ThreatQuotient

A Securonix Company

Resecurity CDF

Version 1.0.0

October 07, 2025

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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Intelligence Botnets Parameters 9
Threat Intelligence IOCs Parameters 11
Threat Intelligence IPs Parameters 12
Threat Intelligence Domains Parameters 14
Threat Intelligence Incidents Parameters 15
Threat Intelligence DarkWeb Parameters 17
Threat Intelligence Alerts Parameters 19
ThreatQ Mapping **21**
Resecurity Threat Intelligence Botnets 21
Resecurity Botnet Type Mapping 22
Resecurity Threat Intelligence IOCs 25
Resecurity Threat Intelligence IPs 27
Resecurity Threat Intelligence Domains 30
Resecurity Threat Intelligence Incidents 33
Incident TLP Mapping 36
Incident Status Mapping 36
Resecurity Threat Intelligence DarkWeb 37
Resecurity Threat Intelligence Alerts 39
Average Feed Run **42**
Resecurity Threat Intelligence Botnets 42
Resecurity Threat Intelligence IOCs 42
Resecurity Threat Intelligence IPs 43
Resecurity Threat Intelligence Domains 43
Resecurity Threat Intelligence Incidents 43
Resecurity Threat Intelligence DarkWeb 44
Resecurity Threat Intelligence Alerts 44
Known Issues / Limitations **45**
Change Log **46**

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	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Resecurity CDF integration allows analysts to automatically ingest threat intelligence data from Resecurity, ensuring timely and consistent access to the latest security insights for enhanced analysis and decision-making.

The integration provides the following feeds:

- **Resecurity Threat Intelligence Botnets** - ingests botnet data.
- **Resecurity Threat Intelligence IOCs** - ingests IOCs.
- **Resecurity Threat Intelligence IPs** - ingests IP Addresses.
- **Resecurity Threat Intelligence Domains** - ingests Domains.
- **Resecurity Threat Intelligence Incidents** - ingests Resecurity Incidents as ThreatQ Events.
- **Resecurity Threat Intelligence DarkWeb** - ingests DarkWeb Posts as ThreatQ Events.
- **Resecurity Threat Intelligence Alerts** - ingests alerts as ThreatQ Incidents.

The integrations ingests the following object types:

- Adversary
- Event
- Incident
- Indicator
- Malware
- Report

Prerequisites

The following is required to run the integration and its feeds:

- A Resecurity API Key.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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(s) will be added to the integrations page. You will still need to configure and then enable the feed(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 **Commercial** option from the *Category* dropdown (optional).

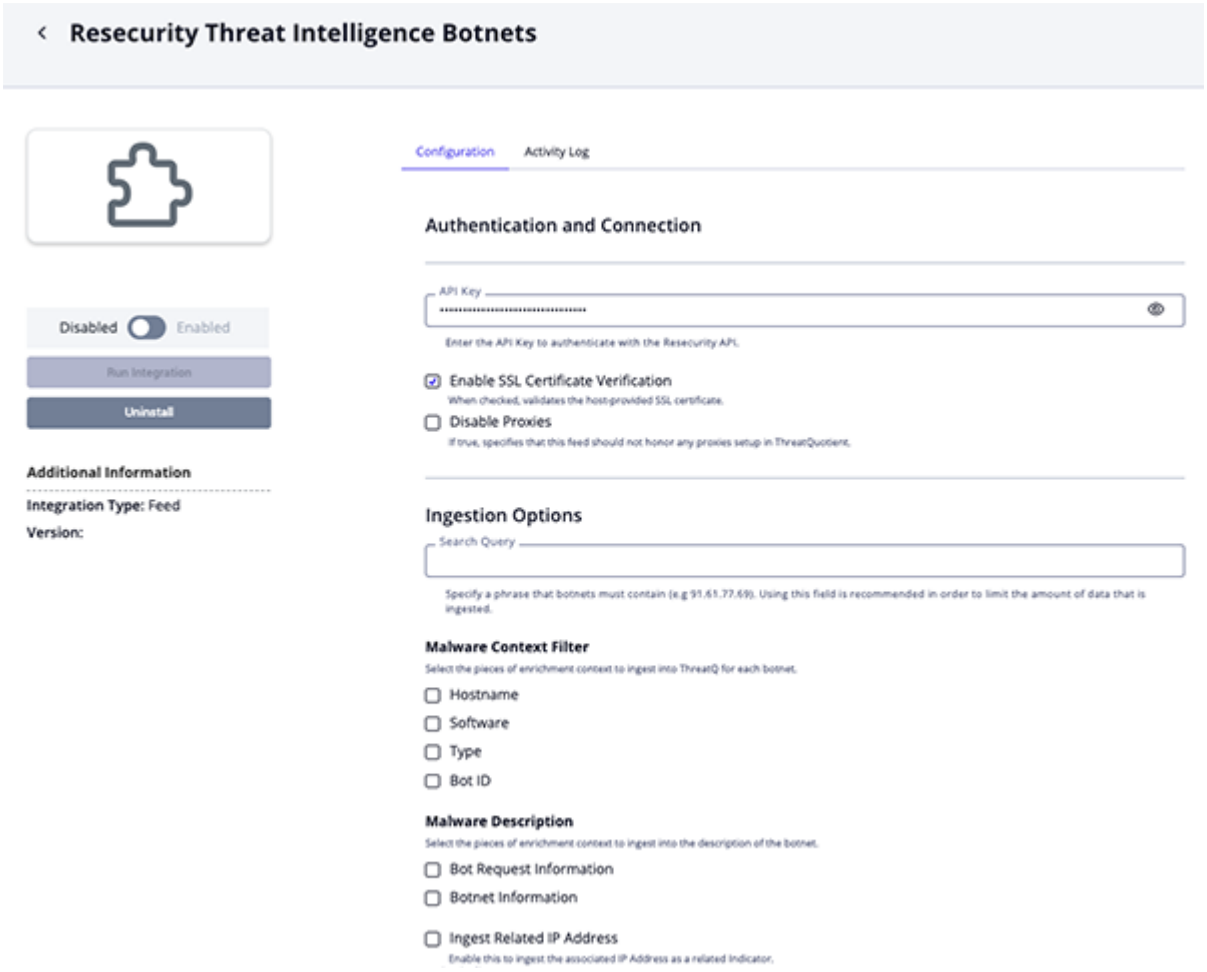
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Intelligence Botnets Parameters

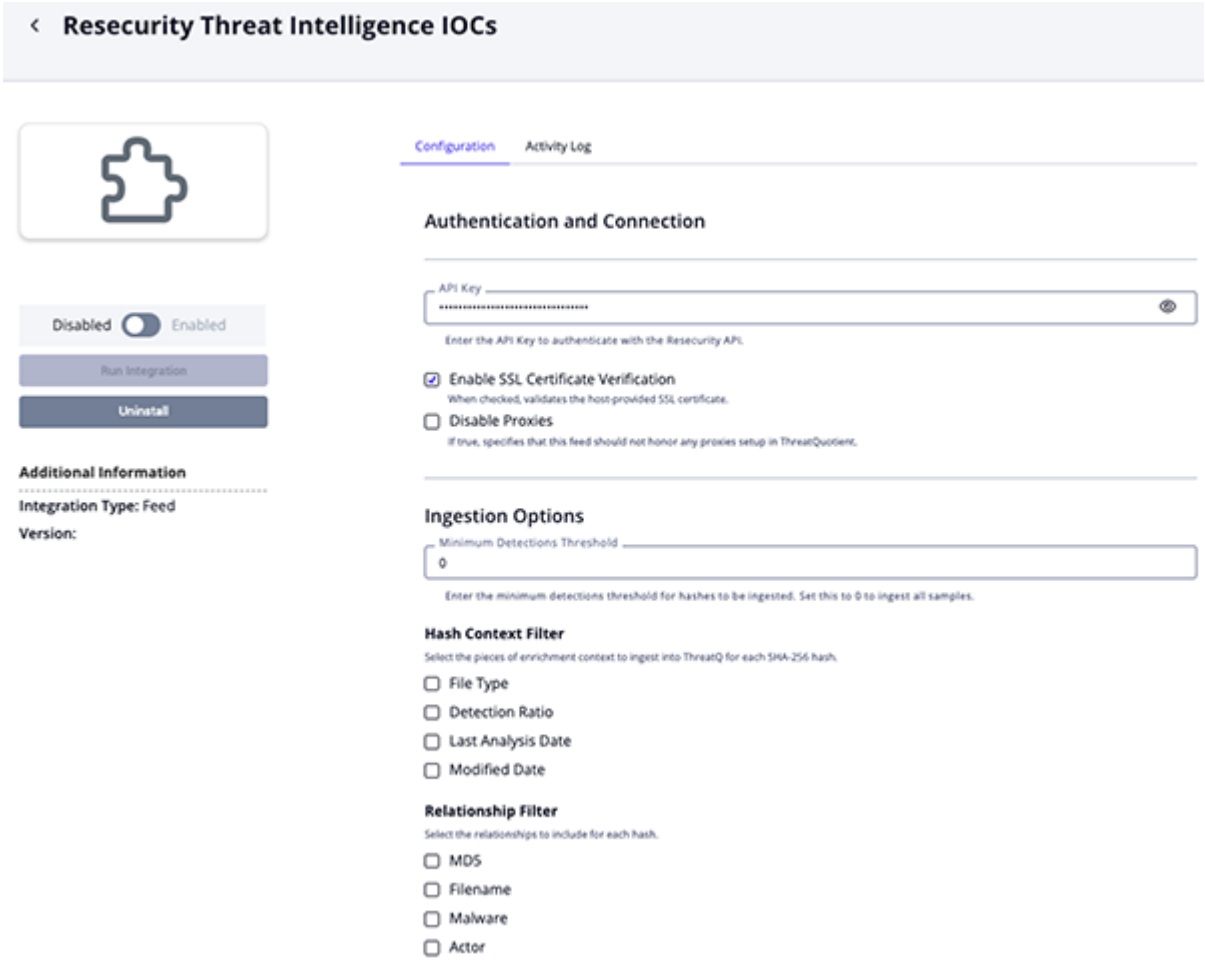
PARAMETER	DESCRIPTION
API Key	Enter the API Key to authenticate with the Resecurity API.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Search Query	Specify a phrase that botnets must contain. The default value is: `91.61.77.69`. > It is recommended to use this parameter in order to limit the amount of data that is ingested.
Malware Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each botnet. Options include: ◦ Hostname *(default)* ◦ Software *(default)*

PARAMETER	DESCRIPTION
	◦ Type *(default)* ◦ Bot ID
Malware Description	Select the pieces of enrichment context to ingest into the description of the botnet. Options include: ◦ Bot Request Information *(default)* ◦ Botnet Information
Ingest Related IP Address	Enable this parameter to ingest the associated IP Address as a related Indicator. This parameter is enabled by default.



Threat Intelligence IOCs Parameters

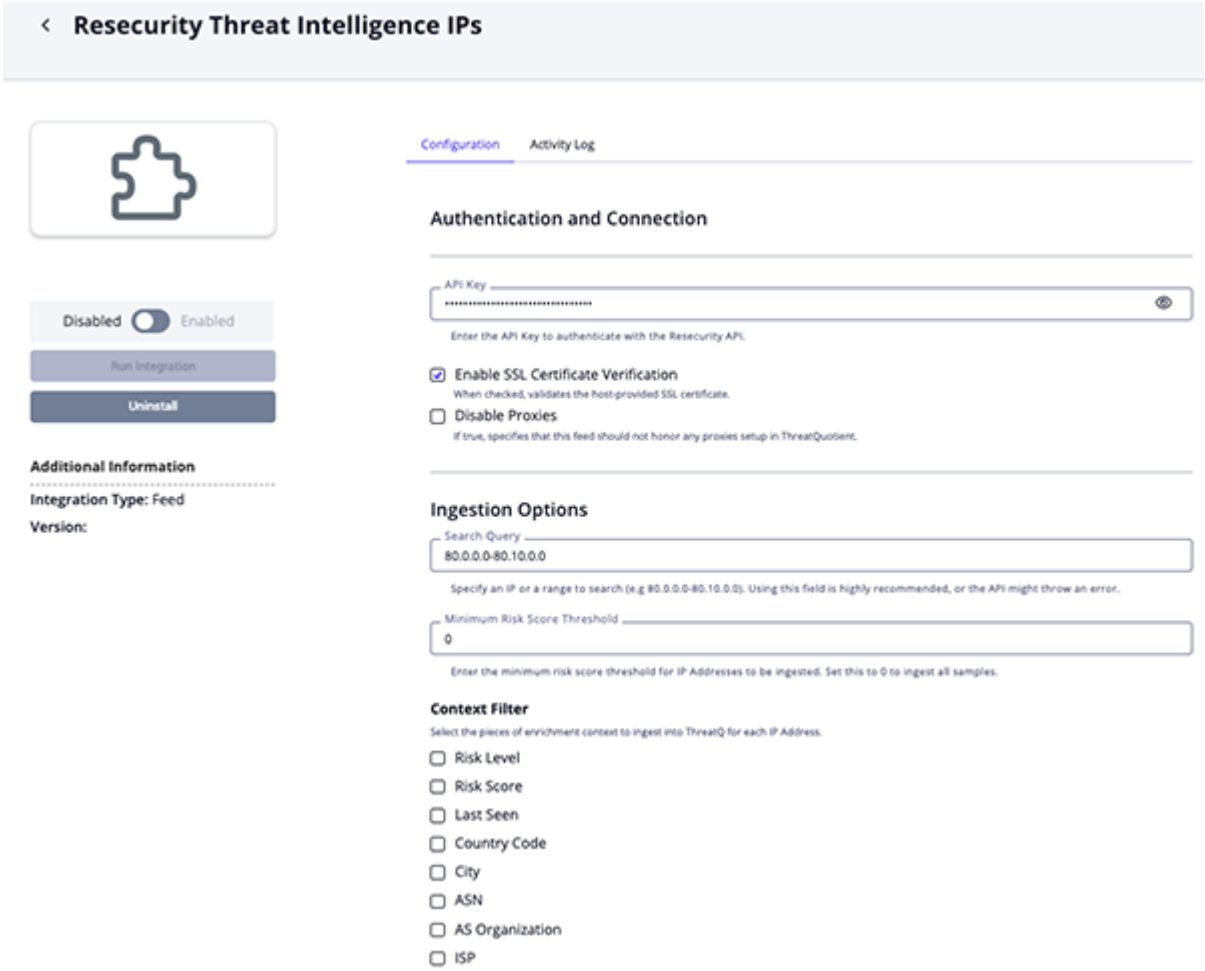
PARAMETER	DESCRIPTION
API Key	Enter the API Key to authenticate with the Resecurity API.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Minimum Detections Threshold	Enter the minimum detections threshold for hashes to be ingested. Set this parameter to `0`, the default value, to ingest all samples.
Hash Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each SHA-256 hash. Options include: ◦ File Type *(default)* ◦ Detection Ratio *(default)* ◦ Last Analysis Date ◦ Modified Date
Relationship Filter	Select the relationships to include for each hash. Options include: ◦ MD5 *(default)* ◦ Filename ◦ Malware ◦ Actor



Threat Intelligence IPs Parameters

PARAMETER	DESCRIPTION
API Key	Enter the API Key to authenticate with the Resecurity API.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Search Query	Specify an IP or a range to search. The default value is: `80.0.0.0-80.10.0.0`.

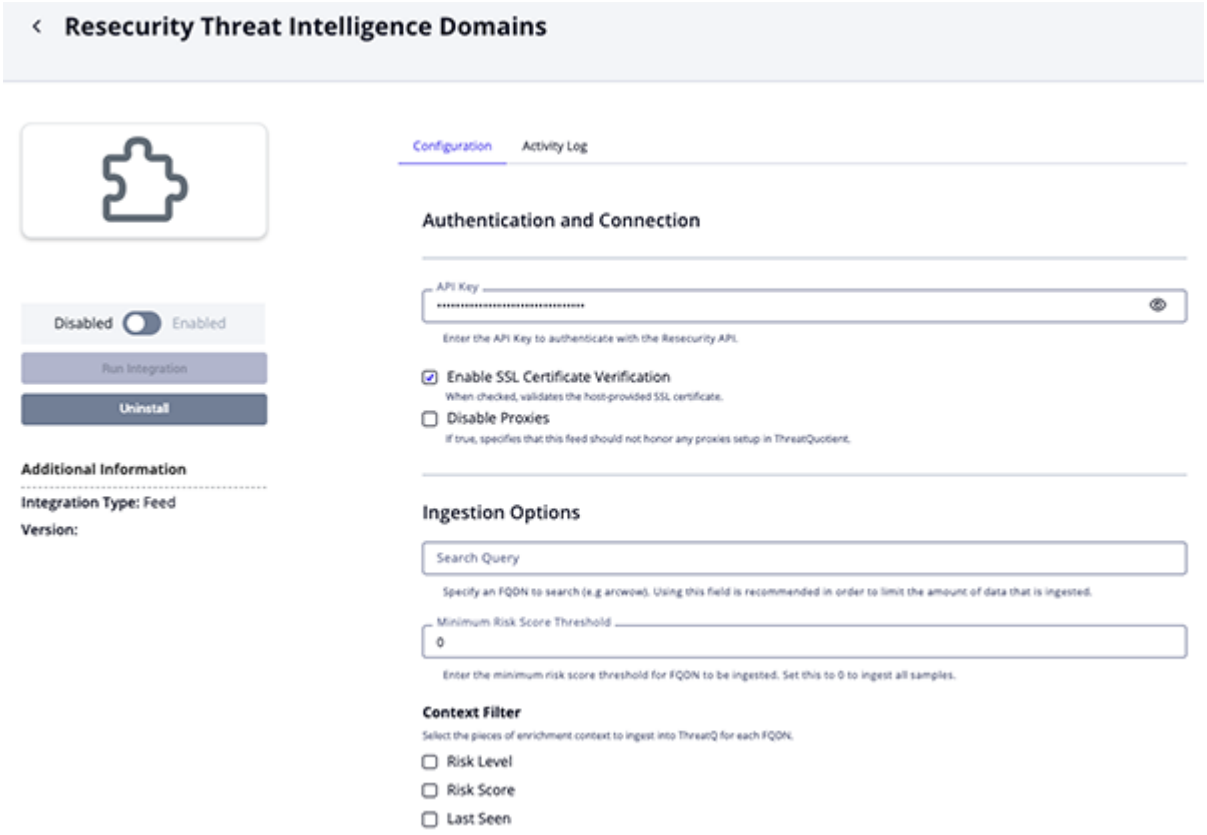
PARAMETER	DESCRIPTION
	Utilizing this parameter is highly recommended to prevent the API from throwing an error.
Minimum Risk Score Threshold	Enter the minimum risk score threshold for IP Addresses to be ingested. Set this parameter to `0`, the default value, to ingest all samples.
Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each IP Address. Options include: ◦ Risk Level *(default)* ◦ Risk Score *(default)* ◦ Last Seen *(default)* ◦ Country Code ◦ City ◦ ASN ◦ AS Organization ◦ ISP
Relationship Filter	Select the relationships to include for each IP Address. Options include: ◦ VPN Related Domains ◦ VPN Related IPs



Threat Intelligence Domains Parameters

PARAMETER	DESCRIPTION
API Key	Enter the API Key to authenticate with the Resecurity API.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Search Query	Specify an FQDN to search in order to limit the amount of data that is ingested. The default value is `arcwow`.

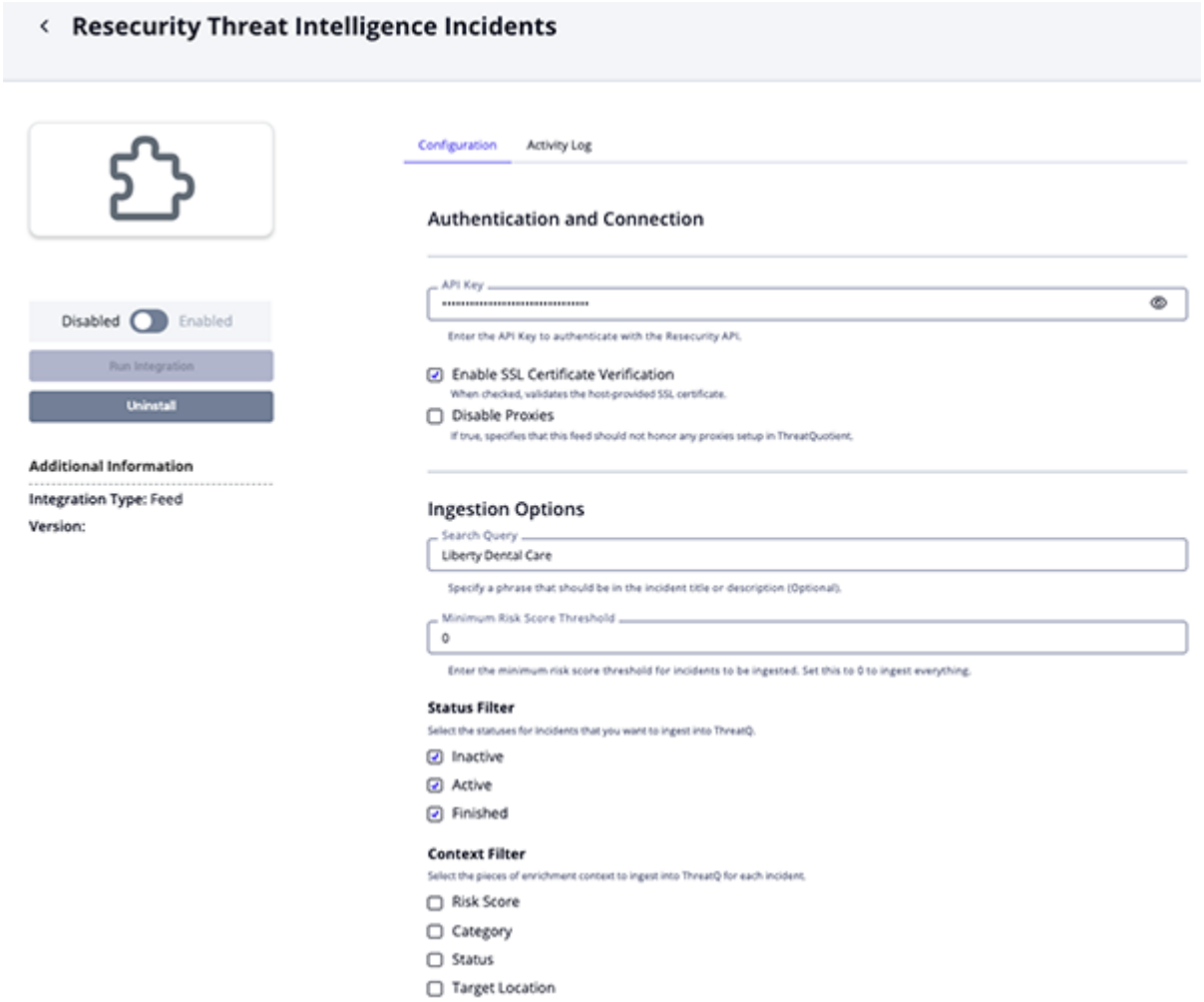
PARAMETER	DESCRIPTION
Minimum Risk Score Threshold	Enter the minimum risk score threshold for FQDN to be ingested. Set this parameter to `0`, the default value, to ingest all samples.
Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each FQDN. Options include: ◦ Risk Level *(default)* ◦ Risk Score *(default)* ◦ Last Seen *(default)*



Threat Intelligence Incidents Parameters

PARAMETER	DESCRIPTION
API Key	Enter the API Key to authenticate with the Resecurity API.

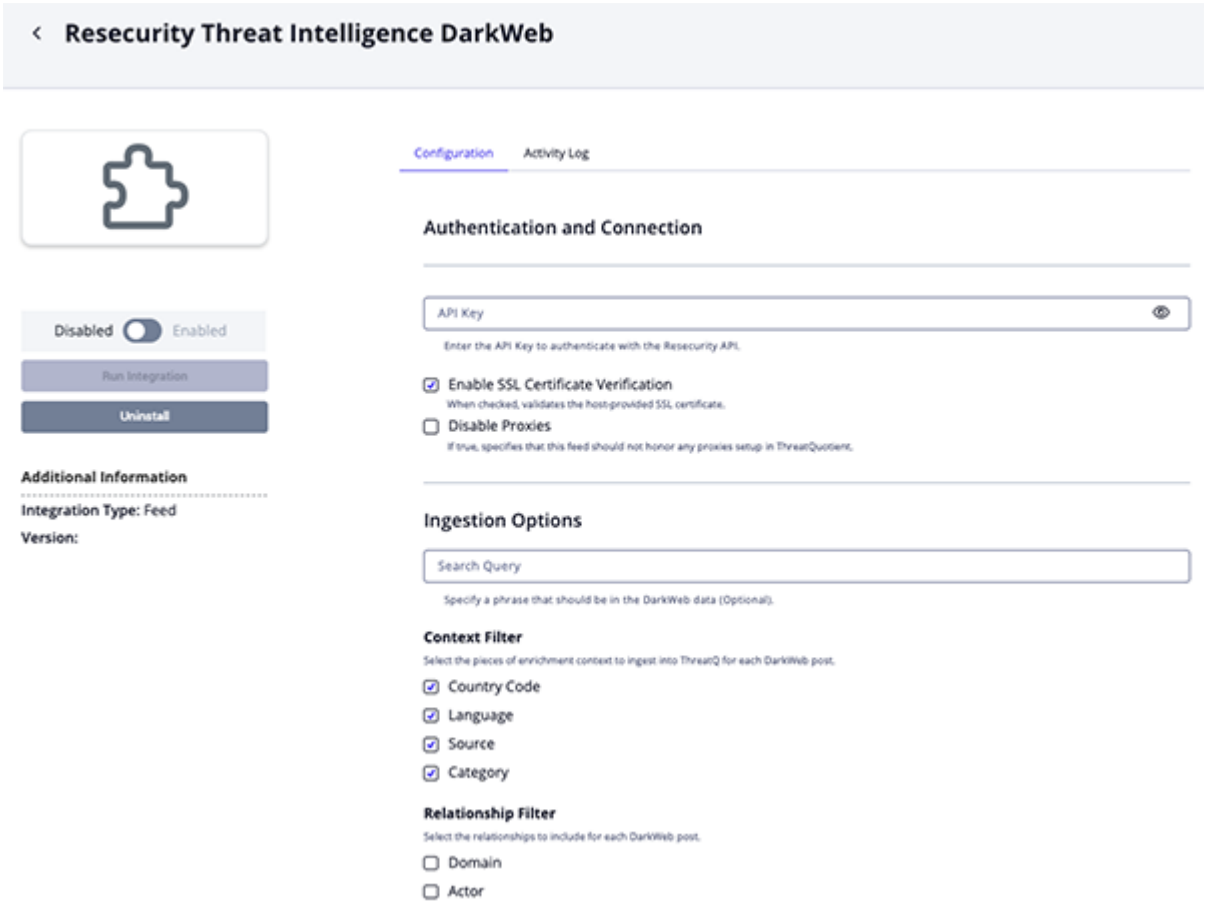
PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Search Query	Optional - Specify a phrase that should be in the incident title or description.
Minimum Risk Score Threshold	Enter the minimum risk score threshold for incidents to be ingested. Set this parameter to `0`, the default value, to ingest everything.
Status Filter	Select the statuses for Incidents that you want to ingest into ThreatQ. Options include: ◦ Inactive ◦ Active *(default)* ◦ Finished *(default)*
Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each incident. Options include: ◦ Risk Score *(default)* ◦ Category *(default)* ◦ Status *(default)* ◦ Target Location ◦ Target Industry ◦ Modified Date
Relationships Filter	Select the relationships to include for each incident. Options include: ◦ IOC Hashes ◦ Malicious Activity IPs ◦ Malicious Activity Domains ◦ Malicious Activity Emails ◦ Victim Information IPs ◦ Victim Information Domains ◦ Victim Information Emails



Threat Intelligence DarkWeb Parameters

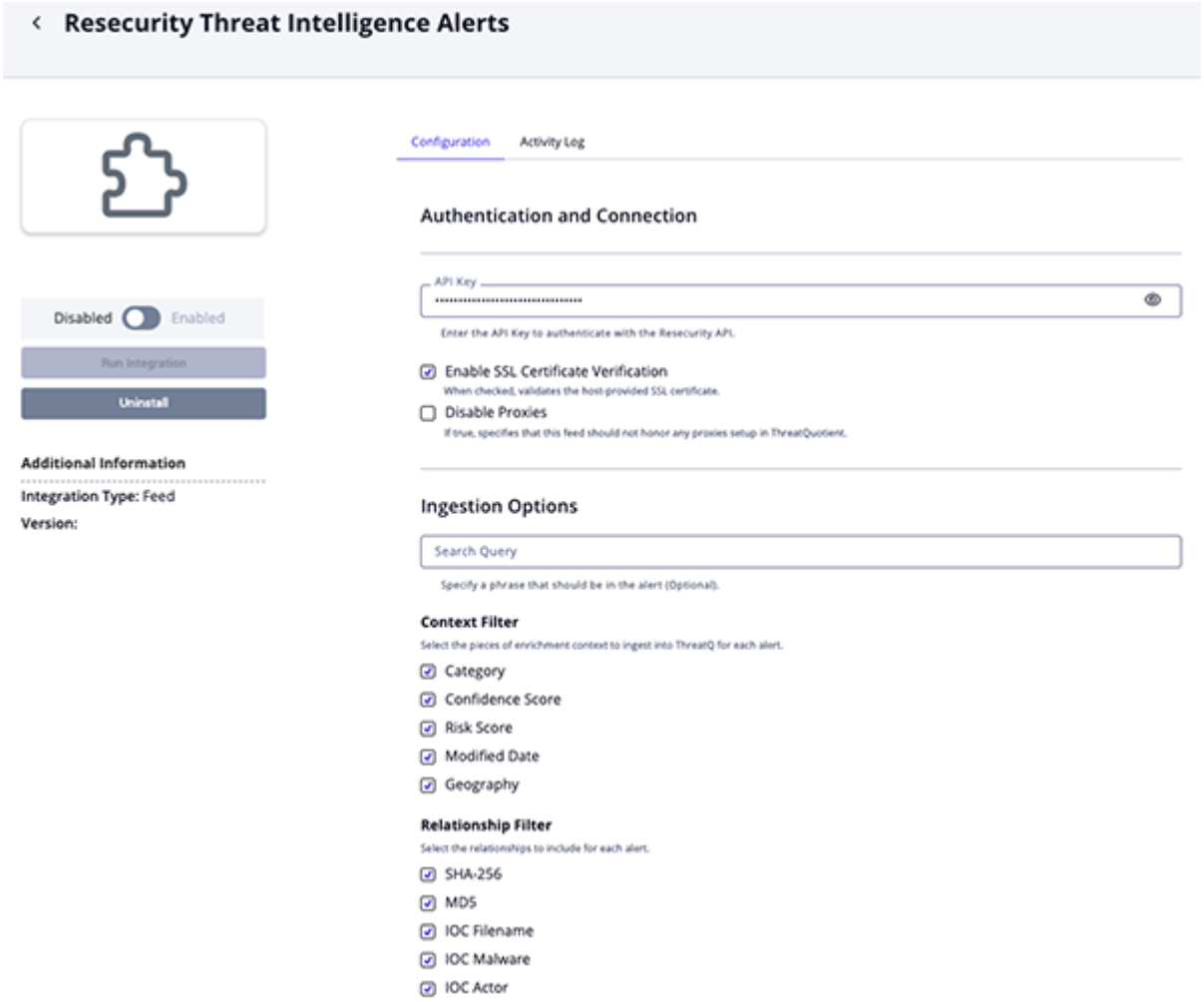
PARAMETER	DESCRIPTION
API Key	Enter the API Key to authenticate with the Resecurity API.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.

PARAMETER	DESCRIPTION
Search Query	Optional - Specify a phrase that should be in the DarkWeb data.
Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each incident. Options include: ◦ Country Code *(default)* ◦ Language *(default)* ◦ Source *(default)* ◦ Category *(default)*
Relationship Filter	Select the relationships to include for each DarkWeb post. Options include: ◦ Domain ◦ Actor



Threat Intelligence Alerts Parameters

PARAMETER	DESCRIPTION
API Key	Enter the API Key to authenticate with the Resecurity API.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Security Query	Optional - Specify a phrase that should be in the alert.
Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each alert. Options include: ◦ Category *(default)* ◦ Confidence Score *(default*) ◦ Risk Score *(default)* ◦ Modified Date ◦ Geography
Relationship Filter	Select the relationships to include for each alert. Options include: ◦ SHA-256 *(default)* ◦ MD5 ◦ IOC Filename ◦ IOC Malware ◦ IOC Actor ◦ TTP Filename
Hash Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for each SHA-256 hash. Options include: ◦ File Type *(default)* ◦ Detection Ratio *(default)* ◦ Last Analysis Date ◦ Modified Date



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Resecurity Threat Intelligence Botnets

The Resecurity Threat Intelligence Botnets feed periodically pulls botnets from Resecurity. The API does not allow to filter by date, but the entries are sorted chronologically. New pages are requested as long as `.time` of the last returned entry is greater than feed run start date.

The value of the user configuration `Search Query` is search in the fields `.ip`, `.bot_info`, `.info`.

`GET https://app.resecurity.com/api/botnets/index`

Request Parameters:

```
{
  "query": "91.61.77.69",
  "per-page": 50,
  "page": 1
}
```

Sample Response:

```
[
  {
    "id": 59967949,
    "ip": "91.61.77.69",
    "type": 1001,
    "bot": "4659ca3b-14cbd1a1-c904d3f3-27ad901f-16de201d",
    "bot_info": "E\r\nMachineID :   4659CA3B-14CBD1A1-
C904D3F3-27AD901F-16DE201D\r\nEXE_PATH  :   C:\\Users\\KRASSE~1\\AppData\
\Local\\Temp\\J4HakZ4P0isdStK9\
\1b009389e9705c143c4f88885cccc0d9.exe\r\n\r\nWindows",
    "botnet": "logs13092019/azorult",
    "hostname": "KRASSER(krasser88)",
    "time": 1567724685,
    "info": "host: https://webmail.o2mail.de\r\nuser:
danieltismer@o2.de\r\npass: ascheberg88",
    "software": "MozillaFirefox"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.botnet`	Malware.Value	Malware	`.time`	`logs13092019/azorult`	N/A
`.info`	Malware.Description	N/A	N/A	`host: https://webmail.o2mail.de...`	If `Bot Request Information` enabled in `Malware Description`.
`.bot_info`	Malware.Description	N/A	N/A	`E\r\nMachineID : 4659CA3B-14CBD1A1...`	If `Bot Information` enabled in `Malware Description`.
`.bot`	Malware.Attribute	Bot ID	`.time`	`4659ca3b-14cbd1a1-c904d3f3-27ad901f-16de201d`	User-configurable.
`.hostname`	Malware.Attribute	Hostname	`.time`	`KRASSER(krasser88)`	User-configurable.
`.software`	Malware.Attribute	Software	`.time`	`MozillaFirefox`	User-configurable.
`.type`	Malware.Attribute	Type	`.time`	`Password`	User-configurable. Updatable. Mapped according to `Resecurity Botnet Type Mapping`.
`.ip`	Related Indicator	IP Address	`.time`	`91.61.77.69`	If `Ingest Related IP Address` enabled.

Resecurity Botnet Type Mapping

Resecurity Botnet type to ThreatQ attribute mapping is as follows:

RESECURITY BOTNET TYPE	THREATQ ATTRIBUTE
0	Unknown
1	Cookies
2	File
3	Web Inject
11	HTTP request
12	HTTPS request
13	Luhn 10 request

RESECURITY BOTNET TYPE	THREATQ ATTRIBUTE
100	Login FTP
101	Login POP3
102	File search
103	Keylogger
104	Device
200	Grabbed UI
201	Grabbed HTTP
202	Grabbed wsocket
203	Grabbed FTP software
204	Grabbed emailsoftware
205	Grabbed web form
299	Grabbed other
300	Commandline result
400	Analytics software
401	Analytics firewall
402	Analytics antivirus
500	Ports

RESECURITY BOTNET TYPE	THREATQ ATTRIBUTE
1000	Megapackage
1001	Password
1002	Browser autocomplete
1003	Credit card
1004	Browser downloads
1005	Browser history

Resecurity Threat Intelligence IOCs

The Resecurity Threat Intelligence IOCs feed periodically pulls IOCs from Resecurity. The API does not allow to filter by date, but the entries are sorted chronologically. New pages are requested as long as `.update_date` of the last returned entry is greater than feed run start date.

The number of detections is parsed from `.detection_ratio` (the value before `/`). The parsed value is compared to the `Minimum Detections Threshold` user configuration. If the value is lower than the entry is discarded.

`GET https://app.resecurity.com/api/ioc/index`

Sample Response:

```
[
  {
    "id": 33379825,
    "sha256":
"dba860617762bc713771de351026eb683546b37489fa0359064948f263438030",
    "md5": "e5eb524308a58190d9feb2244d187eb8",
    "malware_name": "HEUR:Exploit.MSOffice.Agent.n",
    "file_name": "1021E2EC.htm",
    "file_type": "HTML",
    "detection_ratio": "32 / 62",
    "analysis_date": 1758738336,
    "add_date": 1758744973,
    "update_date": 1758745218,
    "actor_name": "Actor1",
    "item_url": "https://app.resecurity.com/ioc?IocSearch[id]=33379825"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.sha256`	Indicator.Value	SHA-256	`.add_date`	`dba860617762bc713771de351026e...`	N/A
`.item_url`	Indicator.Description	N/A	N/A	Resecurity Link	Formated using HTML `<a>` tag.
`.file_type`	Indicator.Attribute	File Type	`.add_date`	`HTML`	User-configurable.
`.detection_ratio`	Indicator.Attribute	Detection Ratio	`.add_date`	`32 / 62`	User-configurable. Updatable.
`.analysis_date`	Indicator.Attribute	Last Analysis Date	`.add_date`	`2025-09-24 18:25:36+00:00`	User-configurable. Updatable. Formated to human-readable date.
`.update_date`	Indicator.Attribute	Modified Date	`.add_date`	`2025-09-24 20:20:18+00:00`	User-configurable. Updatable. Formated to human-readable date.
`.malware_name`	Related Malware.Value	Malware	`.add_date`	`HEUR:Exploit.MSOffice.Agent.n`	User-configurable.
`.file_name`	Related Indicator.Value	Filename	`.add_date`	`1021E2EC.htm`	User-configurable.
`.md5`	Related Indicator.Value	MD5	`.add_date`	`e5eb524308a58190d9feb2244d187eb8`	User-configurable.
`.actor_name`	Related Adversary.Name	Adversary	`.add_date`	`Actor1`	User-configurable.

Resecurity Threat Intelligence IPs

The Resecurity Threat Intelligence IPs feed periodically pulls IP Addresses from Resecurity. The API does not allow to filter by date, but the entries are sorted chronologically. New pages are requested as long as `.last_seen_date` of the last returned entry is greater than feed run start date.

`GET https://app.resecurity.com/api/ip/index`

Request Parameters:

```
{
  "query": "46.166.165.98/28",
  "per-page": 20,
  "page": 1
}
```

Sample Response:

```
[
  {
    "id": 121332481,
    "ip": "46.166.165.101",
    "first_seen_date": 1509731402,
    "last_seen_date": 1759234202,
    "risk_score": 25,
    "flags": [
      2,
      8
    ],
    "highRiskLevelReason": "IP is not high-risk",
    "risk_level": 0,
    "location": {
      "country": "lt",
      "as_number": 16125,
      "as_org": "UAB Cherry Servers",
      "city": "Jonava",
      "isp": "UAB Cherry Servers"
    },
    "malicious_activity": [
      {
        "feed": {
          "id": 27,
          "source": "IP2Location (Proxy)",
          "last_sync": 1510580872
        },
        "malware": {
          "id": 1877,
          "name": "Data Center or Hosting",
          "description": null,
          "alias": [
            "data center or hosting"
```

```
          ]
        },
        "last_seen_date": 1510223401
      }
    ],
    "vpn_related_domains": [
      "vpn.blackvpn.lt"
    ],
    "vpn_related_ips": [
      "162.219.178.234",
      "5.254.125.106"
    ],
    "references": {
      "total_count": 1,
      "modules": [
        {
          "module_title": "Detections",
          "module_id": 1,
          "total_count": 1,
          "module_search_url": "https://app.resecurity.com/search/index?
PostSearch[query]=46.166.165.101",
          "results": [
            {
              "id": 696371067,
              "date": "9 years ago",
              "snippet": " ... :23 INFO [net] From: 2b8c4dba |
46.166.165.101/46.166.165.101:30303 Recv: [DISCONNECT reason=TOO_MANY_PEERS ...
"
            }
          ]
        }
      ]
    }
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.ip`	Indicator.Value	IP Address	`.first_seen_date`	`46.166.165.101`	N/A
`.risk_score`	Indicator.Attribute	Risk Score	`.first_seen_date`	`25`	User-configurable. Updatable.
`.risk_level`	Indicator.Attribute	Risk Level	`.first_seen_date`	`0`	User-configurable. Updatable.
`.last_seen_date`	Indicator.Attribute	Last Seen	`.first_seen_date`	`2025-09-24 18:25:36+00:00`	User-configurable. Updatable. Formated to human-readable date.
`.location.country`	Indicator.Attribute	Country Code	`.first_seen_date`	`LT`	User-configurable. Uppercase.
`.location.city`	Indicator.Attribute	City	`.first_seen_date`	`Jonava`	User-configurable.
`.location.as_number`	Indicator.Attribute	ASN	`.first_seen_date`	`16125`	User-configurable.
`.location.as_org`	Indicator.Attribute	AS Organization	`.first_seen_date`	`UAB Cherry Servers`	User-configurable.
`.location.ips`	Indicator.Attribute	ISP	`.first_seen_date`	`UAB Cherry Servers`	User-configurable.
`.vpn_related_domains`	Related Indicator	FQDN	`.first_seen_date`	`vpn.blackvpn.lt`	User-configurable.
`.vpn_related_ips`	Related Indicator	IP Address	`.first_seen_date`	`162.219.178.234`	User-configurable.

The following paths are added to the indicator's description:

- `.highRiskLevelReason`
- `malicious_activity[].feed.source`
- `malicious_activity[].malware.alias[]`
- `malicious_activity[].last_seen_date`
- `references.total_count`
- `references.modules[].module_title`
- `references.modules[].total_count`
- `references.modules[].module_search_url`

Resecurity Threat Intelligence Domains

The Resecurity Threat Intelligence Domains feed periodically pulls FQDNs from Resecurity. The API does not allow to filter by date, but the entries are sorted chronologically. New pages are requested as long as `.last_seen_date` of the last returned entry is greater than feed run start date.

`GET https://app.resecurity.com/api/domain/index`

Request Parameters:

```
{
  "query": "we*",
  "per-page": 20,
  "page": 1
}
```

Sample Response:

```
[
  {
    "id": 35196838,
    "domain": "we11point.com",
    "first_seen_date": 1447880834,
    "last_seen_date": 1757878382,
    "risk_score": 25,
    "flags": [
      1
    ],
    "whois_status": 1,
    "dns_status": 1,
    "highRiskLevelReason": "Domain is not high-risk",
    "risk_level": 0,
    "references": {
      "total_count": 9,
      "modules": [
        {
          "module_title": "Detections",
          "module_id": 1,
          "total_count": 9,
          "module_search_url": "https://app.resecurity.com/search/index?
PostSearch[query]=we11point.com",
          "results": [
            {
              "id": 726708347,
              "date": "8 years ago",
              "snippet": " hhh u4wz2KL4 Airelle-hrsk.txt ! Title: Airelle-
hrsk.txt ! Liste anti-risk bloquant l'accès à 51886 sites à possible contenu
dangereux ! © Airelle – http://rlwpx.free.fr/WPFF/hosts.htm – 05.03.2017 !
Diffusion et utilisation libres sous réserve de  ... "
            },
            {
```

```
              "id": 703196895,
              "date": "9 years ago",
              "snippet": " ...  https://www.passivetotal.org/passive/
we11point.com https://www.passivetotal.org/passive ... "
            },
            {
              "id": 148761890,
              "date": "10 years ago",
              "snippet": " ...  мошенники использовали поддельное доменное имя
we11point.com (ранее бренд WellPoint использовался компанией ...  used the
counterfeit domain name we11point.com (earlier the brand of WellPoint ... "
            },
            {
              "id": 43214536,
              "date": "10 years ago",
              "snippet": " ...  мошенники использовали поддельное доменное имя
we11point.com (ранее бренд WellPoint использовался компанией ... "
            },
            {
              "id": 54501490,
              "date": "10 years ago",
              "snippet": " ...  мошенники использовали поддельное доменное имя
we11point.com (ранее бренд WellPoint использовался компанией ...  used the
counterfeit domain name we11point.com (earlier the brand of WellPoint ... "
            }
          ]
        }
      ]
    }
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.domain`	Indicator.Value	FQDN	`.first_seen_date`	`we11point.com`	N/A
`.risk_score`	Indicator.Attribute	Risk Score	`.first_seen_date`	`25`	User-configurable. Updatable.
`.risk_level`	Indicator.Attribute	Risk Level	`.first_seen_date`	`0`	User-configurable. Updatable.
`.last_seen_date`	Indicator.Attribute	Last Seen	`.first_seen_date`	`2025-09-24 18:25:36+00:00`	User-configurable. Updatable. Formated to human-readable date.

The following paths are added to the indicator's description:

- `.highRiskLevelReason`
- `references.total_count`
- `references.modules[].module_title`
- `references.modules[].total_count`
- `references.modules[].module_search_url`

Resecurity Threat Intelligence Incidents

The Resecurity Threat Intelligence Incidents feed periodically pulls Incidents from Resecurity and ingests them as ThreatQ Events. Incident filtering is available by date, but it's day-specific—the API disregards the hours, minutes, and seconds.

`GET https://app.resecurity.com/api/incident/index`

Request Parameters:

```
{
  "query": "SQL",
  "per-page": 20,
  "page": 1,
  "date_from": "2025-07-20",
  "date_to": "2025-07-21"
}
```

Sample Response:

```
[
  {
    "id": 263488,
    "date": "2025-08-20",
    "name": "Advanced Blending Solutions",
    "description": "Advanced Blending Solutions is a leading designer,
manufacturer, and supplier of blending and ...",
    "confidence_score": null,
    "tlp": 0,
    "risk_score": 50,
    "target_geo": [
      "British Indian Ocean Territory",
      "India"
    ],
    "target_industries": [
      "Finance"
    ],
    "references": [
      "https://www.cyfirma.com/research/finstealer/"
    ],
    "tags": [
      "phishing",
      "c2 servers"
    ],
    "status": 1,
    "created_at": 1755706673,
    "updated_at": 1755706673,
    "categories": [
      {
        "id": 5,
        "name": "Ransomware"
```

```
    }
  ],
  "ioc_hashes": [
    {
      "id": 10254851,
      "hash": "9d0460f69ed87ee3580c51c4b7c7ed1d",
      "type": 0,
      "created_at": 1739794841
    }
  ],
  "malicious_activity_ips": [
    {
      "id": 1106476,
      "ip": "92.113.19.132",
      "created_at": 1739794841,
      "type": 2
    }
  ],
  "malicious_activity_domains": [
    {
      "id": 523163,
      "name": "mysql-auth.pl",
      "type": 6,
      "created_at": 1580221624
    }
  ],
  "malicious_activity_emails": [
    {
      "id": 19798,
      "email": "mobile.mailer1@proton.me",
      "created_at": 1759227353
    }
  ],
  "victim_information_ips": [
    {
      "id": 234639,
      "ip": "193.151.29.21",
      "created_at": 1528529256,
      "type": 2
    }
  ],
  "victim_information_domains": [
    {
      "id": 467043,
      "name": "www.suffolk.gov.uk",
      "type": 7,
      "created_at": 1553277977
    }
  ],
  "victim_information_emails": [
```

```
      {
        "id": 19798,
        "email": "john.doe@proton.me",
        "created_at": 1759227353
      }
    ]
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.name`	Event.Title	Incident	`.created_at`	`Advanced Blending Solutions`	N/A
`.tags`	Event.Tags	N/A	N/A	`phishing`	N/A
`.tlp`	Event.TLP	N/A	N/A	`WHITE`	See `Incident TLP Mapping`
`.risk_score`	Event.Attribute	Risk Score	`.created_at`	`25`	User-configurable. Updatable.
`.updated_at`	Event.Attribute	Modified Date	`.created_at`	`2025-09-24 18:25:36+00:00`	User-configurable. Updatable. Formated to human-readable date.
`.target_geo`	Event.Attribute	Target Location	`.created_at`	`India`	User-configurable.
`.target_industries`	Event.Attribute	Target Industry	`.created_at`	`Finance`	User-configurable.
`.categories[].name`	Event.Attribute	Category	`.created_at`	`Ransomware`	User-configurable.
`.status`	Event.Attribute	Status	`.created_at`	`Active`	User-configurable. Updatable. See `Incident Status Mapping`
`.ioc_hashes[].hash`	Related Indicator.Value	MD5/SHA-1/SHA-256/ sha-384/SHA-512	`.ioc_hashes[].created_at`	`9d0460f69ed87ee3580c51c4b7c7ed1d`	User-configurable. Type computed based on length.
`.malicious_activity_ips[].ip`	Related Indicator.Value	IP Address/IPv6 Address	`.malicious_activity_ips[].created_at`	`92.113.19.132`	User-configurable. Type computed based on format.
`.victim_information_ips[].ip`	Related Indicator.Value	IP Address/IPv6 Address	`.victim_information_ips[].created_at`	`193.151.29.21`	User-configurable. Type computed based on format.
`.malicious_activity_domains[].name`	Related Indicator.Value	FQDN	`.malicious_activity_domains[].created_at`	`mysql-auth.pl`	User-configurable.
`.victim_information_domains[].name`	Related Indicator.Value	FQDN	`.malicious_activity_domains[].created_at`	`www.suffolk.gov.uk`	User-configurable.
`.malicious_activity_emails[].email`	Related Indicator.Value	Email Address	`.malicious_activity_emails[].created_at`	`mobile.mailer1@proton.me`	User-configurable.
`.victim_information_emails[].email`	Related Indicator.Value	Email Address	`.victim_information_emails[].created_at`	`john.doe@proton.me`	User-configurable.

The following paths are added to the event's description:

- `.description`
- `references`

Incident TLP Mapping

RESECURITY TLP	THREATQ TLP
0	WHITE
1	GREEN
2	AMBER
3	RED

Incident Status Mapping

RESECURITY STATUS	THREATQ STATUS ATTRIBUTE
0	Inactive
1	Active
2	Finished

Resecurity Threat Intelligence DarkWeb

The Resecurity Threat Intelligence DarkWeb feed periodically pulls DarkWeb posts from Resecurity and ingests them as ThreatQ events. The API does not allow to filter by date, but the entries are sorted chronologically. New pages are requested as long as `.timestamp` of the last returned entry is greater than feed run start date.

The value of the user configuration `Search Query` is search in the fields `.post` and `.resource_name`.

`GET https://app.resecurity.com/api/dark-web/index`

Request Parameters:

```
{
  "query": "voodoo",
  "per-page": 20,
  "page": 1
}
```

Sample Response:

```
[
  {
    "id": 2187714561,
    "snippet": "...  {Burnin' Sky} 1977 57. b>Voodoo/b> ( Queen) {The Cosmos
Rocks} ...  | 10,25 MB | 57. b>Voodoo/b> ... ",
    "resource_name": "bestblackhatforum.com",
    "url": "https://bestblackhatforum.com/Thread-Get-EaseUS-Video-Editor-
Lifetime-License-79-95?page=48",
    "country": "us",
    "language": "en",
    "actor": "Burnly",
    "title": "[Get] EaseUS Video Editor - Lifetime License $79.95",
    "post": "Thanks for sharing",
    "timestamp": 1759400160,
    "source": "Dark Web",
    "category": "Cybercrime"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Event.Title	Sighting	`.timestamp`	`DarkWeb Post: [Get] EaseUS Video Editor - Lifetime License $79.95`	Prepended with `DarkWeb Post:`
`.country`	Event.Attribute	Country Code	`.timestamp`	`US`	User-configurable. Uppercase.
`.language`	Event.Attribute	Language	`.timestamp`	`en`	User-configurable.
`.source`	Event.Attribute	Source	`.timestamp`	`Dark Web`	User-configurable.
`.category`	Event.Attribute	Category	`.timestamp`	`Cybercrime`	User-configurable.
`.resource_name`	Related Indicator.Value	FQDN	`.timestamp`	`bestblackhatforum.com`	User-configurable.
`.actor`	Related Adversary.Name	Adversary	`.timestamp`	`Burnly`	User-configurable.

The following paths are added to the indicator's description:

- `.snippet`
- `.resource_name`
- `.url`
- `.country`
- `.language`
- `.actor`
- `.post`
- `.timestamp`

Resecurity Threat Intelligence Alerts

The Resecurity Threat Intelligence Alerts feed periodically pulls alerts from Resecurity and ingests them as ThreatQ Incidents. A query can be used to limit the amount of data that is ingested. This endpoint does not offer support for filtering by date.

`GET https://app.resecurity.com/api/alert/index`

Request Parameters:

```
{
  "query": "yandex.ru",
  "per-page": 20,
  "page": 1
}
```

Sample Response:

```
[
  {
    "category": {
      "id": 15,
      "name": "Threat Actor"
    },
    "confidence_score": 1,
    "content": "p>There was identified underground shop in TOR network, selling
compromised credit cards. /p>",
    "for_splunk": {
      "email": "john@yahoo.com",
      "ip": "1.1.1.1"
    },
    "geography": [
      "al",
      "dz"
    ],
    "id": 123,
    "ioc": {
      "actor_name": "Actor11",
      "add_date": 1495442554,
      "analysis_date": 1495443267,
      "detection_ratio": "52 / 58",
      "file_name": "WannaCry.infected",
      "file_type": "Win32 EXE",
      "id": 6811735,
      "item_url": "https://app.resecurity.com/ioc?IocSearch[id]=6811735",
      "malware_name": "Trojan-Ransom.Win32.Wanna.b",
      "md5": "84c82835a5d21bbcf75a61706d8ab549",
      "sha256":
"ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa",
      "update_date": 1495444010
    },
```

```
    "risk_score": 25,
    "subject": "Jocker/Stash Underground Shop (~300 CNB Credit Cards)",
    "tags": "tag1,tag2,tag3",
    "threat_actors": "Actor1,Actor2,Actor3",
    "tlp_status": "Red",
    "updated_at": "1506790365",
    "ttp": [
      {
        "name": "Apache - Arbitrary Long HTTP Headers Denial of Service ©",
        "id": 345,
        "exploit_type": "dos",
        "exploit_source_code": "code",
        "exploit_port": 80,
        "exploit_platform": "windows",
        "exploit_file": "platforms/linux/dos/371.c",
        "exploit_date": "2004-08-02T00:00:00.000+0000",
        "exploit_actor": "anonymous",
        "description": "Apache - Arbitrary Long HTTP Headers Denial of Service
©span class=\"table__detail\">linux, dos, 0/span>",
        "category": "Exploit"
      }
    ]
  }
]
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.subject`	Incident.Value	Incident	N/A	`Alert: Jocker/Stash Underground Shop ...`	Prepended with `Alert:`
`.tags`	Incident.Tags	N/A	N/A	`tags1`	N/A
`.tlp_status`	Incident.TLP	N/A	N/A	`RED`	N/A
`.category.name`	Incident.Attribute	Category	N/A	`Threat Actor`	User-configurable.
`.confidence_score`	Incident.Attribute	Confidence Score	N/A	`1`	User-configurable. Updatable.
`.risk_score`	Incident.Attribute	Risk Score	N/A	`25`	User-configurable. Updatable.
`.updated_at`	Incident.Attribute	Modified Date	N/A	`2025-09-24 20:20:18+00:00`	User-configurable. Updatable. Formated to human-readable date.
`.geography`	Incident.Attribute	Geography	N/A	`al`	User-configurable.
`.ttp[].exploit_file`	Related Indicator.Value	File Path	`.ttp[].exploit_date`	`platforms/linux/dos/371.c`	User-configurable.
`.ttp[].description`	Related Indicator.Description	N/A	N/A	`Apache - Arbitrary Long HTTP ...`	Description for File Path.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.ttp[].exploit_platform`	Related Indicator.Attribute	Platform	`.ttp[].exploit_date`	`windows`	Attribute for File Path.
`.ttp[].exploit_type`	Related Indicator.Attribute	Type	`.ttp[].exploit_date`	`dos`	Attribute for File Path.
`.ioc.actor_name`	Related Adversary.Name	Adversary	N/A	`Actor11`	User-configurable.
`.ioc.malware_name`	Related Malware.Value	Malware	N/A	`Trojan-Ransom.Win32.Wanna.b`	User-configurable.
`.ioc.sha256`	Related Indicator.Value	SHA-256	`.ioc.add_date`	`ed01ebfbc9eb5bbea545af4d01bf5f10...`	User-configurable.
`.ioc.item_url`	Related Indicator.Description	N/A	N/A	`Resecurity Link`	Formated using HTML <a> tag. Description of SHA-256.
`.ioc.file_type`	Related Indicator.Attribute	File Type	`.ioc.add_date`	`Win32 EXE`	User-configurable. Attribute for SHA-256.
`.ioc.detection_ratio`	Related Indicator.Attribute	Detection Ratio	`.ioc.add_date`	`52 / 58`	User-configurable. Updatable. Attribute for SHA-256.
`.ioc.analysis_date`	Related Indicator.Attribute	Last Analysis Date	`.ioc.add_date`	`2025-09-24 18:25:36+00:00`	User-configurable. Updatable. Formated to human-readable date. Attribute for SHA-256.
`.ioc.update_date`	Related Indicator.Attribute	Modified Date	`.ioc.add_date`	`2025-09-24 20:20:18+00:00`	User-configurable. Updatable. Formated to human-readable date. Attribute for SHA-256.
`.ioc.file_name`	Related Indicator.Value	Filename	`.ioc.add_date`	`WannaCry.infected`	User-configurable.
`.ioc.md5`	Related Indicator.Value	MD5	`.ioc.add_date`	`W84c82835a5d21bbcf75a61706d8ab549`	User-configurable.

The following paths are added to the report's description:

- `.category.name`
- `.confidence_score`
- `.geography`
- `.updated_at`
- `.content`

Average Feed Run

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

Resecurity Threat Intelligence Botnets

METRIC	RESULT
Run Time	1 minute
Indicators	10
Malware	9
Malware Attributes	53

Resecurity Threat Intelligence IOCs

METRIC	RESULT
Run Time	2 minute
Indicators	100
Indicator Attributes	400
Malware	100

Resecurity Threat Intelligence IPs

METRIC	RESULT
Run Time	10 minutes
Indicators	100
Indicator Attributes	800

Resecurity Threat Intelligence Domains

METRIC	RESULT
Run Time	10 minutes
Indicators	100
Indicator Attributes	800

Resecurity Threat Intelligence Incidents

METRIC	RESULT
Run Time	2 minutes
Indicators	49
Indicator Attributes	250

Resecurity Threat Intelligence DarkWeb

METRIC	RESULT
Run Time	10 minutes
Event	100
Event Attributes	400

Resecurity Threat Intelligence Alerts

METRIC	RESULT
Run Time	1 minute
Indicators	1
Indicator Attributes	4
Incidents	1
Incident Attributes	5
Malware	1
Adversary	1

Known Issues / Limitations

- **Resecurity Threat Intelligence Botnets** feed - ThreatQ will only display the most recent entry when a botnet has multiple entries.
- All the API endpoints utilized by this integration may occasionally return a `524 Error Status Code` when querying large data volumes. The recommended workaround is to use the **Search Query** user configuration parameter to limit the amount of ingested data.

Change Log

- **Version 1.0.0**
  - Initial release