ThreatQuotient

Recorded Future Implementation Guide

Version 2.4.0

Monday, September 28, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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 © 2020 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.

ThreatQuotient and Recorded Future are trademarks of their respective companies.

Last Updated: Monday, September 28, 2020

Contents

Recorded Future Implementation Guide 1

Warning and Disclaimer 2

Contents 3

Versioning 4

Introduction 5

Configuration 6

ThreatQ Mapping 10

Domain Risk List 10

IP Risk List 14

URL Risk List 17

Vulnerability Risk List 19

Hash Risk List 22

Analyst Notes 26

Entities Mapping 32

Alerts 36

Alert Details (Supplemental) 41

Average Feed Runs 46

Change Log 49

Versioning

- Current integration version: `2.4.0`
- Supported on ThreatQ versions >= `4.34.0`

Introduction

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

- Domain Risk List
- IP Risk List
- URL Risk List
- Vulnerability Risk List
- Hash Risk List
- Analyst Notes
- Alerts

Configuration

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

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feeds under the **Commercial** tab.
3. Click on the **Feed Settings** link for each feed.
4. Under the **Connection** tab, enter the following configuration parameters:

   All Recoded Future feeds, with the exception of Recorded Future Analyst Note and Alerts, require the following configuration parameters. See the separate accompanying tables for the Recorded Future Analyst Note and Alerts' configuration parameters.

Parameter	Description
Recorded Future API Key	The API Key to be used in HTTP headers for accessing feed data.
Lists to be Retrieved	Select specific Recorded Future lists using the dropdown menu provided.

Recorded Future Vulnerability Risk

The Vulnerability Risk List has one additional configuration parameter:

Parameter	Description
Save CVE Data As	Select whether to ingest CVEs as: • Vulnerability objects • Indicator objects • Both Vulnerability and Indicator objects Indicators objects is the default setting.

Recorded Future Analyst Note

Parameter	Description
Recorded Future API Key	Recorded Future API Key: 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: • Hunting Package • Analyst On-Demand Report • TTP Instance

Parameter	Description
	• Weekly Threat Landscape • Flash Report • Source Profile • Malware/Tool Profile • Validated Intelligence Event • Informational • Threat Lead • Geopolitics • Actor Profile • SNORT Rule • Cyber Threat Analysis • Indicator • YARA Rul
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 are: • ThreatQuotient - Partner Notes • Insikt Group
Tagged Text	Select whether the text should contain tags or not. Possible values: True/False.
Limit	Maximum number of records per request. This will be used in the pagination.

Recorded Future Alerts

Parameter	Description
Recorded Future API Key	The API Key to be used in HTTP headers for accessing feed data.
Triggered	Search for events by the triggered date.
Assignee	Search for events by email of the reported person.
Review Status	Search for events by the status. Options include: • Unassigned • Assigned • No Action • Tuning
Alert Rule ID	Search for events by the ID.
Freetext Search	Search for events by any value.
Maximum Number of Records	The maximum number of records returned per page.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of each feed name to enable the feeds.

ThreatQ Mapping

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 further evidence. This token is a JSON array of dictionaries. Example data is shown below. For better visual display, it is formatted and escaping characters are removed.

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

CSV response sample:

```
    '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. Most recent link (Apr 4,
2015): https://www.virus-
total.com/file/5b7b6e9f9cac22ec0f0c6f79093cb40ca04485e4b09d4a73efbab4b3388c5a62/analysis/',
```

```
            'Timestamp': '2015-04-04T00:00:00.000Z',
            'Criticality': 1,
            'MitigationString':
        },
        {
            '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,
            'MitigationString':
        },
        {
            'CriticalityLabel': 'Very Malicious',
            'Rule': 'C&C DNS Name',
            'EvidenceString': '1 sighting on 1 source: Abuse.ch: ZeuS Domain Blocklist (Stand-
ard).',
            'Timestamp': '2018-12-26T07:12:00.936Z',
            'Criticality': 4,
            'MitigationString':
        }
```

```
        ]
    }"
```

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 further evidence. This token is a JSON array of dictionaries. Example data is shown below. For better visual display, it is formatted and escaping characters are removed.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
0 (first token)	Indicator	FQDN		ns513726.ip-192-99-148.net	This indicator does not have a Timestamp
1 (second token)	Indicator Attribute	Risk Score		66	
2 (third token)	Indicator Attribute	Risk String		2/32	
3 (fourth token)[].CriticalityLabel	Indicator Attribute	Criticality	Timestamp	Suspicious	Timestamp of *this* array element
3 (fourth token)[].Rule	Indicator Attribute	Associated Rule	Timestamp	Blacklisted DNS Name	Timestamp of *this* array element
3 (fourth token)[].EvidenceString	Indicator Attribute	Evidence	Timestamp		Timestamp of *this* array element

IP Risk List

Similar to the above feed, this feed gets IP addresses as indicators. The data and mapping is as shown below.

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

CSV response sample:

```
    '5.120.187.119", '65', '1/49',
    "{'EvidenceDetails':
        [
            {
                'CriticalityLabel': 'Malicious',
                'Rule': 'Recent Positive Malware Verdict',
                'EvidenceString': '1 sighting on 1 source: ReversingLabs. Most recent link (Nov
22, 2018): https://a1000.re-
vers-
inglab-
s.com/ac-
counts/login/?next=/%3Fq%3Df600b62dc91602e2279364268d9cafca3c8d15de7871150883f9e083079e0e12',
                'Timestamp': '2018-11-22T00:00:00.000Z',
                'Criticality': 3,
                'MitigationString':
            }
```

```
        ]
    }"
```

ThreatQ provides the following default mapping for this feed. The mapping summarizes how the information from each field from the feed is converted to ThreatQ objects.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
0 (first token)	Indicator	IP Address		5.120.187.119	This indicator does not have a Timestamp
1 (second token)	Indicator Attribute	Risk Score		65	
2 (third token)	Indicator Attribute	Risk String		1/49	
3 (fourth token)[].CriticalityLabel	Indicator Attribute	Criticality	Timestamp	Malicious	Timestamp of *this* array element
3 (fourth token)[].Rule	Indicator Attribute	Associated Rule	Timestamp	Recent Positive Malware Verdict	Timestamp of *this* array element
3 (fourth token)[].EvidenceString	Indicator Attribute	Evidence	Timestamp		Timestamp of *this* array element

URL Risk List

Similar to the above feeds, this feed gets URLs as indicators. The data and mapping is as shown below:

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

CSV response sample:

```
    '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
            }
        ]
    }"
```

ThreatQ provides the following default mapping for this feed. The mapping summarizes how the information from each field from the feed is converted to ThreatQ objects.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
0 (first token)	Indicator	URL		http://handle.booktobi.com/css/index.html	This indicator does not have a Timestamp
1 (second token)	Indicator Attribute	Risk Score		65	
2 (third token)	Indicator Attribute	Risk String		1/7	
3 (fourth token)[].CriticalityLabel	Indicator Attribute	Criticality	Timestamp	Malicious	Timestamp of *this* array element
3 (fourth token) [].Rule	Indicator Attribute	Associated Rule	Timestamp	Active Phishing URL	Timestamp of *this* array element
3 (fourth token) [].EvidenceString	Indicator Attribute	Evidence	Timestamp		Timestamp of *this* array element

Vulnerability Risk List

Similar to the above feeds, this feed gets CVEs as indicators. The data and mapping is as shown below:

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

CSV response sample:

```
    'CVE-2018-0802', '89', '11/18',
    "{'EvidenceDetails':
        [
            {
                'CriticalityLabel': 'Low',
                'Rule': 'Linked to Historical Cyber Exploit',
                'EvidenceString': '4281 sightings on 351 sources including: YourThailandNet, @Al-
chemic_SH, @jasongori1, JLCW, @TopSecurityVids. Most recent tweet: \""RT oss_py: rtf_11882_0802 -
PoC for CVE-2018-0802 And CVE-2017-11882 https://t.co/dAZajuMuGy\"". Most recent link (Nov 14,
2018): https://twitter.com/securisec/statuses/1062835440519184384',
                '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. Most recent tweet: Cyber
Security Today Exploited VulnerabilitiesCVE-2017-11882 Hits: 17 Related: SHA-256, ReversingLabs,
CVE-2017-8570, CVE-2018-0802 CVE-2017-15944 Hits: 15 Related: Palo Alto Networks, PAN-OS, Metas-
ploit Framework, Remote Root CVE-2018-6789 Hits: 12…https://t.co/XizgvBjegT. Most recent link
(May 7, 2018): https://twitter.com/DTechCloud/statuses/993589156788998144',
                'Timestamp': '2018-05-07T20:31:29.000Z', 'Criticality': 1
            },
        ]
    }"
```

ThreatQ provides the following default mapping for this feed. The mapping summarizes how the information from each field from the feed is converted to ThreatQ objects.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
0 (first token)	Indicator	CVE		CVE-2018-0802	This indicator does not have a Timestamp
1 (second token)	Indicator Attribute	Risk Score		89	
2 (third token)	Indicator Attribute	Risk String		11/18	
3 (fourth token)[].CriticalityLabel	Indicator Attribute	Criticality	Timestamp	Low	Timestamp of *this* array element
3 (fourth token) [].Rule	Indicator Attribute	Associated Rule	Linked to Historical Cyber Exploit	Timestamp of *this* array element	
3 (fourth token) [].EvidenceString	Indicator Attribute	Evidence	Timestamp		Timestamp of *this* array element

Hash Risk List

Similar to the above feeds, this feed gets Hashes as indicators. There is one difference with this feed: it brings in an additional field *algorithm*, which indicates the hash type (MD5, SHA1, or SHA256). The data and mapping is as shown below:

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

CSV response sample:

```
    'ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa', 'SHA-256', '89', '4/10',
    "{'EvidenceDetails':
        [
            {
                'CriticalityLabel': 'Unusual',
                'Rule': 'Threat Researcher',
                'EvidenceString': '21 sightings on 9 sources including: Security Affairs,
SecureWorks, Cylance Blog, McAfee, Trend Micro. Most recent link (Jan 28, 2018): https://www.cyl-
ance.com/content/cylance/ja_jp/blog/jp-threat-spotlight-wannacry-ransomware.html',
                'Timestamp': '2018-01-28T11:24:35.942Z',
                'Criticality': 1.0
            },
            {
                'CriticalityLabel': 'Suspicious',
                'Rule': 'Linked to Vulnerability',
```

```
                'EvidenceString': '5 sightings on 2 sources: fb.me, comae.io. 3 related cyber vul-
nerabilities: MS17-010, CWE-20, CVE-2017-0148. Most recent link (Aug 8, 2017): https://f-
b.me/8IiLKtP82',
                'Timestamp': '2017-08-08T14:10:11.410Z',
                'Criticality': 2
            },
            {
                'CriticalityLabel': 'Suspicious',
                'Rule': 'Linked to Malware',
                'EvidenceString': 'Previous sightings on 36 sources including: SecureWorks, blog_
trendmicro_co_jp, Facebook, Security Affairs, GitHub. 81 related malwares including Tro-
jan.Win32.Wanna.u!c, W97M.Downloader, Win32:WanaCry-A [Trj], malicious_confidence_100% (W), Tro-
jan.Filecoder!LcLqI1eM+lA. Most recent tweet: Please lock out this file hash sha256:
ed01ebfbc9eb5bbea545af4d01bf5fxxxxxxxxxxxxxxxxc6e5babe8e080e41aa #Ransomware. Most recent link
(May 12, 2017): https://twitter.com/SoftcatSecurity/statuses/863056045941415936',
                'Timestamp': '2017-05-12T15:39:30.000Z',
                'Criticality': 2
            },
        ]
    }"
```

ThreatQ provides the following default mapping for this feed. The mapping summarizes how the information from each field from the feed is converted to ThreatQ objects.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
0 (first token)	Indicator	MD5		00d48afbba5ef9eadb572730b2d0cafa	This indicator does not have a Timestamp If algorithm (second token) == MD5
0 (first token)	Indicator	SHA-1		002e3d9dd841dd36c7b434eee0e3416f0860b83a	This indicator does not have a Timestamp If algorithm (second token) == SHA-1
0 (first token)	Indicator	SHA-256		ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa	This indicator does not have a Timestamp If algorithm (second token) == SHA-256
2 (third token)	Indicator Attribute	Risk Score		89	
3 (fourth token)	Indicator Attribute	Risk String		4/10	
4 (fifth token)	Indicator	Criticality	Timestamp	Suspicious	Timestamp of *this* array ele-

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
[].CriticalityLabel	Attribute				ment
5 (fifth token) [].Rule	Indicator Attribute	Associated Rule	Timestamp	Linked to Malware	Timestamp of *this* array element
6 (fifth token) [].EvidenceString	Indicator Attribute	Evidence	Timestamp		Timestamp of *this* array element

Analyst Notes

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

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

CSV response sample:


```
{
    "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
    }
}
```

ThreatQ provides the following default mapping for this feed. The mapping summarizes how the information from each field from the feed is converted to ThreatQ objects.

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"	
.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"	
.data.results[].source.name	report.attribute	Recorded Future Source	"Insikt Group"	
.data.results[].attributes.topic[].name	report.attribute	Topic Name	"Flash Report"	
.data.results[].attributes.validated_on	report.attribute	Validated On	"2020-02-06T06:59:32.784Z"	
.data.results[].at-				*See Entities Mapping

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
tributes.context_entit-ies				
.data.results[].at-tributes.note_entities				*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:

JSON response sample:

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

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

The integration 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"	
.text	report.attribute	.description	"some description"	
.name	indicator.value	Indicator	"Bleeping Computer"	
.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 analysed and based on it it will be either `MD5` or `SHA-256`.
.description	indicator.attribute	Description	"some	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
			description"	
See note	indicator.attribute	Analyst Note	"some description"	
.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). If the ingested name is 'T1001', the value will be 'T1001 - Data Obfuscation'.
.description	attack_pattern.attribute	Entity Description	"some description"	
See note	attack_pattern.attribute	Analyst Note	"some description"	
.name	malware.value	Malware	"Bleeping Computer"	
.description	malware.attribute	Entity	"some	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
		Description	description"	
See note	malware.attribute	Analyst Note	"some description"	

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

Alerts

'GET https://api.recordedfuture.com/v2/alert/search'

JSON response sample:


```
{
  "data": {
    "results": [
      {
        "review": {
          "assignee": null,
          "noteAuthor": null,
          "note": null,
          "status": "no-action",
          "noteDate": null
        },
        "url": "https://app.recordedfuture.com/live/sc/notification/?id=eWnL8e",
        "rule": {
          "url": "https://app.recordedfuture.com/live/sc/ViewIdkobra_view_report_item_alert_edit-
or?view_opts-
=%7B%22r-
```

```
eportId%22%3A%22d-
pNEJw%22%2C%22bTitle%22%3Atrue%2C%22title%22%3A%22Possible+Fraud+related+to+COVID-
19%22%7D&state.bNavbar=false",
          "name": "Possible Fraud related to COVID-19",
          "id": "dpNEJw"
        },
        "triggered": "2020-06-28T10:09:31.681Z",
        "id": "eWnL8e",
        "title": "Possible Fraud related to COVID-19 - New references in 18 documents",
        "type": "REFERENCE"
      }
    ]
  },
  "counts": {
    "returned": 1,
    "total": 63
  }
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.data.results[].title	Event.Title	N/A	.data.results[].review.noteDate / .data.results[].triggered	Possible Fraud related to COVID-19 - New references in 18 documents	If '.noteDate' is not present '.triggered' is used as 'Published Date'
.data.results[].triggered	Event.Happened_at	N/A	N/A	2020-06-28 10:09:31-00:00	N/A
.data.results[].review.note	Event.Description	N/A	N/A	This is an event that was created today	N/A
.data.results[].review.assignee	Event.Attribute	Assignee	.data.results[].review.noteDate / .data.results[].triggered	joe@gmail.com	N/A
.data.results[].review.noteAuthor	Event.Attribute	Note Author	.data.results[].review.noteDate /	Joe	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
			.data.results[].triggered		
.data.results[].review.status	Event.Attribute	Alert Status	.data.results[].review.noteDate / .data.results[].triggered	no-action	N/A
.data.results[].url	Event.Attribute	Reference URL	.data.results[].review.noteDate / .data.results[].triggered	https://app.recordedfuture.com/live/sc/notification/?id=eWnL8e	N/A
.data.results[].rule.url	Event.Attribute	Triggered Rule URL	.data.results[].review.noteDate / .data.results[].triggered	https://app.recordedfuture.com/live/sc/ViewIdkobra_view_report_item_alert_editor?view_opts-s=%7B%22reportId%22%3A%22dpNEJw%22%2C%22bTitle%22%3Atrue%2C%22	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
				title%22%3A%22Possible+Fraud+related+to+COVID-19%22%7D&state.bNavbar=false	
.data.results[].rule.-name	Event.Attribute	Triggered Rule Name	.data.results[].re-view.noteDate / .data.results[].triggered	Possible Fraud related to COVID-19	N/A
.data.results[].type	Event.Attribute	Alert Type	.data.results[].re-view.noteDate / .data.results[].triggered	REFERENCE	N/A

Alert Details (Supplemental)

This is used to fetch related data for each of the ingested events retrieved from the Alert endpoint. The JSON Key 'data.results[].id' is used to call the supplemental feed.

```
GET https://api.recordedfuture.com/v2/alert/{id}
```

JSON response sample:


```
{
  "data": {
    "review": {
      "assignee": null,
      "noteAuthor": null,
      "note": null,
      "status": "no-action",
      "noteDate": null
    },
    "entities": [
      {
        "entity": null,
        "risk": {},
        "trend": {},
        "documents": [
```

```
          {
            "references": [
              {
                "fragment": "https://www.youtube.com/watch?v=hXm",
                "entities": [
                  {
                    "id": "url:ht-
tps://www.-
google.com/sorry/index?continue=https://www.youtube.com/watch%3Fv%3DhXm&q=EgQ2xjflGKXbq_
kFIhkA8aeDSwvdzIPWTTJyonXEKu0LsTYQsIHKMgFy",
                    "name": "https://www.-
google.com/sorry/index?continue=https://www.youtube.com/watch%3Fv%3DhXm&q=EgQ2xjflGKXbq_
kFIhkA8aeDSwvdzIPWTTJyonXEKu0LsTYQsIHKMgFy",
                    "type": "URL"
                  }
                ],
                "language": "eng"
              }
            ],
            "source": {
              "id": "a0-Mp5",
```

```
            "name": "4chan Pol Forum",
            "type": "Source"
          },
          "url": "https://boards.4chan.org/pol/thread/274300558",
          "title": "be-european"
        },
      ]
    }
  ],
  "url": "https://app.recordedfuture.com/live/sc/notification/?id=fDC4dx",
  "rule": {
    "url": "https://app.recordedfuture.com/live/sc/ViewIdkobra_view_report_item_alert_edit-
or?view_opts-
s=%7B%22reportId%22%3A%22ezLL1S%22%2C%22bTitle%22%3Atrue%2C%22title%22%3A%22Domains+on+Non-
Mainstream+Sources%22%7D&state.bNavbar=false",
    "name": "Domains on Non-Mainstream Sources",
    "id": "ezLL1S"
  },
  "triggered": "2020-08-26T12:46:03.135Z",
  "id": "fDC4dx",
  "counts": {
```

```
      "references": 10,
      "entities": 0,
      "documents": 9
    },
    "title": "Domains on Non-Mainstream Sources - New references in 9 documents",
    "type": "EVENT"
  }
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.data.results[].url	Related.Indicator	URL	.data.results[].review.noteDate / .data.results[].triggered	https://app.recordedfuture.com/live/sc/notification/?id=fDC4dx	N/A
.data.results[].documents[].references[].fragment	Related.Indicator.Attribute	Fragment	.data.results[].review.noteDate / .data.results[].triggered	https://www.youtube.com/watch?v=hXm	N/A
.data.results[].documents[].references[].language	Related.Indicator.Attribute	Language	.data.results[].review.noteDate / .data.results[].triggered	eng	N/A
.data.results[].documents[].references[].entities[].name	Related.Indicator.Attribute	data.results[].documents[].references[].entities[].type	.data.results[].review.noteDate / .data.results[].triggered	https://www.google.com/sorry/index?continue	N/A

Average Feed Runs

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.

Domain Risk List

Metric	Result
Run Time	1 minute
Indicators	156
Indicator Attributes	1352

IP Risk List

Metric	Result
Run Time	1 minute
Indicators	1
Indicator Attributes	13

URL Risk List

Metric	Result
Run Time	1 minute
Indicators	109
Indicator Attributes	1,675

Vulnerability Risk List

Metric	Result
Run Time	1 minute
Indicators	3
Indicator Attributes	59

Hash Risk List

Metric	Result
Run Time	24 hours
Indicators	266,171
Indicator Attributes	184,614

Analyst Note

Metric	Result
Run Time	21 minutes
Indicators	113
Indicator Attributes	732
Malware	24
Malware Attributes	131
Reports	19
Reports Attributes	335

Alerts *with Maximum Number of Records: 10*

Metric	Result
Run Time	10 minutes
Events	1,000
Events Attributes	53,405
Indicators	4,461
Indicator Attributes	4,465

Change Log

- **Version 2.4.0**
  - Added new data feed: Recorded Future Alerts
- **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**
  - Fixed an issue regarding MITRE Mapping.
  - Fixed a multiple selection bug.
- **Version 2.1.0**
  - Users can now select the desired value for the list to be retrieved.
- **Version 2.0.1**
  - Linked Associated Rule and Evidence attributes have been added to the Associated Rule and Criticality names.
- **Version 2.0.0**
  - Added Configuration parameters to the feed to optimize performance.
- **Version 1.1.0**
  - Fixed issue regarding time stamp format errors.
- **Version 1.0.0**
  - Initial Release