ThreatQuotient

Intel 471 Alerts Feed Implementation Guide

Version 1.0.0

Monday, January 6, 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: Monday, January 6, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.28.0`

Introduction

Intel 471 Alerts Feed ingests threat intelligence data from the following endpoint:

- **Intel 471 Alerts** - https://api.intel471.com/v1/alerts

Notes

- Time constrained data fetching is possible.
- Uses basic HTTP authentication based on email address and API key.

Installation

Perform the following steps to install the feed:

The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Intel 471 Alerts** feed file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

The feed will be added to the **Commercial** tab for Incoming Feeds. 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. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
Email Address	The vendor-supplied email address.
API Key	The vendor-supplied API Key.
Count	Maximum number of records to retrieve from the provider per request. Default value: 10. Size range: 0-100.

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

ThreatQ Mapping

Intel471 Alerts

JSON response sample:


```
{
  "alertTotalCount": 312,
  "alerts": [
       {
          "uid": "59413a3c441d6663bf8795bc",
          "status": "read",
          "watcherUid": "aa957845d56c4773f379843afc507ea9",
          "watcherGroupUid": "f5db9f26-f0c6-408d-8dac-
542e8c036aa2",
          "foundTime": 1497446972076,
          "privateMessage": {
              "uid": "6613f939099a5db1b7b627478c74f6e9",
              "date": 1265707719000,
              "subject": "Important message from the forum
administration!",
              "message": "Dear, Волна!\r\n\r\nA virus alert
was noticed on your computer. \r\nWe highly recommend you to
check your computer and perform online virus check at our site
immediately: [url]http://security-tool2010.com/Волна
[/url]\r\n----------------------------------------------------
\r\nForum Administration [url]www.carder.info[/url].",
              "links": {
                  "authorActor": {
```

```
                    "uid": "5328c3099d-
bc67b62cf7ee620ffee4c2",
                    "handle": "BestForumTeam"
                },
                "recipientActor": {
                    "uid": "37fb05b-
c65bf6a1435e06a98e4266bc7",
                    "handle": "Волна"
                },
                "forum": {
                    "uid":
"96a3be3cf272e017046d1b2674a52bd3",
                    "name": "carder.pro",
                    "description": "carder.pro is a forum
focused on carding (credit card fraud)."
                }
            },
            "lastUpdated": 1497370483069
        }
    },
    {
        "uid": "59413a3c441d6663bf8795bb",
        "status": "read",
        "watcherUid": "aa957845d56c4773f379843afc507ea9",
        "watcherGroupUid": "f5db9f26-f0c6-408d-8dac-
542e8c036aa2",
        "foundTime": 1497446972076,
        "post": {
            "uid": "41ca85374b5e87717a8474c6add09292",
```

```
            "date": 1265916553000,
            "message": ":) kit for anonymous Web surfing
which helps to protect your [COLOR=\"Yellow\"]ASS[/COLOR]:
from cyber frens\r\n\r\n1) hide your real IP address\r\n2)send
anonymous love letters or Emails (just kidding)\r\n3) chat
with [COLOR=\"Yellow\"](ur%20ass%20hidden)[/COLOR] with ur
fren when is the next tea party held :p\r\n4)clear browser his-
tory and much more.\r\n5)and more and more etc etc\r\n6)dont
be F**king lazy check it urself\r\n\r\n:D Contents
:D\r\n\r\nSteganos Internet Anonym VPN 2008\r\nHide-Ip-Browser
v1.5\r\nAuto Hide IP v4.6.3.2\r\nEasy-Hide-IP v2.1\r\nHide IP
NG v1.53\r\nReal Hide IP v3.5.4.2\r\nIP Address Shield
9.21\r\nProxy Switcher 4.2.0.5101\r\nMax AnonySurf 1.9\r\nMask
Surf Pro v2.3\r\nInvisible Browsing v7.0 2009\r\nSun River Sys-
tems Heatseek Gold v1.4.1.8\r\nHistory Sweeper v3.04\r\nHis-
tory Killer Pro 4.1.1\r\nWinMend History Cleaner 1.3.2\r\nAuto
Clear History v2.1.2.6\r\nAuto Clear Cookies
v2.1.2.6\r\n\r\n\r\nDOWNLOAD:\r\n\r\n[QUOTE][url]ht-
tp://rapidshare.com/files/349243995/Anonymous_Surfing_Kit_
2010_by_Robinhood.rar.html[/url][/QUOTE]\r\n[QUOTE]\r\n[url]ht-
tp://www.filefactory.com/file/b00eh7d/n/Anonymous_Surfing_Kit_
2010_by_Robinhood.rar[/url][/QUOTE] \r\n\r\n[QUOTE][url]ht-
tp://hotfile.com/dl/28162874/e2ecae0/Anonymous_Surfing_Kit_
2010_by_Robinhood.rar.html[/url][/QUOTE]\r\n\r\n[QUOTE][url]ht-
tp://rapidshare.de/files/49138439/Anonymous_Surfing_Kit_2010_
by_Robinhood.rar.html[/url]\r\n[/QUOTE]\r\n\r\nps: check it
with ur anti virus , i have checked it showed me clean \r\n-
again the false alarm is for patch but still check it again
\r\ngr8 stuff if u like it leave a comment",
```

```
            "links": {
                "authorActor": {
                    "uid":
"237c5e85787983f58c13ec1591e6d489",
                    "handle": "axelevents"
                },
                "forum": {
                    "uid":
"96a3be3cf272e017046d1b2674a52bd3",
                    "name": "carder.pro",
                    "description": "carder.pro is a forum
focused on carding (credit card fraud)."
                },
                "thread": {
                    "uid":
"41ca85374b5e87717a8474c6add09292",
                    "topic": "Anonymous Surfing Kit 2010",
                    "count": 233
                }
            },
            "lastUpdated": 1497370111457
        }
    }
  ],
  "watcherGroups": [
    {
        "name": "testG",
        "type": "owned_by_me",
        "owner": "testApiInt",
```

```
            "uid": "f5db9f26-f0c6-408d-8dac-542e8c036aa2",
            "watchers": [
                {
                    "uid": "aa957845d56c4773f379843afc507ea9",
                    "description": "virus",
                    "type": "search",
                    "patterns": [
                        {
                            "types": [
                                "FreeText"
                            ],
                            "pattern": "virus"
                        }
                    ]
                }
            ]
        }
    ]
}
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.alerts[].foundTime	event.title	Alert	Intel 471 Alert 1497446972076	Event title generated from the following template: Intel 471 Alert {{foundTime}}
.alerts[].uid	event.attribute	UID	59413a3c441d6663bf8795bb	
.alerts[].foundTime	event.happened_at	N/A	1497446972076	
.alerts[].status	event.attribute	Status	active	
.watcherGroups[].name	event.attribute	Watcher Group Name	testG	
.watcherGroups[].uid	event.attribute	Watcher Group Link	https://titan.intel471.com/watchers/groups/f5db9f26-f0c6-408d-8dac-542e8c036aa2	https://titan.intel471.com/watchers/groups/{{value.uid}}
.alerts[].privateMessage.subject	indicator.value	Email Subject	Important message from the forum administration!	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.alerts[].privateMessage.uid	indicator.attribute	UID	6613f939099a5db1b7b627478c74f6e9	
.alerts[].privateMessage.date	indicator.attribute	Date	1265707719000	
.alerts[].privateMessage.message	indicator.attribute	Message	Dear, Волна!\r\n\r\nA virus alert was noticed on your computer	
.alerts[].privateMessage.links[].forum.uid	event.attribute	Forum Link	https://titan.intel471.com/forums/37fb05bc65bf-6a1435e06a98e4266bc7/topics	https://titan.intel471.com/forums/{{value.privateMessage.links.forum.uid}}/topics
.alerts[].privateMessage.links[].forum.name	event.attribute	Forum Name	carder.pro	
.alerts[].privateMessage.links[].forum.description	event.attribute	Forum Description	carder.pro is a forum focused on carding (credit card fraud).	
.alerts[].privateMessage.authorActor.handle	adversary.name	N/A	BestForumTeam	
.alerts[].privateMessage.authorActor.uid	adversary.attribute	UID	5328c3099dbc67b62cf7ee620ffee4c2	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.alerts[].privateMessage.recipientActor.handle	adversary.name	N/A	Волна	
.alerts[].privateMessage.recipientActor.uid	adversary.attribute	UID	37fb05bc65bf6a1435e06a98e4266bc7	
.alerts[].post.uid	event.attribute	Post UID	6613f939099a5db1b7b627478c74f6e9	
.alerts[].post.date	event.attribute	Post Date	1265707719000	
.alerts[].post.message	event.attribute	Message	Dear, Волна!\r\n\r\nA virus alert was noticed on your computer	
.alerts[].post.links[].forum.uid	event.attribute	Forum Link	https://titan.intel471.com/forums/37fb05bc65bf6a1435e06a98e4266bc7/topics	https://titan.intel471.com/forums/{{value.post.links.forum.uid}}/topics
.alerts[].post.links[].forum.name	event.attribute	Forum Name	carder.pro	
.alerts[].post.links[].forum.description	event.attribute	Forum Description	carder.pro is a forum focused on carding (credit card fraud).	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.alerts[].post.links[].thread.uid	event.attribute	Thread UID	41ca85374b5e87717a8474c6add09292	
.alerts[].post.links[].thread.topic	event.attribute	Thread Topic	Anonymous Surfing Kit 2010	
.alerts[].post.links[].thread.count	event.attribute	Thread Count	233	
.alerts[].post.authorActor.handle	adversary.name	N/A	BestForumTeam	
.alerts[].post.authorActor.uid	adversary.at-tribute	UID	5328c3099dbc67b62cf7ee620ffee4c2	