ThreatQuotient

Recorded Future Implementation Guide

Version 2.0.1

Wednesday, March 4, 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.

Last Updated: Wednesday, March 4, 2020

Contents

Versioning

- Current integration version: `2.0.1`
- Supported on ThreatQ versions >= `4.30.0`

Introduction

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

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

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, require the following configuration parameters. See the next table for the Recorded Future Analyst Note's configuration parameters.

Parameter	Description
Recorded Future API Key	Recorded Future API Key: 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 Analyst Note

Parameter	Description
Recorded Future API Key	Recorded Future API Key: API Key to be used in HTTP headers for accessing feed data.

Parameter	Description
EntityRecorded Future API Key	Filter objects ingested by Report Entity ID.
Author	Filter objects ingested by Report Author ID.
Title	Filter objects ingested by Report Title.
Topic	Filter objects ingested by Report Topic ID.
Label	Filter objects ingested by Report Label Name.
Source	Filter objects ingested by Report Source.
Tagged Text	Enable if the text should contain tags.
Limit	The maximum number of objects per request.

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.

```
    '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/5b7b6e9f9cac22ec0f0c6f79093cb40ca04485e4b09d4a73ef-
bab4b3388c5a62/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 (Standard).',
                '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.

```
    '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-
count-
s/lo-
gin/?nex-
t=/%3Fq%3Df600b62-
2dc91602e2279364268d9cafca3c8d15de7871150883f9e083079e0e12',
                '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	Normalization	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
Indicator Attribute	Indicator Attribute	Evidence	Timestamp			Timestamp of *this* array element

A set of (Criticality Label, Rule and Evidence) attributes is created for each entry of the list from the response. They are linked through the name of the Criticality Label and Rule attributes, which include the value of the Evidence attribute they are linked to.

URL Risk List

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

```
    '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	Normalization	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

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
3 (fourth token) [].EvidenceString	Indicator Attribute	Evidence		Timestamp		Timestamp of *this* array element

A set of (Criticality Label, Rule and Evidence) attributes is created for each entry of the list from the response. They are linked through the name of the Criticality Label and Rule attributes, which include the value of the Evidence attribute they are linked to.

Vulnerability Risk List

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

```
    'CVE-2018-0802', '89', '11/18',
    "{'EvidenceDetails':
        [
            {
                'CriticalityLabel': 'Low',
                'Rule': 'Linked to Historical Cyber Exploit',
                'EvidenceString': '4281 sightings on 351
sources including: YourThailandNet, @Alchemic_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, Metasploit
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	Normalization	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

A set of (Criticality Label, Rule and Evidence) attributes is created for each entry of the list from the response. They are linked through the name of the Criticality Label and Rule attributes, which include the value of the Evidence attribute they are linked to.

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:

```
    'ed01ebf-
bc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa',
'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.cylance.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 vulnerabilities: MS17-010,
CWE-20, CVE-2017-0148. Most recent link (Aug 8, 2017):
https://fb.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 Trojan.Win32.Wanna.u!c, W97M.Downloader, Win32:WanaCry-A [Trj], malicious_confidence_100% (W), Trojan.Filecoder!LcLqI1eM+lA. Most recent tweet: Please lock out this file hash sha256: ed01ebfbc9eb5bbea545af4d01bf5fxxxxxxxxxxxxxxxc6e5babe8e080e41aa #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	Normalization	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

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
						(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	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
4 (fifth token) [].CriticalityLabel	Indicator Attribute	Criticality		Timestamp	Suspicious	Timestamp of *this* array element
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

A set of (Criticality Label, Rule and Evidence) attributes is created for each entry of the list from the response. They are linked through the name of the Criticality Label and Rule attributes, which include the value of the Evidence attribute they are linked to.

Analyst Notes

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

```
{
    "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 Enter-
prise Networks",
                    "note_entities": [
                        {
                            "id": "bLfMiL",
                            "name": "Mailto Ransomware",
                            "type": "Malware"
                        }
                    ],
                    "context_entities": [
                        {
                            "id": "J6UzbO",
                            "name": "Bleeping Computer",
                            "type": "Source"
                        }
                    ],
                    "validation_urls": [
                        {
                            "id": "url:url:ht-
tps://www.bleepingcomputer.com/news/security/mailto-netwalker-
ransomware-targets-enterprise-networks/",
                            "name": "url:ht-
tps://www.bleepingcomputer.com/news/security/mailto-netwalker-
ransomware-targets-enterprise-networks/",
                            "type": "URL"
                        },
                        {
                            "id": "url:url:ht-
tps://twitter.com/VK_Intel/status/1225086186445733889?s=20",
                            "name": "url:ht-
tps://twitter.com/VK_Intel/status/1225086186445733889?s=20",
                            "type": "URL"
                        }
                    ]
                },
                "id": "cu1WGK"
            }
        ]
    },
    "counts": {
        "returned": 10,
        "total": 19216
    }
}
```

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[].id	report.attribute	ID	"cu1WGK"	
.data.results[].source.id	report.attribute	Source ID	"VKz42X"	
.data.results[].source.-name	report.attribute	Source Name	"Insikt Group"	
.data.results[].attributes.validated_on	report.attribute	Validated on	"2020-02-06T06:59:32.784Z"	
.data.results[].attributes.topic[].id	report.attribute	Topic ID	"TXSFt0"	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.data.results[].attributes.topic[].name	report.attribute	Topic Name	"Flash Report"	
.data.results[].attributes.validation_urls[].name	report.attribute	Validation URL	"url:https://twitter.com/VK_Intel/status/1225086189?s=20"	
.data.results[].attributes.context_entities				*See entities mapping
.data.results[].attributes.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:

```
"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
.id	report.attribute	Entity ID	"J6UzbO"	
.name	report.attribute	Entity Name	"Bleeping Computer"	
.type	report.attribute	Entity Type	"Source"	
.description	report.attribute	Entity Description	"some description"	
.id	indicator.attribute	Entity ID	"J6UzbO"	
.name	indicator.value	Indicator	"Bleeping Computer"	
.type	indicator.type	*See notes	"IpAddress	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

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
				on it it will be either `MD5` or `SHA-256`.
.description	indicator.attribute	Description	"some description"	
.id	attack_pattern.attribute	Entity ID	"J6UzbO"	
.name	attack_pattern.value	Attack Pattern	"Bleeping Computer"	
.description	attack_pattern.attribute	Entity Description	"some description"	
.id	malware.attribute	Entity ID	"J6UzbO"	
.name	malware.value	Malware	"Bleeping Computer"	
.description	malware.attribute	Entity Description	"some description"	