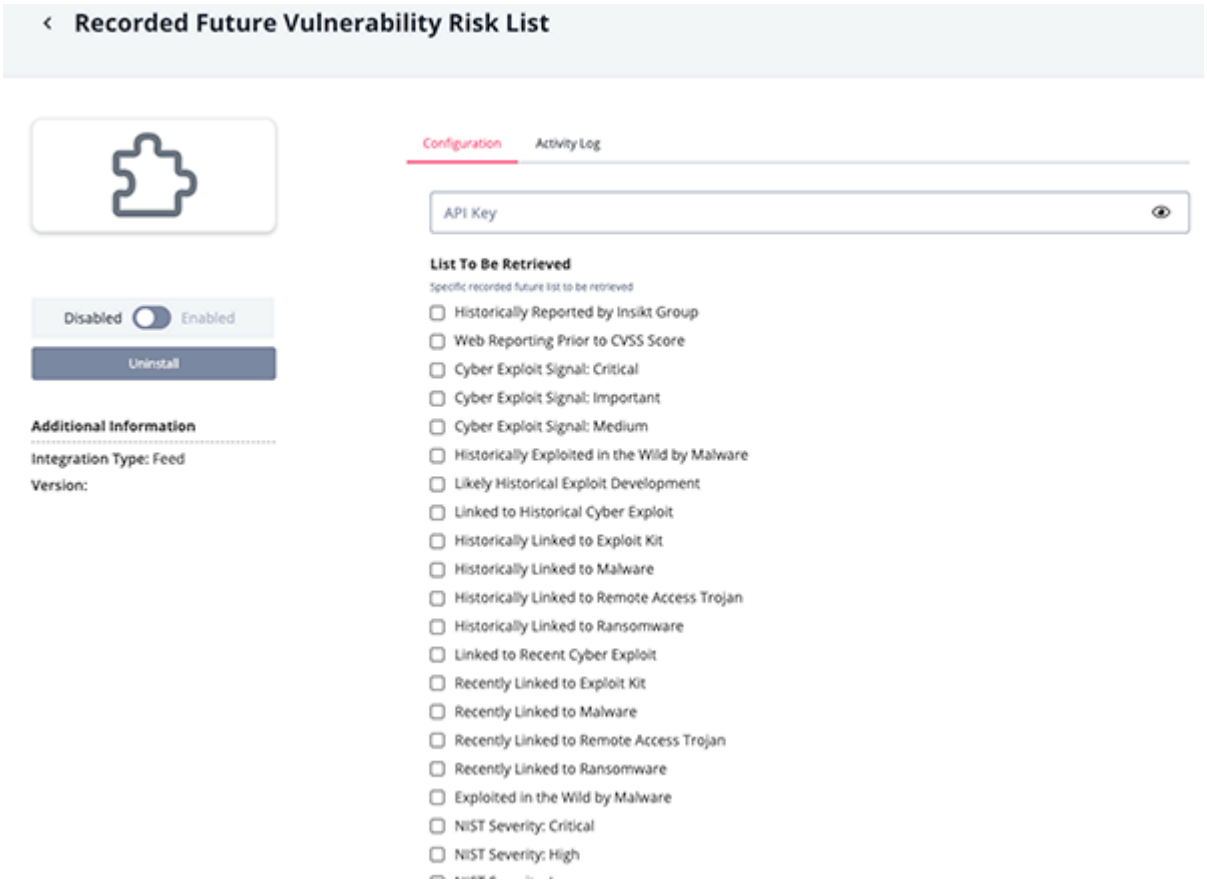
PARAMETER	DESCRIPTION
	◦ Historically Detected Web Filter Avoidance Proxy Domain ◦ Historical Punycode Domain ◦ Recently Reported by Insikt Group ◦ Recently Reported Botnet Domain ◦ Recent C&C DNS Name ◦ Recent COVID-19-Related Domain Lure: Malicious ◦ Recent COVID-19-Related Domain Lure: Suspicious ◦ Recently Reported as a Defanged DNS Name ◦ Recently Reported by DHS AIS ◦ Recently Defaced Site ◦ Historically Referenced by Insikt Group ◦ Recently Resolved to Malicious IP ◦ Recently Resolved to Suspicious IP ◦ Recently Resolved to Unusual IP ◦ Recently Resolved to Very Malicious IP ◦ Trending in Recorded Future Analyst Community ◦ Historically Reported Spam or Unwanted Content ◦ Historical Suspected CANDC DNS Name ◦ Historical Threat Researcher ◦ Historical Typosquat Similarity - DNS Sandwich ◦ Historical Typosquat Similarity - Typo or Homograph ◦ Historical Ukraine-Related Domain Lure ◦ Historically Active Weaponized Domain
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.


Recorded Future Domain Risk List
Disabled
Enabled
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
API Key
List To Be Retrieved
Specific Recorded Future list to be retrieved
All
Historically Reported by Insikt Group
Historically Reported Botnet Domain
Newly Registered Certificate With Potential for Abuse - DNS Sandwich
Newly Registered Certificate With Potential for Abuse - Typo or Homograph
C&C Nameserver
Historical C&C DNS Name
Historical COVID-19-Related Domain Lure
Recently Resolved to Host of Many DDNS Names
Historically Reported as a Defanged DNS Name
Historically Reported by DHS AIS
Recent Fast Flux DNS Name
Historically Reported Fraudulent Content
Frequently Abused Free DNS Provider
Historically Reported in Threat List

Recorded Future Vulnerability Risk List Parameters

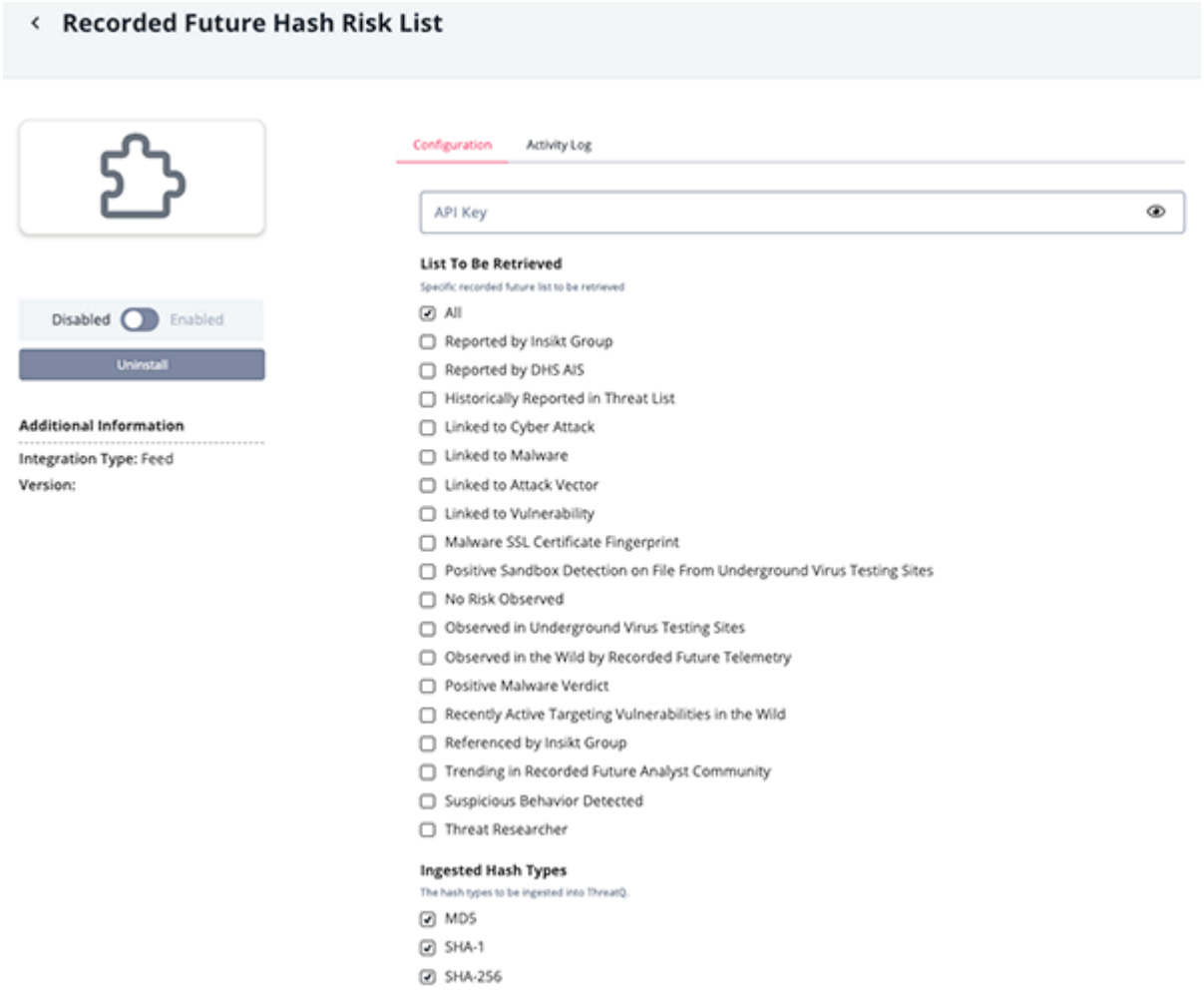
PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved. Options include: ° Historically Reported by Insikt Group ° Web Reporting Prior to CVSS Score ° Cyber Exploit Signal: Critical ° Cyber Exploit Signal: Important ° Cyber Exploit Signal: Medium ° Historically Exploited in the Wild by Malware ° Likely Historical Exploit Development ° Linked to Historical Cyber Exploit ° Historically Linked to Exploit Kit ° Historically Linked to Malware ° Historically Linked to Remote Access Trojan ° Historically Linked to Ransomware ° Linked to Recent Cyber Exploit ° Recently Linked to Exploit Kit ° Recently Linked to Malware ° Recently Linked to Remote Access Trojan ° NIST Severity: Low ° NIST Severity: Medium ° Web Reporting Prior to NVD Disclosure ° Historical Unverified Proof of Concept Available ° Historical Verified Proof of Concept Available ° Historical Verified Proof of Concept Available Using Remote Execution ° Recently Reported by Insikt Group ° Exploit Likely in Active Development ° Exploited in the Wild by Recently Active Malware ° Recent Unverified Proof of Concept Available ° Recent Verified Proof of Concept Available ° Recent Verified Proof of Concept Available Using Remote Execution ° Recently Referenced by Insikt Group ° Recently Linked to Penetration Testing Tools ° Historically Referenced by Insikt Group ° Historically Linked to Penetration Testing Tools ° Vendor Severity: Critical ° Vendor Severity: High ° Vendor Severity: Low ° Vendor Severity: Medium

PARAMETER	DESCRIPTION
	◦ Recently Linked to Ransomware ◦ Exploited in the Wild by Malware ◦ NIST Severity: Critical ◦ NIST Severity: High
Save CVE Data As	Select whether to ingest CVEs as: Vulnerabilities, Indicators, or Both. The default setting is to ingest Indicators objects.
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.



Recorded Future Hash Risk List Parameters

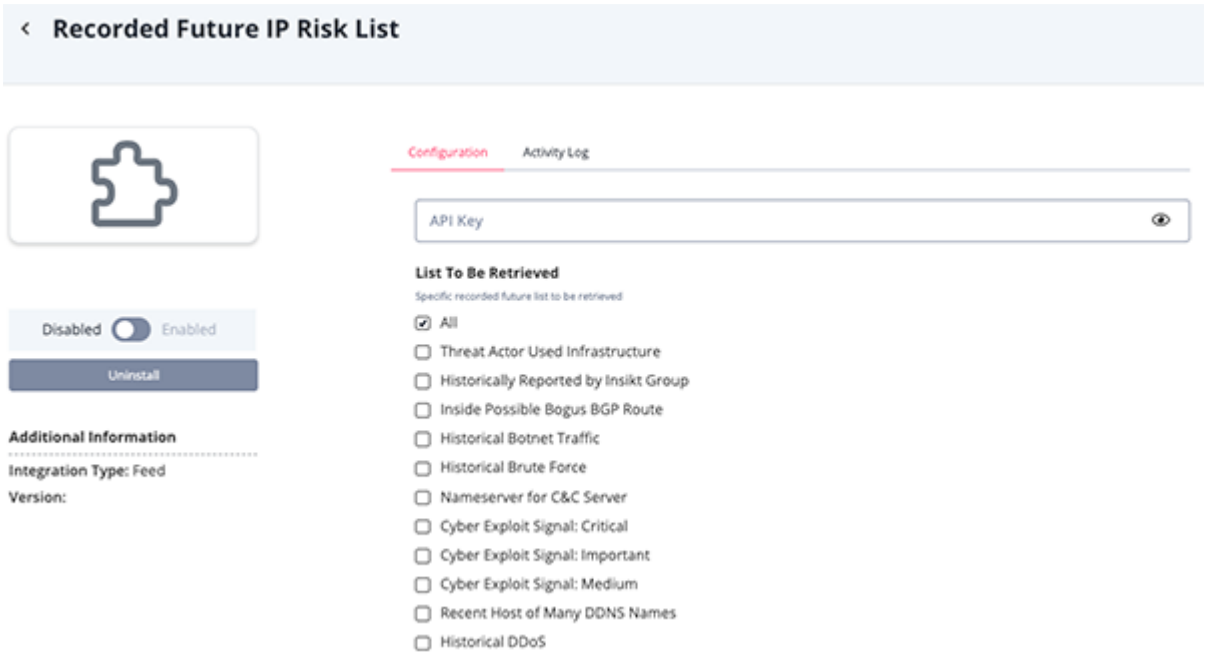
PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved. ⚠ It is highly recommended to use the **All** option as it will ingest the latest information from Recorded Future. If you are using the **All** option, confirm that you have unselected the other options. Running the feed with the **All** option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the **All** option. Options include: ◦ All (default) ◦ Reported by Insikt Group ◦ Reported by DHS AIS ◦ Historically Reported in Threat List ◦ Linked to Cyber Attack ◦ Linked to Malware ◦ Linked to Attack Vector ◦ Linked to Vulnerability ◦ Malware SSL Certificate Fingerprint ◦ Positive Sandbox Detection on File From Underground Virus Testing Sites ◦ No Risk Observed ◦ Observed in Underground Virus Testing Sites ◦ Observed in the Wild by Recorded Future Telemetry ◦ Positive Malware Verdict ◦ Recently Active Targeting Vulnerabilities in the Wild ◦ Referenced by Insikt Group ◦ Trending in Recorded Future Analyst Community ◦ Suspicious Behavior Detected ◦ Threat Researcher
Ingested Hash Types	Select the type of hashes to be ingested into ThreatQ. Options include ◦ MD5 ◦ SHA-1 ◦ SHA-256


Recorded Future Hash Risk List
Disabled
Enabled
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
API Key
List To Be Retrieved
Specific recorded future list to be retrieved
All
Reported by Insikt Group
Reported by DHS AIS
Historically Reported in Threat List
Linked to Cyber Attack
Linked to Malware
Linked to Attack Vector
Linked to Vulnerability
Malware SSL Certificate Fingerprint
Positive Sandbox Detection on File From Underground Virus Testing Sites
No Risk Observed
Observed in Underground Virus Testing Sites
Observed in the Wild by Recorded Future Telemetry
Positive Malware Verdict
Recently Active Targeting Vulnerabilities in the Wild
Referenced by Insikt Group
Trending in Recorded Future Analyst Community
Suspicious Behavior Detected
Threat Researcher
Ingested Hash Types
The hash types to be ingested into ThreatQ.
MD5
SHA-1
SHA-256

Recorded Future IP Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved. ⚠ It is highly recommended to use the **All** option as it will ingest the latest information from Recorded Future. If you are using the **All** option, confirm that you have unselected the other options. Running the feed with the **All** option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the **All** option. Options include: ◦ All (default) ◦ Threat Actor Used Infrastructure ◦ Historically Reported by Insikt Group ◦ Inside Possible Bogus BGP Route ◦ Historical Botnet Traffic ◦ Historical Brute Force ◦ Nameserver for C&C Server ◦ Cyber Exploit Signal: Critical ◦ Cyber Exploit Signal: Important ◦ Cyber Exploit Signal: Medium ◦ Recent Host of Many DDNS Names ◦ Historical DDoS ◦ Historically Reported as a Defanged IP ◦ Historically Reported by DHS AIS ◦ Historical DNS Abuse ◦ Resolution of Fast Flux DNS Name ◦ Recent DNS Abuse ◦ Recent Honeypot Sighting ◦ Recently Linked to Intrusion Method ◦ Recently Linked to APT ◦ Recently Linked to Cyber Attack ◦ Recent Malicious Infrastructure Admin Server ◦ Recent Malware Delivery ◦ Recent Multicategory Blocklist ◦ Recent Open Proxies ◦ Recent Phishing Host ◦ Recent Positive Malware Verdict ◦ Recently Referenced by Insikt Group ◦ Recently Reported C&C Server ◦ Recently Communicating With Reported C&C Server ◦ Recent Spam Source

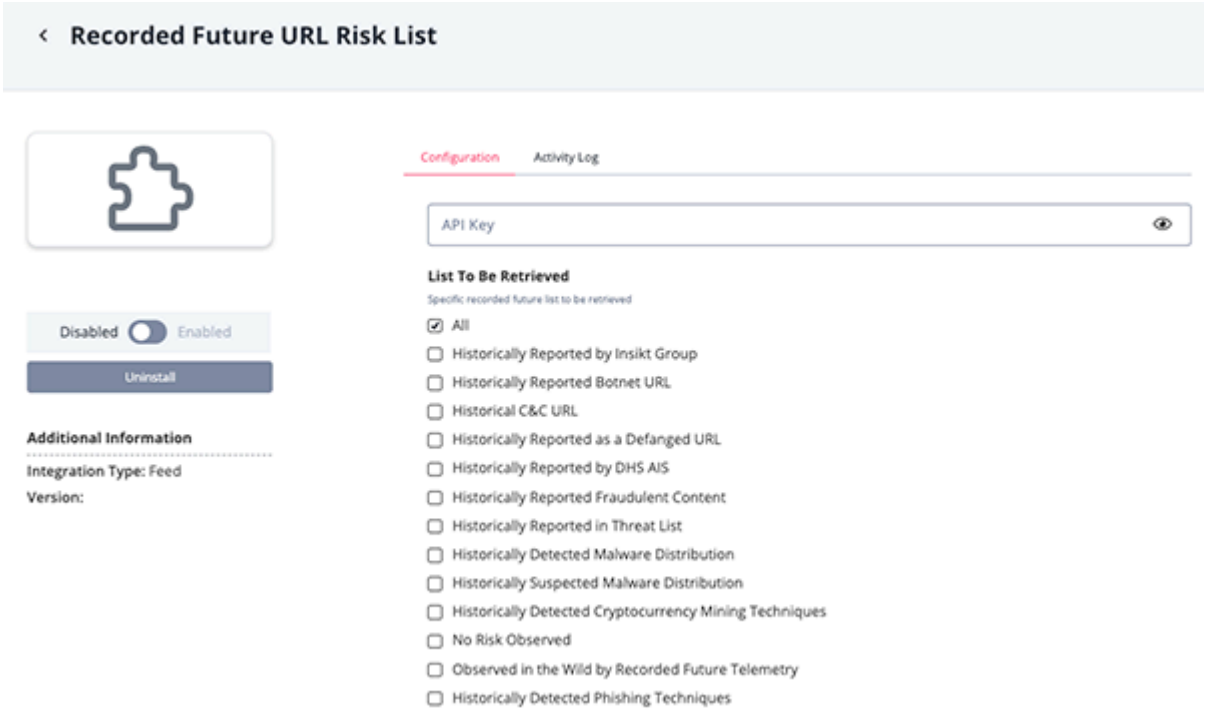
PARAMETER	DESCRIPTION
	◦ Historically Reported in Threat List ◦ Historical Honeypot Sighting ◦ Honeypot Host ◦ Recently Communicating Validated C&C Server ◦ Historically Linked to Intrusion Method ◦ Historically Linked to APT ◦ Historically Linked to Cyber Attack ◦ Historical Malicious Infrastructure Admin Server ◦ Suspected Malicious Packet Source ◦ Historical Malware Delivery ◦ Historical Multicategory Blocklist ◦ Observed in the Wild by Recorded Future Telemetry ◦ Historical Open Proxies ◦ Historical Phishing Host ◦ Historical Positive Malware Verdict ◦ Recorded Future Predictive Risk Model ◦ Actively Communicating Validated C&C Server ◦ Recently Reported by Insikt Group ◦ Recent Botnet Traffic ◦ Recent Brute Force ◦ Recent DDoS ◦ Recently Reported as a Defanged IP ◦ Recently Reported by DHS AIS ◦ Recent SSH/Dictionary Attacker ◦ Recent Bad SSL Association ◦ Recent Suspected C&C Server ◦ Recent Threat Researcher ◦ Recent Tor Node ◦ Recent Unusual IP ◦ Validated C&C Server ◦ Recently Communicating With Validated C&C Server ◦ Recently Defaced Site ◦ Historically Referenced by Insikt Group ◦ Historically Reported C&C Server ◦ Trending in Recorded Future Analyst Community ◦ Historical Spam Source ◦ Historical SSH/Dictionary Attacker ◦ Historical Bad SSL Association ◦ Historical Suspected C&C Server ◦ Suspected Phishing Host ◦ Historical Threat Researcher ◦ Tor Node ◦ Unusual IP ◦ Previously Validated C&C Server ◦ Vulnerable Host ◦ Observed High-Impact Vulnerability
Save CVE Data As	Select whether to ingest CVEs as: Vulnerabilities, Indicators, or Both.  The default setting is to ingest Indicators objects.
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.


Recorded Future IP Risk List
Disabled
Enabled
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
API Key
List To Be Retrieved
Specific recorded future list to be retrieved
All
Threat Actor Used Infrastructure
Historically Reported by Insikt Group
Inside Possible Bogus BGP Route
Historical Botnet Traffic
Historical Brute Force
Nameserver for C&C Server
Cyber Exploit Signal: Critical
Cyber Exploit Signal: Important
Cyber Exploit Signal: Medium
Recent Host of Many DDNS Names
Historical DDoS

Recorded Future URL Risk List Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
List to be Retrieved	Use the checkboxes provided to select specific Recorded Future lists to be retrieved. It is highly recommended to use the **All** option as it will ingest the latest information from Recorded Future. If you are using the **All** option, confirm that you have unselected the other options. Running the feed with the **All** option selected along with other individual list options, will cause the feed to fail. This is a known issue and will be addressed in a future release of the integration. You should schedule feed runs hourly or longer when using the **All** option. Options include: ° All (default) ° Historically Reported by Insikt Group ° Historically Reported Botnet URL ° Historical C&C URL ° Historically Reported as a Defanged URL ° Historically Reported by DHS AIS ° Historically Reported Fraudulent Content ° Historically Reported in Threat List ° Historically Detected Malware Distribution ° Historically Suspected Malware Distribution ° Historically Detected Cryptocurrency Mining Techniques ° No Risk Observed ° Recently Reported as a Defanged URL ° Recently Reported by DHS AIS ° Recently Reported Fraudulent Content ° Recently Detected Malware Distribution ° Recently Suspected Malware Distribution ° Recently Detected Cryptocurrency Mining Techniques ° Recently Detected Phishing Techniques ° Recently Suspected Phishing Techniques ° Recent Web Filter Avoidance Proxy URL

PARAMETER	DESCRIPTION
	° Observed in the Wild by Recorded Future Telemetry ° Historically Detected Phishing Techniques ° Historically Suspected Phishing Techniques ° Historically Detected Web Filter Avoidance Proxy URL ° Recently Reported by Insikt Group ° Recently Reported Botnet URL ° Recent C&C URL ° Recently Referenced by Insikt Group ° Recent Reported C&C URL ° Recently Reported Spam or Unwanted Content ° Recent Suspected C&C URL ° Recently Active URL on Weaponized Domain ° Historically Referenced by Insikt Group ° Historical Reported C&C URL ° Historically Reported Spam or Unwanted Content ° Historical Suspected C&C URL
Save CVE Data As	Select whether to ingest CVEs as: Vulnerabilities, Indicators, or Both.  The default setting is to ingest Indicators objects.
Minimum Risk Score Threshold	The numeric value representing the minimum risk score required to ingest an IOC. The default setting is 50.

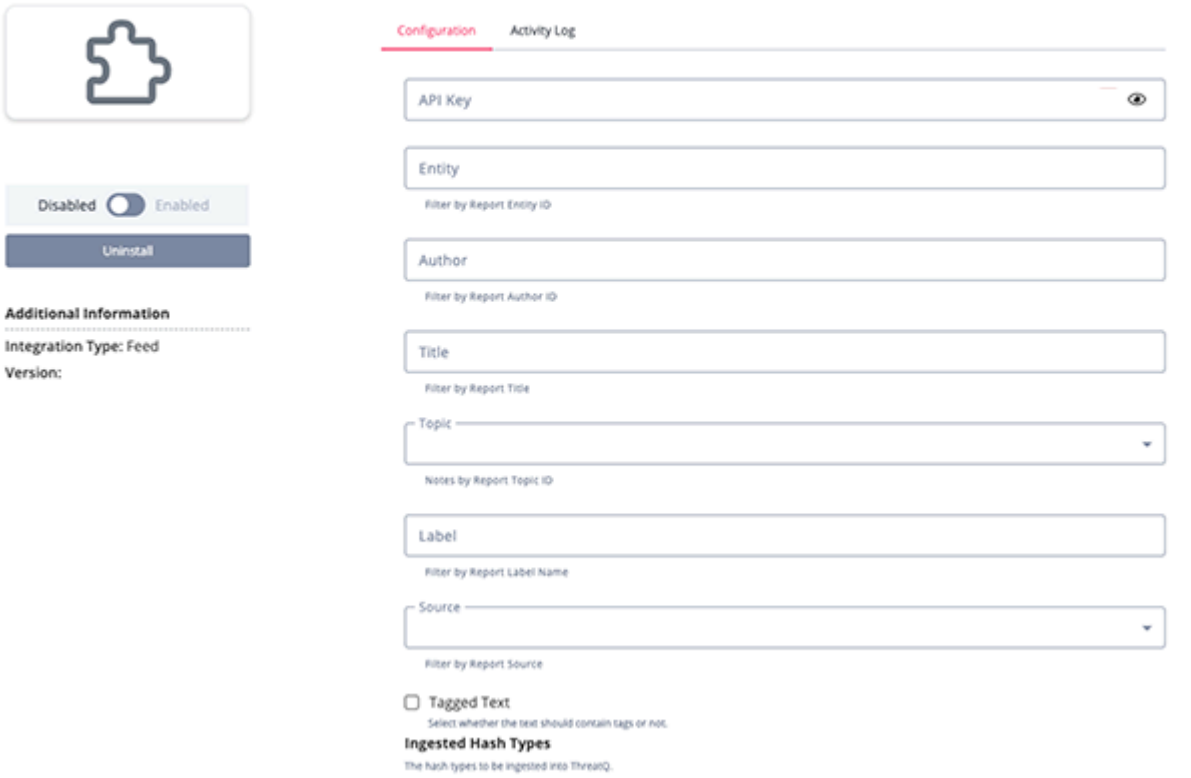

Recorded Future URL Risk List
Disabled
Enabled
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
API Key
List To Be Retrieved
Specific recorded future list to be retrieved
All
Historically Reported by Insikt Group
Historically Reported Botnet URL
Historical C&C URL
Historically Reported as a Defanged URL
Historically Reported by DHS AIS
Historically Reported Fraudulent Content
Historically Reported in Threat List
Historically Detected Malware Distribution
Historically Suspected Malware Distribution
Historically Detected Cryptocurrency Mining Techniques
No Risk Observed
Observed in the Wild by Recorded Future Telemetry
Historically Detected Phishing Techniques

Recorded Future Analyst Note Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
Entity	A string to search for notes by entity ID.
Author	A string to search for notes by author ID.
Title	A string to search for notes by title.
Topic	A string to search for notes by topic ID. The options for this user field are: • Actor Profile • Analyst On-Demand Report • Cyber Threat Analysis • Flash Report • Geopolitical Intelligence Summary • Geopolitical Flash Event • Geopolitical Threat Forecast • Geopolitical Validated Event • Hunting Package • Indicator • Insikt Research Lead • Informational • Malware/Tool Profile • Regular Vendor Vulnerability Disclosures • Sigma Rule • SNORT Rule • Source Profile • The Record by Recorded Future • Threat Lead • TTP Instance • Validated Intelligence Event • Weekly Threat Landscape • YARA Rule
Label	A string that helps searching for notes by label, by name.
Source	A string that helps sorting by the source of note. The options for this user field will be: ◦ Insikt Group ◦ ThreatQuotient - Partner Notes

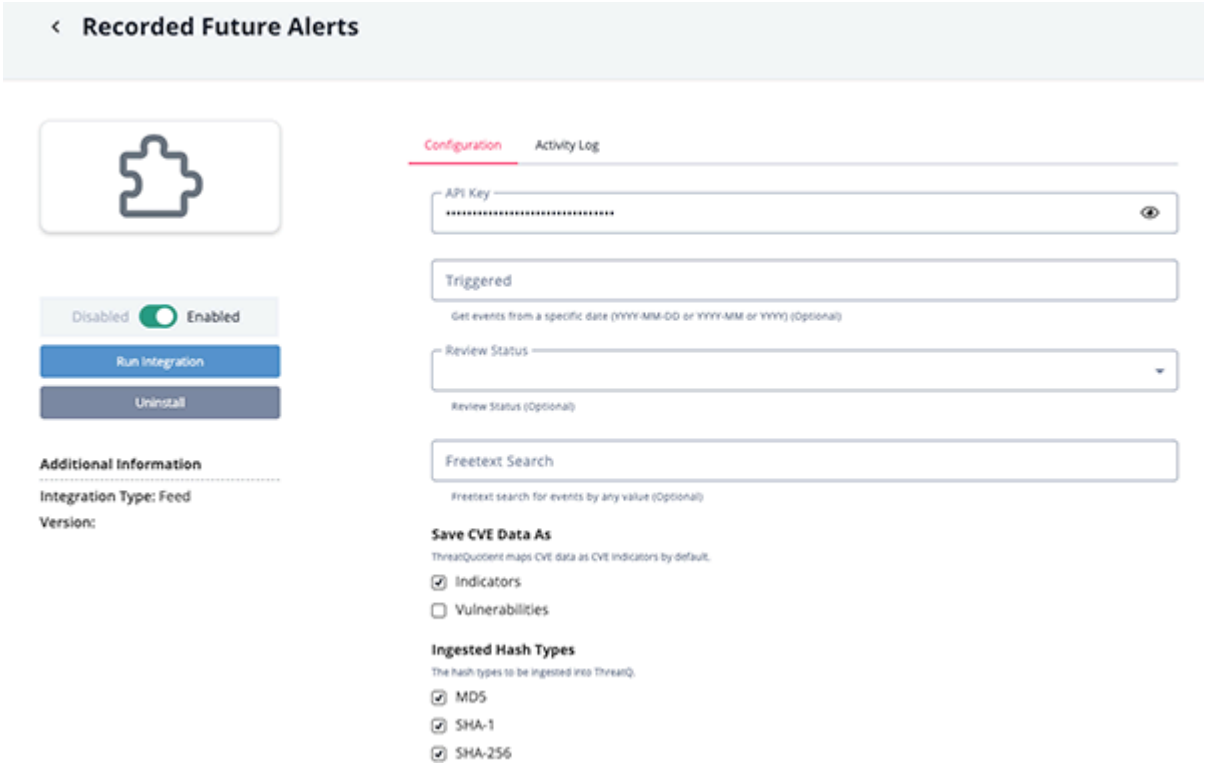
PARAMETER	DESCRIPTION
Tagged Text	Select whether the text should contain tags or not. Possible values are: ◦ True ◦ False
Limit	The maximum number of records per request. This will be used in the pagination.
Ingested Hash Types	Select the type of hashes to be ingested into ThreatQ. Options include ◦ MD5 ◦ SHA-1 ◦ SHA-256

Recorded Future Analyst Note



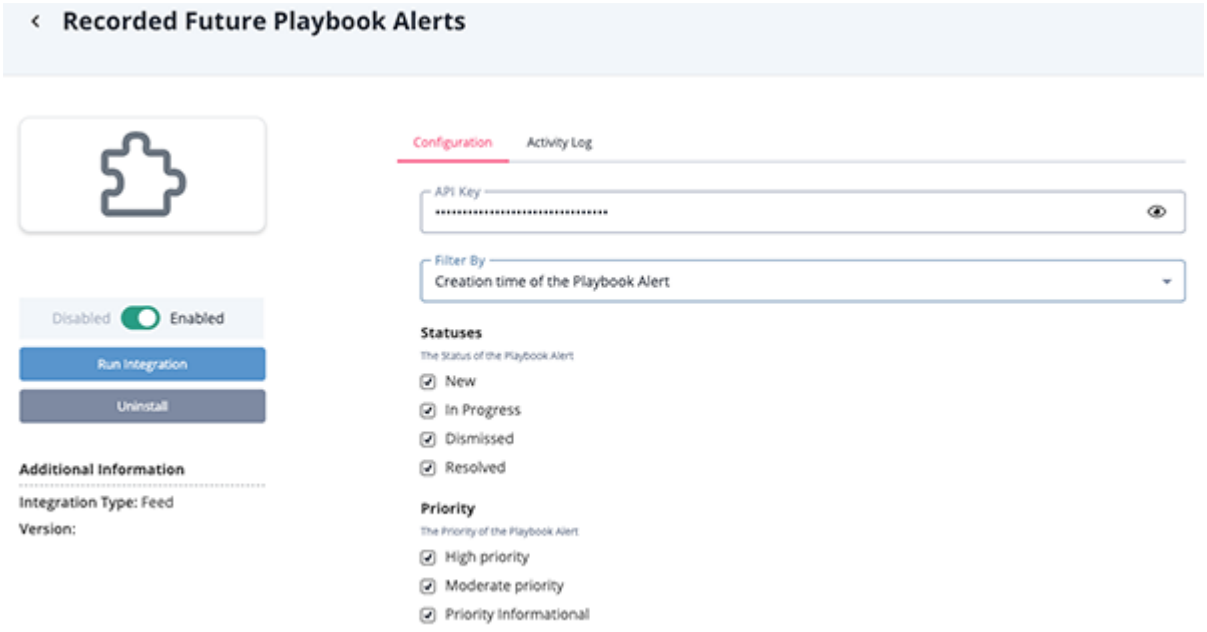
Recorded Future Alerts Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
Triggered	A string to search for events from a specific date (**YYYY-MM-DD** or **YYYY-MM** or **YYYY**).
Review Status	A string to search for events by status (Unassigned, Assigned, No Action and Tuning). If no specific status is selected, all event statuses are returned by the provider.
Freetext Search	A string to search for events by any value.
Save CVE Data as	Select whether to ingest CVEs as: Vulnerabilities, Indicators, or Both.  The default setting is to ingest Indicators objects.
Ingested Hash Types	Select the type of hashes to be ingested into ThreatQ. Options include ◦ MD5 ◦ SHA-1 ◦ SHA-256


Recorded Future Alerts
Disabled
Enabled
Run Integration
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
API Key
Triggered
Get events from a specific date (YYYY-MM-DD or YYYY-MM or YYYY) (Optional)
Review Status
Review Status (Optional)
Freetext Search
Freetext search for events by any value (Optional)
Save CVE Data As
ThreatQuotient maps CVE data as CVE indicators by default.
Indicators
Vulnerabilities
Ingested Hash Types
The hash types to be ingested into ThreatQ.
MD5
SHA-1
SHA-256

Recorded Future Playbook Alerts Parameters

PARAMETER	DESCRIPTION
API Key	Your API Key to be used in HTTP headers for accessing feed data.
Filter By	The date that will be used for filtering the alerts: `Creation` or `Update` time of the Playbook Alert.
Statuses	The Status of the Playbook Alert. Options include: ◦ New ◦ In Progress ◦ Dismissed ◦ Resolved
Priority	The Priority of the Playbook Alert. Options include: ◦ High Priority ◦ Moderate Priority ◦ Priority Informational



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

Recorded Future Domain Risk List

The data on this feed comes in form of a CSV list. The first token is the actual risk data (domain), and the last token (EvidenceDetails) contains supporting context. This token is a JSON-formatted string of an array of dictionaries.

`GET https://api.recordedfuture.com/v2/domain/risklist`

Sample Response:

```
'ns513726.ip-192-99-148.net', '92', '3/32',
'{"EvidenceDetails":
    [
        {
            "CriticalityLabel": "Unusual",
            "Rule": "Historical Malware Analysis DNS Name",
            "EvidenceString": "6 sightings on 1 source: VirusTotal...",
            "Timestamp": "2015-04-04T00:00:00.000Z",
            "Criticality": 1
        },
        {
            "CriticalityLabel": "Suspicious",
            "Rule": "Blacklisted DNS Name",
            "EvidenceString": "1 sighting on 1 source: DShield: Suspicious
Domain List.",
            "Timestamp": "2018-12-26T07:12:00.936Z",
            "Criticality": 2
        },
        {
            "CriticalityLabel": "Very Malicious",
            "Rule": "C&C DNS Name",
            "EvidenceString": "1 sighting on 1 source: Abuse.ch: ZeuS Domain
Blocklist (Standard).",
            "Timestamp": "2018-12-26T07:12:00.936Z",
            "Criticality": 4
        }
    ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	FQDN	N/A	ns513726.ip-192-99-148.net	N/A
1 (second token)	Indicator.Attribute	Risk Score	N/A	66	Attribute updated if already exists.
2 (third token)	Indicator.Attribute	Risk String	N/A	2/32	Attribute updated if already exists.
3 (fourth token) []CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) []Timestamp	Suspicious	Attribute updated if already exists.
3 (fourth token) []Rule	Indicator.Attribute	Associated Rule	3 (fourth token) []Timestamp	Blacklisted DNS Name	N/A
3 (fourth token) []EvidenceString	Indicator.Attribute	Evidence	3 (fourth token) []Timestamp	1 sighting on 1 source: Abuse.ch: ZeuS Domain Blocklist (Standard).	N/A

Recorded Future IP Risk List

Similar to the above feed, this feed gets IP addresses as indicators.

`GET https://api.recordedfuture.com/v2/ip/risklist`

Sample Response:

```
'5.120.187.119", '65', '1/49',
'{"EvidenceDetails":
    [
        {
            "CriticalityLabel": "Malicious",
            "Rule": "Recent Positive Malware Verdict",
            "EvidenceString": "1 sighting on 1 source: ReversingLabs....",
            "Timestamp": "2018-11-22T00:00:00.000Z",
            "Criticality": 3
        }
    ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	IP Address	N/A	5.120.187.119	N/A
1 (second token)	Indicator.Attribute	Risk Score	N/A	65	Attribute updated if already exists.
2 (third token)	Indicator.Attribute	Risk String	N/A	1/49	Attribute updated if already exists.
3 (fourth token) []CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) []Timestamp	Malicious	Attribute updated if already exists.
3 (fourth token) []Rule	Indicator.Attribute	Associated Rule	3 (fourth token) []Timestamp	Recent Positive Malware Verdict	N/A
3 (fourth token) []EvidenceString	Indicator.Attribute	Evidence	3 (fourth token) []Timestamp	1 sighting on 1 source: ReversingLabs.	N/A

Recorded Future URL Risk List

Similar to the above feeds, this feed gets URLs as indicators.

```
GET https://api.recordedfuture.com/v2/url/risklist
```

Sample Response:

```
'http://handle.booktobi.com/css/index.html', '65', '1/7',
'{"EvidenceDetails":
    [
        {
            "CriticalityLabel": "Malicious",
            "Rule": "Active Phishing URL",
            "EvidenceString": "1 sighting on 1 source: PhishTank: Phishing
Reports.",
            "Timestamp": "2018-12-26T16:15:44.750Z",
            "Criticality": 3
        }
    ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	URL	N/A	http://handle.booktobi.com/css/index.html	N/A
1 (second token)	Indicator.Attribute	Risk Score	N/A	65	Attribute updated if already exists.
2 (third token)	Indicator.Attribute	Risk String	N/A	1/7	Attribute updated if already exists.
3 (fourth token) [].CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) [].Timestamp	Malicious	Attribute updated if already exists.
3 (fourth token) [].Rule	Indicator.Attribute	Associated Rule	3 (fourth token) [].Timestamp	Active Phishing URL	N/A
3 (fourth token) [].EvidenceString	Indicator.Attribute	Evidence	3 (fourth token) [].Timestamp	1 sighting on 1 source: PhishTank: Phishing Reports.	N/A

Recorded Future Vulnerability Risk List

Similar to the above feeds, this feed gets CVEs.

`GET https://api.recordedfuture.com/v2/vulnerability/risklist`

Sample Response:

```
'CVE-2018-0802', '89', '11/18',
'{"EvidenceDetails":
    [
        {
            "CriticalityLabel": "Low",
            "Rule": "Linked to Historical Cyber Exploit",
            "EvidenceString": "4281 sightings on 351 sources including: ...",
            "Timestamp": "2018-11-14T22:31:30.000Z",
            "Criticality": 1
        },
        {
            "CriticalityLabel": "Low",
            "Rule": "Historically Linked to Penetration Testing Tools",
            "EvidenceString": "1 sighting on 1 source: @DTechCloud....",
            "Timestamp": "2018-05-07T20:31:29.000Z", "Criticality": 1
        },
    ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value/ Vulnerability.Value	CVE/N/A	N/A	CVE-2018-0802	N/A
1 (second token)	Indicator.Attribute/ Vulnerability.Attribute	Risk Score	N/A	89	Attribute updated if already exists.
2 (third token)	Indicator.Attribute/ Vulnerability.Attribute	Risk String	N/A	11/18	Attribute updated if already exists.
3 (fourth token) []CriticalityLabel	Indicator.Attribute/ Vulnerability.Attribute	Criticality	3 (fourth token) []Timestamp	Low	Attribute updated if already exists.
3 (fourth token) []Rule	Indicator.Attribute/ Vulnerability.Attribute	Associated Rule	3 (fourth token) []TimeStamp	Linked to Historical Cyber Exploit	N/A
3 (fourth token) []EvidenceString	Indicator.Attribute/ Vulnerability.Attribute	Evidence	3 (fourth token) []Timestamp	1 sighting on 1 source: @DTechCloud....	N/A

Recorded Future Hash Risk List

Similar to the above feeds, this feed gets Hashes.

`GET https://api.recordedfuture.com/v2/hash/risklist`

Sample Response:

```
'ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa', 'SHA-256',
'89', '4/10',
'{"EvidenceDetails":
    [
        {
            "CriticalityLabel": "Unusual",
            "Rule": "Threat Researcher",
            "EvidenceString": "21 sightings on 9 sources including: ...",
            "Timestamp": "2018-01-28T11:24:35.942Z",
            "Criticality": 1.0
        },
        {
            "CriticalityLabel": "Suspicious",
            "Rule": "Linked to Vulnerability",
            "EvidenceString": "5 sightings on 2 sources: ...",
            "Timestamp": "2017-08-08T14:10:11.410Z",
            "Criticality": 2
        },
        {
            "CriticalityLabel": "Suspicious",
            "Rule": "Linked to Malware",
            "EvidenceString": "Previous sightings on 36 sources
including: ...",
            "Timestamp": "2017-05-12T15:39:30.000Z",
            "Criticality": 2
        },
    ]
}'
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	1 (second token)	N/A	00d48afbba5ef9eadb572730b2d0cafa	N/A
2 (third token)	Indicator.Attribute	Risk Score	N/A	89	Attribute updated if already exists.
3 (fourth token)	Indicator.Attribute	Risk String	N/A	4/10	Attribute updated if already exists.
4 (fifth token) [].CriticalityLabel	Indicator.Attribute	Criticality	4 (fifth token) [].Timestamp	Suspicious	Attribute updated if already exists.
4 (fifth token)[].Rule	Indicator.Attribute	Associated Rule	4 (fifth token) [].Timestamp	Linked to Malware	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
4 (fifth token) []. EvidenceString	Indicator.Attribute	Evidence	4 (fifth token) []. Timestamp	Previous sightings on 36 sources including: ...	N/A

Recorded Future Analyst Note

This feed gets Reports, Indicators and Attack Patterns. The data sample and mapping are below:

`GET https://api.recordedfuture.com/v2/analystnote/search`

Sample Response:


```
{
    "data": {
        "results": [
            {
                "source": {
                    "id": "VKz42X",
                    "name": "Insikt Group",
                    "type": "Source"
                },
                "attributes": {
                    "validated_on": "2020-02-06T06:59:32.784Z",
                    "published": "2020-02-06T06:59:32.784Z",
                    "text": "some text",
                    "topic": [
                        {
                            "id": "TXSFt0",
                            "name": "Flash Report",
                            "type": "Topic"
                        }
                    ],
                    "title": "Mailto Ransomware Targets Enterprise Networks",
                    "note_entities": [
                        {
                            "id": "bLfMiL",
                            "name": "Mailto Ransomware",
                            "type": "Malware"
                        }
                    ],
                    "context_entities": [
                        {
                            "id": "J6UzbO",
                            "name": "Bleeping Computer",
                            "type": "Source"
                        }
                    ],
                    "validation_urls": [
                        {
                            "id": "url:url:https://www.bleepingcomputer.com/
news/security/mailto-netwalker-ransomware-targets-enterprise-networks/",
                            "name": "url:https://www.bleepingcomputer.com/news/
security/mailto-netwalker-ransomware-targets-enterprise-networks/",
                            "type": "URL"
```

```
                        },
                        {
                            "id": "url:url:https://twitter.com/VK_Intel/status/
1225086186445733889?s=20",
                            "name": "url:https://twitter.com/VK_Intel/status/
1225086186445733889?s=20",
                            "type": "URL"
                        }
                    ]
                },
                "id": "cu1WGK"
            }
        ]
    },
    "counts": {
        "returned": 10,
        "total": 19216
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data.results[].attributes.title	Report.Name	Report	"Mailto Ransomware Targets Enterprise Networks"	N/A
.data.results[].attributes.published	Report.Published_at	N/A	"2020-02-06T06:59:32.784Z"	This date will also be used for related indicators and attack patterns.
.data.results[].attributes.text	Report.Description	Description	"text"	N/A
.data.results[].source.name	Report.Attribute	Recorded Future Source	"Insikt Group"	N/A
.data.results[].attributes.topic[].name	Report.Attribute	Topic Name	"Flash Report"	N/A
.data.results[].attributes.validated_on	Report.Attribute	Validated On	"2020-02-06T06:59:32.784Z"	Attribute updated if already exists.
.data.results[].attributes.context_entities	N/A	N/A	N/A	*See entities mapping
.data.results[].attributes.note_entities	N/A	N/A	N/A	*See entities mapping

Entities Mapping

This mapping will be used to map both values from `context_entities` and `note_entities`. The data sample and mapping are below:

Sample Response:

```
{
    "context_entities": [
        {
            "id": "J6UzbO",
            "name": "Bleeping Computer",
            "type": "Source",
            "description": "some description"
        }
    ]
}
```

```
  indicator_type_map:
    IpAddress: IP Address
    URL: URL
    CyberVulnerability: CVE
```

ThreatQ will filter based by type. If the value of the `type` key is contained in the indicator_type_map below or is equal to `Hash`, an indicator will be ingested (the published_at date will be the same as for the report object). If the `type` key is equal to `Malware`, an object of type Malware type will be ingested. If the `type` key is equal to `MitreAttackIdentifier`, an object of Attack Pattern type will be ingested. Else, attributes will be created for the main `report` object.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
value	Report.Attribute	.name	"Bleeping Computer"	N/A
.text	Report.Attribute	.description	"some description"	N/A
.name	Indicator.Value	Indicator	"Bleeping Computer"	N/A
.type	Indicator.Type	.name	"Ip Address"	The value for this will be `indicator_type_map[.type]` if it exists there. If the value is `Hash`, the value length will be analyzed and based on it it will be either `MD5`, `SHA-1`, or `SHA-256`.
.description	Indicator.Attribute	Description	"some description"	N/A
See note	Indicator.Attribute	Analyst Note	"some description"	N/A
.name	Attack_pattern.Value	Attack Pattern	"T1001 - Data Obfuscation"	The value for the Attack Pattern objects is generated based on the ingested name and the values of already ingested MITRE attack patterns (by MITRE ATT&CK feeds).

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
				If the ingested name is 'T1001', the value will be 'T1001 - Data Obfuscation'.
.description	Attack_pattern.Attribute	Entity Description	"some description"	N/A
See note	Attack_pattern.Attribute	Analyst Note	"some description"	N/A
.name	Malware.Value	Malware	"Bleeping Computer"	N/A
.description	Malware.Attribute	Entity Description	"some description"	N/A
See note	Malware.Attribute	Analyst Note	"some description"	N/A

The Analyst Note attribute inherits its value from the parent report's description.

Recorded Future Alerts

The Alerts feed retrieves Alerts from the provider.

`GET https://api.recordedfuture.com/v3/alert/`

Sample Response:


```
{
  "data": [
    {
      "review": {
        "note": null,
        "status_in_portal": "New",
        "assignee": null,
        "status": "no-action"
      },
      "owner_organisation_details": {
        "organisations": [
          {
            "organisation_id": "uhash:ER135KQ6oL",
            "organisation_name": "ThreatQ - Partner"
          }
        ],
        "enterprise_id": "uhash:DimzHe41vx",
        "enterprise_name": "ThreatQ - Partner"
      },
      "url": {
        "api": "https://api.recordedfuture.com/v3/alerts/rj540x",
        "portal": "https://app.recordedfuture.com/live/sc/notification/?id=rj540x"
      },
      "rule": {
        "name": "Cyber Espionage, Related Vulnerabilities",
        "id": "nt4XZZ",
        "url": {
          "portal": "https://app.recordedfuture.com/live/sc/
ViewIdkobra_view_report_item_alert_editor?
view_opts=%7B%22reportId%22%3A%22nt4XZZ%22%2C%22bTitle%22%3Atrue%2C%22title%22%3A%22Cyber+Espionage
%2C+Related+Vulnerabilities%22%7D"
        }
      },
      "id": "rj540x",
      "hits": [
        {
          "entities": [
            {
              "id": "B_HE4",
              "name": "Google",
              "type": "Company"
            },
            {
              "id": "idn:reuters.com",
              "name": "reuters.com",
              "type": "InternetDomainName"
            },
            {
              "id": "Xw2PY",
              "name": "Frankfurt",
              "type": "Airport"
            },
            {
              "id": "rVnb7k",
```

```
              "name": "Rhysida",
              "type": "Malware"
            },
            {
              "id": "J0Nl-p",
              "name": "Ransomware",
              "type": "MalwareCategory"
            },
            {
              "id": "K_4o-y",
              "name": "Anonymous Sudan",
              "type": "Organization"
            },
            {
              "id": "I_7J4G",
              "name": "Hacktivist",
              "type": "CyberThreatActorCategory"
            },
            {
              "id": "mitre:T1048",
              "name": "T1048",
              "type": "MitreAttackIdentifier"
            },
            {
              "id": "email:mary.silverstein@delta.com",
              "name": "mary.silverstein@delta.com",
              "type": "EmailAddress"
            },
            {
              "id": "jc5TL-",
              "name": "ProxyShell",
              "type": "CyberVulnerability",
              "description": "ProxyShell and Log4J Vulnerabilities Were the Most Exploited Flaws in
2021."
            }
          ],
          "document": {
            "source": {
              "id": "source:hPTFPY",
              "name": "RedAlert | Blog",
              "type": "Source"
            },
            "title": "2022 Activities Summary of SectorA groups (ENG)",
            "url": "https://redalert.nshc.net/2023/06/08/2022-activities-summary-of-sectora-groups-
eng/",
            "authors": []
          },
          "fragment": "In this operation, the group targeted engineering companies in the <e
id=0qjp>energy</e> and military sectors and damaged their systems by <i id=HE-xwAAZh-v>exploiting
the <e id=kvXvR5>Log4Shell</e></i> vulnerability with an initial infiltration method.",
          "id": "HE-xwAAZh-v",
          "language": "eng",
          "primary_entity": {
            "id": "kvXvR5",
            "name": "CVE-2021-44228",
            "type": "CyberVulnerability",
            "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases
2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not
protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can
control log messages or log message parameters can execute arbitrary code loaded from LDAP servers
when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by
default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been
completely removed. Note that this vulnerability is specific to log4j-core and does not affect
log4net, log4cxx, or other Apache Logging Services projects."
```

```
          },
          "analyst_note": null
        }
      ],
      "ai_insights": {
        "comment": "The Recorded Future AI requires more references in order to produce a summary.",
        "text": null
      },
      "log": {
        "note_author": null,
        "note_date": null,
        "status_date": null,
        "triggered": "2023-06-08T04:53:13.444Z",
        "status_change_by": null
      },
      "title": "Cyber Espionage, Related Vulnerabilities - Rise: CVE-2021-44228",
      "type": "ENTITY"
    }
  ],
  "counts": {
    "returned": 10,
    "total": 2653
  }
}
```

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[].title	Event.Title	N/A	.data[].log.note_date / .data[].log.triggered	Cyber Espionage, Related Vulnerabilities - Rise: CVE-2021-44228	If `.data[].log.note_date` is not present `.data[].log.triggered` is used as `Published Date`
.data[].log.triggered	Event.Happened_at	N/A	N/A	2023-06-08T04:53:13.444Z	N/A
.data[].ai_insights.text	Event.Description	N/A	N/A	N/A	N/A
.data[].ai_insights.comment	Event.Description	N/A	N/A	The Recorded Future AI requires more references in order to produce a summary.	If `.data[].ai_insights.text` not present.
.data[].review.assignee	Event.Attribute	Assignee	.data[].log.note_date / .data[].log.triggered	N/A	If the attribute already exists, the value will be updated.
.data[].log.note_author	Event.Attribute	Note Author	.data[].log.note_date / .data[].log.triggered	N/A	N/A
.data[].review.status_in_portal	Event.Attribute	Alert Status	.data[].log.note_date / .data[].log.triggered	no-action	If the attribute already exists, the value will be updated.
.data[].url.portal	Event.Attribute	Reference URL	.data[].log.note_date / .data[].log.triggered	https://app.recordedfuture.com/live/sc/notification/?id=rj540x	N/A
.data[].rule.url.portal	Event.Attribute	Triggered Rule URL	.data[].log.note_date / .data[].log.triggered	https://app.recordedfuture.com/live/sc/ViewIdkobra_view_report_item_alert_editor?view_opts=...	N/A
.data[].rule.name	Event.Attribute	Triggered Rule Name	.data[].log.note_date / .data[].log.triggered	Cyber Espionage, Related Vulnerabilities	N/A
.data[].type	Event.Attribute	Alert Type	.data[].log.note_date / .data[].log.triggered	ENTITY	N/A
.data[].owner_organisation_details.enterprise_name	Event.Attribute	Organisation Enterprise name	.data[].log.note_date / .data[].log.triggered	ThreatQ - Partner	N/A
.data[].hits[].document.url	Related.Indicator.Value	URL	N/A	https://redalert.nshc.net/2023/06/08/2022-activities-summary-of-sectora-groups-eng/	Ingested as indicator if 'www.virustotal.com' not in .url
.data[].hits[].document.url	Related.Event.Attribute	URL	N/A	https://www.virustotal.com/84387248326473645	Ingested as attribute if 'www.virustotal.com' in .url

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].hits[].document.title, .data[].hits[].entities[].name	Related.Indicator.Description	N/A	N/A	2022 Activities Summary of SectorA groups (ENG)\n Airport:Frankfurt	Title is concatenated with all the names for which `data.hits[].entities[].type` is not not in the mapping tables below.
.data[].hits[].fragment	Related.Indicator.Attribute	Fragment	N/A	In this operation, the group targeted engineering companies in the <e id=0qjp>energy</e> ...	N/A
.data[].hits[].language	Related.Indicator.Attribute	Language	n/A	eng	N/A
.data[].hits[].entities[].name	Related.Indicator.Tags	N/A	N/A	ddosattacks	If `data.hits[].entities[].type` is `Hashtag`. Character # is removed.
.data[].hits[].entities[].name	Related.Indicator.Value	data.hits[].entities[].type	N/A	N/A	See `Related Indicator Type Mapping` table below.
.data[].hits[].entities[].name	Related.Indicator.Attribute	data.hits[].entities[].type	N/A	N/A	See `Related Indicator Attributes Mapping` table below.
.data[].hits[].entities[].description	Related.Indicator/ Vulnerability.Description	N/A	N/A	ProxyShell and Log4J Vulnerabilities Were the Most Exploited Flaws in 2021	If `data.hits[].entities[].type` is in `Related Indicator Type Mapping` or is a Vulnerability
.data[].hits[].entities[].name	Related.Malware.Value	N/A	N/A	Rhysida	If `data.hits[].entities[].type` is `Malware`
.data[].hits[].entities[].name	Related.Malware.Attribute	Malware Category	N/A	Ransomware	If `data.hits[].entities[].type` is `MalwareCategory`
.data[].hits[].entities[].name	Related.Adversary.Value	N/A	N/A	Anonymous Sudan	If `data.hits[].entities[].type` is `Organization` or `Person`
.data[].hits[].entities[].type	Related.Adversary.Attribute	Type	N/A	Organization	If `data.hits[].entities[].type` is

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`Organization` or `Person`
.data[].hits[].entities[].name	Related.Adversary.Tags	N/A	N/A	Hacktivist	If `data.hits[].entities[].type` is `CyberThreatActorCategory`
.data[].hits[].entities[].name	Related.Attack Patten.Value	N/A	N/A	T1048	If `data.hits[].entities[].type` is `MitreAttackIdentifier`
.data[].hits[].entities[].name	Related.Vulnerability.Value	N/A	N/A	ProxyShell	If `data.hits[].entities[].type` is `CyberVulnerability` or user config `Save CVE Data` as contains `Vulnerabilities`
.data[].hits[].entities[].name	Related.Identitiy.Value	N/A	N/A	mary.silverstein@delta.com	N/A

In the previous table, there is a Related Indicator that is set dynamically. This is because the ThreatQ Object Type is extracted from the same path `.data.hits[].entities[].type` if the `.data.hits[].entities[].type` is one from the Related Indicator Type Mapping table listed below.

Related Indicator Type Mapping

RECORDED FUTURE INDICATOR TYPE	THREATQ INDICATOR TYPE	NOTES
InternetDomainName	FQDN	N/A
URL	URL	N/A
Hash	MD5	If the length of the hash value is 32 characters
Hash	SHA-1	If the length of the hash value is 40 characters
Hash	SHA-256	If the length of the hash value is 64 characters
pAddress	IP Address	N/A
EmailAddress	Email Address	N/A
FileName	FileName	N/A
Username	Username	N/A
CyberVulnerability	CVE	If '.data.hits[].entities[].name' contains 'CVE' and user config `Save CVE Data` as contains `Indicators`

Related Indicator Attributes Mapping

In the previous table, **Related Indicator Type Mapping**, there is a **Related Indicator Attribute** that is set dynamically. We do this because the `Attribute Key` is extracted from the same path `.data.hits[].entities[].type` if the `.data.hits[].entities[].type` is one from the table listed below.

RECORDED FUTURE ATTRIBUTE TYPE	THREATQ ATTRIBUTE KEY
AttackVector	Attack Vector
Product	Product
Company	Company
City	City
Country	Country
Facility	Facility
FileNameExtension	File Extension
FileType	File Type
GeoEntity	Geo Entity
Industry	Industry
IndustryTerm	Industry Term
Operation	Operation
OrgEntity	Organization Entity
PhoneNumber	Phone Number

RECORDED FUTURE ATTRIBUTE TYPE	THREATQ ATTRIBUTE KEY
ProvinceOrState	State
Region	Region
Technology	Technology
Topic	Topic

Recorded Future Playbook Alerts

The Recorded Future Playbook Alerts feed retrieves a list of alerts filtered by the values provided in the configuration section.

`POST https://api.recordedfuture.com/playbook-alert/search`

Sample Response:


```
{
    "status": {
        "status_code": "Ok",
        "status_message": "Playbook alert search successful"
    },
    "data": [
        {
            "playbook_alert_id": "task:2803c5f5-aa32-41ce-98c1-41a7771cd9ad",
            "created": "2022-11-08T09:44:02.447Z",
            "updated": "2022-11-08T09:44:06.584Z",
            "status": "New",
            "category": "domain_abuse",
            "priority": "Informational",
            "title": "juhaokan.ga",
            "owner_id": "uhash:ER135KQ6oL",
            "owner_name": "ThreatQ - Partner",
            "organisation_id": "uhash:DimzHe41vx",
            "organisation_name": "ThreatQ - Partner"
        }
    ]
}
```


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[].title	Event.Title	Recorded Future Alert	.data[].created	juhaokan.ga	N/A
.data[].status	Event.Attribute	Status	.data[].created	New	Attribute updated if already exists.
.data[].category	Event.Attribute	Category	.data[].created	domain_abuse	Attribute updated if already exists.
.data[].priority	Event.Attribute	Priority	.data[].created	Informational	Attribute updated if already exists.
.data[].owner_name	Event.Attribute	Owner	.data[].created	ThreatQ - Partner	Attribute updated if already exists.
.data[].organisation_name	Event.Attribute	Organisation	.data[].created	ThreatQ - Partner	N/A

Domain Abuse Playbook Alert (Supplemental)

The Domain Abuse Playbook Alert supplemental feed related data for each of the ingested events retrieved from the Alert endpoint.

`POST https://api.recordedfuture.com/playbook-alert/domain_abuse`

Sample Response:


```
{
    "status": {
        "status_code": "Ok",
        "status_message": "Domain Abuse lookup successful"
    },
    "data": {
        "panel_status": {
            "entity_name": "lonsdale.social",
            "entity_criticality": "Low",
            "risk_score": 5,
            "context_list": [
                {
                    "context": "Phishing Host"
                },
                {
                    "context": "Active Mail Server"
                }
            ],
            "targets": [
                "idn:lonsdale.fr",
                "idn:lonsdale.us",
                "idn:lonsdale.porn",
                "idn:lonsdale.club"
            ],
            "status": "New",
            "priority": "High",
            "created": "2022-11-09T08:20:15.778Z",
            "case_rule_id": "report:nvAj-X",
            "case_rule_label": "Domain Abuse",
            "owner_id": "uhash:ER135KQ6oL",
            "owner_name": "ThreatQ - Partner",
            "organisation_id": "uhash:DimzHe41vx",
            "organisation_name": "ThreatQ - Partner"
        },
        "panel_action": [],
        "panel_evidence_summary": {
            "explanation": "Alert was created as a result of a triggered
typosquat detection",
            "resolved_record_list": [
                {
                    "entity": "idn:ns1025.ui-dns.org",
```

```
                    "risk_score": 5,
                    "criticality": "Low",
                    "record_type": "NS",
                    "context_list": []
                },
                {
                    "entity": "ip:217.160.0.153",
                    "risk_score": 27,
                    "criticality": "Medium",
                    "record_type": "A",
                    "context_list": [
                        {
                            "context": "Phishing Host"
                        }
                    ]
                },
                {
                    "entity": "idn:mx00.ionos.co.uk",
                    "risk_score": 0,
                    "criticality": "0",
                    "record_type": "MX",
                    "context_list": [
                        {
                            "context": "Active Mail Server"
                        }
                    ]
                },
                {
                    "entity": "idn:mx01.ionos.co.uk",
                    "risk_score": 0,
                    "criticality": "0",
                    "record_type": "MX",
                    "context_list": [
                        {
                            "context": "Active Mail Server"
                        }
                    ]
                }
            ],
            "screenshots": [
                {
                    "description": "An image associated with the Playbook
Alert",
                    "image_id": "img:349f92e2-fa93-4282-be15-e7a330130686",
                    "created": "2022-11-09T08:20:51.685Z"
                }
            ]
        },
        "panel_evidence_dns": {
            "ip_list": [
```

```
            {
                "entity": "ip:217.160.0.153",
                "risk_score": 27,
                "criticality": "Medium",
                "record_type": "A",
                "context_list": [
                    {
                        "context": "Phishing Host"
                    }
                ]
            }
        ],
        "mx_list": [
            {
                "entity": "idn:mx00.ionos.co.uk",
                "risk_score": 0,
                "criticality": "0",
                "record_type": "MX",
                "context_list": [
                    {
                        "context": "Active Mail Server"
                    }
                ]
            }
        ],
        "ns_list": [
            {
                "entity": "idn:ns1115.ui-dns.de",
                "risk_score": 0,
                "criticality": "0",
                "record_type": "NS",
                "context_list": [
                    {
                        "context": "Active Mail Server"
                    }
                ]
            },
            {
                "entity": "idn:ns1090.ui-dns.biz",
                "risk_score": 5,
                "criticality": "Low",
                "record_type": "NS",
                "context_list": []
            }
        ]
    },
    "panel_evidence_whois": {
        "body": [
            {
                "provider": "whois",
```

```
                    "entity": "idn:lonsdale.social",
                    "attribute": "attr:whois",
                    "value": {
                        "privateRegistration": false,
                        "status": "clientTransferProhibited addPeriod",
                        "nameServers": [
                            "idn:ns1066.ui-dns.com",
                            "idn:ns1025.ui-dns.org",
                            "idn:ns1115.ui-dns.de",
                            "idn:ns1090.ui-dns.biz"
                        ],
                        "registrarName": "IONOS SE",
                        "createdDate": "2022-11-08T19:44:16.000Z"
                    },
                    "added": "2022-11-09T08:21:13.682Z"
                },
                {
                        "provider": "whois",
                        "entity": "idn:btbo2.top",
                        "attribute": "attr:whoisContacts",
                        "value": {
                            "organization": "REDACTED FOR PRIVACY",
                            "city": "REDACTED FOR PRIVACY",
                            "name": "REDACTED FOR PRIVACY",
                            "state": "REDACTED FOR PRIVACY",
                            "street1": "REDACTED FOR PRIVACY",
                            "country": "REDACTED FOR PRIVACY",
                            "postalCode": "REDACTED FOR PRIVACY",
                            "telephone": "REDACTED FOR PRIVACY",
                            "type": "technicalContact"
                        },
                        "added": "2022-11-08T10:28:20.712Z"
                    }
            ]
        },
        "panel_log": [
            {
                "id": "uuid:26b4be48-e1e0-4773-97d7-b8c8260fe53b",
                "created": "2022-11-09T08:27:31.377Z",
                "modified": "2022-11-09T08:27:31.377Z",
                "action_priority": "Informational"
            }
        ]
    }
}
```

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.panel_status.entity_name	Related.Indicator	FQDN	.data.panel_status.created	jlonsdale.social	N/A
.data.panel_status.risk_score	Related.Indicator.Attribute	Risk Score	.data.panel_status.created	5	Attribute updated if already exists
.data.panel_status.entity_criticality	Related.Indicator.Attribute	Criticality	.data.panel_status.created	Low	Attribute updated if already exists
.data.panel_status.context_list[].context	Related.Indicator.Attribute	Context Data	.data.panel_status.created	Phishing Host	N/A
.data.panel_evidence_dns.ip_list[].entity	Related.Indicator	IP Address	.data.panel_status.created	ip:217.160.0.153	N/A
.data.panel_evidence_dns.ip_list[].risk_score	Related.Indicator.Attribute	Risk Score	.data.panel_status.created	27	Attribute updated if already exists
.data.panel_evidence_dns.ip_list[].criticality	Related.Indicator.Attribute	Criticality	.data.panel_status.created	Medium	Attribute updated if already exists
.data.panel_evidence_dns.ip_list[].context_list[].context	Related.Indicator.Attribute	Context Data	.data.panel_status.created	Phishing Host	N/A
.data.panel_evidence_dns.mx_list[].entity	Related.Indicator	FQDN	.data.panel_status.created	idn:mx00.ionos.co.uk	N/A
.data.panel_evidence_dns.mx_list[].risk_score	Related.Indicator.Attribute	Risk Score	.data.panel_status.created	0	Attribute updated if already exists
.data.panel_evidence_dns.mx_list[].criticality	Related.Indicator.Attribute	Criticality	.data.panel_status.created	0	Attribute updated if already exists
.data.panel_evidence_dns.mx_list[].context_list[].context	Related.Indicator.Attribute	Context Data	.data.panel_status.created	Active Mail Server	N/A
.data.panel_evidence_dns.ns_list[].entity	Related.Indicator	FQDN	.data.panel_status.created	idn:ns1025.ui-dns.org	N/A
.data.panel_evidence_dns.ns_list[].risk_score	Related.Indicator.Attribute	Risk Score	.data.panel_status.created	5	Attribute updated if already exists
.data.panel_evidence_dns.ns_list[].criticality	Related.Indicator.Attribute	Criticality	.data.panel_status.created	Low	Attribute updated if already exists

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.panel_evidence_dns.ns_list[].context_list[].context	Related.Indicator.Attribute	Context Data	.data.panel_status.created	Active Mail Server	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.

Recorded Future Domain Risk List

METRIC	RESULT
Run Time	1 minute
Indicators	393
Indicator Attributes	3,226

Recorded Future IP Risk List

METRIC	RESULT
Run Time	1 minute
Indicators	95
Indicator Attributes	1,979

Recorded Future URL Risk List

METRIC	RESULT
Run Time	23 minutes

METRIC	RESULT
Indicators	10,653
Indicator Attributes	92,877

Recorded Future Vulnerability Risk

METRIC	RESULT
Run Time	1 minute
Indicators	3
Indicator Attributes	158
Vulnerabilities	5
Vulnerability Attributes	158

Recorded Future Hash Risk List

METRIC	RESULT
Run Time	1 minute
Indicators	534
Indicator Attributes	4,707

Recorded Future Analyst Note

METRIC	RESULT
Run Time	2 minutes
Attack Patterns	1
Attack Pattern Attributes	2
Indicators	113
Indicator Attributes	732
Malware	24
Malware Attributes	131
Reports	19
Reports Attributes	335

Recorded Future Alerts

METRIC	RESULT
Run Time	1 minute
Events	13
Events Attributes	65
Indicators	48

METRIC	RESULT
Indicator Attributes	151
Malware	6
Malware Attributes	6
Adversary	2
Adversary Attributes	2

Recorded Future Playbook Alerts

METRIC	RESULT
Run Time	1 minute
Events	23
Events Attributes	115
Indicators	14
Indicator Attributes	24

Known Issues / Limitations

- The 5 main Recorded Future feeds take progressively longer to complete as more and more lists are specified for the **Recorded Future List** configuration parameter. ThreatQ recommends pulling a targeted subset of lists for each feed instead of all of the available lists.
- If Recorded Future deletes a list, the feed will return an empty response for it.
- The Recorded Future **Analyst Notes** and **Alerts** feeds have an API limit and will only return the first 1,000 results.
- Recorded Future CDF 2.8.7 introduced the **All** option for the **List to be Retrieved** configuration parameter with the Recorded Future Domain, Risk List Recorded Future Hash Risk List, Recorded Future IP Risk List, and Recorded Future URL Risk List feeds. There is a known bug where users can select the **All** option and also individual items in the list. Doing will cause the feed to error when run. If you are using the **All** option, you must unselect all other individual items for the **List to be Retrieved** configuration for that feed.

  Feed runs will typically complete within 40 minutes using this option so it is advised to schedule run times no more frequently than one hour.

Change Log

- **Version 2.8.7**
  - Added an **All** option to the **List to be Retrieved** parameter for the following feeds:
    - Recorded Future Domain Risk List
    - Recorded Future Hash Risk List
    - Recorded Future IP Risk List
    - Recorded Future URL Risk List

    > Feed runs will typically complete within 40 minutes using this option so it is advised to schedule run times no more frequently than one hour.

  - Added new Known Issue regarding the **All** option for the **List to be Retrieved** parameter. If utilizing the **All** option, all other items in the **List to be Retrieved** parameter must be unselected. Attempting to run a feed with the **All** and other items in the list selected will cause the feed to fail.
  - Added a new attribute for the Recorded Future playbook Alerts feed: `Context data`.
  - Added `Target Entities` for related entities in the Recorded Future Alerts feed.
- **Version 2.8.6**
  - Performed optimization improvements for all feeds that contain the Risk List in their name in a effort to reduce the possibility of timeout errors.
- **Version 2.8.5**
  - Resolved a timeout error that was caused by large evidence details.
  - Removed the following no longer supported lists from Recorded Future Domain Risk List:
    - `Historical Malware Analysis DNS Name`
    - `Recent Malware Analysis DNS Name`
  - Added the following new lists to Recorded Future Domain Risk List:
    - `Frequently Abused Free DNS Provider`
    - `Historically Suspected Malware Operation`
    - `Recently Suspected Malware Operation`
    - `Recent Cryptocurrency Mining Pool`
  - Added the following new lists to Recorded Future IP Risk List
    - `Historical Malicious Infrastructure Admin Server`
    - `Recent Malicious Infrastructure Admin Server`
  - Added the following new lists to Recorded Future URL Risk List
    - `Historically Suspected Malware Distribution`
    - `Recently Suspected Malware Distribution`
    - `Recent Reported C&C URL`
    - `Historical Reported C&C URL`
- **Version 2.8.4**
  - Commonly updated attributes, such as attributes that involve timestamps and criticality, will now be updated when ingesting new data as opposed to creating duplicate attributes. See the Mapping Tables of each feed for details.
- **Version 2.8.3**

  - Introduced a results limitation for the **Recorded Future Analyst Note** feed to resolve an offset issue.
  - Added the following new **Topic** configuration options for the **Recorded Future Analyst Note** feed:
    - Geopolitical Intelligence Summary
    - Geopolitical Flash Event
    - Geopolitical Threat Forecast
    - Geopolitical Validated Event
    - Insikt Research Lead
    - Regular Vendor Vulnerability Disclosures
    - Sigma Rule
    - The Record by Recorded Future
  - Added a new issue to the **Known Issues / Limitations** chapter regarding the API limit for the Analyst Notes and Alerts feeds.
- **Version 2.8.2**
  - Improved the **Recorded Future Alerts** feed to ingest more information regarding alerts.
    - Added new configuration field for the feed: **Save CVE Data As**.
    - Guide Update - updated Recorded Future Alerts sample response, default mapping table, Related Indicator Type mapping, and added a new Related Indicator Attributes mapping entry.
- **Version 2.8.1**
  - Updated the Recorded Future Alerts endpoint to API version 3.
  - Removed support from the following problematic lists:
    - Positive Malware Verdict
    - Historical Ransomware Distribution URL
    - Recent Ransomware Distribution URL
- **Version 2.8.0**
  - The integration now synchronizes Risk lists.
- **Version 2.7.0**
  - Added a new feed: Recorded Future Playbook Alerts.
  - Added the ability to filter by minimum risk score for the Risk List feeds (Recorded Future Domain Risk List, Recorded Future IP Risk List, Recorded Future URL Risk List, Recorded Future Vulnerability Risk List and Recorded Future Hash Risk List).
  - Added the ability to select the hash types that are ingested by the Recorded Future Hash Risk List, Recorded Future Analyst Note, and Recorded Future Alerts feeds.
  - Added the ability to ingest SHA-1 indicators.
- **Version 2.6.2**
  - Synchronized the Risk lists for the Risk List feeds to match option updates that Recorded Future performed.
  - Added time constrained data ingestion for all feeds so manual runs can be performed. Previously, the manual run option was only supported by the Analyst Note feed.
- **Version 2.6.1**
  - Fixed a parsing error that would occur when no evidence details are provided.
- **Version 2.6.0**
  - Removed lists from Recorded Future Domain Risk List feed:
    - Ransomware Distribution URL
    - Ransomware Payment DNS Name

    - Removed lists from Recorded Future Vulnerability Risk feed:
        - Observed Exploit/Tool Development in the Wild
        - Historically Observed Exploit/Tool Development in the Wild
- **Version 2.5.0**
    - Refactored Recorded Future Feeds (aside from Analyst Note).
    - Fixed a bug that caused an Error applying FilterMapping error from the URL Risk List and other similar feeds.
    - Removed lists that are no longer support that would cause the feed to throw a 404 error. Lists removed include:
        - Recorded Future Domain Risk List:
            - C&C URL
        - Recorded Future URL Risk List:
            - C&C
            - Compromised URL
            - Historically Detected Malicious Browser Exploits
            - Recently Detected Malicious Browser Exploits
            - Recently Detected Suspicious Content
            - Historically Detected Suspicious Content
        - Recorded Future Vulnerability Risk List:
            - Recently Observed Exploit/Tool Development in the Wild
- **Version 2.4.1**
    - Fixed a parsing error with Analyst Note.
- **Version 2.4.0**
    - Added Alert details
- **Version 2.3.0**
    - Added support for MITRE Attack Pattern Sub-Techniques
    - Added 'Save CVE Data As' user configuration parameter for Recorded Future Vulnerability Risk List
- **Version 2.2.0**
    - Added support to multiple selection for list
    - Fixed issue with MITRE map
- **Version 2.1.0**
    - Added support for configuration list in the request
- **Version 2.0.1**
    - Fixed issue with attributes
- **Version 2.0.0**
    - Added Analyst Note Integration
- **Version 1.0.0**
    - Initial release