Recorded Future Implementation Guide

Version 1.0.0

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, January 9, 2019

Contents

Versioning

- Current integration version `1.0.0`
- Supported on ThreatQ versions `4.13` or later

Introduction

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

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

ThreatQ Mapping

Domain Risk List

The data on this feed comes in the 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.virustotal.com/file/
            5b7b6e9f9cac22ec0f0c6f79093cb40ca04485e4b09d4
            a73efbab4b3388c5a62/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':
        }
    ]
}"
```

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 Attrib-ute Key	Published Date	Examples
0 (first token)	Indicator	FQDN		ns513726.ip-192-99-148.net
1 (second token)	Indicator	Risk Score		66
2 (third token)	Indicator	Risk String		2/32
3 (fourth token) []CriticalityLabel	Indicator	Criticality	Timestamp	Suspicious
3 (fourth token) [].Rule	Indicator	Associated Rule	Timestamp	Blacklisted DNS Name
3 (fourth token) [].EvidenceString	Indicator	Filename	Timestamp	

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.reversinglabs.com/accounts/
               login/?next=/%3Fq%3Df600b62dc91602e2279364268
               d9cafca3c8d15de7871150883f9e083079e0e12',
          '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 Attrib-ute Key	Published Date	Examples
0 (first token)	Indicator	IP Address		5.120.187.119

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
1 (second token)	Indicator	Risk Score		65
2 (third token)	Indicator	Risk String		1/49
3 (fourth token) [].CriticalityLabel	Indicator	Criticality	Timestamp	Malicious
3 (fourth token) [].Rule	Indicator	Associated Rule	Timestamp	Recent Positive Malware Verdict
3 (fourth token) [].EvidenceString	Indicator	Evidence	Timestamp	

URL Risk List

Similar to the above feeds, this feed receives 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	Published Date	Examples
0 (first token)	Indicator	URL		http://handle.book-tobi.com/css/index.htm
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
3 (fourth token) [].Rule	Indicator Attribute	Associated Rule	Timestamp	Active Phishing URL
3 (fourth token) [].EvidenceString	Indicator Attribute	Evidence	Timestamp	

Vulnerability Risk List

Similar to the above feeds, this feed receives 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
               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	Published Date	Examples
0 (first token)	Indicator	CVE		CVE-2018-0802
1 (second token)	Indicator	Risk Score		89
2 (third token)	Indicator	Risk String		11/18
3 (fourth token) []CriticalityLabel	Indicator	Criticality	Timestamp	Low
3 (fourth token) []Rule	Indicator	Associated Rule	Linked to Historical Cyber	Timestamp of *this* array ele-

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
			Exploit	ment
3 (fourth token) []:EvidenceString	Indicator	Evidence	Timestamp	

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:
            ed01ebfbc9eb5bbea545af4d01bf5fxxxxxxxxxxxxxxxx
            c6e5babe8e080e41aa #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
0 (first token)	Indicator	MD5		00d48afbba5ef9eadb572730b2d0cafa
0 (first token)	Indicator	SHA-1		002e3d9dd841dd36c7b434eee0e3416f0860b83a
0 (first token)	Indicator	SHA-256	analysis_start_time	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
2 (third token)	Indicator Attribute	Risk Score		89
3 (fourth token)	Indicator	Risk String		4/10

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
	Attribute			
4 (fifth token) []CriticalityLabel	Indicator Attribute	Criticality	Timestamp	Suspicious
5 (fifth token) [].Rule	Indicator Attribute	Associated Rule	Timestamp	Linked to Malware
6 (fifth token) [].EvidenceString	Indicator Attribute	Evidence	Timestamp	

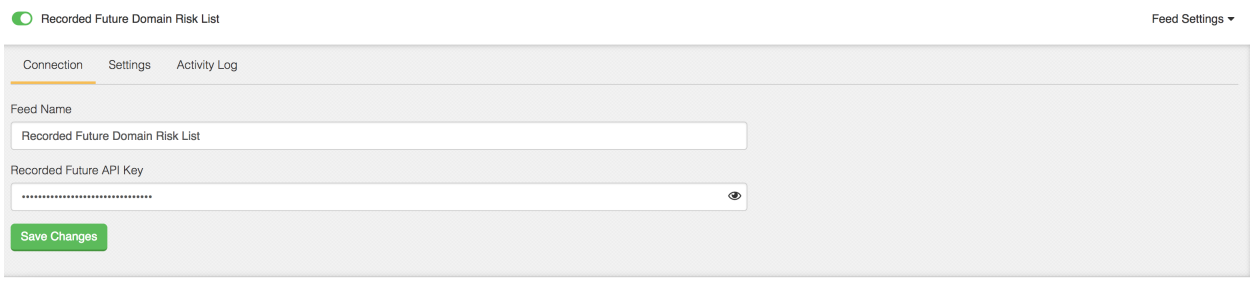
Installation

The following artisan command on ThreatQ platform will install the feed definition (in `yaml` format).

```
sudo php artisan threatq:feed-install recorded_future.yaml
```

ThreatQ UI Configuration

The connector installs as a feed under **Commercial** as shown below. The button next to Recorded Future Domain Risk List must be activated for the feed to initialize.



The feed provides the following two configuration parameter:

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

An example feed run is shown below: