

ThreatQuotient



Intel 471 Reports CDF User Guide

Version 2.0.0

September 26, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
All Feeds	8
Intel 471 Reports Feed - Additional Parameters	10
Intel 471 Spot Reports Feed Additional Parameters	11
Intel 471 Breach Alerts Feed	11
ThreatQ Mapping.....	13
Intel 471 Reports.....	13
Intel 471 Spot Reports.....	17
Intel 471 Breach Alerts	19
Shared Table Mapping	21
Average Feed Run.....	24
Intel 471 Reports.....	24
Intel 471 Spot Reports.....	25
Intel 471 Breach Alerts	25
Known Issues / Limitations	26
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 © 2023 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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.0.0
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Intel 471 Reports CDF returns a list of Information Reports or Intel Reports matching filter criteria ordered by creation date descending (the most recent are on the top).

The integration provides the following feeds:

- **Intel 471 Reports** - ingests reports and relevant context from intelligence streams.
- **Intel 471 Breach Alerts** - ingests reports & relevant context from the Breach Alerts intelligence stream.
- **Intel 471 Spot Reports** - ingests reports and relevant context from the Spot Reports intelligence stream.

The integration ingests the following system objects:

- Adversaries
 - Adversary Attributes
- Attack Patterns
- Indicators
 - Indicator Attributes
- Malware
- Reports
 - Report Attributes

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 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.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

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

Configuration



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

All Feeds

PARAMETER	DESCRIPTION
Email Address	Your Intel 471 account email address.
API Key	Your Intel 471 account API key.
Count per Page	The maximum number of records to retrieve from the provider per request (0-100). The default value is 10.
Fetch GIR names	When disabled, GIRs will be left in their raw format (i.e. 3.1.1). When enabled, GIR names will be fetched and used (i.e. 5.2.1 - Initial access tactic).
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: <ul style="list-style-type: none"> ◦ Actors Subject of Report (default) ◦ Handles (Adversaries) ◦ Malware Families (default)
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include:

PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ Malicious URLs (default) ◦ Malicious Domains (default) ◦ IP Addresses (default) ◦ CVE IDs (default) ◦ MD5 Hashes (default) ◦ SHA-1 Hashes (default) ◦ SHA-256 Hashes (default) ◦ Actor Domains ◦ Actor Websites ◦ File Paths ◦ Email Addresses ◦ Jabber Usernames ◦ Telegram Usernames
URL Status (Non-Malicious)	<p>Select the status to use for URLs. Options include:</p> <ul style="list-style-type: none"> ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted <div>  <p>The default setting is Indirect as these are typically are not malicious.</p> </div>
Actor Domain Status	<p>Select the status to use for actor domains. Options include:</p> <ul style="list-style-type: none"> ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted <div>  <p>The default setting is Indirect as these are typically are not malicious.</p> </div>
Actor Website Status	<p>Select the status to use for actor websites. Options include:</p> <ul style="list-style-type: none"> ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted <div>  <p>The default setting is Indirect as these are typically are not malicious.</p> </div>

Intel 471 Reports Feed - Additional Parameters

PARAMETER	DESCRIPTION
Report Location	Display reports related to a certain country or region. Examples: "European Union" (as a region), "United Kingdom" (as a country). The feed can only search for one location at a time.
Report Tag	Display reports related to a certain tag. Examples: "Banking & Finance", "Tools", "Airlines", "Phishing", "Spam", "Credit Card Fraud". The feed can only search for one tag at a time.
Report Type Filter	<p>Select which report types to ingest into ThreatQ when the Fetch Related Reports parameter is enabled. Options included:</p> <ul style="list-style-type: none"> ◦ Info Reports (default) ◦ Breach Reports (default) ◦ Intelligence Bulletins (default) ◦ Underground Pulses (default) ◦ Threat Briefs (default) ◦ Whitepapers (default) ◦ Intelligence Summaries (default) ◦ Malware Campaigns (default) ◦ Actor Profiles (default)
Fetch Related Reports	When true, related reports will be fetched, parsed, and ingested. This will require additional API calls. This may increase the chances of timeout errors. This parameter is disabled by default.
Related Report Family Filter	<p>Select which report types to ingest into ThreatQ when the Fetch Related Reports parameter is enabled. Options included:</p> <ul style="list-style-type: none"> ◦ Info Reports (default) ◦ Finished Intelligence (default) ◦ Spot Reports (default)
Attribute Filter	<p>Select the context to ingest into the ThreatQ platform. Options included:</p> <ul style="list-style-type: none"> ◦ GIRs ◦ Victims (default) ◦ Motivations (default)


PARAMETER	DESCRIPTION
	<ul style="list-style-type: none"> ◦ Region Information (default) ◦ Country Information (default) ◦ Admiralty Codes (default) ◦ Source Characterization ◦ Sensitive Source ◦ Portal URL (default)
Ingest Tags	Enable this parameter to ingest tags.

Intel 471 Spot Reports Feed Additional Parameters

PARAMETER	DESCRIPTION
Search Query	Query for spot reports using this free text search field.
Victim Name	Optional - Search for spot reports related to a certain victim. You can only search for one victim at a time.
Attribute Filter	<p>Select the context to ingest into the ThreatQ platform. Options included:</p> <ul style="list-style-type: none"> ◦ GIRs ◦ Victims ◦ Victim Industries ◦ Victim Countries ◦ Confidence Level ◦ First Activity Date ◦ Last Activity Date

Intel 471 Breach Alerts Feed

PARAMETER	DESCRIPTION
Search Query	Query for breach alerts using this free text search field.
Victim Name	Optional - Search for breach alerts related to a certain victim. You can only search for one victim at a time.

PARAMETER	DESCRIPTION
Confidence Level	Search for breach alerts of a certain confidence level. You can only search for one confidence level at a time. The default value is high.
Actor / Group	Search for breach alerts pertaining to a specific actor or group. <div>  You can only search for one confidence level at a time. </div>
Attribute Filter	Select the context to ingest into the ThreatQ platform. Options included: <ul style="list-style-type: none"> ◦ GIRs ◦ Victims ◦ Confidence Level ◦ First Activity Date ◦ Last Activity 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

Intel 471 Reports

The Intel 471 Reports feed ingests reports & relevant context/attribution from the following intelligence streams:

- Info Reports
- Finished Intelligence
 - Breach Reports
 - Intelligence Bulletins
 - Underground Pulses
 - Threat Briefs
 - Whitepapers
 - Intelligence Summaries
 - Malware Campaigns
 - Actor Profiles



The feed will ingest related reports, if enabled, which may also include Spot Reports.

GET `https://api.intel471.com/v1/reports`

GET `https://api.intel471.com/v1/reports/{{ uid }}`

Sample Response:

```
{
  "uid": "cf1d3297dba669b0cbf13c275f973135cd27a4de279899aadb4f7cbde80e04c7",
  "documentFamily": "INFOREP",
  "documentType": "INFOREP",
  "admiraltyCode": "B2",
  "motivation": ["CC"],
  "subject": "Russian actor, bulletproof hoster yalishanda (aka downlow, stas_vl) adds 12 front-end proxies to fast-flux offering; Current proxy-net size sits at 250 IP addresses",
  "created": 1686921777000,
  "dateOfInformation": 1686873600000,
  "sourceCharacterization": "Information was derived from a reliable source in direct contact with yalishanda and visibility into the actor's bulletproof hosting service.",
  "relatedReports": [
    {
      "uid": "63c31296bcb43fd226513fb15bb1db08a76dd36d8c3cbb30b434a4d0beab4210",
      "documentFamily": "INFOREP"
    },
    {

```

```

        "uid":
"1c895446738ca1280fae73fb1ba3219480a606e469f543ab985a05b1155585c3",
        "documentFamily": "INFOREP"
    },
    ],
    "entities": [
        {
            "type": "SHA256",
            "value":
"4c9b551910643eb2c5a4adaf517f41cf1c5035c1526b11f108accd970e675e31"
        },
        {
            "type": "MaliciousDomain",
            "value": "amazo-ne.com-system-1359650.xyz"
        },
        {
            "type": "MaliciousDomain",
            "value": "amazo-ne.com-system-7558190.xyz"
        },
        {
            "type": "MaliciousDomain",
            "value": "babypetstore.shop"
        },
        {
            "type": "IPAddress",
            "value": "109.234.38.205"
        },
        {
            "type": "Handle",
            "value": "yalishanda"
        }
    ],
    "locations": [
        {
            "region": "Oceania",
            "country": "Australia",
            "link": "impacts"
        },
        {
            "region": "North America",
            "country": "Canada",
            "link": "impacts"
        },
        {
            "region": "Europe",
            "country": "Germany",
            "link": "impacts"
        },
        {
            "region": "Europe",

```

```

        "country": "Netherlands",
        "link": "impacts"
    },
    {
        "region": "Europe",
        "country": "Russia",
        "link": "impacts"
    },
    {
        "region": "Europe",
        "country": "United Kingdom",
        "link": "impacts"
    },
    {
        "region": "North America",
        "country": "United States",
        "link": "impacts"
    },
    {
        "region": "Europe",
        "country": "Russia",
        "link": "originated_from"
    }
],
"tags": [
    "Banking & Finance",
    "Bulletproof Hosting",
    "Bulletproof Hosting Tracking",
    "Extortion",
    "Malware - Usage",
    "Phishing",
    "Ransomware"
],
"portalReportUrl": "https://titan.intel471.com/report/inforep/
0d7f4312db15947e3ac8e330a8e55175",
"lastUpdated": 1686921779000,
"actorSubjectOfReport": [
    {
        "handle": "yalishanda"
    }
],
"classification": {
    "intelRequirements": ["3.1.1"]
},
"reportAttachments": [
    {
        "url": "https://api.intel471.com/v1/reports/download/
0d7f4312db15947e3ac8e330a8e55175/
d7481f4c2a545304d4d806d586a62bc53c0f33ed2b39ea35066d424f48957dd0",
        "fileName": "2023-06-16_yalishanda.csv",
    }
]

```

```
    "malicious": false,
    "mimeType": "text/csv",
    "fileSize": 955544
  }
],
"researcherComments": "<p>[Redacted]</p>",
"executiveSummary": "<p>As of 10 a.m. GMT, June 16, 2023, the actor
<strong>yalishandaâ€™sÂ </strong>fast-flux network stands at 250 total hosts.
There were 12 hosts added to the network in the last 24 hours, while 15
hosts were dropped during this period.</p><p>The actor hosted phishing
campaigns targeting Amazon and National Australia Bank (NAB) customers, and
PrivateLoader malware samples.</p>"
}
```



The mapping for this feed is defined in the [Shared Table Mapping](#) section.

Intel 471 Spot Reports

The Intel471 Spot Reports feed ingests reports and relevant context/attribution from the Spot Reports intelligence stream.

GET <https://api.intel471.com/v1/spotReports>

GET <https://api.intel471.com/v1/spotReports/{{ uid }}>

Sample Response:

```
{
  "activity": {
    "first": 1646665224000,
    "last": 1646747082000
  },
  "last_updated": 1646747082000,
  "uid": "053ba72b1878c5b43241037a18cc781d",
  "data": {
    "spot_report": {
      "uid": "053ba72b1878c5b43241037a18cc781d",
      "spot_report_data": {
        "related_reports": [
          "94fa5d7114312f942173821ab0cc8458",
          "99313d87ca836e9aaaf761cedd75c66f",
          "fc2300976c64b6e5b175e8c48e9a20bd"
        ],
        "victims": [
          {
            "name": "Saudia",
            "urls": ["http://www.saudia.com/"]
          }
        ],
        "date_of_information": 1646352000000,
        "text": "[POSSIBLE BREACH ALERT] On March 4, 2022, the actor behind the Telegram channel AnonyMous IslaMic at @anony_islamic claimed a data breach impacting the Saudi Arabia-based airline Saudia, formerly Saudi Arabian Airlines, at the saudia.com website. The post credited the actor The Yemeni Ghost for the breach and mentioned 2 GB of information allegedly was leaked. The actor also posted several resume files of Saudi citizens and a data sample that contained credit card information as proof of the breach, however, the information provided was insufficient to prove the claim.",
        "intel_requirements": [
          "5.5.3",
          "6.1.1.2",
          "6.2.5.11",
          "4.2.3",
          "4.2.5",
          "5.2.9",
          "5.2.11"
        ]
      }
    }
  }
}
```

```

    ],
    "version": "1",
    "links": [
      {
        "type": "internal",
        "url": "https://titan.intel471.com/ims_thread/
c8461bf13fca8a2b9912ab2eb1668e4b?message_uid=84e377651e5fbae47900c71e664a5cb3",
        "title": "Telegram post"
      }
    ],
    "released_at": 1646665224000,
    "title": "Actor The Yemeni Ghost claims data breach impacting Saudia"
  }
},
"entities": [
  {
    "type": "Telegram",
    "value": "@anony_islamic"
  },
  {
    "type": "Handle",
    "value": "AnonyMous IslaMic"
  },
  {
    "type": "Handle",
    "value": "The Yemeni Ghost"
  }
]
}
}

```



The mapping for this feed is defined in the [Shared Table Mapping](#) section after selecting the data within the `spot_report` key.

Intel 471 Breach Alerts

This feed ingests reports & relevant context/attribution from the Breach Alerts intelligence stream.

GET <https://api.intel471.com/v1/breachAlerts>

GET <https://api.intel471.com/v1/breachAlerts/{{ uid }}>

Sample Response:

```
{
  "activity": {
    "first": 1687264522000,
    "last": 1687268325000
  },
  "last_updated": 1687268325000,
  "uid": "4f38ec47e6a75e28c532171237b039cd",
  "data": {
    "breach_alert": {
      "date_of_information": 1686960000000,
      "confidence": {
        "level": "high",
        "description": "Assessment is based upon high-quality, corroborated
intelligence from trustworthy sources."
      },
      "intel_requirements": [
        "1.1.1",
        "1.2.2",
        "4.2.5",
        "5.2.9",
        "5.2.11",
        "5.2.12",
        "5.5.3",
        "5.5.4",
        "6.1.6.4",
        "6.2.6.5",
        "6.2.6",
        "6.1.6"
      ],
      "released_at": 1687264522000,
      "title": "Akron-Summit County Public Library possibly compromised by
actor/group Akira on Jun 17, 2023",
      "victim": {
        "name": "Akron-Summit County Public Library",
        "industries": [
          {
            "industry": "Education",
            "sector": "Public sector"
          }
        ]
      }
    }
  }
}
```

```

    "urls": ["http://www.akronlibrary.org/"],
    "country": "United States",
    "revenue": "US $25.8 Million",
    "region": "North America"
  },
  "summary": "<p>On June 17, 2023, Intel 471 collected a sample of the
Akira ransomware with the
57e4a5c937bc58b01622997ca2acaa91cea2ff5cc9e7f9c4c8bf82349c23e0a9 SHA-256. Our
monitoring of ransomware attacker communication revealed the sample likely was
used in an attack against the Ohio, U.S.-based Akron-Summit County Public
Library at the akronlibrary.org website. The perpetrators allegedly deployed
the ransomware on or about May 30, 2023, exfiltrated about 71.2 GB of data and
demanded US$ $300,000 in ransom. They also shared a complete listing of stolen
files with the victim as the proof of the claim.</p>",
  "actor_or_group": "Akira"
},
"entities": [
  {
    "type": "SHA256",
    "value":
"57e4a5c937bc58b01622997ca2acaa91cea2ff5cc9e7f9c4c8bf82349c23e0a9"
  },
  {
    "type": "Handle",
    "value": "Akira"
  },
  {
    "type": "BitcoinAddress",
    "value": "bc1ql5f3m75qx3ueu2pz5eeveyqsw6pdjs3ufk8r20"
  },
  {
    "type": "MalwareFamily",
    "value": "Akira"
  }
]
}

```



The mapping for this feed is defined in the [Shared Table Mapping](#) section after selecting the data within the breach_alert key.

Shared Table Mapping

All feeds share the same mapping table.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.subject, .title	Report Value, Adversary Name	N/A	N/A	N/A	
.activity.first	Report Attribute	First Activity	N/A	N/A	Updated at each run
.activity.last	Report Attribute	Last Activity	N/A	N/A	Updated at each run
.executiveSummary, .summary, .researcherComments, .rawTextTranslated, .rawText, .text, .links[], .sources[]	Report Description, Adversary Description	N/A	N/A	N/A	N/A
.rawText	Attack Pattern	N/A	N/A	N/A	TIDs are parsed & mapped
.victim.industries[]	Report Attribute	Victim Industry	N/A	Education	
.locations[].region	Report Attribute	{{ link }} Region	N/A	North America	N/A
.locations[].country	Report Attribute	{{ link }} Country	N/A	United States	N/A
.classification.intelRequirements[], .intel_requirements[]	Report Attribute	GIR	N/A	6.2.2.5 - {{ requirement }}	N/A
.actorSubjectOfReport.handle	Adversary	N/A	N/A	yalshinda	N/A
.actorSubjectOfReport.aliases[]	Adversary Attribute	Alias	N/A	N/A	N/A
.actor_or_group	Adversary	Adversary	N/A	yalshinda	N/A
.entities[]	Adversary	N/A	N/A	N/A	When type == Handle
.entities[]	Adversary Attribute	Bitcoin Address	N/A	bc1ql5f3m75qx3u eu2pz5eeveyqsw6 pdjs3ufk8r20	When type == BitcoinAddress
.entities[]	Related Indicator	FQDN	.published_at	N/A	When type == ActorDomain
.entities[]	Related Indicator	FQDN	.published_at	N/A	When type == ActorWebsite
.entities[]	Related Indicator	URL	.published_at	N/A	When type == MaliciousURL
.entities[]	Related Indicator	FQDN	.published_at	N/A	When type == MaliciousDomain
.entities[]	Related Indicator	CVE	.published_at	N/A	When type == CveID

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.entities[]	Related Indicator	IP Address	.published_at	N/A	When type == IPAddress
.entities[]	Related Indicator	Email Address	.published_at	N/A	When type == EmailAddress
.entities[]	Related Indicator	File Path	.published_at	N/A	When type == FileType
.entities[]	Related Indicator	Email Address	.published_at	N/A	When type == EmailAddress
.entities[]	Related Indicator	MD5	.published_at	N/A	When type == MD5
.entities[]	Related Indicator	SHA-1	.published_at	N/A	When type == SHA1
.entities[]	Related Indicator	SHA-256	.published_at	N/A	When type == SHA256
.entities[]	Related Indicator	URL	.published_at	N/A	When type == URL
.entities[]	Related Indicator	Username	.published_at	N/A	When type == Telegram
.entities[]	Related Indicator	Username	.published_at	N/A	When type == Jabber
.entities[]	Related Malware	N/A	N/A	ALPHV	When type == MalwareFamily
.victims[].name	Report Attribute	Victim	N/A	N/A	N/A
.tags[]	Report Tag	N/A	N/A	Actor Profile	N/A
.uid	Report Attribute	Report ID	N/A	N/A	N/A
.documentFamily	Report Attribute	Report Family	N/A	INFOREP	N/A
.documentType	Report Attribute	Report Type	N/A	MALWARE_CAMPAIGN	N/A
.sourceCharacterization	Report Attribute	Source	N/A	N/A	N/A
.portalReportUrl	Report Attribute	Portal URL	N/A	N/A	N/A
.motivation	Report Attribute	Motivation	N/A	CC	N/A
.victim.name	Report Attribute	Victim	N/A	N/A	N/A
.victim.country	Report Attribute	Victim Country	N/A	N/A	N/A
.confidence.level	Report Attribute	Confidence Level	N/A	medium	N/A
.sensitiveSource	Report Attribute	Sensitive Source	N/A	true	N/A
.admiraltyCode[0]	Report Attribute	Admiralty Reliability	N/A	A	N/A
.admiraltyCode[1]	Report Attribute	Admiralty Credibility	N/A	1	N/A
Telegram/Jabber	Indicator Attribute	Platform	N/A	N/A	Telegram or Jabber based on indicator type and if Telegram

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					Ustream or Jabber Ustream is selected in Indicator Filter

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.

Intel 471 Reports

METRIC	RESULT
Run Time	13 minutes
Adversaries	81
Adversary Attributes	500
Attack Patterns	42
Indicators	5,959
Indicator Attributes	18
Malware	55
Report	182
Report Attributes	5,974

Intel 471 Spot Reports

METRIC	RESULT
Run Time	1 minute
Malware	2
Reports	6
Report Attributes	35

Intel 471 Breach Alerts

METRIC	RESULT
Run Time	1 minute
Adversaries	14
Indicators	1
Malware	1
Report	43
Report Attributes	685

Known Issues / Limitations

- Feed runs of very long periods of time (ex. 7 months) might result in exceeding the offset limit, resulting in 412 errors. To avoid this, ThreatQuotient recommends running the feeds for shorter periods (ex. 24 hours) of time.



The number of reports for a defined period will also impact the allowed time period for a run.

Change Log

- **Version 2.0.0**
 - Updated minimum ThreatQ version to 5.6.0.
 - Added new Breach Alerts feed.
 - Added new Spot Reports feed.
 - Add support for the following document types:
 - Breach Reports
 - Intelligence Bulletins
 - Underground Pulses
 - Threat Briefs
 - Whitepapers
 - Intelligence Summaries
 - Malware Campaigns
 - Actor Profiles
 - Report descriptions are no longer truncated at 65k characters.
 - Added the option to fetch GIR human-readable names to use in attributes.
 - Added support for ingesting related malware family entries.
 - Added improved country/region attribution support.
 - Added support for the following entities: CVE, Malicious Domain, and specific username.
 - Added the following configuration fields:
 - Relationship Filter - all feeds
 - Report Type Filter - Intel 471 Reports feed.
 - Indicator Filter - all feeds.
 - Adds user field for selecting statuses for certain indicator types
 - URL Status (Non-Malicious) - all feeds
 - Actor Domain Status - all feeds
 - Actor Website Status - all feeds
 - Ingest Tags - Intel 471 Reports feed. Tags were previously ingested as attributes.
 - Added improved victim attribution support.
 - Added support for parsing MITRE ATT&CK techniques for Actor Profiles.
 - Resolved an issue where report titles containing 4-byte unicode characters would cause the feed to complete with errors.
 - Added performance updates to optimize feed runs and prevent rate limiting.
 - Added a new [known issue / limitation](#) regarding feed run time frames.
- **Version 1.1.1**
 - Resolved an issue that would occur when the **title** attribute was not included in the response.
- **Version 1.1.0**
 - Added new **Detailed Spot Report** supplemental feed call for SPOTREP reports.
 - Removed BREACH_ALERT reports to prevent 404 responses from Detailed Reports supplemental call.
 - Updated report descriptions to truncate at 32,630 characters.
- **Version 1.0.3**

-
- Fix added to handle an empty response from the supplemental feed.
 - **Version 1.0.2**
 - Updated report description.
 - **Version 1.0.1**
 - Created Indicators and Adversaries have the same attributes as the Report objects.
 - **Version 1.0.0**
 - Initial release.