

ThreatQuotient



Kaspersky Threat Intelligence Portal Operation Guide

Version 1.1.3

January 31, 2022

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

Support	4
Versioning.....	5
Introduction	6
Installation.....	7
Configuration	8
Actions	9
Lookup Malware.....	10
Lookup IP Address	12
Lookup URL.....	21
Lookup FQDN	24
Change Log.....	27

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.

Copyright © 2022 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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: 1.1.3
- Compatible with ThreatQ versions $\geq$ 4.40.0

Introduction

The Kaspersky Threat Intelligence Portal operation provides data enrichment of indicators via the Kaspersky Threat Intelligence Portal.

The operation provides the following actions:

- **Lookup Malware** - lookup a malware indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.
- **Lookup IP Address** - lookup an IP Address indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.
- **Lookup URL** - lookup a URL indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.
- **Lookup FQDN** - lookup a FQDN indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.

See the [Actions](#) chapter for further details on these actions.

The operation is compatible with the following indicator sub-types:

- IP Address
- MD5
- SHA-1
- SHA-256
- URL

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 operation 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 operation and will require user confirmation before proceeding.

6. You will still need to [configure and then enable the operation](#).

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* 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:

PARAMETER	DESCRIPTION
Portal Username	Your Kaspersky Threat Intelligence Portal username.
Portal Password	Your Kaspersky Threat Intelligence Portal password.
Portal Certificate Location	The location of your Portal certificate.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

The Kaspersky Threat Intelligence Portal operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Lookup Malware	Get Malware Information and Related Indicators	Indicator	MD5, SHA-1, SHA-256
Lookup IP Address	Get IP Reputation, Whois, and Related Indicators	Indicator	IP Address
Lookup URL	Get URL Reputation, Whois, and Related Indicators	Indicator	URL
Lookup FQDN	Get FQDN Reputation, Whois, and Related Indicators	Indicator	URL

Lookup Malware

The Lookup Malware action will lookup a malware indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.

POST <https://tip.kaspersky.com/api/hash/<Indicator Value>>

See below a sample response for an MD5.

```
{
  'LicenseInfo': {
    'DayRequests': 2,
    'ZoneDayRequests': 0,
    'AccessType': 'Commercial',
    'DayQuota': 1000,
    'ZoneDayQuota': 10000
  },
  'FileGeneralInfo': {
    'Type': 'unix shell',
    'Sha256': 'D7E30E17C271BE6E32C4492C65432D96ADDDE5DE51B5A2F296F6BB0C9B8E73D1',
    'RelatedAptReports': [],
    'Signer': None,
    'Sha1': '160C5434DED6D24E5806810887FD4CD48AC3AF3A',
    'HasApt': False,
    'HitsCount': 10,
    'Packer': None,
    'Size': 86735,
    'Md5': '00EC67EE8BE7710997D332721F02B288',
    'LastSeen': '2021-12-20T21:17Z',
    'FirstSeen': '2021-12-20T18:44Z'
  },
  'RelatedObjects': {
    'HasRedZone': True
  },
  'Zone': 'Red',
  'DetectionsInfo': [
    {
      'DetectionMethod': 'HEUR',
      'DescriptionUrl': 'https://threats.kaspersky.com/en/threat/HackTool.Python.Meterp',
      'DetectionName': 'HEUR:HackTool.Python.Meterp.b',
      'LastDetectDate': '2021-12-21T04:00Z',
      'Zone': 'Red'
    }
  ]
}
```

ThreatQ provides the following default mapping for this Action:

SOURCE	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
response.FileGeneralInfo.LastSeen	Attribute	Last Seen	2021-12-20T21:17Z
response.FileGeneralInfo.FirstSeen	Attribute	First Seen	2021-12-20T18:44Z
response.FileGeneralInfo.Type	Attribute	File Type	unix shell
response.FileGeneralInfo.HitsCount	Attribute	Hits Count	10
response.FileGeneralInfo.HasApt	Attribute	Related to APT	False
response.DetectionsInfo[.DescriptionUrl	Attribute	Detection Description URL	https://threats.kaspersky.com/en/threat/HackTool.Python.Meterp
response.Zone	Attribute	Zone	Red
response.DetectionsInfo[.DetectionMethod	Attribute	Detection Method	HEUR
response.DetectionsInfo[.DetectionName	Attribute	Detection Name	HEUR:HackTool.Python.Meterp.b
response.FileGeneralInfo.Sha1	Indicator	SHA-1	160C5434DED6D24E5806810887FD 4CD48AC3AF3A
response.FileGeneralInfo.Sha256	Indicator	SHA-256	D7E30E17C271BE6E32C4492C65432 D96ADDDE5DE51B5A2F296F6BB0C9B8E73D1

Lookup IP Address

The Lookup IP Address action will lookup an IP Address indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.

POST <https://tip.kaspersky.com/api/hash/<Indicator Value>>

See below a sample response for an IP Address.

```
{
  'LicenseInfo': {
    'AccessType': 'Commercial',
    'DayRequests': 2,
    'DayQuota': 1000,
    'ZoneDayQuota': 10000,
    'ZoneDayRequests': 0
  },
  'IpGeneralInfo': {
    'Ip': '35.158.226.16',
    'HasApt': False,
    'Status': 'known',
    'Categories': [],
    'FirstSeen': '2017-09-23T11:10Z',
    'HitsCount': 10,
    'CountryCode': 'DE',
    'ThreatScore': None,
    'RelatedAptReports': [],
    'CategoriesWithZone': []
  },
  'IpWhoIs': {
    'Type': 'IpWhoIs',
    'Contacts': [
      {
        'Phone': '+1-206-266-4064',
        'Address': None,
        'Name': 'Amazon EC2 Abuse',
        'Fax': None,
        'Email': 'abuse@amazonaws.com',
        'OrganizationId': None,
        'ContactType': 'organization',
        'ContactRole': 'abuse'
      },
      {
        'Phone': '+1-206-266-4064',
        'Address': None,
        'Name': 'Amazon AWS Network Operations',
        'Fax': None,
        'Email': 'amzn-noc-contact@amazon.com',
        'OrganizationId': None,
        'ContactType': 'organization',
        'ContactRole': 'noc'
      },
      {
        'Phone': None,
        'Address': ['410 Terry Ave N.'],
        'Name': 'Amazon Technologies Inc.'
      }
    ]
  }
}
```

```
'Fax': None,
'Email': None,
'OrganizationId': None,
'ContactType': 'organization',
'ContactRole': 'owner'
},
{
  'Phone': '+1-206-266-4064',
  'Address': None,
  'Name': 'Amazon EC2 Network Operations',
  'Fax': None,
  'Email': 'amzn-noc-contact@amazon.com',
  'OrganizationId': None,
  'ContactType': 'organization',
  'ContactRole': 'tech'
}
],
'Asn': None,
'Net': {
  'Created': '2016-08-09T00:00Z',
  'Changed': '2016-08-09T00:00Z',
  'Description': None,
  'Name': 'AT-88-Z',
  'RangeStart': '35.152.0.0',
  'RangeEnd': '35.183.255.255'
}
},
'HostedUrls': [
  {
    'FirstSeen': '2017-09-23T11:10Z',
    'IsUrlTruncated': False,
    'UrlHitsCount': 10,
    'LastSeen': '2017-09-23T11:10Z',
    'Zone': 'Grey',
    'Url': '35.158.226.16/qhyaec3yypc2jxfmiv9p7w_gbhbkdv1q1ctyjcz9j0csb-xpwkskwn1zzxeuxyht12hbs0m03pue-
tejkyyqq3y0wmfzp-uampvmisqc8cowyhzj3mlz1w2_nyuheehbriuaxx0dipwalo1hpcp92'
  },
  {
    'FirstSeen': '2017-09-23T11:10Z',
    'IsUrlTruncated': False,
    'UrlHitsCount': 10,
    'LastSeen': '2017-09-23T11:10Z',
    'Zone': 'Grey',
    'Url': '35.158.226.16/-
z10ysph09m3xeqorizgmaqkju9q1hoqwcdknihlexlgzdxh_p8wq7jrmbwufb7hf2aqmeax1h_d_kfgsjkz37k4qub_tj1w-mpgmc1ns-
cyymv5xsagn8q1xcaaq97vap71bmmyjq0p8ad1xjklrrhedjx1yjb4_vut01dwvjwg'
  },
  {
    'FirstSeen': '2017-09-23T11:10Z',
    'IsUrlTruncated': False,
    'UrlHitsCount': 10,
    'LastSeen': '2017-09-23T11:10Z',
    'Zone': 'Grey',
    'Url': '35.158.226.16/y-o_3j1fursia4e0hj9y3gcdyqgja1-rnrr73qcodw8feojyazbt7cbsxorhqggyexzzlgx9o21_khlpps2-
rvou5rhiyuwzn4yfuwedto0nv2-dwllqhy-761ofdarri8wutumljosc2y5ded76ydxzsn4im4wsg-7fq'
  },
  {
    'FirstSeen': '2017-09-23T11:10Z',
    'IsUrlTruncated': False,
    'UrlHitsCount': 10,
    'LastSeen': '2017-09-23T11:10Z',
    'Zone': 'Grey',
    'Url': '35.158.226.16/y-o_3j1fursia4e0hj9y3gcdyqgja1-rnrr73qcodw8feojyazbt7cbsxorhqggyexzzlgx9o21_khlpps2-
rvou5rhiyuwzn4yfuwedto0nv2-dwllqhy-761ofdarri8wutumljosc2y5ded76ydxzsn4im4wsg-7fq'
  }
]
```

```
'Zone': 'Grey',
'Url': '35.158.226.16/
kykcr1jb9ngwqpsepyushqszxvm5zz4yzpfkzblmqmhl1y0nxykmahb_jkaawtrwlxjlx8klw6ifqyadrg0nqqnfg8ldeeb0edqpm3c1aprooluzfdr
vmit-gfo1xjfb-04mebomwq9ismwixmhn'
},
{
'FirstSeen': '2017-09-23T11:10Z',
'IsUrlTruncated': False,
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url': '35.158.226.16/k1iyautrl9cfp1pp_99bsazjf4pbcxyenh_dqxk5yl0mabq-
v6ottp6zwd7usirbleladqh3fanlssj81rlp3pitd0oandjo_2sk6p3amb0_-sqcvjonavyoffk1l0d9jmxjyqshbbumoek8m-8cjlw'
},
{
'FirstSeen': '2017-09-23T11:10Z',
'IsUrlTruncated': False,
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url': '35.158.226.16/ezpllays7kwuo1mulxktigwatqto-
sruuxwnbcxembc9tuqi2k2ya93un73ulp_uwrocpxa_rfffdigiszmkwreanzdvyawc561acjlsu7moyy2ag-b0eg0-ysrfcsitq-
baqtaqoohtttgnqj4'
},
{
'FirstSeen': '2017-09-23T11:10Z',
'IsUrlTruncated': False,
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url': '35.158.226.16/wqcehi1t6gfk-5_4fj1zqwpeu9yuw5primm6udgysaq0l5bospw3pkbbboyibwflr3o1f-
rnqlbz9pnu8trvqcfsdaoxe1lrxffs_mmplorp9fcxitsxg3tz87nbi4x9wtttyevrzs1wxhpmrcfx9'
},
{
'FirstSeen': '2017-09-23T11:10Z',
'IsUrlTruncated': False,
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url': '35.158.226.16/2rrewucv3m5njwgl14uraa6mpsnhxigkuls1vbcxrfmkykq4paik9zgyibk7l1tr786agdam-
ufbevzmfwx7ny9rbczsjblf5gya2joeggf6xc2kbxr4sh-abb5ceyqw2w9likk75uzixhoxcx4m732yqek8snjzdzjnhw5d2m_faw'
},
{
'FirstSeen': '2017-09-23T11:10Z',
'IsUrlTruncated': False,
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url': '35.158.226.16/shgigflkuujjef5nvvmmreaqcthi1qkek2hd3mchsye7nt-vwa2n0tvn-8ac8eej-
ufe6wrng0gyssm_povvcapff7hy4jaeviyqkcuprotxikobfo5wo3uhqjvtdebg1wmr1rxng2itkxrwqtkxqk_'
},
{
'FirstSeen': '2017-09-23T11:10Z',
'IsUrlTruncated': False,
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url':
'35.158.226.16/1znfu4paihpfbnt2dbjbggzjwmepur7cpmgrbvsgt6wlp7k4vix1h57upq-1fusmy7somoa43tsqfncmopl0xdomwrsud8z08bwvx3
itent2almdq4zjn9uvyogoclyyvicwelcrgdkbxe6h-axoaat'
},
}
```

```
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/gfmfnuyeeajgzyaei-gaqd5z1zfztvjid0lbkkf-k-
mj65urhnf1fs4r29lxe6vjydwxy_kcuiyrzsr74ryqhrwxcbaqvjhgainecf6k5oyp4t4k_0zlo-
arpix235rwufxnttw_oigj5ly1ru8xiocdiyxx4uweakio2pt_tw'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/uankc_7b4m3lq_pc3wde3q8xaomnqambyhpl3o9z-
nhd8jnhzqrgridwqquramrivxcpg7xrwpeq4r6nr4_bdzs0qmeotv5o0sb3tiw5nhx0pmraik3aqqovxg8jifdoa9ited3uitu6xcfbfylzmlnm-
yf0fq0xf5dxhnc687a'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/nhfx63hgjrteh8zi8vugqdewgzketnwf-
zehuv9haibjuqh8lxdq9mdnipddsuebnu1movaibnx4ockbtkeinswsvyvtjgujrsqg7mcmxex11uzmswecdukqfsg6egeevmtejfe411iqwpm5he9gt'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/al9o5ys10feokurxkvs_warsdiyzjg29tiyqfzwi0ghkv1gurdqaeaxpatz8-
m3s3tnlgzm3v3ltdghhah8v4u2jznlicdzlmgmqdexp8i8voudcqav0uxbiv06lri3rnptvn0wfxax4i-pvgecspg'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/hts_nkh0j-
dqvdy4s82oeq6uh2__jwvcubgkwbl_vj285fqzyuiiqz6vh5y26mlad0kcywfh4g3rw17zoa0txyjcukalt1u62xb1oadiaqp8sdlf_0bawom-
ccti3cvvkaofcoiec0gi1-ietqkpb'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/yggn8hwc6qcne8n54v00iaupg8l-
vl7hqbilmjgeqqimp7yb6acoauzwsdnjgatybviv1b6icrsvdorat3fhiqnb995ebau9np5k6vns1knjtbnl1fhtorwdeskscedskgkbeuantj7xe5
7fyi3slg28gmwpn92ecdcpufhuq'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
```

```
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url': '35.158.226.16/
mu7lswxe9zaahaiawhmwgq9ipgnubdiktyvklk0r_iiovp9acrmvlbykrpgqthtvlqgzjh-772femdkwnlfvssfm6otl14fwq2g4s3vdy1heeknbsher
vsdcvln6-zojd4-wpfeaaajsdwjs2ktwq'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/
ovaqyg03cl_3yvmqbvoy5gs4m0kfo8mjpk8gakuouhvob1wm4hptci94oc9l_xj5i9gxmwbcbp5shtdd5ytpferepj1vxz98oieqhafn6o6z1njfhp2ph
pesc3lw_xemw_5mtkeimzmlfpcynbsbah'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/vycauj-m2zn3g0bxufe3ua0yxosupgtgpuzhlckximlci07ckwxnt_m44ypw7vu1yxfb4d1jdr3rfj-
hph6z8raqcu8pxvydoc75njggu0nv_hqrn43gj0c9b-yzpbmddxbjnf1bohzhsg1jhjivgcyawd0rзраokmuzx2tnn-a'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/r4n-psya-azfrghcb9s3kqv5lq6lp5ofun7fwd00gw8unwswqk9w4to3h-1i_0caoehuat-sxq8lgpudjnk-
mlsjxgludec3octizw1w2owqzfaitqheiw49huu3ipr46c064aeseioy_zvfsqayugzrmtboedelffirtsv_pjw'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/
mcm1ws7b3nbaanbiyoqnral9k31bsfhxn77sy96vxfjh_qhespqahq5dniq5xlufev6an4svtyp5zkhy3bv01gzjqozym18ncvpmvut0aht7omo9dji_
wp_p_qcjoyoluu2qaepiu5ge5fhwfmjsyt'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
  'Url': '35.158.226.16/
pttghtaixesmc5rmdc59wffebaiuc8esicnajt-7wij-2eio6scwrn8infh8hk4mkev8t3fdsbbezy7jx_kffq4zwnvrqekpzvcymgf5s8osc1ynrr2k
vvcjnadar12uw0fnre20-zqtdwxh7z9uk'
},
{
  'FirstSeen': '2017-09-23T11:10Z',
  'IsUrlTruncated': False,
  'UrlHitsCount': 10,
  'LastSeen': '2017-09-23T11:10Z',
  'Zone': 'Grey',
```

Kaspersky Threat Intelligence Portal Operation
Version 1.1.3

```
'FirstSeen': '2017-09-23T11:10Z',
'IsUrlTruncated': False,
'UrlHitsCount': 10,
'LastSeen': '2017-09-23T11:10Z',
'Zone': 'Grey',
'Url': '35.158.226.16/tmm5q1jiecjuub1pnftqkbzm_fe3k6obg7i3a7e-uzolje63rrxlxxi6jmlsdunsdmtqzifakbyf00mixbjjoix_o4fgs1dwe9idcarj-5proysjddb2lozl4taimbqeyzk6-jllxnftl2a83g'
},
],
'RelatedObjects': {
'HasRedZone': False
},
'IpDnsResolutions': [
{
'PeakDate': '2021-01-08T00:00Z',
'FirstSeen': '2020-08-20T12:59Z',
'HitsCount': 10,
'Categories': [],
'DailyPeak': 10,
'Zone': 'Grey',
'Domain': 'rijkzijn.nl',
'LastSeen': '2021-01-11T06:30Z'
},
{
'PeakDate': '2018-01-31T00:00Z',
'FirstSeen': '2018-01-31T18:38Z',
'HitsCount': 10,
'Categories': [],
'DailyPeak': 10,
'Zone': 'Grey',
'Domain': 'd.surprize.wtf',
'LastSeen': '2018-01-31T20:26Z'
},
{
'PeakDate': '2018-01-31T00:00Z',
'FirstSeen': '2018-01-31T18:38Z',
'HitsCount': 10,
'Categories': [
{
'Zone': 'Grey',
'Name': 'CATEGORY_FILE_SHARING'
},
{
'Zone': 'Grey',
'Name': 'CATEGORY_INFORMATION_TECHNOLOGIES'
},
{
'Zone': 'Grey',
'Name': 'CATEGORY_INTERNET_SERVICES'
},
{
'Zone': 'Grey',
'Name': 'CATEGORY_SEARCH_ENGINES_AND_SERVICES'
},
{
'Zone': 'Grey',
'Name': 'CATEGORY_SOFTWARE_AUDIO_VIDEO'
}
],
'DailyPeak': 10,
'Zone': 'Green',
```

```
'Domain': 'd.aws-proxy.disk.yandex.ua',
'LastSeen': '2018-01-31T20:26Z'
},
],
'FilesDownloadedFromIp': [
{
'DownloadHitsCount': 10,
'Md5': '9EC0A28A6A9FDA4AD56EA6C3143F731D',
'FirstSeen': '2017-09-23T11:10Z',
'DetectionName': 'not-a-virus:AdWare.Win32.FileTour.cias',
'Url': '35.158.226.16/5gwuilaweo0kk6fu-
rsrqgqocbemnpw2mb1jqexilxy1b7sgehap1rikvzf95s3usmkmahc1lcqtdek1_kbx7avsnx_rpswdz0hrq9nbvexojevznzixmeprh1a3xxh57mdyh
s88zritwm8iqese1xrasrh_ukovj-tfd4tjpg',
'Zone': 'Yellow',
'LastSeen': '2017-09-23T11:10Z'
},
{
'DownloadHitsCount': 100000000,
'Md5': 'FB44E569E95C0B9B5257F2A72793B387',
'FirstSeen': '2017-09-23T11:11Z',
'DetectionName': None,
'Url': '35.158.226.16/3hccxqo7y_keugkbvladbwizmnmygwknkwlchlratol0ccqylxsyrduku-
_h5utedkowx2pr0emon1ujvbtntksab_i987zkw-nv81gz-nswghgkfhx0__vjbkhrqs1p301qrl2t2hag1iojvb41j',
'Zone': 'Green',
'LastSeen': '2017-09-23T11:11Z'
},
{
'DownloadHitsCount': 100000000,
'Md5': '0C7B305BD8A070CFC22240C472DEB2EC',
'FirstSeen': '2017-09-23T11:11Z',
'DetectionName': None,
'Url': '35.158.226.16/
ovaqyg03cl_3yvmqbvoy5gs4m0kfo8mjpg8gakuouhvob1wm4hptci94oc9l_xj5i9gxmwbhpb5shtdd5ytpferepj1vxz98oieqhafn6o6z1njfhp2ph
pesc3lw_xemw_5mtkeimzmlfpcynbsbah',
'Zone': 'Green',
'LastSeen': '2017-09-23T11:11Z'
},
{
'DownloadHitsCount': 100000000,
'Md5': '3BB184B7A39FA79910FD1BA149FBB943',
'FirstSeen': '2017-09-23T11:11Z',
'DetectionName': None,
'Url': '35.158.226.16/
pttghtaixesmc5rmdc59wffebaiuc8esicnaj-7wij-2eio6scwrn8infh8hk4mkev8t3fdsbbezy7jx_kffq4zwwnrqekpzvcymgf5s8osc1ynrr2k
vvcjnadar12uw0fnre20-zqtdwxh7z9uk',
'Zone': 'Green',
'LastSeen': '2017-09-23T11:11Z'
},
{
'DownloadHitsCount': 100000000,
'Md5': '57235107A9362E763E7CD605EB8CCA55',
'FirstSeen': '2017-09-23T11:11Z',
'DetectionName': None,
'Url': '35.158.226.16/e5gvuepmq0cvn0umduhqnqbnrqj3aqolrxi_wqzaoprzww4hob_ie1123mcbsobjldihrzp3-
jc2pbiuct4jzxigbeso-2edlgqeycrnh3qfcmy_qp5ul6g3v2d0-w9synww9etcsloasbrgnv93y',
'Zone': 'Green',
'LastSeen': '2017-09-23T11:11Z'
},
{
'DownloadHitsCount': 100000000,
'Md5': '673741221B590900905D41B3265338BC',
```

```
{
  'FirstSeen': '2017-09-23T11:11Z',
  'DetectionName': None,
  'Url': '35.158.226.16/14dtxe-ejmeykizcs3lgpw2fmzgvd0mowyrhuyq8duyve-
xc2abyww2owfb0es2gj7bpxbjp49nn5te_bnbkdaet1lspzickkv1otfrubthodsx-lwjdnnaav15c70j89wim2tby9ar-sgfkdgdaq',
  'Zone': 'Green',
  'LastSeen': '2017-09-23T11:11Z'
}
],
'Zone': 'Grey'
}
```

ThreatQ provides the following default mapping for this Action:

SOURCE	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
response.IpGeneralInfo.FirstSeen	Attribute	First Seen	2017-09-23T11:10Z
response.IpWhoIs.Net.RangeStart	Attribute	Network Range Start	35.152.0.0
response.IpWhoIs.Net.RangeEnd	Attribute	Network Range End	35.183.255.255
response.IpWhoIs.Net.Created	Attribute	Network Created Date	2016-08-09T00:00Z
response.IpWhoIs.Net.Changed	Attribute	Network Changed Date	2016-08-09T00:00Z
response.HostedUrls[]	Indicator	URL	http://35.158.226.16/e5gvue pmq0cvn0umdzuqnqsbnrqj3 aqolrxi_wqzaoprzww4hob_ie1 123mcbsobjldihrzp3-jc2pbiuct 4jzxigbeso-2edlgqeycrnh3qfcm y_qp5ul6g3v2d0-w9synww9etc sloasbrgnv93y/
response.IpDnsResolutions[]	Indicator	FQDN	rijkzijn.nl
response.FilesDownloadedFromIp[]	Indicator	MD5	673741221B590900905D41B3265338BC

Lookup URL

The Lookup URL action will lookup a URL indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.

POST <https://tip.kaspersky.com/api/hash/<Indicator Value>>

See below a sample response for an IP Address.

```
{
  'UrlDomainWhoIs': {
    'DomainName': 'dcttl.com',
    'Created': '2021-11-30T00:00Z',
    'NameServers': [
      'dns1.registrar-servers.com',
      'dns2.registrar-servers.com'
    ],
    'RegistrationOrganization': 'Privacy service provided by Withheld for Privacy ehf',
    'Contacts': [
      {
        'CountryCode': 'ICELAND',
        'Name': 'Redacted for Privacy',
        'Organization': 'Privacy service provided by Withheld for Privacy ehf',
        'ContactType': 'registrant',
        'State': 'Capital Region',
        'Phone': None,
        'Fax': None,
        'City': None,
        'Email': None,
        'Address': None,
        'PostalCode': None
      },
      {
        'CountryCode': 'ICELAND',
        'Name': 'Redacted for Privacy',
        'Organization': 'Privacy service provided by Withheld for Privacy ehf',
        'ContactType': 'administrative',
        'State': 'Capital Region',
        'Phone': None,
        'Fax': None,
        'City': None,
        'Email': None,
        'Address': None,
        'PostalCode': None
      },
      {
        'CountryCode': 'ICELAND',
        'Name': 'Redacted for Privacy',
        'Organization': 'Privacy service provided by Withheld for Privacy ehf',
        'ContactType': 'technical',
        'State': 'Capital Region',
        'Phone': None,
        'Fax': None,
        'City': None,
        'Email': None,
        'Address': None,
        'PostalCode': None
      }
    ]
  }
}
```

```
    'PostalCode': None
  }
],
'Expires': '2022-11-30T00:00Z',
'DomainStatus': ['clientTransferProhibited'],
'Updated': '2021-11-30T00:00Z',
'Registrar': {
  'Info': 'NameCheap, Inc.',
  'IanaId': '1068',
  'Email': None
}
},
'RelatedObjects': {
  'HasRedZone': True
},
'LicenseInfo': {
  'DayQuota': 1000,
  'AccessType': 'Commercial',
  'ZoneDayRequests': 0,
  'ZoneDayQuota': 10000,
  'DayRequests': 3
},
'Zone': 'Grey',
'DomainDnsResolutions': [
  {
    'Ip': '190.123.45.227',
    'LastSeen': '2021-12-08T14:55Z',
    'Status': 'known',
    'ThreatScore': 100,
    'FirstSeen': '2021-12-01T18:07Z',
    'Zone': 'Red',
    'DailyPeak': 10,
    'PeakDate': '2021-12-04T00:00Z',
    'HitsCount': 10,
    'CountryCode': 'PA'
  }
],
'UrlGeneralInfo': {
  'Ipv4Count': 1,
  'Categories': [],
  'Url': 'dcttl.com/change',
  'CategoriesWithZone': [],
  'RelatedAptReports': None,
  'Host': 'dcttl.com',
  'HasApt': False,
  'FilesCount': 0
}
}
```

ThreatQ provides the following default mapping for this Action:

SOURCE	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
response.UrlGeneralInfo.FilesCount	Attribute	Malicious File Count	0
response.UrlGeneralInfo.Ipv4Count	Attribute	Number of IPs	1
response.UrlGeneralInfo.HasApt	Attribute	Related to APT	False
response.UrlDomainWhois.Updated	Attribute	Whois Updated Date	2021-11-30T00:00Z
response.UrlDomainWhois.Expires	Attribute	Whois Expires Date	2022-11-30T00:00Z
response.UrlDomainWhois.Created	Attribute	Whois Created Date	2021-11-30T00:00Z
response.UrlDomainWhois.NameServers[]	Attribute	Domain Name Server	dns1.registrar-servers.com
response.DomainDnsResolutions[]	Indicator	IP Address	190.123.45.227

Lookup FQDN

The Lookup FQDN action will lookup a FQDN indicator in the Kaspersky Threat Labs Database and format the output accordingly for customers.

POST <https://tip.kaspersky.com/api/hash/<Indicator Value>>

See below a sample response for an IP Address.

```
{
  'RelatedObjects': {
    'HasRedZone': True
  },
  'Zone': 'Red',
  'DomainWhoIsInfo': {
    'Contacts': [
      {
        'ContactType': 'registrant',
        'Organization': 'See PrivacyGuardian.org',
        'CountryCode': 'UNITED STATES',
        'PostalCode': 'REDACTED FOR PRIVACY',
        'Phone': None,
        'Address': ['REDACTED FOR PRIVACY'],
        'City': 'REDACTED FOR PRIVACY',
        'Fax': None,
        'Name': 'REDACTED FOR PRIVACY',
        'Email': None,
        'State': 'AZ'
      },
      {
        'ContactType': 'administrative',
        'Organization': 'REDACTED FOR PRIVACY',
        'CountryCode': 'REDACTED FOR PRIVACY',
        'PostalCode': 'REDACTED FOR PRIVACY',
        'Phone': None,
        'Address': ['REDACTED FOR PRIVACY'],
        'City': 'REDACTED FOR PRIVACY',
        'Fax': None,
        'Name': 'REDACTED FOR PRIVACY',
        'Email': None,
        'State': 'REDACTED FOR PRIVACY'
      },
      {
        'ContactType': 'technical',
        'Organization': 'REDACTED FOR PRIVACY',
        'CountryCode': 'REDACTED FOR PRIVACY',
        'PostalCode': 'REDACTED FOR PRIVACY',
        'Phone': None,
        'Address': ['REDACTED FOR PRIVACY'],
        'City': 'REDACTED FOR PRIVACY',
        'Fax': None,
        'Name': 'REDACTED FOR PRIVACY',
        'Email': None,
        'State': 'REDACTED FOR PRIVACY'
      }
    ]
  },
}
```

```
'Expires': '2022-08-19T00:00Z',
'Updated': '2021-08-24T00:00Z',
'DomainName': 'jobcomesterd17.buzz',
'Registrar': {
  'Info': 'NameSilo, LLC',
  'Email': None,
  'IanaId': '1479'
},
'Created': '2021-08-19T00:00Z',
'NameServers': [
  'desi.ns.cloudflare.com',
  'zahir.ns.cloudflare.com'
],
'RegistrationOrganization': 'See PrivacyGuardian.org',
'DomainStatus': ['clientTransferProhibited']
},
'FeedMasks': [
  {
    'Zone': 'Red',
    'NormalizedMask': 'jobcomesterd17.buzz',
    'MaskType': 'MASK_TYPE_DOMAIN2_OBJECTS',
    'FeedNames': [
      'Botnet_CnC_URL_Data_Feed',
      'Malicious_URL_Data_Feed'
    ]
  }
],
'DomainGeneralInfo': {
  'Ipv4Count': 2,
  'UrlsCount': 10,
  'Categories': [
    'CATEGORY_BOTNET_CNC',
    'CATEGORY_MALWARE'
  ],
  'Domain': 'jobcomesterd17.buzz',
  'FilesCount': 0,
  'RelatedAptReports': [],
  'HitsCount': 10,
  'CategoriesWithZone': [
    {
      'Name': 'CATEGORY_BOTNET_CNC',
      'Zone': 'Red'
    },
    {
      'Name': 'CATEGORY_MALWARE',
      'Zone': 'Red'
    }
  ],
  'HasApt': False
},
'LicenseInfo': {
  'DayRequests': 4,
  'ZoneDayQuota': 10000,
  'DayQuota': 1000,
  'AccessType': 'Commercial',
  'ZoneDayRequests': 0
},
'DomainDnsResolutions': [
  {
    'FirstSeen': '2021-08-20T07:26Z',
    'Zone': 'Green',
```

```
{
  'CountryCode': 'US',
  'Ip': '172.67.166.65',
  'DailyPeak': 10,
  'PeakDate': '2021-08-21T00:00Z',
  'ThreatScore': 0,
  'Status': 'known',
  'LastSeen': '2021-12-20T13:08Z',
  'HitsCount': 10
},
{
  'FirstSeen': '2021-08-20T07:26Z',
  'Zone': 'Green',
  'CountryCode': 'US',
  'Ip': '104.21.75.12',
  'DailyPeak': 10,
  'PeakDate': '2021-08-21T00:00Z',
  'ThreatScore': 0,
  'Status': 'known',
  'LastSeen': '2021-12-20T13:07Z',
  'HitsCount': 10
}
]
```

ThreatQ provides the following default mapping for this Action:

SOURCE	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
response.DomainWhoIsInfo.Updated	Attribute	Whois Updated Date	2021-08-24T00:00Z
response.DomainWhoIsInfo.Expires	Attribute	Whois Expires Date	2022-08-19T00:00Z
response.DomainWhoIsInfo.Created	Attribute	Whois Created Date	2021-08-19T00:00Z
response.DomainWhoIsInfo.NameServers[]	Attribute	Domain Name Server	desi.ns.cloudflare.com
response.DomainDnsResolutions[]	Indicator	IP Address	104.21.75.12

Change Log

- **Version 1.1.3**
 - Added support for proxy use in ThreatQ. The proxy details are located under the Proxy tab of the System Configuration page on the ThreatQ Platform (System Settings > System Configurations).
- **Version 1.1.2**
 - Updated the integration logo.
 - Fixed a json mimetype error.
- **Version 1.0.0**
 - Initial Release