ThreatQuotient

Recorded Future CDF Guide

Version 2.6.1

December 13, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `2.6.0`
- Supported on ThreatQ versions >= `4.34.0`

Introduction

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

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

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 feed-related credentials.

To configure the feed:

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

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

PARAMETER	DESCRIPTION
Recorded Future API Key	API Key to be used in HTTP headers for accessing feed data.
Recorded Future List	A string to search for notes by entity ID.

Recorded Future Vulnerability Risk List

PARAMETER	DESCRIPTION

PARAMETER	DESCRIPTION
Recorded Future API Key	API Key to be used in HTTP headers for accessing feed data.
Recorded Future List	Specific Recorded Future lists to be retrieved.
Save CVE Data As	Select whether to ingest CVEs as: • ThreatQ Vulnerability objects • Indicator objects • both The default setting is to ingest Indicators objects.

Recorded Future Analyst Note

PARAMETER	DESCRIPTION
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.

PARAMETER	DESCRIPTION
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 • Geopolitics • Hunting Package • Indicator • Informational • Malware/Tool Profile • SNORT Rule • Source Profile • 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.

PARAMETER	DESCRIPTION
	The options for this user field will be: • Insikt Group • ThreatQuotient - Partner Notes
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	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.

PARAMETER	DESCRIPTION
Freetext Search	A string to search for events by any value.

5. Review the **Settings** configuration, 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

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`

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...",
            "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
        }
    ]
}'
```

ThreatQ 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	N/A
2 (third token)	Indicator.Attribute	Risk String	N/A	2/32	N/A
3 (fourth token) []CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) []Timestamp	Suspicious	N/A
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

IP Risk List

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

```
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....",
            "Timestamp": "2018-11-22T00:00:00.000Z",
            "Criticality": 3
        }
    ]
}'
```

ThreatQ 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	N/A
2 (third token)	Indicator.Attribute	Risk String	N/A	1/49	N/A
3 (fourth token) []CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) [].Timestamp	Malicious	N/A
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

URL Risk List

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

```
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:

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	N/A
2 (third token)	Indicator.Attribute	Risk String	N/A	1/7	N/A
3 (fourth token) []CriticalityLabel	Indicator.Attribute	Criticality	3 (fourth token) []Timestamp	Malicious	N/A
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

Vulnerability Risk List

Similar to the above feeds, this feed gets CVEs.

```
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: ...",
            "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
        },
    ]
}'
```

ThreatQ 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	N/A
2 (third token)	Indicator.Attribute/ Vulnerability.Attribute	Risk String	N/A	11/18	N/A
3 (fourth token) []CriticalityLabel	Indicator.Attribute/ Vulnerability.Attribute	Criticality	3 (fourth token) [].Timestamp	Low	N/A
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

Hash Risk List

Similar to the above feeds, this feed gets Hashes.

```
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: ...",
            "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
        },
    ]
}'
```

ThreatQ 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	N/A
3 (fourth token)	Indicator.Attribute	Risk String	N/A	4/10	N/A
4 (fifth token) []CriticalityLabel	Indicator.Attribute	Criticality	4 (fifth token) []Timestamp	Suspicious	N/A
4 (fifth token)[].Rule	Indicator.Attribute	Associated Rule	4 (fifth token) []Timestamp	Linked to Malware	N/A
4 (fifth token) []EvidenceString	Indicator.Attribute	Evidence	4 (fifth token) []Timestamp	Previous sightings on 36 sources including: ...	N/A

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'

JSON 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:

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"	N/A
.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:

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
```

Going forward, 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 analysed and based on it it will be either `MD5` 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). 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.

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_editor?
view_opts=%7B%22reportId%22%3A%22dpNEJw%22%2C%22bTitle%22%3Atrue%2C%22title%22%3A%22Possible+Fraud+related+to+COVID-1
9%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
.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
.data.results[].triggered	Event.Happened_at	N/A	N/A	2020-06-28 10:09:31-00:00
.data.results[].review.note	Event.Description	N/A	N/A	This is an event that was created to
.data.results[].review.assignee	Event.Attribute	Assignee	.data.results[].review.noteDate / .data.results[].triggered	joe@gmail.com
.data.results[].review.noteAuthor	Event.Attribute	Note Author	.data.results[].review.noteDate / .data.results[].triggered	Joe
.data.results[].review.status	Event.Attribute	Alert Status	.data.results[].review.noteDate / .data.results[].triggered	no-action
.data.results[].url	Event.Attribute	Reference URL	.data.results[].review.noteDate / .data.results[].triggered	https://app.recordedfuture.com/liv sc/notification/?id=eWnL8e
.data.results[].rule.url	Event.Attribute	Triggered Rule URL	.data.results[].review.noteDate / .data.results[].triggered	https://app.recordedfuture.com/liv /sc/ViewIdkobra_view_report_item_ alert_editor?view_opts=%7B%22rep ortId%22%3A%22dpNEJw%22%2C% 22bTitle%22%3Atrue%2C%22title% 2%3A%22Possible+Fraud+related+t +COVID-19%22%7D&state.bNavbar
.data.results[].rule.name	Event.Attribute	Triggered Rule Name	.data.results[].review.noteDate / .data.results[].triggered	Possible Fraud related to COVID-19
.data.results[].type	Event.Attribute	Alert Type	.data.results[].review.noteDate / .data.results[].triggered	REFERENCE

Alert Details (Supplemental)

This is used to fetch related data for each of the ingested events retrieved from the Alert endpoint. The 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:https://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_editor?
view_opts=%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
.data.results[].url	Related.Indicator	URL	.data.results[].review.noteDate / .data.results[].triggered	https://boards.4chan.org/pol/thread/280936775
.data.results[].url	Related.Indicator.Attribute	URL	.data.results[].review.noteDate / .data.results[].triggered	https://www.virustotal.com/gui/url/b8a9468323b46d6058dbcc1598aad13fc9a331d4d9f5f4912ae43b55776bfc75
.data.results[].documents[].references[].fragment	Related.Indicator.Attribute	Fragment	.data.results[].review.noteDate / .data.results[].triggered	https://www.youtube.com/watch?v=hXm
.data.results[].documents[].references[].language	Related.Indicator.Attribute	Language	.data.results[].review.noteDate / .data.results[].triggered	eng
.data.results[].documents[].references[].entities[].name	Related.Indicator	data.results[].documents[].references[].entities[].type	.data.results[].review.noteDate / .data.results[].triggered	https://www.google.com/sorry/index?continue

In the previous table, there is a 'Related Indicator' that is set dynamically. We do this because the 'ThreatQ Object Type' is extracted from the same path '.data.results[].documents[].references[].entities[].type'.

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-256	If the length of the hash value is not 32 characters. This is the only other hash type returned by the Alert Details endpoint

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.

Recorded Future Domain Risk List with Recorded Future List set as only C&C DNS Name

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

Recorded Future Domain Risk List set as:

- C&C Nameserver
- C&C DNS Name
- Compromised URL
- Recently Resolved to Host of Many DDNS Names
- Historically Reported as a Defanged DNS Name

METRIC	RESULT
Run Time	20 minutes
Indicators	5,209
Indicator Attributes	47,806

Recorded Future IP Risk List with Recorded Report Future List set as only Threat Actor Used Infrastructure

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

Recorded Future IP Risk List with Recorded Report Future List set as:

- Threat Actor Used Infrastructure
- Historically Reported by Insikt Group
- Inside Possible Bogus BGP Route
- Historical Botnet Traffic
- Namesever for CC Server

METRIC	RESULT
Run Time	11 minutes
Indicators	1,940
Indicator Attributes	33,026

Recorded Future URL Risk List with Recorded Future List set as only Active Phishing URL

METRIC	RESULT
Run Time	23 minutes
Indicators	10,653
Indicator Attributes	92,877

Recorded Future URL Risk List with Recorded Future List set as:

- Recently Referenced by Insikt Group
- Recently Reported Spam or Unwanted Content
- Recently Active URL on Weaponized Domain
- Historically Referenced by Insikt Group
- Historically Reported Spam or Unwanted Content

METRIC	RESULT
Run Time	30 minutes
Indicators	10,653
Indicator Attributes	92,874

Recorded Future Vulnerability Risk List with Recorded Future List set as only Cyber Exploit Signal: Important

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

Recorded Future Vulnerability Risk List with Recorded Future List set as:

- Exploited in the Wild by Recently Active Malware
- Recently Referenced by Insikt Group
- Recently Linked to Penetration Testing Tools
- Historically Referenced by Insikt Group
- Historically Linked to Penetration Testing Tools

METRIC	RESULT
Run Time	2 hours
Indicators	22,113
Indicator Attributes	202,599
Vulnerabilities	29,013
Vulnerability Attributes	240,111

Recorded Future Hash Risk List with Recoded Future List set as only to Linked Cyber Attack

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

Recorded Future Hash Risk List with Recorded Future List set as:

- Malware SSL Certificate Fingerprint
- Observed in Underground Virus Testing Sites
- Positive Malware Verdict

METRIC	RESULT
Run Time	2 hours
Indicators	59,347
Indicator Attributes	453,550

Recorded Future Analyst Note

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

Recorded Future Alerts

METRIC	RESULT
Run Time	15 minutes
Events	997
Events Attributes	4,985
Indicators	6,861
Indicator Attributes	41,747

Known Issues/Limitations

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

Change Log

- **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 Obserbed 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