ThreatQuotient

A Securonix Company

Intel 471 Reports CDF

Version 3.0.0

May 12, 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.

Copyright © 2026 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: 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	3.0.0
Compatible with ThreatQ Versions	>= 5.24.0
Support Tier	ThreatQ Supported

Introduction

The Intel 471 Reports CDF integration enables ThreatQ users to ingest and operationalize intelligence from Intel 471's report streams, providing access to a wide range of curated Information Reports and Intel Reports. Reports are retrieved based on user-defined filter criteria and are ordered by creation date, ensuring that the most recent intelligence is prioritized for analysis.

The integration provides the following feeds:

- **Intel 471 Breach Alerts** - queries the Intel 471 breach alert report stream and retrieves the complete details of each breach alert report using its unique identifier.
- **Intel 471 FINTEL Reports** - queries the Intel 471 FINTEL report stream and retrieves the complete details of each FINTEL report using its unique identifier.
- **Intel 471 Geopolitical Reports** - queries the Intel 471 geopolitical report stream and retrieves the complete details of each geopolitical report using its unique identifier.
- **Intel 471 Information Reports** - queries the Intel 471 information report stream and retrieves the complete details of each information report using its unique identifier.
- **Intel 471 Spot Reports** - queries the Intel 471 spot report stream and retrieves the complete details of each spot report using its unique identifier.

The integration ingests the following system objects:

- Adversary
  - Adversary Attributes
- Attack Pattern
  - Attack Pattern Attributes
- Indicator
  - Indicator Attributes
- Malware
  - Malware Attributes
- Report
  - Report Attributes

Prerequisites

The following is required to run the integration:

- An Intel471 Client ID
- An Intel471 Client Secret
- Here's a clearer, smoother rewording: MITRE ATT&CK attack patterns must already be ingested through a prior run of the MITRE ATT&CK CDF feeds for MITRE TIDs extracted from Actor Profiles to correctly map to their corresponding attack patterns. The MITRE ATT&CK CDF includes the following feeds:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE ICS ATT&CK

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
6. Select the individual feeds to install, when prompted, and click **Install**.

   > 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.

7. 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:

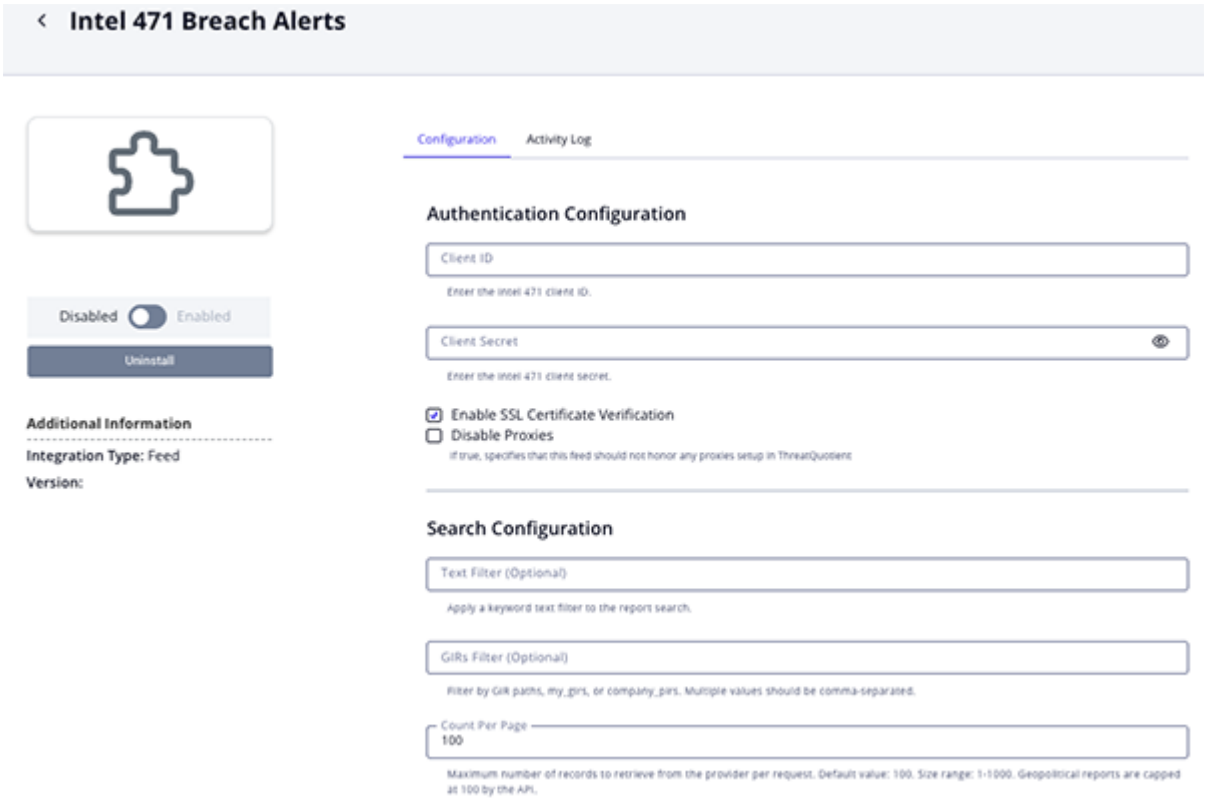
Intel 471 Breach Alerts Parameters

PARAMETER	DESCRIPTION
Client ID	Your Intel 471 Client ID.
Client Secret	Your Intel 471 Client Secret.
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.
Text Filter	Optional - enter a free-text value to filter the reports.
GIRs Filter	Optional - specify a GIR value to filter the reports.

PARAMETER	DESCRIPTION
Count per Page	The maximum number of records to retrieve from the provider per request (0-1000). The default value is 100.
Attribute Filter	Select the contextual attributes to ingest into ThreatQ. Options include: ◦ GIRs ◦ Victims *(default)* ◦ Confidence Level *(default)* ◦ Sensitive Source *(default)* ◦ Portal URL *(default)*
Ingest Tags	Enable this parameter to ingest tags into ThreatQ. This parameter is enabled by default.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report *(default)* ◦ Handles (Adversaries) ◦ Malware Families *(default)*
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include: ◦ Malicious URLs *(default)* ◦ Malicious Domains *(default)* ◦ IP Addresses *(default)* ◦ CVE IDs *(default)* ◦ Actor Websites ◦ URLs ◦ File Paths ◦ File Names ◦ Email Addresses ◦ Jabber Usernames

PARAMETER	DESCRIPTION
	◦ MD5 Hashes *(default)* ◦ SHA-1 Hashes *(default)* ◦ SHA-256 Hashes *(default)* ◦ Actor Domains ◦ Telegram Usernames
URL Status (Non-Malicious)	Select the status to use for URLs. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default)

PARAMETER	DESCRIPTION
	◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.



Intel 471 FINTEL Reports Parameters

PARAMETER	DESCRIPTION
Client ID	Your Intel 471 Client ID.
Client Secret	Your Intel 471 Client Secret.

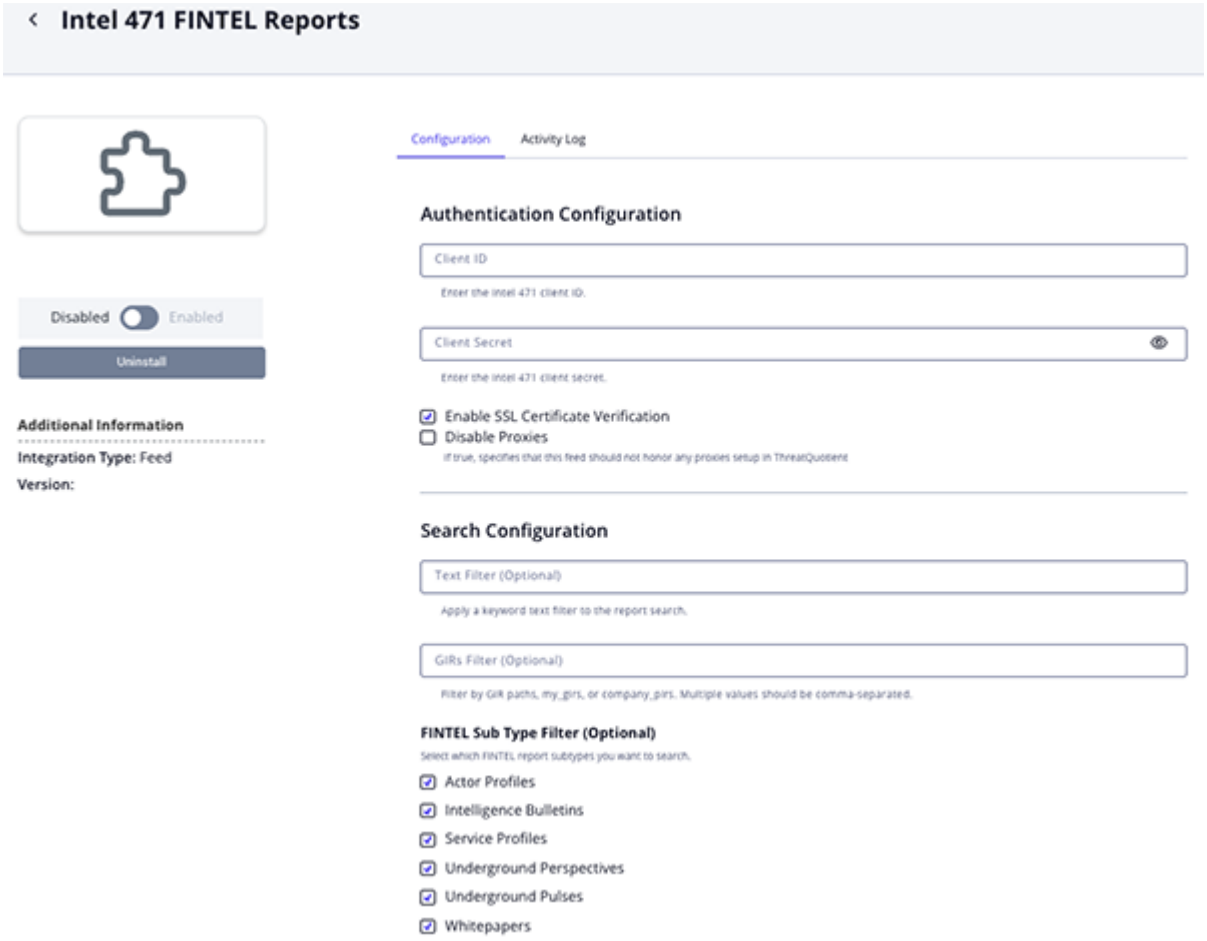
PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Text Filter	Optional - enter a free-text value to filter the reports.
GIRs Filter	Optional - specify a GIR value to filter the reports.
FINTEL Sub Type Filter	Optional - select which FINTEL report subtypes to search. Options include: ◦ Actor Profiles *(default)* ◦ Intelligence *(default)* ◦ Service Profiles *(default)* ◦ Underground Perspectives *(default)* ◦ Underground Pulses *(default)* ◦ Whitepapers *(default)* ◦ Threat Briefs *(default)* ◦ Breach Reports *(default)* ◦ Intelligence Summaries *(default)* ◦ Malware Campaigns *(default)* ◦ FINTEL Blogs *(default)*
Count per Page	The maximum number of records to retrieve from the provider per request (0-1000). The default value is 100.
Attribute Filter	Select the contextual attributes to ingest into ThreatQ. Options include:

PARAMETER	DESCRIPTION
	◦ GIRs ◦ Victims *(default)* ◦ Region Information ◦ Country Information *(default)* ◦ Admiralty Codes *(default)* ◦ Motivations *(default)* ◦ Source Characterization ◦ Sensitive Source ◦ Portal URL *(default)*
Ingest Tags	Enable this parameter to ingest tags into ThreatQ. This parameter is enabled by default.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report *(default)* ◦ Handles (Adversaries) ◦ Malware Families *(default)*
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include: ◦ Malicious URLs *(default)* ◦ Malicious Domains *(default)* ◦ IP Addresses *(default)* ◦ CVE IDs *(default)* ◦ MD5 Hashes *(default)* ◦ Actor Websites ◦ URLs ◦ File Paths ◦ File Names ◦ Email Addresses ◦ Jabber Usernames

PARAMETER	DESCRIPTION
	◦ SHA-1 Hashes *(default)* ◦ SHA-256 Hashes *(default)* ◦ Actor Domains ◦ Telegram Usernames
URL Status (Non-Malicious)	Select the status to use for URLs. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default) ◦ Active ◦ Review

PARAMETER	DESCRIPTION
	◦ Whitelisted

The default setting is **Indirect** as these are typically are not malicious.



Intel 471 Geopolitical Reports Parameters

PARAMETER	DESCRIPTION
Client ID	Your Intel 471 Client ID.
Client Secret	Your Intel 471 Client Secret.

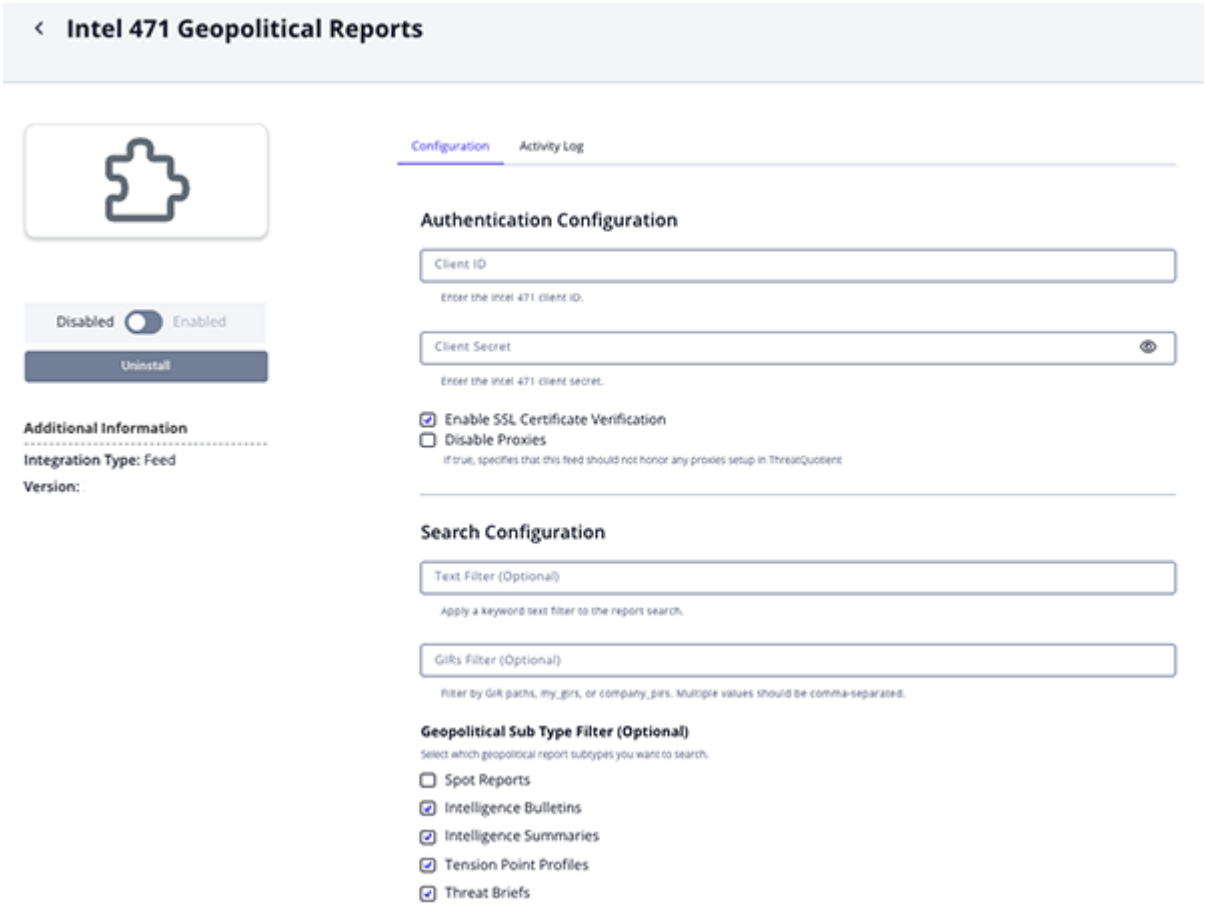
PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Text Filter	Optional - enter a free-text value to filter the reports.
GIRs Filter	Optional - specify a GIR value to filter the reports.
Geopolitical Sub Type Filter	Optional - select which geopolitical report subtypes to search. Options include: ◦ Spot Reports ◦ Intelligence Bulletins *(default)* ◦ Intelligence Summaries *(default)* ◦ Tension Point Profiles *(default)* ◦ Threat Briefs *(default)* ◦ Significant Activity Reports *(default)* ◦ Intelligence Estimates *(default)* ◦ Adversary Profiles *(default)*
Country	Optional - filter reports by country.
Report Location Country	Optional - filter reports by the country associated with the report's location.
Count per Page	The maximum number of records to retrieve from the provider per request (0-1000). The default value is 100.

PARAMETER	DESCRIPTION
Attribute Filter	Select the contextual attributes to ingest into ThreatQ. Options include: ◦ GIRs ◦ Victims *(default)* ◦ Region Information *(default)* ◦ Country Information *(default)* ◦ Sensitive Source ◦ Portal URL *(default)*
Ingest Tags	Enable this parameter to ingest tags into ThreatQ. This parameter is enabled by default.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report *(default)* ◦ Handles (Adversaries) ◦ Malware Families *(default)*
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include: ◦ Malicious URLs *(default)* ◦ Malicious Domains *(default)* ◦ IP Addresses *(default)* ◦ CVE IDs *(default)* ◦ MD5 Hashes *(default)* ◦ Actor Websites ◦ URLs ◦ File Paths ◦ File Names ◦ Email Addresses ◦ Jabber Usernames ◦ Telegram Usernames

PARAMETER	DESCRIPTION
	◦ SHA-1 Hashes *(default)* ◦ SHA-256 Hashes *(default)* ◦ Actor Domains
URL Status (Non-Malicious)	Select the status to use for URLs. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default) ◦ Active ◦ Review

PARAMETER	DESCRIPTION
	◦ Whitelisted

The default setting is **Indirect** as these are typically are not malicious.



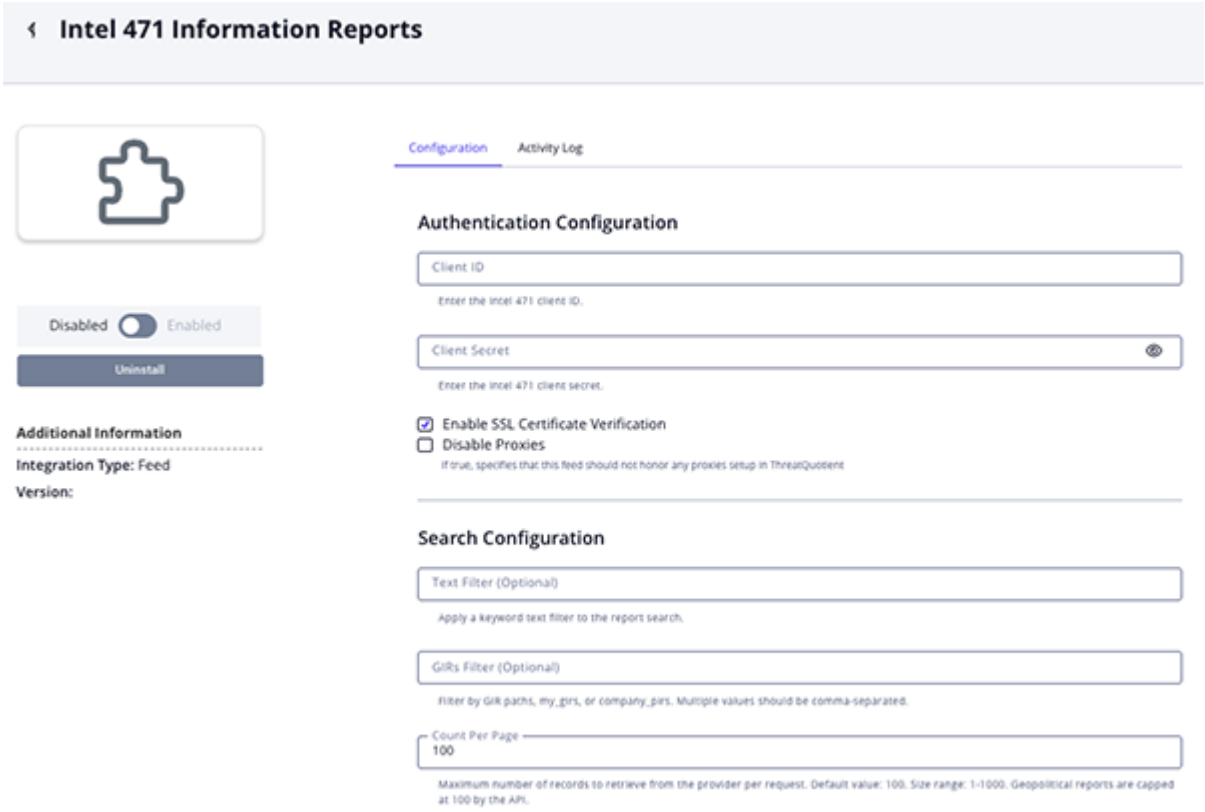
Intel 471 Information Reports Parameters

PARAMETER	DESCRIPTION
Client ID	Your Intel 471 Client ID.
Client Secret	Your Intel 471 Client Secret.

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.
Text Filter	Optional - enter a free-text value to filter the reports.
GIRs Filter	Optional - specify a GIR value to filter the reports.
Count per Page	The maximum number of records to retrieve from the provider per request (0-1000). The default value is 100.
Attribute Filter	Select the contextual attributes to ingest into ThreatQ. Options include: ◦ GIRs ◦ Victims *(default)* ◦ Region Information ◦ Country Information *(default)* ◦ Admiralty Codes *(default)* ◦ Motivations *(default)* ◦ Source Characterization ◦ Sensitive Source ◦ Portal URL *(default)*
Ingest Tags	Enable this parameter to ingest tags into ThreatQ. This parameter is enabled by default.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report *(default)*

PARAMETER	DESCRIPTION
	◦ Handles (Adversaries) ◦ Malware Families *(default)*
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include: ◦ 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 ◦ URLs ◦ File Paths ◦ File Names ◦ Email Addresses ◦ Jabber Usernames ◦ Telegram Usernames
URL Status (Non-Malicious)	Select the status to use for URLs. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.

PARAMETER	DESCRIPTION
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.



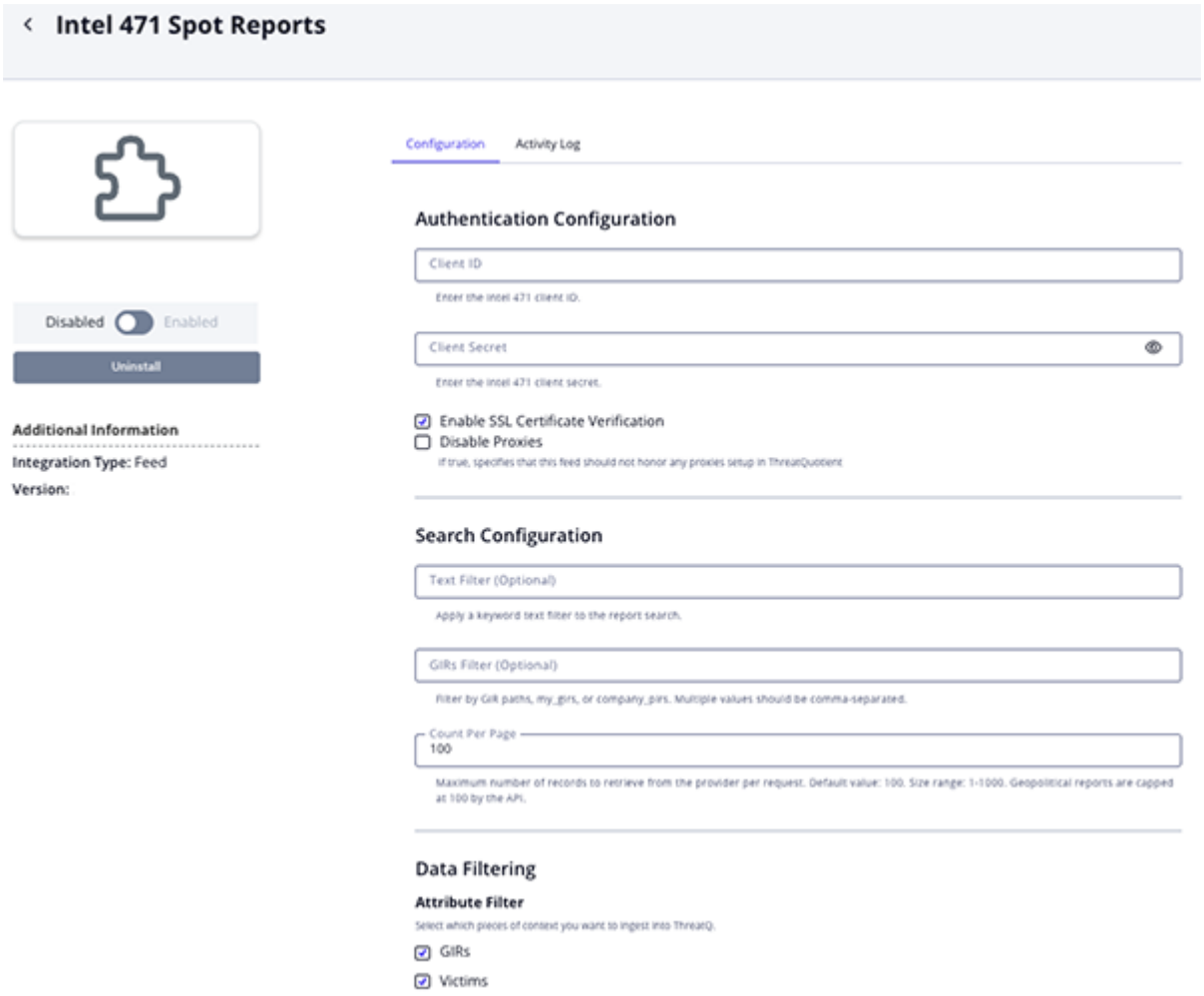
Intel 471 Spot Reports Parameters

PARAMETER	DESCRIPTION
Client ID	Your Intel 471 Client ID.
Client Secret	Your Intel 471 Client Secret.
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.
Text Filter	Optional - enter a free-text value to filter the reports.

PARAMETER	DESCRIPTION
GIRs Filter	Optional - specify a GIR value to filter the reports.
Count per Page	The maximum number of records to retrieve from the provider per request (0-1000). The default value is 100.
Attribute Filter	Select the contextual attributes to ingest into ThreatQ. Options include: ◦ GIRs ◦ Victims *(default)* ◦ Sensitive Source ◦ Portal URL *(default)*
Ingest Tags	Enable this parameter to ingest tags into ThreatQ. This parameter is enabled by default.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report *(default)* ◦ Handles (Adversaries) ◦ Malware Families *(default)*
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include: ◦ Malicious URLs *(default)* ◦ Malicious Domains *(default)* ◦ IP Addresses *(default)* ◦ CVE IDs *(default)* ◦ Actor Websites ◦ URLs ◦ File Paths ◦ File Names ◦ Email Addresses

PARAMETER	DESCRIPTION
	◦ MD5 Hashes *(default)* ◦ SHA-1 Hashes *(default)* ◦ SHA-256 Hashes *(default)* ◦ Actor Domains ◦ Jabber Usernames ◦ Telegram Usernames
URL Status (Non-Malicious)	Select the status to use for URLs. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect *(default)* ◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default)

PARAMETER	DESCRIPTION
	◦ Active ◦ Review ◦ Whitelisted The default setting is **Indirect** as these are typically are not malicious.



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 Breach Alerts

The Intel 471 Breach Alerts feed queries the Intel 471 breach alert report stream and retrieves the full details of each breach alert report using its unique ID.

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/breach-alert/stream`

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/breach-alert/{{ id }}`

Sample Response (truncated):


```
{
  "id": "report--49e247e4-2a50-5994-9c04-cd4fecbf324d",
  "type": "breach_alert",
  "title": "Lawson Software (Thailand) Co. Ltd. possibly compromised
by actor/group The Gentlemen on Apr 23, 2026",
  "creation_ts": "2026-04-24T20:14:56Z",
  "released_ts": "2026-04-24T20:14:56Z",
  "last_updated_ts": "2026-04-24T20:14:56Z",
  "information_ts": "2026-04-23T00:00:00Z",
  "entities": [
    {
      "type": "Handle",
      "value": "The Gentlemen"
    }
  ],
  "sources": [
    {
      "type": "internal",
      "title": "Lawson Software",
      "links": {
        "verity_portal": {
          "href": "https://verity.intel471.com/sources/data-leak-
sites/website--ecedcedd-3df4-541e-976d-2f2d8aed0320/threads/
thread--78e0fc85-3ada-5922-b4e5-89e719cee3b6"
        }
      },
      "index": 2,
```

```
      "last_updated_ts": "2026-04-23T00:00:00Z",
      "source_type": "Data Leak Post"
    }
  ],
  "classification": {
    "girs": [
      {
        "path": "1.1.1",
        "name": "Ransomware malware"
      }
    ]
  },
  "victims": [
    {
      "name": "Lawson Software (Thailand) Co. Ltd.",
      "links": [
        {
          "external": {
            "href": "https://lawson.co.th"
          }
        }
      ],
      "country": "Thailand",
      "revenue": "< US $5 million",
      "region": "Asia",
      "industries": [
        {
          "industry": "IT or technology consulting industry",
          "sector": "Professional services and consulting sector"
        }
      ]
    }
  ],
  "actor_or_group": "The Gentlemen",
  "body": "<p>On April 23, 2026, the operator or operators
running...</p>",
  "confidence": {
    "level": "medium",
    "description": "The intelligence picture is developing, cannot be
corroborated or has some limitations."
  },
  "links": {
```

```
    "verity_api": {
      "href": "https://api.intel471.cloud/integrations/intel-report/
v1/reports/breach-alert/report--49e247e4-2a50-5994-9c04-cd4fecbf324d"
    },
    "verity_portal": {
      "href": "https://verity.intel471.com/intelligence/
breachAlertReportView/report--49e247e4-2a50-5994-9c04-cd4fecbf324d"
    }
  },
  "related_reports": []
}
```


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, .id	Report Value	N/A	.released_ts	Lawson Software (Thailand) Co. Ltd. possibly compromised by actor/group The Gentlemen on Apr 23, 2026	N/A
.body, .sources[]	Report Description	N/A	N/A	On April 23, 2026, the operator or operators running...	N/A
.id	Report Attribute	Report ID	N/A	report--49e247e4-2a50-5994-9c04-cd4fecbf324d	N/A
.type	Report Attribute	Report Family	N/A	BREACH_ALERT	N/A
.type	Report Attribute	Report Type	N/A	BREACH_ALERT	N/A
.classification.girs[]	Report Attribute	GIR	N/A	1.1.1 - Ransomware malware	User configurable
.victims[].name	Report Attribute	Victim	N/A	Lawson Software (Thailand) Co. Ltd.	User configurable
.confidence.level	Report Attribute	Confidence Level	N/A	medium	User configurable
.is_sensitive_source	Report Attribute	Sensitive Source	N/A	N/A	User configurable
.links.verity_portal.href	Report Attribute	Portal URL	N/A	https://verity.intel471.com/intelligence/breachAlertReportView/report--49e247e4-2a50-5994-9c04-cd4fecbf324d	User configurable
.actor_or_group	Adversary	N/A	.released_ts	The Gentlemen	User configurable
.entities[]	Adversary	N/A	.released_ts	Handle: The Gentlemen	When type == Handle; User configurable
.entities[]	Adversary Attribute	Bitcoin Address	.released_ts	N/A	When type == BitcoinAddress;

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					User configurable
.entities[]	Adversary Attribute	Crypto Address	.released_ts	N/A	When type == OtherCryptoCurrencies; User configurable
.entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorDomain; User configurable
.entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorWebsite; User configurable
.entities[]	Related Indicator	URL	.released_ts	N/A	When type == MaliciousURL; User configurable
.entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == MaliciousDomain; User configurable
.entities[]	Related Indicator	CVE	.released_ts	N/A	When type == CveID; User configurable
.entities[]	Related Indicator	IP Address	.released_ts	N/A	When type == IPAddress; User configurable
.entities[]	Related Indicator	Email Address	.released_ts	N/A	When type == EmailAddress; User configurable
.entities[]	Related Indicator	File Path	.released_ts	N/A	When type == FileType; User configurable
.entities[]	Related Indicator	Filename	.released_ts	N/A	When type == FileName; User configurable
.entities[]	Related Indicator	MD5	.released_ts	N/A	When type == MD5; User configurable
.entities[]	Related Indicator	SHA-1	.released_ts	N/A	When type == SHA1; User configurable
.entities[]	Related Indicator	SHA-256	.released_ts	N/A	When type == SHA256; User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.entities[]	Related Indicator	URL	.released_ts	N/A	When type == URL; User configurable
.entities[]	Related Indicator	Username	.released_ts	N/A	When type == Telegram; User configurable
.entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Telegram; User configurable
.entities[]	Related Indicator	Username	.released_ts	N/A	When type == Jabber; User configurable
.entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Jabber; User configurable
.entities[]	Related Malware	N/A	.released_ts	N/A	When type == MalwareFamily; User configurable

Intel 471 FINTEL Reports

The Intel 471 FINTEL Reports feed queries the Intel 471 FINTEL report stream and retrieves the complete details of each FINTEL report using its unique identifier.

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/fintel/stream`

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/fintel/{{ id }}`

Sample Response (truncated):


```
{
  "id": "report--57981044-4889-55fd-a0e1-b3c370212a2b",
  "type": "fintel",
  "sub_type": "underground_perspective",
  "title": "TeamPCP threat group allegedly compromises Bitwarden
password management service",
  "information_ts": "2026-04-28T00:00:00Z",
  "creation_ts": "2026-04-28T20:46:35Z",
  "released_ts": "2026-04-28T20:46:35Z",
  "entities": [
    {
      "type": "Handle",
      "value": "blackwall"
    }
  ],
  "locations": [
    {
      "region": "North America",
      "country": "United States",
      "link": "impacts"
    }
  ],
  "last_updated_ts": "2026-04-29T07:34:03Z",
  "classification": {
    "girs": [
      {
        "path": "1.1.5",
        "name": "Information-stealer malware"
      }
    ]
```

```
  },
  "body": "<p>On April 23, 2026, the Bitwarden open source
password...</p>",
  "sources": [
    {
      "type": "internal",
      "title": "Node package manager supply chain attack dubbed Shai-
Hulud compromises hundreds of packages",
      "links": {
        "verity_api": {
          "href": "https://api.intel471.cloud/integrations/intel-
report/v1/reports/fintel/report--b9d69580-f653-5407-82a3-
c732f0d65bd1"
        },
        "verity_portal": {
          "href": "https://verity.intel471.com/intelligence/
fintelReportView/report--b9d69580-f653-5407-82a3-c732f0d65bd1"
        }
      },
      "index": 6,
      "last_updated_ts": "2025-09-19T00:00:00Z",
      "source_type": "Underground Perspective"
    }
  ],
  "victims": [
    {
      "name": "Bitwarden Inc.",
      "links": [
        {
          "external": {
            "href": "https://bitwarden.com/"
          }
        }
      ]
    }
  ],
  "is_sensitive_source": true,
  "attachments": [
    {
      "url": "https://api.intel471.cloud/integrations/intel-report/
v1/reports/fintel/report--57981044-4889-55fd-a0e1-b3c370212a2b/
attachments/
```

```
8b8759011fa38b7aa2578a14221c301e954fb837dea6bb7b5a72cf7b83a471fc",
      "file_name": "Figure 1.png",
      "malicious": false,
      "file_size": 305319,
      "mime_type": "image/png",
      "description": ""
    }
  ],
  "related_reports": [],
  "derived_entities": [],
  "links": {
    "verity_api": {
      "href": "https://api.intel471.cloud/integrations/intel-report/
v1/reports/fintel/report--57981044-4889-55fd-a0e1-b3c370212a2b"
    },
    "verity_portal": {
      "href": "https://verity.intel471.com/intelligence/
fintelReportView/report--57981044-4889-55fd-a0e1-b3c370212a2b"
    }
  }
}
```


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, .id	Report Value	N/A	.released_ts	TeamPCP threat group allegedly compromises Bitwarden password management service	N/A
.body, .sources[]	Report Description	N/A	N/A	On April 23, 2026, the Bitwarden open source password...	N/A
.body	Attack Pattern	N/A	N/A	N/A	ACTOR_PROFILE only
.id	Report Attribute	Report ID	N/A	report--57981044-4889-55fd-a0e1-b3c370212a2b	N/A
.type	Report Attribute	Report Family	N/A	FINTEL	N/A
.sub_type	Report Attribute	Report Type	N/A	UNDERGROUND_PERSPECTIVE	N/A
.classification.girs[]	Report Attribute	GIR	N/A	1.1.5 - Information-stealer malware	User configurable
.locations[].region	Report Attribute	Impacted Region	N/A	North America	User configurable
.locations[].country	Report Attribute	Impacted Country	N/A	United States	User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.victims[].name	Report Attribute	Victim	N/A	Bitwarden Inc.	User configurable
.is_sensitive_source	Report Attribute	Sensitive Source	N/A	true	User configurable
.links.verity_portal.href	Report Attribute	Portal URL	N/A	https://verity.intel471.com/intelligence/fintelReportView/report--57981044-4889-55fd-a0e1-b3c370212a2b	User configurable
.entities[], .derived_entities[]	Adversary	N/A	.released_ts	Handle: blackwall	When type == Handle; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Bitcoin Address	.released_ts	N/A	When type == BitcoinAddress; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Crypto Address	.released_ts	N/A	When type == OtherCryptoCurrencies; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	ActorDomain: audit.checkmarx.cx	When type == ActorDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorWebsite; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == MaliciousURL; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == MaliciousDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	CVE	.released_ts	N/A	When type == CveID; User configurable
.entities[], .derived_entities[]	Related Indicator	IP Address	.released_ts	IPAddress: 94.154.172.43	When type == IPAddress; User configurable
.entities[], .derived_entities[]	Related Indicator	Email Address	.released_ts	N/A	When type == EmailAddress; User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.entities[], .derived_entities[]	Related Indicator	File Path	.released_ts	N/A	When type == FileType; User configurable
.entities[], .derived_entities[]	Related Indicator	Filename	.released_ts	FileName: @bitwarden/cli@2026.4.0	When type == FileName; User configurable
.entities[], .derived_entities[]	Related Indicator	MD5	.released_ts	N/A	When type == MD5; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-1	.released_ts	N/A	When type == SHA1; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-256	.released_ts	SHA256: 18f784b3bc9a0bcdcb1a8d7f51bc5f54323fc40cbd874119354ab609bef6e4cb	When type == SHA256; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == URL; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	N/A	When type == Telegram; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Telegram; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Related Malware	N/A	.released_ts	N/A	When type == MalwareFamily; User configurable

Intel 471 Geopolitical Reports

The Intel 471 Geopolitical Reports feed queries the Intel 471 geopolitical report stream and retrieves the complete details of each geopolitical report using its unique identifier.

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/geopol/stream`

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/geopol/{{ id }}`

Sample Response (truncated):


```
{
  "id": "report--83cd3937-5953-5501-a990-60ab9fc96504",
  "type": "geopol_report",
  "sub_type": "significant_activity_report",
  "title": "Russian President Putin hosts Iranian foreign minister,
pledges to support Iran in pursuit of peace",
  "creation_ts": "2026-04-28T18:15:59Z",
  "released_ts": "2026-04-28T18:15:59Z",
  "last_updated_ts": "2026-04-28T18:15:59Z",
  "information_ts": "2026-04-27T00:00:00Z",
  "sources": [
    {
      "type": "external",
      "title": "Meeting with Iranian Foreign Minister Abbas
Araghchi",
      "links": {
        "external": {
          "href": "http://kremlin.ru/events/president/news/79633"
        }
      },
      "index": 1,
      "last_updated_ts": "2026-04-27T00:00:00Z",
      "source_type": "External Link"
    }
  ],
  "classification": {
    "girs": [
      {
        "path": "6.1.6.2",
        "name": "National government"
```

```
      }
    ]
  },
  "links": {
    "verity_api": {
      "href": "https://api.intel471.cloud/integrations/intel-report/
v1/reports/geopol/report--83cd3937-5953-5501-a990-60ab9fc96504"
    },
    "verity_portal": {
      "href": "https://verity.intel471.com/intelligence/
geopolReportView/report--83cd3937-5953-5501-a990-60ab9fc96504"
    }
  },
  "body": "<p>On April 27, 2026, Russian President Vladimir Putin
hosted...</p>",
  "entities": [],
  "locations": [
    {
      "region": "Europe",
      "country": "Russia",
      "link": "originated from"
    }
  ],
  "attachments": [],
  "related_reports": [],
  "country_profiles": [
    {
      "id": "report--ecede7d6-74a5-5fd9-ac63-5d7aab39a270",
      "country": "Russia",
      "country_iso_code": "RU",
      "threat_rating": "severe",
      "security_assessment": "high",
      "information_ts": "2025-02-28T00:00:00Z",
      "is_country_of_interest": false
    }
  ],
  "regional_tension_points": [
    {
      "id": "report--559f91e8-d8de-58f7-858b-09dac64ba4f6",
      "name": "Russia-Ukraine war continues: Russian President Putin
signals intent for long war of attrition, prolonged indirect conflict
with West",
```

```
      "information_ts": "2025-10-01T00:00:00Z"
    }
  ],
  "derived_entities": [],
  "significant_activity": {
    "summary": "<p>On April 27, 2026, Russian President Vladimir
Putin hosted...</p>",
    "comments": "<p>Almost immediately after the outbreak of the
latest conflict...</p>",
    "event_tag": "political"
  }
}
```

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, .id	Report Value	N/A	.released_ts	Russian President Putin hosts Iranian foreign minister, pledges to support Iran in pursuit of peace	N/A
.significant_activity.summary, .body, .sources[], .attachments[]	Report Description	N/A	N/A	On April 27, 2026, Russian President Vladimir Putin hosted...	N/A
.significant_activity.comments	Report Description	N/A	N/A	Almost immediately after the outbreak of the latest conflict...	N/A
.id	Report Attribute	Report ID	N/A	report--83cd3937-5953-5501-a990-60ab9fc96504	N/A
.type	Report Attribute	Report Family	N/A	GEOPOL	N/A
.sub_type	Report Attribute	Report Type	N/A	SIGNIFICANT_ACTIVITY_REPORT	N/A
.classification.girs[]	Report Attribute	GIR	N/A	6.1.6.2 - National government	User configurable
.locations[].region, .locations[].country	Report Attribute	Originated From	N/A	Russia (Europe)	User configurable
.locations[].region, .locations[].country	Report Attribute	Active	N/A	Russia (Europe)	User configurable
.locations[].region	Report Attribute	Impacted Region	N/A	Middle East	User configurable
.locations[].country	Report Attribute	Impacted Country	N/A	Iran	User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.victims[].name	Report Attribute	Victim	N/A	N/A	User configurable
.is_sensitive_source	Report Attribute	Sensitive Source	N/A	N/A	User configurable
.links.verity_portal.href	Report Attribute	Portal URL	N/A	https://verity.intel471.com/intelligence/geopolReportView/report--83cd3937-5953-5501-a990-60ab9fc96504	User configurable
.significant_activity.event_tag	Report Tag	N/A	N/A	political	User configurable
.entities[], .derived_entities[]	Adversary	N/A	.released_ts	N/A	When type == Handle; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Bitcoin Address	.released_ts	N/A	When type == BitcoinAddress; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Crypto Address	.released_ts	N/A	When type == OtherCryptoCurrencies; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorWebsite; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == MaliciousURL; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == MaliciousDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	CVE	.released_ts	N/A	When type == CveID; User configurable
.entities[], .derived_entities[]	Related Indicator	IP Address	.released_ts	N/A	When type == IPAddress; User configurable
.entities[], .derived_entities[]	Related Indicator	Email Address	.released_ts	N/A	When type ==

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					EmailAddress; User configurable
.entities[], .derived_entities[]	Related Indicator	File Path	.released_ts	N/A	When type == FileType; User configurable
.entities[], .derived_entities[]	Related Indicator	Filename	.released_ts	N/A	When type == FileName; User configurable
.entities[], .derived_entities[]	Related Indicator	MD5	.released_ts	N/A	When type == MD5; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-1	.released_ts	N/A	When type == SHA1; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-256	.released_ts	N/A	When type == SHA256; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == URL; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	N/A	When type == Telegram; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Telegram; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Related Malware	N/A	.released_ts	N/A	When type == MalwareFamily; User configurable

Intel 471 Information Reports

The Intel 471 Information Reports feed queries the Intel 471 information report stream and retrieves the complete details of each information report using its unique identifier.

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/info/stream`

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/info/{{ id }}`

Sample Response:


```
{
  "id": "report--e712c94b-354c-51d2-ac6f-4125ffbd614b",
  "type": "info_report",
  "assessment": {
    "admiralty_code": "F6"
  },
  "motivation": ["CC"],
  "title": "Actor nameek (aka lynxx0x) offers underground travel
services",
  "information_ts": "2026-04-12T00:00:00Z",
  "creation_ts": "2026-04-29T18:26:52Z",
  "released_ts": "2026-04-29T18:26:52Z",
  "source_characterization": "Information was derived from the
Exploit forum, our reliable source and our actors' database.",
  "entities": [
    {
      "type": "Handle",
      "value": "1oooooo"
    }
  ],
  "locations": [
    {
      "region": "Asia",
      "country": "Japan",
      "link": "impacts"
    }
  ],
  "last_updated_ts": "2026-04-29T18:26:52Z",
  "actor_subject_of_report": [
    {
```

```
      "handle": "nameek",
      "aliases": ["lynxx0x"]
    }
  ],
  "classification": {
    "girs": [
      {
        "path": "1.3.8",
        "name": "Malware spamming"
      }
    ]
  },
  "is_sensitive_source": false,
  "attachments": [
    {
      "url": "https://api.intel471.cloud/integrations/intel-report/
v1/reports/info/report--e712c94b-354c-51d2-ac6f-4125ffbd614b/
attachments/
0a1a091d0726053d80793281d453c337daeee2cd6948b92f5ed0ea4513638c35",
      "file_name": "Exploit.png",
      "malicious": false,
      "file_size": 95169,
      "mime_type": "image/png",
      "description": ""
    }
  ],
  "related_reports": [],
  "derived_entities": [],
  "researcher_comments": "<p>Actor and information assessment The
actor nameek has been...</p>",
  "body": "<p>On March 8, 2026, the actor nameek posted the...</p>",
  "body_translated": "<p>On March 8, 2026, the actor nameek posted
the...</p>",
  "victims": [],
  "executive_summary": "<p>This is an Activity Report on the actor
nameek...</p>",
  "links": {
    "verity_api": {
      "href": "https://api.intel471.cloud/integrations/intel-report/
v1/reports/info/report--e712c94b-354c-51d2-ac6f-4125ffbd614b"
    },
    "verity_portal": {
```

```
      "href": "https://verity.intel471.com/intelligence/
infoReportView/report--e712c94b-354c-51d2-ac6f-4125ffbd614b"
    }
  }
}
```

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, .id	Report Value	N/A	.released_ts	Actor nameek (aka lynxx0x) offers underground travel services	N/A
.executive_summary, .researcher_comments, .body_translated, .body	Report Description	N/A	N/A	On March 8, 2026, the actor nameek posted the...	N/A
.id	Report Attribute	Report ID	N/A	report--e712c94b-354c-51d2-ac6f-4125ffbd614b	N/A
.type	Report Attribute	Report Family	N/A	INFOREP	N/A
.type	Report Attribute	Report Type	N/A	INFOREP	N/A
.classification.girs[]	Report Attribute	GIR	N/A	1.3.8 - Malware spamming	User configurable
.locations[].region	Report Attribute	Impacted Region	N/A	Asia	User configurable
.locations[].country	Report Attribute	Impacted Country	N/A	Japan	User configurable
.assessment.admiralty_code	Report Attribute	Admiralty Reliability	N/A	F	User configurable. Uses 1st character of the code
.assessment.admiralty_code	Report Attribute	Admiralty Credibility	N/A	6	User configurable. Uses 2nd character of the code
.motivation[]	Report Attribute	Motivation	N/A	CC	User configurable
.source_characterization	Report Attribute	Source	N/A	Information was derived from the Exploit forum, our reliable source and our actors' database.	User configurable
.victims[].name	Report Attribute	Victim	N/A	N/A	User configurable
.is_sensitive_source	Report Attribute	Sensitive Source	N/A	false	User configurable
.links.verity_portal.href	Report Attribute	Portal URL	N/A	https://verity.intel471.com/intelligence/infoReportView/	User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				report--e712c94b-354c-51d2-ac6f-4125ffbd614b	
.actor_subject_of_report[].handle	Adversary	N/A	.released_ts	nameek	User configurable
.actor_subject_of_report[].aliases[]	Adversary Attribute	Alias	N/A	lynxx0x	User configurable
.entities[], .derived_entities[]	Adversary	N/A	.released_ts	Handle: 1oooooo	When type == Handle; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Bitcoin Address	.released_ts	N/A	When type == BitcoinAddress; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Crypto Address	.released_ts	N/A	When type == OtherCryptoCurrencies; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorWebsite; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == MaliciousURL; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == MaliciousDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	CVE	.released_ts	N/A	When type == CveID; User configurable
.entities[], .derived_entities[]	Related Indicator	IP Address	.released_ts	N/A	When type == IPAddress; User configurable
.entities[], .derived_entities[]	Related Indicator	Email Address	.released_ts	N/A	When type == EmailAddress; User configurable
.entities[], .derived_entities[]	Related Indicator	File Path	.released_ts	N/A	When type == FileType; User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.entities[], .derived_entities[]	Related Indicator	Filename	.released_ts	N/A	When type == FileName; User configurable
.entities[], .derived_entities[]	Related Indicator	MD5	.released_ts	N/A	When type == MD5; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-1	.released_ts	N/A	When type == SHA1; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-256	.released_ts	N/A	When type == SHA256; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == URL; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	Telegram: @anonymousXLX	When type == Telegram; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	Telegram	When type == Telegram; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Related Malware	N/A	.released_ts	MalwareFamily: Angel Drainer	When type == MalwareFamily; User configurable

Intel 471 Sport Reports

The Intel 471 Spot Reports feed queries the Intel 471 spot report stream and retrieves the complete details of each spot report using its unique identifier.

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/spot/stream`

`GET https://api.intel471.cloud/integrations/intel-report/v1/reports/spot/{{ id }}`

Sample Response (truncated):


```
{
  "id": "report--dc7d5b66-d36d-563f-9ff8-4e43276fda24",
  "type": "spot_report",
  "title": "ShinyHunters (aka SP1D3R HUNTERS) group launches
#FederalB0yz aka #FBIHunters Telegram channel to expose competing
threat actors",
  "last_updated_ts": "2026-04-29T13:30:09Z",
  "creation_ts": "2026-04-28T14:08:56Z",
  "released_ts": "2026-04-28T14:08:56Z",
  "information_ts": "2026-04-27T00:00:00Z",
  "body": "On April 24, 2026, the ShinyHunters aka SP1D3R HUNTERS,
Scattered...",
  "classification": {
    "girs": [
      {
        "path": "3.3",
        "name": "Dedicated criminal infrastructure"
      }
    ]
  },
  "sources": [
    {
      "type": "internal",
      "title": "Telegram channel",
      "links": {
        "verity_portal": {
          "href": "https://verity.intel471.com/sources/messaging-
services/thread/room--fec53450-debb-5f54-acc4-0cb0613885cc"
        }
      }
```

```
    }
  ],
  "entities": [
    {
      "type": "Handle",
      "value": "Mr. Raccoon"
    }
  ],
  "victims": [],
  "is_sensitive_source": true,
  "related_reports": [],
  "derived_entities": [],
  "links": {
    "verity_api": {
      "href": "https://api.intel471.cloud/integrations/intel-report/
v1/reports/spot/report--dc7d5b66-d36d-563f-9ff8-4e43276fda24"
    },
    "verity_portal": {
      "href": "https://verity.intel471.com/intelligence/
spotReportView/report--dc7d5b66-d36d-563f-9ff8-4e43276fda24"
    }
  }
}
```


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, .id	Report Value	N/A	.released_ts	ShinyHunters (aka SP1D3R HUNTERS) group launches #FederalB0yz aka #FBIHunters Telegram channel to expose competing threat actors	N/A
.body, .sources[]	Report Description	N/A	N/A	On April 24, 2026, the ShinyHunters aka SP1D3R HUNTERS, Scattered...	N/A
.id	Report Attribute	Report ID	N/A	report--dc7d5b66-d36d-563f-9ff8-4e43276fda24	N/A
.type	Report Attribute	Report Family	N/A	SPOTREP	N/A
.type	Report Attribute	Report Type	N/A	SPOTREP	N/A
.classification.girs[]	Report Attribute	GIR	N/A	3.3 - Dedicated criminal infrastructure	User configurable
.victims[].name	Report Attribute	Victim	N/A	N/A	User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.is_sensitive_source	Report Attribute	Sensitive Source	N/A	true	User configurable
.links.verity_portal.href	Report Attribute	Portal URL	N/A	https://verity.intel471.com/intelligence/spotReportView/report--dc7d5b66-d36d-563f-9ff8-4e43276fda24	User configurable
.entities[], .derived_entities[]	Adversary	N/A	.released_ts	Handle: Mr. Raccoon	When type == Handle; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Bitcoin Address	.released_ts	N/A	When type == BitcoinAddress; User configurable
.entities[], .derived_entities[]	Adversary Attribute	Crypto Address	.released_ts	N/A	When type == OtherCryptoCurrencies; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == ActorWebsite; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == MaliciousURL; User configurable
.entities[], .derived_entities[]	Related Indicator	FQDN	.released_ts	N/A	When type == MaliciousDomain; User configurable
.entities[], .derived_entities[]	Related Indicator	CVE	.released_ts	N/A	When type == CveID; User configurable
.entities[], .derived_entities[]	Related Indicator	IP Address	.released_ts	N/A	When type == IPAddress; User configurable
.entities[], .derived_entities[]	Related Indicator	Email Address	.released_ts	N/A	When type == EmailAddress; User configurable
.entities[], .derived_entities[]	Related Indicator	File Path	.released_ts	N/A	When type == FileType; User configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.entities[], .derived_entities[]	Related Indicator	Filename	.released_ts	N/A	When type == FileName; User configurable
.entities[], .derived_entities[]	Related Indicator	MD5	.released_ts	N/A	When type == MD5; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-1	.released_ts	N/A	When type == SHA1; User configurable
.entities[], .derived_entities[]	Related Indicator	SHA-256	.released_ts	N/A	When type == SHA256; User configurable
.entities[], .derived_entities[]	Related Indicator	URL	.released_ts	N/A	When type == URL; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	Telegram: @fb1hunt3rz	When type == Telegram; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	Telegram	When type == Telegram; User configurable
.entities[], .derived_entities[]	Related Indicator	Username	.released_ts	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Indicator Attribute	Platform	N/A	N/A	When type == Jabber; User configurable
.entities[], .derived_entities[]	Related Malware	N/A	.released_ts	N/A	When type == MalwareFamily; User configurable

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 Breach Alerts

METRIC	RESULT
Run Time	1 minute
Adversaries	30
Indicators	1
Indicator Attributes	1
Reports	33
Report Attributes	528

Intel 471 FINTEL Reports

METRIC	RESULT
Run Time	1 minute
Adversaries	5
Indicators	8
Indicator Attributes	4

METRIC	RESULT
Reports	1
Report Attributes	14

Intel 471 Geopolitical Reports

METRIC	RESULT
Run Time	1 minute
Adversaries	5
Reports	2
Report Attributes	71

Intel 471 Information Reports

METRIC	RESULT
Run Time	1 minute
Adversaries	4
Adversary Attributes	8
Indicators	24
Indicator Attributes	17
Malware	5

METRIC	RESULT
Reports	4
Report Attributes	105

Intel 471 Spot Reports

METRIC	RESULT
Run Time	1 minute
Indicators	3
Indicator Attributes	1
Malware	1
Reports	4
Report Attributes	29

Known Issues / Limitations

- Large report descriptions, embedded images, or attachments may exceed platform or database size limits. In such cases, oversized inline content may be truncated or removed to ensure the report can be successfully ingested.

Change Log

- **Version 3.0.0**
  - Migrated to the Intel 471 Reports API (`api.intel471.cloud/integrations/intel-report/v1`).
  - Updated authentication to use Basic Authentication with `client_id` and `client_secret`.
  - Updated Breach Alerts and Spot Reports to leverage the new Reports API stream and detail endpoints.
  - Added new feeds for FINTEL Reports, Geopolitical Reports, and Information Reports.
  - Implemented handling for `401` (authentication) and `403` (authorization) errors.
  - Introduced SSL verification and proxy control options for each feed.
- **Version 2.0.2**
  - Resolved an issue where missing date fields would result in reports not being ingested.
- **Version 2.0.1**
  - Resolved the following issues where:
    - Embedded images were stripped out from descriptions.
    - Users encountered a `filter-mapping` error when loading MITRE Attack Patterns from the ThreatQ API.
  - Improved the HTML formatting for descriptions.
  - Added a new entry to the **Known Issues / Limitations** regarding ingestion behavior of images with long descriptions.
  - Updated the minimum ThreatQ version to 5.24.0.
- **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.