ThreatQuotient

A Securonix Company

Kaspersky Threat Intelligence Portal Action Bundle

Version 1.0.0

June 28, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: tq-support@securonix.com
Support Web: https://ts.securonix.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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Kaspersky Threat Intelligence Portal Action Bundle enables ThreatQ users to enrich supported indicators with reputation, classification, and contextual intelligence from the Kaspersky OpenTIP platform. The actions provide on-demand lookups for file hashes, IP addresses, URLs, and domains, returning threat context such as reputation, malware detection details, network ownership, categories, WHOIS information, and related metadata to support threat analysis, investigation, and triage.

The integration provides the following actions:

- **Kaspersky – Lookup Malware** - queries Kaspersky OpenTIP using a submitted file hash and returns file reputation, malware classification, contextual intelligence, optional detection details, and synonymous file hashes when available.
- **Kaspersky - Lookup IP Address** - queries Kaspersky OpenTIP using a submitted IP address and returns reputation, threat classification, Autonomous System Number (ASN), and network ownership information to provide additional context for analysis and investigation.
- **Kaspersky - Lookup URL** - queries Kaspersky OpenTIP using a submitted URL and returns reputation, threat categories, and WHOIS information for the associated hosting domain, providing additional context for threat analysis and investigation.
- **Kaspersky - Lookup FQDN** - queries Kaspersky OpenTIP using a submitted fully qualified domain name (FQDN) and returns reputation, threat categories, and WHOIS registration information to provide additional context for threat analysis and investigation.

The integration is compatible with the following indicator types:

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

The integration enriches indicators and indicator attributes.

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A Kaspersky OpenTIP API Token.
- A data collection containing at least one of the following indicator types:
  - IP Address
  - URL
  - FQDN
  - MD5
  - SHA-1
  - SHA-256

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine
6. Select the actions to install, when prompted, and click on **Install**.

   > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

The action(s) will now be installed on your instance. You will still need to configure the action(s).

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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

Lookup Malware Parameters

PARAMETER	DESCRIPTION
API Token	Enter your Kaspersky OpenTIP API token
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Attribute Filter	Select the pieces of file context to ingest into ThreatQ from Kaspersky OpenTIP. Options include: ◦ Zone *(Default)* ◦ File Status *(Default)*

PARAMETER	DESCRIPTION
	◦ First Seen *(Default)* ◦ Last Seen *(Default)* ◦ File Size *(Default)* ◦ File Type *(Default)* ◦ Hits Count *(Default)* ◦ Signer
Detection Info	Enable this parameter to have detection details from `DetectionsInfo` rendered in the indicator description as an HTML table when available. This parameter is enabled by default.
Related Hashes to Ingest	Select which synonymous hashes to ingest back into ThreatQ. Options include: ◦ SHA-1 *(Default)* ◦ SHA-256 *(Default)* ◦ MD5
Related Hash Status	Select the status applied to synonymous hashes returned by the malware lookup. Options include: ◦ Indirect *(Default)* ◦ Active ◦ Review ◦ Whitelisted
Objects Per Run	Enter the max number of objects to process per run. The default value is `10000`.

Lookup IP Address Parameters

PARAMETER	DESCRIPTION

PARAMETER	DESCRIPTION
API Token	Enter your Kaspersky OpenTIP API token
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Attribute Filter	Select the pieces of context to ingest into ThreatQ from Kaspersky OpenTIP. Options include: ◦ Zone *(Default)* ◦ Status *(Default)* ◦ Country Code *(Default)* ◦ Hits Count *(Default)* ◦ First Seen *(Default)* ◦ Category *(Default)* ◦ Category Name *(Default)* ◦ Category Zone *(Default)* ◦ ASN Number *(Default)* ◦ ASN Description *(Default)* ◦ Network Range Start *(Default)* ◦ Network Range End *(Default)* ◦ Network Created Date ◦ Network Changed Date ◦ Network Name *(Default)* ◦ Network Description
Objects Per Run	Enter the max number of objects to process per run. The default value is `10000`.

Lookup URL Parameters

PARAMETER	DESCRIPTION
API Token	Enter your Kaspersky OpenTIP API token
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Attribute Filter	Select the pieces of context to ingest into ThreatQ from Kaspersky OpenTIP. Options include: ◦ Zone *(Default)* ◦ Host *(Default)* ◦ Number of IPs *(Default)* ◦ Malicious File Count *(Default)* ◦ Category *(Default)* ◦ Category Name *(Default)* ◦ Category Zone *(Default)* ◦ Whois Created Date *(Default)* ◦ Whois Updated Date *(Default)* ◦ Whois Expires Date *(Default)* ◦ Domain Name Server *(Default)* ◦ Domain Status *(Default)* ◦ Registration Organization ◦ Registrar *(Default)* ◦ Registrar IANA ID *(Default)* ◦ Whois Contact Type *(Default)* ◦ Whois Contact Organization ◦ Whois Contact State *(Default)*

PARAMETER	DESCRIPTION
	◦ Whois Contact Country Code *(Default)*
Objects Per Run	Enter the max number of objects to process per run. The default value is `10000`.

Lookup FQDN Parameters

PARAMETER	DESCRIPTION
API Token	Enter your Kaspersky OpenTIP API token
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Attribute Filter	Select the pieces of context to ingest into ThreatQ from Kaspersky OpenTIP. Options include: ◦ Zone *(Default)* ◦ Malicious File Count *(Default)* ◦ URL Count *(Default)* ◦ Hits Count *(Default)* ◦ Number of IPs *(Default)* ◦ Category *(Default)* ◦ Category Name *(Default)* ◦ Category Zone *(Default)* ◦ Whois Created Date *(Default)* ◦ Whois Updated Date *(Default)* ◦ Whois Expires Date *(Default)* ◦ Domain Name Server *(Default)*

PARAMETER	DESCRIPTION
	◦ Domain Status *(Default)* ◦ Registration Organization *(Default)* ◦ Registrar *(Default)* ◦ Registrar IANA ID *(Default)* ◦ Whois Contact Type *(Default)* ◦ Whois Contact Name *(Default)* ◦ Whois Contact Organization *(Default)* ◦ Whois Contact State *(Default)* ◦ Whois Contact Country Code *(Default)*
Objects Per Run	Enter the max number of objects to process per run. The default value is `10000`.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Kaspersky - Lookup Malware	Look up file hashes and return file reputation, file context, optional detection details, and synonymous hashes.	Indicator	MD5, SHA-1, SHA-256
Kaspersky - Lookup IP Address	Look up IP addresses and return reputation, ASN, and network ownership context.	Indicator	IP Address
Kaspersky - Lookup URL	Look up URLs and return reputation, categories, and hosting-domain WHOIS context.	Indicator	URL
Kaspersky - Lookup FQDN	Look up domains and return reputation, categories, and WHOIS registration context.	Indicator	FQDN

Kaspersky - Lookup Malware

The Kaspersky – Lookup Malware action queries Kaspersky OpenTIP using a submitted file hash to retrieve reputation, malware classification, detection details, and additional contextual intelligence for the associated file.

```
GET https://opentip.kaspersky.com/api/v1/search/hash?
request={indicator}
```

Sample Response:

```
{
  "Zone": "Red",
  "FileGeneralInfo": {
    "Sha256":
"275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F",
    "Sha1": "3395856CE81F2B7382DEE72602F798B642F14140",
    "Md5": "44D88612FEA8A8F36DE82E1278ABB02F",
    "FileStatus": "Malware",
    "FirstSeen": "2010-07-26T02:22:00Z",
    "LastSeen": "2026-06-18T12:07:00Z",
    "Type": "text",
    "HitsCount": 10000000
  },
  "DetectionsInfo": [
    {
      "LastDetectDate": "2025-07-01T08:17:33.66Z",
      "DescriptionUrl": "https://threats.kaspersky.com/en/threat/
Backdoor.Win32.Androm",
      "Zone": "Red",
      "DetectionName": "Backdoor.Win32.Androm"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

All mapped fields are subject to user-configured filtering options.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Zone	Indicator.Attribute	Zone	N/A	Red	User-configurable. Updatable
.FileGeneralInfo.FileStatus	Indicator.Attribute	File Status	N/A	Malware	User-configurable. Updatable
.FileGeneralInfo.FirstSeen	Indicator.Attribute	First Seen	N/A	2021-12-20T15:44:00Z	User-configurable. Updatable
.FileGeneralInfo.LastSeen	Indicator.Attribute	Last Seen	N/A	2025-09-22T07:21:00Z	User-configurable. Updatable
.FileGeneralInfo.Size	Indicator.Attribute	File Size	N/A	86735	User-configurable. Updatable
.FileGeneralInfo.Type	Indicator.Attribute	File Type	N/A	unix shell	User-configurable. Updatable
.FileGeneralInfo.HitsCount	Indicator.Attribute	Hits Count	N/A	10	User-configurable. Updatable
.FileGeneralInfo.Signer	Indicator.Attribute	Signer	N/A	Microsoft Corporation	User-configurable. Updatable
.DetectionsInfo[].DetectionName, .DetectionsInfo[].DetectionMethod, .DetectionsInfo[].DescriptionUrl, .DetectionsInfo[].LastDetectDate, .DetectionsInfo[].Zone	Indicator.Description	Detection Details	N/A	HEUR:HackTool.Python.Meterp.b	Rendered as an HTML table in the indicator description when **Detection Info** is enabled. Only columns with available data are shown.
.FileGeneralInfo.Sha1	Indicator.Value	SHA-1	N/A	160C5434DED6D24E5806810887FD4CD48AC3AF3A	Related indicator. Only ingested when selected and different from the source hash
.FileGeneralInfo.Sha256	Indicator.Value	SHA-256	N/A	D7E30E17C271BE6E32C4492C65432D96ADDDE5DE51B5A2F296F6BB0C9B8E73D1	Related indicator. Only ingested when selected and different from the source hash
.FileGeneralInfo.Md5	Indicator.Value	MD5	N/A	44D88612FEA8A8F36DE82E1278ABB02F	Related indicator. Only ingested when selected and different from the source hash

Kaspersky - Lookup IP Address

The Kaspersky – Lookup IP Address action queries Kaspersky OpenTIP using a submitted IP address to retrieve reputation, threat classification, network ownership details, Autonomous System Number (ASN) information, and other contextual intelligence associated with the address.

```
GET https://opentip.kaspersky.com/api/v1/search/ip?
request={indicator}
```

Sample Response:


```
{
  "Zone": "Grey",
  "IpGeneralInfo": {
    "Status": "known",
    "CountryCode": "EG",
    "HitsCount": null,
    "FirstSeen": null,
    "Categories": null,
    "CategoriesWithZone": []
  },
  "IpWhoIs": {
    "Asn": [
      {
        "Number": 8452,
        "Description": [
          "Telecom-Egypt-Data"
        ]
      }
    ],
    "Net": {
      "RangeStart": "41.40.0.0",
      "RangeEnd": "41.43.255.255",
      "Name": "All-04-NNN",
      "Description": "TE Data"
    }
  }
}
```

ThreatQuotient provides the following default mapping for this action:

All mapped fields are subject to user-configured filtering options.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Zone	Indicator.Attribute	Zone	N/A	Green	User-configurable. Updatable
.IpGeneralInfo.Status	Indicator.Attribute	Status	N/A	known	User-configurable. Updatable
.IpGeneralInfo.CountryCode	Indicator.Attribute	Country Code	N/A	AU	User-configurable. Updatable
.IpGeneralInfo.HitsCount	Indicator.Attribute	Hits Count	N/A	100000	User-configurable. Updatable
.IpGeneralInfo.FirstSeen	Indicator.Attribute	First Seen	N/A	2014-06-03T07:52:00Z	User-configurable. Updatable
.IpGeneralInfo.Categories[]	Indicator.Attribute	Category	N/A	CATEGORY_ANONYMIZERS	User-configurable. Updatable
.IpGeneralInfo.CategoriesWithZone[].Name	Indicator.Attribute	Category Name	N/A	CATEGORY_NAT_GATEWAY	User-configurable. Updatable
.IpGeneralInfo.CategoriesWithZone[].Zone	Indicator.Attribute	Category Zone	N/A	Grey	User-configurable. Updatable
.IpWhoIs.Asn[].Numbe r	Indicator.Attribute	ASN Number	N/A	8452	User-configurable. Updatable
.IpWhoIs.Asn[].Description[]	Indicator.Attribute	ASN Description	N/A	Telecom-Egypt-Data	User-configurable. Updatable
.IpWhoIs.Net.RangeStart	Indicator.Attribute	Network Range Start	N/A	1.1.1.0	User-configurable. Updatable
.IpWhoIs.Net.RangeEnd	Indicator.Attribute	Network Range End	N/A	1.1.1.255	User-configurable. Updatable
.IpWhoIs.Net.Created	Indicator.Attribute	Network Created Date	N/A	2011-08-10T23:12:35Z	User-configurable. Updatable
.IpWhoIs.Net.Changed	Indicator.Attribute	Network Changed Date	N/A	2023-04-26T22:57:58Z	User-configurable. Updatable
.IpWhoIs.Net.Name	Indicator.Attribute	Network Name	N/A	APNIC-LABS	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.IpWhoIs.Net.Description`	`Indicator.Attribute`	`Network Description`	`N/A`	`APNIC and Cloudflare DNS Resolver project`	`User-configurable. Updatable`

Kaspersky - Lookup URL

The Kaspersky – Lookup URL actioni queries Kaspersky OpenTIP using a submitted URL to retrieve reputation, threat classification, hosting domain information, and WHOIS registration details, providing additional context for threat analysis and investigation.

```
GET https://opentip.kaspersky.com/api/v1/search/url?
request={indicator}
```

Sample Response:


```
{
  "Zone": "Green",
  "UrlGeneralInfo": {
    "Status": null,
    "Url": "www.eicar.org/download/eicar.com.txt",
    "Domain": null,
    "FirstSeen": null,
    "CategoriesWithZone": [
      {
        "Name": "CATEGORY_INFORMATION_TECHNOLOGIES",
        "Zone": "Grey"
      },
      {
        "Name": "CATEGORY_INFORMATIONSECURITY",
        "Zone": "Grey"
      }
    ]
  },
  "UrlDomainWhoIs": {
    "RegistrarInfo": null,
    "Created": "1998-03-24T21:00:00Z",
    "Updated": "2026-05-07T21:00:00Z",
    "Expires": "2027-03-23T21:00:00Z"
  }
}
```

ThreatQuotient provides the following default mapping for this action:

All mapped fields are subject to user-configured filtering options.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Zone	Indicator.Attribute	Zone	N/A	Grey	User-configurable. Updatable
.UrlGeneralInfo.Host	Indicator.Attribute	Host	N/A	dcttl.com	User-configurable. Updatable
.UrlGeneralInfo.Ipv4Count	Indicator.Attribute	Number of IPs	N/A	382	User-configurable. Updatable
.UrlGeneralInfo.FilesCount	Indicator.Attribute	Malicious File Count	N/A	0	User-configurable. Updatable
.UrlGeneralInfo.Categories[]	Indicator.Attribute	Category	N/A	CATEGORY_INFORMATIONSECURITY	User-configurable. Updatable
.UrlGeneralInfo.CategoriesWithZone[].Name	Indicator.Attribute	Category Name	N/A	CATEGORY_INFORMATION_TECHNOLOGIES	User-configurable. Updatable
.UrlGeneralInfo.CategoriesWithZone[].Zone	Indicator.Attribute	Category Zone	N/A	Grey	User-configurable. Updatable
.UrlDomainWhoIs.Created	Indicator.Attribute	Whois Created Date	N/A	2021-11-29T21:00:00Z	User-configurable. Updatable
.UrlDomainWhoIs.Updated	Indicator.Attribute	Whois Updated Date	N/A	2026-05-07T21:00:00Z	User-configurable. Updatable
.UrlDomainWhoIs.Expires	Indicator.Attribute	Whois Expires Date	N/A	2027-03-23T21:00:00Z	User-configurable. Updatable
.UrlDomainWhoIs.NameServers[]	Indicator.Attribute	Domain Name Server	N/A	dns1.registrar-servers.com	User-configurable. Updatable
.UrlDomainWhoIs.DomainStatus[]	Indicator.Attribute	Domain Status	N/A	active	User-configurable. Updatable
.UrlDomainWhoIs.RegistrationOrganization	Indicator.Attribute	Registration Organization	N/A	EICAR - European Institute for Computer Anti-Virus Research e.V.	User-configurable. Updatable
.UrlDomainWhoIs.Registrar.Info	Indicator.Attribute	Registrar	N/A	NameCheap, Inc.	User-configurable. Updatable
.UrlDomainWhoIs.Registrar.IanaId	Indicator.Attribute	Registrar IANA ID	N/A	1068	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.UrlDomainWhoIs.Contacts[].ContactType	Indicator.Attribute	Whois Contact Type	N/A	registrant	User-configurable. Updatable
.UrlDomainWhoIs.Contacts[].Organization	Indicator.Attribute	Whois Contact Organization	N/A	EICAR - European Institute for Computer Anti-Virus Research e.V.	User-configurable. Updatable
.UrlDomainWhoIs.Contacts[].State	Indicator.Attribute	Whois Contact State	N/A	Capital Region	User-configurable. Updatable
.UrlDomainWhoIs.Contacts[].CountryCode	Indicator.Attribute	Whois Contact Country Code	N/A	DE	User-configurable. Updatable

Kaspersky - Lookup FQDN

The Kaspersky – Lookup FQDN action queries Kaspersky OpenTIP using a submitted fully qualified domain name (FQDN) to retrieve reputation, threat classification, and WHOIS registration information, providing additional context for threat analysis and investigation.

```
GET https://opentip.kaspersky.com/api/v1/search/domain?request={indicator}
```

Sample Response:


```
{
  "Zone": "Grey",
  "DomainGeneralInfo": {
    "Status": null,
    "Domain": "dcttl.com",
    "FirstSeen": null,
    "CategoriesWithZone": []
  },
  "DomainWhoIsInfo": {
    "RegistrarInfo": null,
    "Created": "2021-11-29T21:00:00Z",
    "Updated": "2021-12-07T21:00:00Z",
    "Expires": "2022-11-29T21:00:00Z"
  }
}
```

ThreatQuotient provides the following default mapping for this action:

All mapped fields are subject to user-configured filtering options.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.Zone	Indicator.Attribute	Zone	N/A	Green	User-configurable. Updatable
.DomainGeneralInfo.FilesCount	Indicator.Attribute	Malicious File Count	N/A	100000000	User-configurable. Updatable
.DomainGeneralInfo.UrlsCount	Indicator.Attribute	URL Count	N/A	100000000	User-configurable. Updatable
.DomainGeneralInfo.HitsCount	Indicator.Attribute	Hits Count	N/A	1000000000	User-configurable. Updatable
.DomainGeneralInfo.Ipv4Count	Indicator.Attribute	Number of IPs	N/A	1000	User-configurable. Updatable
.DomainGeneralInfo.Categories[]	Indicator.Attribute	Category	N/A	CATEGORY_INFORMATION_TECHNOLOGIES	User-configurable. Updatable
.DomainGeneralInfo.CategoriesWithZone[].Name	Indicator.Attribute	Category Name	N/A	CATEGORY_INTERNET_SERVICES	User-configurable. Updatable
.DomainGeneralInfo.CategoriesWithZone[].Zone	Indicator.Attribute	Category Zone	N/A	Grey	User-configurable. Updatable
.DomainWhoIsInfo.Created	Indicator.Attribute	Whois Created Date	N/A	1997-09-14T20:00:00Z	User-configurable. Updatable
.DomainWhoIsInfo.Updated	Indicator.Attribute	Whois Updated Date	N/A	2019-09-08T21:00:00Z	User-configurable. Updatable
.DomainWhoIsInfo.Expires	Indicator.Attribute	Whois Expires Date	N/A	2028-09-13T21:00:00Z	User-configurable. Updatable
.DomainWhoIsInfo.NameServers[]	Indicator.Attribute	Domain Name Server	N/A	ns1.google.com	User-configurable. Updatable
.DomainWhoIsInfo.DomainStatus[]	Indicator.Attribute	Domain Status	N/A	client transfer prohibited	User-configurable. Updatable
.DomainWhoIsInfo.RegistrationOrganization	Indicator.Attribute	Registration Organization	N/A	Google LLC	User-configurable. Updatable
.DomainWhoIsInfo.Registrar.Info	Indicator.Attribute	Registrar	N/A	Markmonitor Inc.	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.DomainWhoIsInfo.Registrar.IanaId	Indicator.Attribute	Registrar IANA ID	N/A	292	User-configurable. Updatable
.DomainWhoIsInfo.Contacts[].ContactType	Indicator.Attribute	Whois Contact Type	N/A	registrant	User-configurable. Updatable
.DomainWhoIsInfo.Contacts[].Name	Indicator.Attribute	Whois Contact Name	N/A	REDACTED REGISTRANT	User-configurable. Updatable
.DomainWhoIsInfo.Contacts[].Organization	Indicator.Attribute	Whois Contact Organization	N/A	Google LLC	User-configurable. Updatable
.DomainWhoIsInfo.Contacts[].State	Indicator.Attribute	Whois Contact State	N/A	Capital Region	User-configurable. Updatable
.DomainWhoIsInfo.Contacts[].CountryCode	Indicator.Attribute	Whois Contact Country Code	N/A	US	User-configurable. Updatable

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

Kaspersky - Lookup Malware

METRIC	RESULT
Run Time	1 minute
Indicators	6
Indicator Attributes	15

Kaspersky - Lookup IP Address

METRIC	RESULT
Run Time	1 minute
Indicators	3
Indicator Attributes	33

Kaspersky - Lookup URL

METRIC	RESULT
Run Time	1 minute

METRIC	RESULT
Indicators	2
Indicator Attributes	18

Kaspersky - Lookup FQDN

METRIC	RESULT
Run Time	1 minute
Indicators	2
Indicator Attributes	28

Use Case Example

- **Kaspersky - Lookup Malware** - Use this action to enrich a collection of MD5, SHA-1, or SHA-256 file hashes with threat intelligence from Kaspersky OpenTIP. The action helps determine whether the submitted hashes are associated with known malicious files and provides additional context, including file reputation, first and last seen timestamps, file type, hit counts, optional detection details, and synonymous hashes to support threat investigation and pivoting.
- **Kaspersky - Lookup IP Address** - Use this action to enrich a collection of IP addresses with threat intelligence from Kaspersky OpenTIP. The action helps identify IP addresses associated with suspicious or malicious infrastructure by providing reputation, threat classification, country, ASN information, network ownership details, and other contextual intelligence to support threat triage and investigation.
- **Kaspersky - Lookup URL** - Use this action to enrich a collection of URLs with threat intelligence from Kaspersky OpenTIP. The action helps identify URLs associated with malicious or suspicious web activity by providing reputation, threat categories, hosting domain information, and WHOIS registration details, enabling analysts to quickly investigate phishing campaigns, malware delivery infrastructure, and other web-based threats.
- **Kaspersky - Lookup FQDN** - Use this action to enrich a collection of fully qualified domain names (FQDNs) with threat intelligence from Kaspersky OpenTIP. The action helps identify domains associated with suspicious or malicious activity by providing reputation, threat categories, hit counts, and WHOIS registration information, enabling analysts to investigate malicious infrastructure, phishing domains, and DNS-related threats more effectively.

Change Log

- **Version 1.0.0**
  - Initial release