ThreatQuotient

A Securonix Company

Intel 471 Malware Intelligence CDF

Version 2.0.0

June 08, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

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

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

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.0.0
Compatible with ThreatQ Versions	>= 5.24.0
Support Tier	ThreatQ Supported

Introduction

The Intel 471 Malware Intelligence CDF ingests malware intelligence reports from Intel 471 and enriches them with related malware indicators and malware signatures to provide comprehensive context for malware analysis and threat research. Reports are ingested as the primary object type, while supplemental feeds automatically retrieve and associate additional indicators and signatures related to the malware family referenced in each report.

To enhance the depth of intelligence available within ThreatQ, the primary reports feed invokes supplemental lookups that query Intel 471 for associated indicators and signatures. Because these supplemental feeds generate additional API requests, they may increase overall feed execution time and API consumption.

The integration includes the following feeds:

- **Intel 471 Malware Intelligence** - ingests malware intelligence reports as the primary object type and automatically associates related indicators and malware signatures.
- **Intel 471 Malware Indicators (Supplemental)** – retrieves malware-related indicators associated with a report's malware family.
- **Intel 471 Malware Signatures (Supplemental)** – retrieves malware signatures associated with a report's malware family.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes
- Signatures
  - Signature Attributes

Prerequisites

The following is required to run the integration:

- An Intel471 Client ID
- An Intel471 Client Secret

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.

The feed will now be installed. 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:

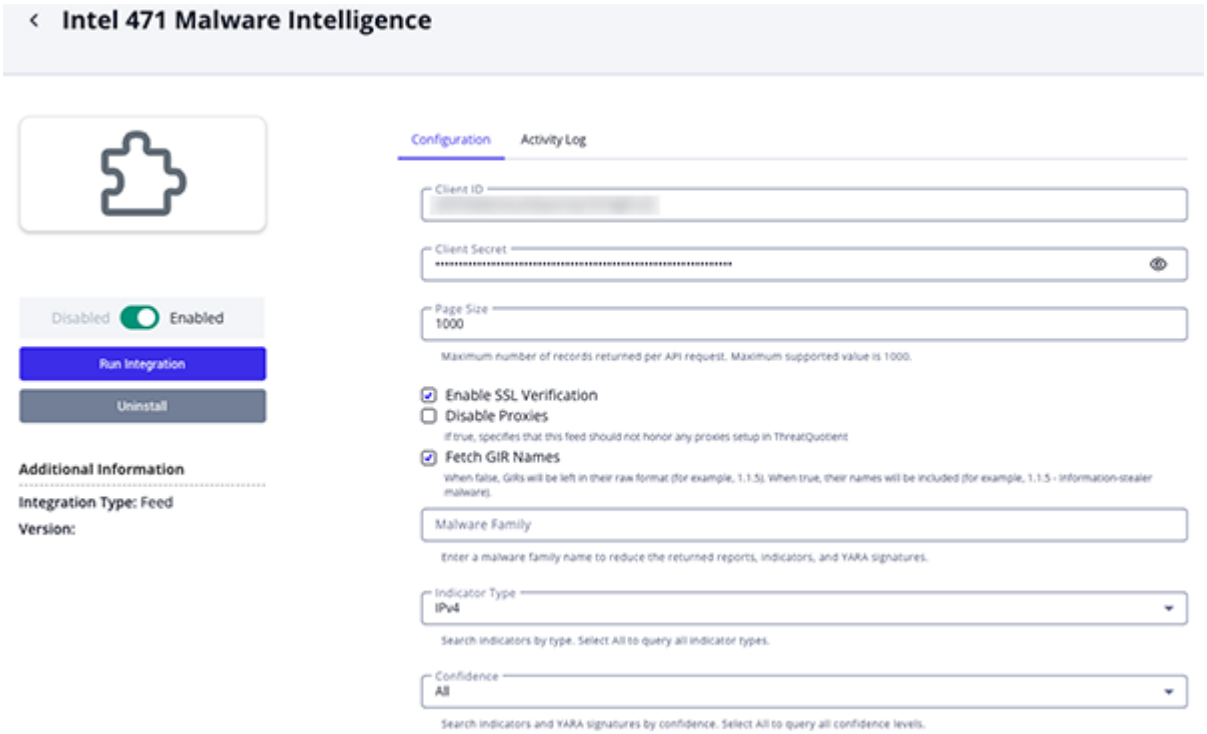
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   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:

PARAMETER	DESCRIPTION
Client ID	Enter your Intel 471 API Client ID.
Client Secret	Enter your Intel 471 API Client Secret.
Page Size	Specify the maximum number of records to retrieve per API request. The maximum supported value is `1000`. The default value is `1000`.
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.
Fetch GIR Names	Enable this parameter to store GIR values in the format **path - name**. When disabled, GIR values are stored using the raw path only. This parameter is enabled by default.

PARAMETER	DESCRIPTION
Malware Family	Optional - specify a malware family name to filter results. When configured, only reports, indicators, and YARA signatures associated with the specified malware family will be retrieved, reducing the volume of returned data. If left blank, data for all malware families will be returned.
Indicator Type	Optional - select one or more non-YARA indicator types to filter the results returned by the **Intel 471 Malware Indicators** supplemental feed. Select `All` to retrieve indicators of all supported types. Options include: ◦ All ◦ IPv4 *(Default)* ◦ Domain ◦ Email ◦ File ◦ URL This setting applies only to non-YARA indicators and does not affect YARA signature retrieval.
Confidence	Optional - select a confidence level to filter both indicators and YARA signatures returned by the supplemental feeds. This setting is applied to the **Intel 471 Malware Indicators** and **Intel 471 Malware Signatures** supplemental feeds, ensuring the same confidence criteria is used for both data types. Select `All` to retrieve indicators and signatures across all confidence levels. Options include: ◦ All *(Default* ◦ High ◦ Medium ◦ Low



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 Malware Intelligence

The Intel 471 Malware Intelligence feed ingests malware intelligence reports from Intel 471 and enriches them with related indicators and malware signatures. For each malware report, the feed automatically retrieves additional intelligence associated with the malware family, providing analysts with expanded context and supporting data to aid malware analysis, threat hunting, and investigation activities.

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

Sample Response:


```
{
  "count": 362,
  "cursor_next": "abc123",
  "reports": [
    {
      "id": "report--8d11b63b-f7d6-5061-bb17-290ee5af9464",
      "type": "malware_report",
      "title": "Pony Loader",
      "last_updated_ts": "2022-07-14T15:43:22Z",
      "creation_ts": "2019-01-31T14:16:22Z",
      "information_ts": "2025-11-07T12:51:01Z",
      "released_ts": "2018-10-16T11:30:25Z",
      "version": "1",
      "body": "Malware Analysis Report: Pony loader...",
      "classification": {
        "girs": [
          {
            "path": "1.1.5",
            "name": "Information-stealer malware"
          }
        ]
      },
      "threat": {
        "id": "malware-family--8fa56b30-3236-566e-8bbb-849d3f165eac",
        "type": "malware",
        "family": "smokeloader"
      },
```

```
      "links": {
        "verity_api": {
          "href": "https://api.intel471.cloud/..."
        },
        "verity_portal": {
          "href": "https://verity.intel471.com/..."
        }
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES	
.reports[].title	Report.Value	N/A	.reports[].released_ts	Pony Loader	Primary report value
.reports[].body	Report.Description	N/A	.reports[].released_ts	Malware Analysis Report ...	HTML body from Intel 471
.reports[].id	Report.Attribute	Report ID	.reports[].released_ts	report--8d11b63b-f7d6-5061-bb17-290ee5af9464	N/A
.reports[].type	Report.Attribute	Report Type	.reports[].released_ts	malware_report	N/A
.reports[].last_updated_ts	Report.Attribute	Last Updated	.reports[].released_ts	2022-07-14T15:43:22Z	N/A
.reports[].creation_ts	Report.Attribute	Created At	.reports[].released_ts	2019-01-31T14:16:22Z	N/A
.reports[].information_ts	Report.Attribute	Information Time	.reports[].released_ts	2025-11-07T12:51:01Z	N/A
.reports[].version	Report.Attribute	Version	.reports[].released_ts	1	N/A
.reports[].threat.id	Report.Attribute	Threat ID	.reports[].released_ts	malware-family--8fa56b30-...	N/A
.reports[].threat.type	Report.Attribute	Threat Type	.reports[].released_ts	malware	N/A
.reports[].threat.family	Report.Attribute	Malware Family	.reports[].released_ts	smokeloader	N/A
.reports[].classification.girs[]	Report.Attribute	Intelligence Requirement	.reports[].released_ts	1.1.5 - Information-stealer malware	Stored as path - name when Fetch GIR Names is enabled; otherwise stored as the raw GIR path
.reports[].links.verity_api.href	Report.Attribute	Verity API Link	.reports[].released_ts	https://api.intel471.cloud/...	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES	
.reports[].links.verity_portal.href	Report.Attribute	Verity Portal Link	.reports[].released_ts	https://verity.intel471.com/...	N/A
.reports[].released_ts	Report.Published At	N/A	N/A	2018-10-16T11:30:25Z	Primary published date

Intel 471 Malware Indicators (Supplemental)

The Intel 471 Malware Indicators Supplemental feed retrieves malware-related indicators from Intel 471 and associates them with malware intelligence reports. For each indicator returned by the Intel 471 Indicators API where the indicator type is not `yara`, the feed creates one or more corresponding ThreatQ Indicator objects.

```
GET https://api.intel471.cloud/integrations/indicators/v1/indicators/stream
```

Sample Response:


```
{
  "count": 271879,
  "indicators": [
    {
      "id": "malware-indicator--5aa25bb2-08df-5f28-
aef5-4c834b5a8606",
      "type": "url",
      "description": "pony controller URL",
      "confidence": 50,
      "expiration_ts": "2025-10-24T20:11:06Z",
      "activity": {
        "first_seen_ts": "2018-08-21T02:33:38Z",
        "last_seen_ts": "2025-09-24T20:11:06Z"
      },
      "pattern": "[url:value = 'http://tarati.se/rAnDoM/gate.php']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "kill_chain_phases": [
        {
          "kill_chain_name": "mitre-attack",
          "phase_name": "command_and_control"
        }
      ],
      "classification": {
        "girs": [
          {
            "path": "1.1.5",
            "name": "Information-stealer malware"
          }
        ]
      },
```

```
      "data": {
        "url": "http://tarati.se/rAnDoM/gate.php"
      },
      "threat": {
        "type": "malware",
        "data": {
          "malware": {
            "id": "malware--f12da3fa-...",
            "family": "pony"
          },
          "malware_family": {
            "id": "malware-family--f12da3fa-...",
            "name": "pony"
          }
        }
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES	
.indicators[].type	Indicator.Type	N/A	.indicators[].activity.first_seen_ts	url, ipv4, domain, email, file	Drives ThreatQ type conversion
.indicators[].data.url	Indicator.Value	URL	.indicators[].activity.first_seen_ts	http://tarati.se/rAnDoM/gate.php	When .type == "url"
.indicators[].data.ipv4.ip_address	Indicator.Value	IP Address	.indicators[].activity.first_seen_ts	82.65.227.131	When .type == "ipv4"
.indicators[].data.domain	Indicator.Value	FQDN	.indicators[].activity.first_seen_ts	oyraglw.info	When .type == "domain"
.indicators[].data.email	Indicator.Value	Email Address	.indicators[].activity.first_seen_ts	info@mth.ae	When .type == "email"
.indicators[].data.file.md5	Indicator.Value	MD5	.indicators[].activity.first_seen_ts	2e353bf26b6d7329c76efe492cbd6d4e	File indicators create separate MD5/SHA-1/SHA-256 indicators
.indicators[].data.file.sha1	Indicator.Value	SHA-1	.indicators[].activity.first_seen_ts	ac206745aadf006663b22c1916703ee43c987027	File indicators create separate MD5/SHA-1/SHA-256 indicators
.indicators[].data.file.sha256	Indicator.Value	SHA-256	.indicators[].activity.first_seen_ts	e330752b3750a012cb4c97a9b6e2c55bfce0ad4e	File indicators create separate MD5/SHA-1/SHA-256 indicators

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
			5ccb5c0ec4f3019b4ddf00c5	
.indicators[].id	Indicator.Attribute	Indicator ID	.indicators[].activity.first_seen_ts	malware-indicator--5aa25bb2-...	N/A
.indicators[].description	Indicator.Attribute	Description	.indicators[].activity.first_seen_ts	pony controller URL	N/A
.indicators[].confidence	Indicator.Attribute	Confidence	.indicators[].activity.first_seen_ts	50	N/A
.indicators[].expiration_ts	Indicator.Attribute	Expires At	.indicators[].activity.first_seen_ts	2025-10-24T20:11:06Z	N/A
.indicators[].activity.first_seen_ts	Indicator.Attribute	First Seen	.indicators[].activity.first_seen_ts	2018-08-21T02:33:38Z	N/A
.indicators[].activity.last_seen_ts	Indicator.Attribute	Last Seen	.indicators[].activity.first_seen_ts	2025-09-24T20:11:06Z	N/A
.indicators[].pattern	Indicator.Attribute	Pattern	.indicators[].activity.first_seen_ts	[url:value = 'http://tarati.se/rAnDoM/gate.php']	N/A
.indicators[].pattern_type	Indicator.Attribute	Pattern Type	.indicators[].activity.first_seen_ts	stix	N/A
.indicators[].pattern_version	Indicator.Attribute	Pattern Version	.indicators[].activity.first_seen_ts	2.1	N/A
.indicators[].kill_chain_phases[].phase_name	Indicator.Attribute	MITRE Tactics	.indicators[].activity.first_seen_ts	command_and_control	Multi-valued
.indicators[].classification.girs[]	Indicator.Attribute	Intelligence Requirement	.indicators[].activity.first_seen_ts	1.1.5 - Information-stealer malware	Stored as path - name when Fetch GIR Names is enabled; otherwise stored as the raw GIR path
.indicators[].threat.type	Indicator.Attribute	Threat Type	.indicators[].activity.first_seen_ts	malware	N/A
.indicators[].threat.data.malware.id	Indicator.Attribute	Malware ID	.indicators[].activity.first_seen_ts	malware--f12da3fa-...	When present
.indicators[].threat.data.malware.family	Indicator.Attribute	Malware Family	.indicators[].activity.first_seen_ts	pony	N/A
.indicators[].threat.data.malware.version	Indicator.Attribute	Threat Version	.indicators[].activity.first_seen_ts	0.7d	When present
.indicators[].threat.data.malware.variant	Indicator.Attribute	Malware Variant	.indicators[].activity.first_seen_ts	v3_variant_a	When present

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES	
.indicators[].threat.data.malware_family.id	Indicator.Attribute	Malware Family ID	.indicators[].activity.first_seen_ts	malware-family--f12da3fa-...	N/A
.indicators[].threat.data.malware_family.name	Indicator.Attribute	Malware Family Name	.indicators[].activity.first_seen_ts	pony	N/A
.indicators[].data.file.type	Indicator.Attribute	File Type	.indicators[].activity.first_seen_ts	PEEXE_x86	File indicators only
.indicators[].data.file.size	Indicator.Attribute	File Size	.indicators[].activity.first_seen_ts	221184	File indicators only
.indicators[].data.file.ssdeep	Indicator.Attribute	SSDEEP	.indicators[].activity.first_seen_ts	3072:zGWSdk...	File indicators only
.indicators[].data.ipv4.geo_ip.country	Indicator.Attribute	Country	.indicators[].activity.first_seen_ts	France	IPv4 only, when present
.indicators[].data.ipv4.geo_ip.country_code	Indicator.Attribute	Country Code	.indicators[].activity.first_seen_ts	FR	IPv4 only, when present
.indicators[].data.ipv4.geo_ip.city	Indicator.Attribute	City	.indicators[].activity.first_seen_ts	Paris	IPv4 only, when present
.indicators[].data.ipv4.geo_ip.subdivision[]	Indicator.Attribute	Subdivision	.indicators[].activity.first_seen_ts	Île-de-France	IPv4 only, multi-valued
.indicators[].data.ipv4.geo_ip.isp.isp	Indicator.Attribute	ISP	.indicators[].activity.first_seen_ts	Free SAS	IPv4 only, when present
.indicators[].data.ipv4.geo_ip.isp.organization	Indicator.Attribute	Organization	.indicators[].activity.first_seen_ts	Free SAS	IPv4 only, when present
.indicators[].data.ipv4.geo_ip.isp.autonomous_system	Indicator.Attribute	Autonomous System	.indicators[].activity.first_seen_ts	AS12322 Free SAS	IPv4 only, when present
.indicators[].data.ipv4.geo_ip.isp.network	Indicator.Attribute	Network	.indicators[].activity.first_seen_ts	82.64.0.0/15	IPv4 only, when present

Intel 471 Malware Signatures

The **Intel 471 Malware Signatures (Supplemental)** feed retrieves YARA signatures associated with malware intelligence from Intel 471. For each indicator returned by the Intel 471 Indicators API where the indicator type is `yara`, the feed creates a corresponding **ThreatQ Signature** object of type **YARA**. This enrichment provides analysts with detection logic that can be used to identify and track malware associated with the referenced malware family.

```
GET https://api.intel471.cloud/integrations/indicators/v1/indicators/stream?type=yara
```

Sample Response:


```
{
  "count": 28,
  "indicators": [
    {
      "id": "malware-indicator--4152337d-1f42-59e8-959d-2a6cd10db64a",
      "type": "yara",
      "pattern_type": "yara",
      "pattern_version": "4",
      "confidence": 85,
      "activity": {
        "first_seen_ts": "2025-10-14T17:44:03Z",
        "last_seen_ts": "2025-10-14T17:44:03Z"
      },
      "classification": {
        "girs": [
          {
            "path": "1.1",
            "name": "Malware variants"
          }
        ]
      },
      "data": {
        "yara": {
          "title": "lazarus_stealer",
          "signature": "rule lazarus_stealer { ... }"
        }
      },
      "pattern": "rule lazarus_stealer { ... }",
```

```
      "threat": {
        "type": "malware",
        "data": {
          "malware_family": {
            "id": "malware-family--786a071e-0dc4-5ee7-b3fe-
f12ba45079dc",
            "name": "lazarus_stealer"
          }
        }
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].data.yara.title	Signature.Name	N/A	.indicators[].activity.first_seen_ts	lazarus_stealer	Primary signature name
.indicators[].data.yara.signature	Signature.Value	YARA	.indicators[].activity.first_seen_ts	rule lazarus_stealer { ... }	Full YARA rule text
YARA	Signature.Type	N/A	.indicators[].activity.first_seen_ts	YARA	Constant value
.indicators[].id	Signature.Attribute	Signature ID	.indicators[].activity.first_seen_ts	malware-indicator--4152337d-...	N/A
.indicators[].type	Signature.Attribute	Indicator Type	.indicators[].activity.first_seen_ts	yara	N/A
.indicators[].confidence	Signature.Attribute	Confidence	.indicators[].activity.first_seen_ts	85	N/A
.indicators[].activity.first_seen_ts	Signature.Attribute	First Seen	.indicators[].activity.first_seen_ts	2025-10-14T17:44:03Z	N/A
.indicators[].activity.last_seen_ts	Signature.Attribute	Last Seen	.indicators[].activity.first_seen_ts	2025-10-14T17:44:03Z	N/A
.indicators[].pattern	Signature.Attribute	Pattern	.indicators[].activity.first_seen_ts	rule lazarus_stealer { ... }	N/A
.indicators[].pattern_type	Signature.Attribute	Pattern Type	.indicators[].activity.first_seen_ts	yara	N/A
.indicators[].pattern_version	Signature.Attribute	Pattern Version	.indicators[].activity.first_seen_ts	4	N/A
.indicators[].classification.girs[]	Signature.Attribute	Intelligence Requirement	.indicators[].activity.first_seen_ts	1.1 - Malware variants	Stored as path - name when Fetch GIR Names is enabled; otherwise

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					stored as the raw GIR path
.indicators[].threat.type	Signature.Attribute	Threat Type	.indicators[].activity.first_seen_ts	malware	N/A
.indicators[].threat.data.malware_family.id	Signature.Attribute	Malware Family ID	.indicators[].activity.first_seen_ts	malware-family--786a071e-...	N/A
.indicators[].threat.data.malware_family.name	Signature.Attribute	Malware Family	.indicators[].activity.first_seen_ts	lazarus_stealer	N/A

Known Issues / Limitations

- **Large Report Content** – some reports may contain extensive descriptions, inline images, or attachments that exceed ThreatQ platform or database size limitations. In these cases, oversized inline content may be removed from the report description to allow the report to be successfully ingested while preserving the associated intelligence and metadata.

Change Log

- **Version 2.0.0**
  - Migrated the integration to the Intel 471 Cloud APIs at `api.intel471.cloud`.
  - Updated authentication to use Basic authentication with `client_id` and `client_secret`.
  - Updated the primary malware reports feed to use the Intel 471 Reports API stream endpoint.
  - Updated the malware indicators and malware signatures supplemental feeds to use the Intel 471 Indicators API stream endpoint.
  - Added support for malware family, indicator type, and confidence-based filtering.
  - Added handling for large report descriptions to ensure oversized HTML content can be ingested safely.
  - Added support for `401` authentication and `403` authorization error handling as part of the Intel 471 Cloud API migration.
  - Updated the minimum ThreatQ version to 5.24.0
- **Version 1.1.0**
  - Updated the **Malware Indicators** supplemental feed endpoint to use the streaming API.
- **Version 1.0.2**
  - N/A
- **Version 1.0.1**
  - N/A