

Resilient Integration with Twitter Search API

This package contains one function which targets the Twitter Search API. Takes in an input of multiple possible hashtags and a number of Tweets to be returned and contacts the Twitter Search API to return the results. Requires Twitter Access Key and Secret to obtain a OAuth2 read-only token.

Customization Settings

Layouts Rules Scripts **Workflows** Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

Workflows / Example Twitter: Popular Tweets For Tag(s) Cancel Save & Close Save

Name * Example Twitter: Popular Tweets For Tag(s)

API Name * twitter_most_popular_tweets_for_tag

Description An example workflow which is used to retrieve a number of popular tweets for 1 or more provided tags. Default amount returned is 15 however this is customisable using a input

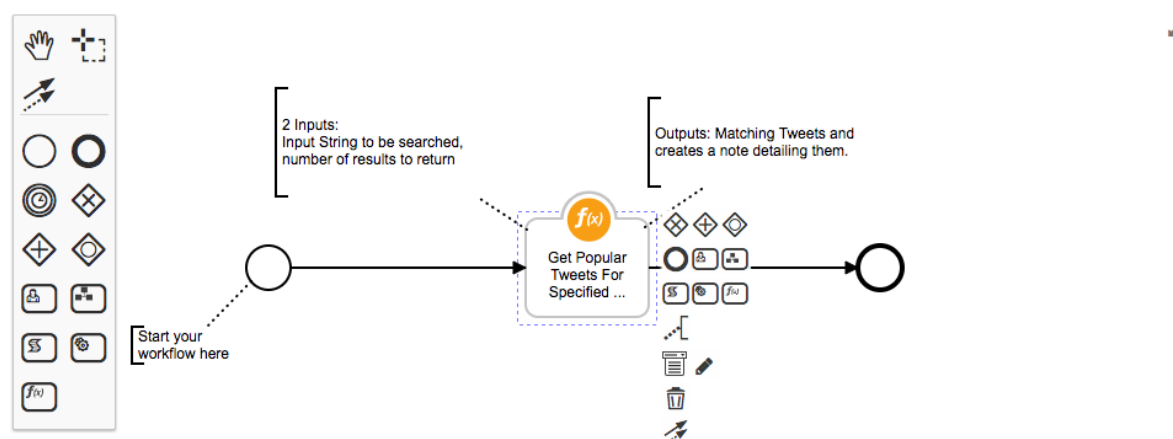
Object Type * Incident

Creator Resilient Sysadmin

Last Modified 31/10/2018 11:25

Last Modified By Resilient Sysadmin

Associated Rules Get Popular Tweets For Specified T



Input Pre-Process Script Output Post-Process Script

Input Parameter	Value
twitter_search_tweet_string * ?	{ "hashtags":["Magecart", "Wannacry", "Spectre", "XFTAS", "Emotet"] }
twitter_search_tweet_count ?	5

app.config settings:

```
twitter_api_key = <API_KEY>
twitter_api_secret = <API_SECRET>
```

Function Inputs:

Function Name	Type	Required	Example
twitter_search_tweet_string	String Representation of JSON	Yes	'{"hashtags": ["Malware", "Ransomware", "Phishing"]}'
twitter_search_tweet_count	Number	Yes	10

Function Output:

```
results = {
  success = True,
  inputs :{
    twitter_search_tweet_string: '{"hashtags": [ "Malware", "Ransomware",
"Phishing"]}',
    twitter_search_tweet_count: 10
  }
  tweets: {
    statuses: [{
      text: "Hello World",
      id_str: "123",
      entities: {
        urls:[{
          url : "https://twitter.com/i/web/status/123"
        }]
      },
      ...OtherAttributes
    ]
  }
}
```

Review the [Twitter API documentation](#) for more info on all the attributes returned.

The [Twython documentation](#) has details specific to the Twython package used by this integration

Pre-Process Script:

Rather than manipulating potential inputs in the Pre-Processing script, this integration uses inputs taken from the Inputs tab. See screenshot for example.

Post-Process Script:

This example **adds a Note to the Incident.**

```
#Prepare the start of the note text
noteText = u""""<br>Twitter search:
            Successful : {0}
            <b>Searched Tags:<b>{1}</b>"""".format("True" if
results["success"] is True else False, results["inputs"]
["twitter_search_tweet_string"])

if (results.success):
    # For each returned tweet add the text and URL of the tweet to the
noteText
    for tweet in results.tweets["statuses"]:
        noteText += u""""<br><br>Tweet Text: <br><b>{0}</b>
        <b>Tweet URL</b> :<a>{1}</a>"""".format(tweet["text"],tweet["entities"]
["urls"][0]["url"])
    else:
        noteText += u""""<b>No Results found</b>""""
# Now add the note to our incident
incident.addNote(helper.createRichText(noteText))
```

Rules

Rule Name	Object Type	Workflow Triggered
Get Popular Tweets For Specified Tag(s)	Incident	Example Twitter: Popular Tweets For Tag(s)