ThreatQuotient

Intel 471 Reports Action Bundle

Version 1.0.0

December 03, 2024

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

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: 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	1.0.0
Compatible with ThreatQ Versions	>= 6.5.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Intel 471 Reports Action Bundle integration enriches ThreatQ objects with threat intelligence reports from the feeds published by Intel 471.

The integration provides the following actions:

- **Intel 471 Reports Enrichment** - queries data against Intel 471 Reports.
- **Intel 471 Breach Alerts Enrichment** - queries data against Intel 471 Breach Alerts.
- **Intel 471 Spot Reports Enrichment** - queries data against Intel 471 Spot Reports.

The actions are compatible with the following object types:

- Adversary
- Indicator
- Malware

The actions return the following enriched system objects:

- Adversary
- Attack Pattern
- Indicator
- Malware
- Report

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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following object types:
  - Adversary
  - Indicator
  - Malware
- An Intel 471 API Key and associated Email account.
- The ThreatQ MITRE Enterprise ATT&CK CDF, MITRE Mobile CDF, and MITRE PRE-ATT&CK feeds should be installed on your ThreatQ instance. These three feeds are provided by the MITRE ATT&CK CDF integration, which is available on the ThreatQ Marketplace.

  MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for the MITRE TIDs extracted from Actor Profiles to be mapped to the corresponding MITRE ATT&CK attack patterns.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action(s).

Configuration

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

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

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

Reports Enrichment Parameters

PARAMETER	DESCRIPTION
Email Address	Enter the Intel 471 Email Address associated with your API Key.
API Key	Enter your Intel 471 API Key found within the Intel 471 Titan Portal.
Enable SSL Verification	Enable or Disable Host SSL certificate verification.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Report Location	Optional - Display reports related to a certain country or region. Examples include: "European Union" (as a region), "United Kingdom" (as a country). This parameter can only search for one location at a time.

PARAMETER	DESCRIPTION
Report Tag	Optional - Display reports related to a certain tag. Examples include: "Banking & Finance", "Tools", "Airlines", "Phishing", "Spam", "Credit Card Fraud". This parameter can only search for one tag at a time.
Report Type Filter	Select which report types to ingest into ThreatQ when the **Fetch Related Reports** parameter is enabled. Options include: ◦ Info Reports ◦ Breach Reports ◦ Intelligence Bulletins ◦ Underground Pulses ◦ Whitepapers ◦ Threat Briefs ◦ Intelligence Summaries ◦ Malware Campaigns ◦ Actor Profiles
Fetch Related Reports	When enabled, related reports will be fetched, parsed, and ingested. Enabling this parameter will require additional API calls and may increase the chance of timeout errors.
Related Report Family Filter	Select which related report types to ingest into ThreatQ when the **Fetch Related Reports** parameter is enabled. Options include ◦ Info Reports ◦ Finished Intelligence ◦ Spot Reports
Attribute Filter	Select which pieces of context to ingest into ThreatQ. Options include: ◦ GIRs ◦ Victims ◦ Victim Country ◦ Victim Industry ◦ Region Information ◦ Country Information ◦ Confidence Level ◦ Admiralty Codes ◦ Motivations ◦ Source Characterization ◦ Sensitive Source ◦ Portal URL ◦ First Activity ◦ Last Activity

PARAMETER	DESCRIPTION
Ingest Tags	Enable this parameter to ingest tags.
Fetch GIR Names	When enabled, GIR names will be fetched and used. **Example**: 5.2.1 - Initial Access Tactic. When disabled, GIRs names will be left in their raw format. **Example**: 3.1.1.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report ◦ Actor or Group ◦ Handles (Adversaries) ◦ Malware Families
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include: ◦ Malicious URLs ◦ Malicious Domains ◦ IP Addresses ◦ CVE IDs ◦ MD5 Hashes ◦ SHA-1 Hashes ◦ SHA-256 Hashes ◦ Actor Domains ◦ Actor Websites ◦ URLs ◦ File Paths ◦ Filenames ◦ 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 Indirect option is selected by default because the URLs are typically not malicious.
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect (default) ◦ Active

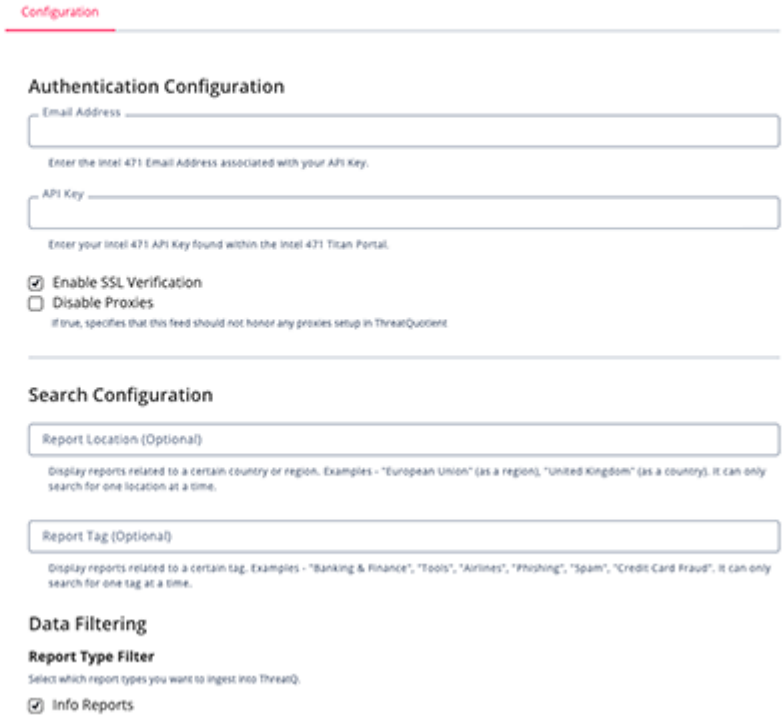
PARAMETER	DESCRIPTION
	◦ Review ◦ Whitelisted The Indirect option is selected by default because the actor domains are typically not malicious.
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted The Indirect option is selected by default because the actor websites are typically not malicious.
Objects Per Run	The number of objects to process per run of the workflow.

Intel 471 Reports Enrichment

Uninstall

Additional Information

Integration Type: Action
Version:
Action ID: 1
Accepted Data Types:
Adversaries
Malware
Indicators
CVE
Email Address
Filename
File Path
FQDN
IP Address
IPv6 Address
MD5
SHA-1
SHA-256
URL

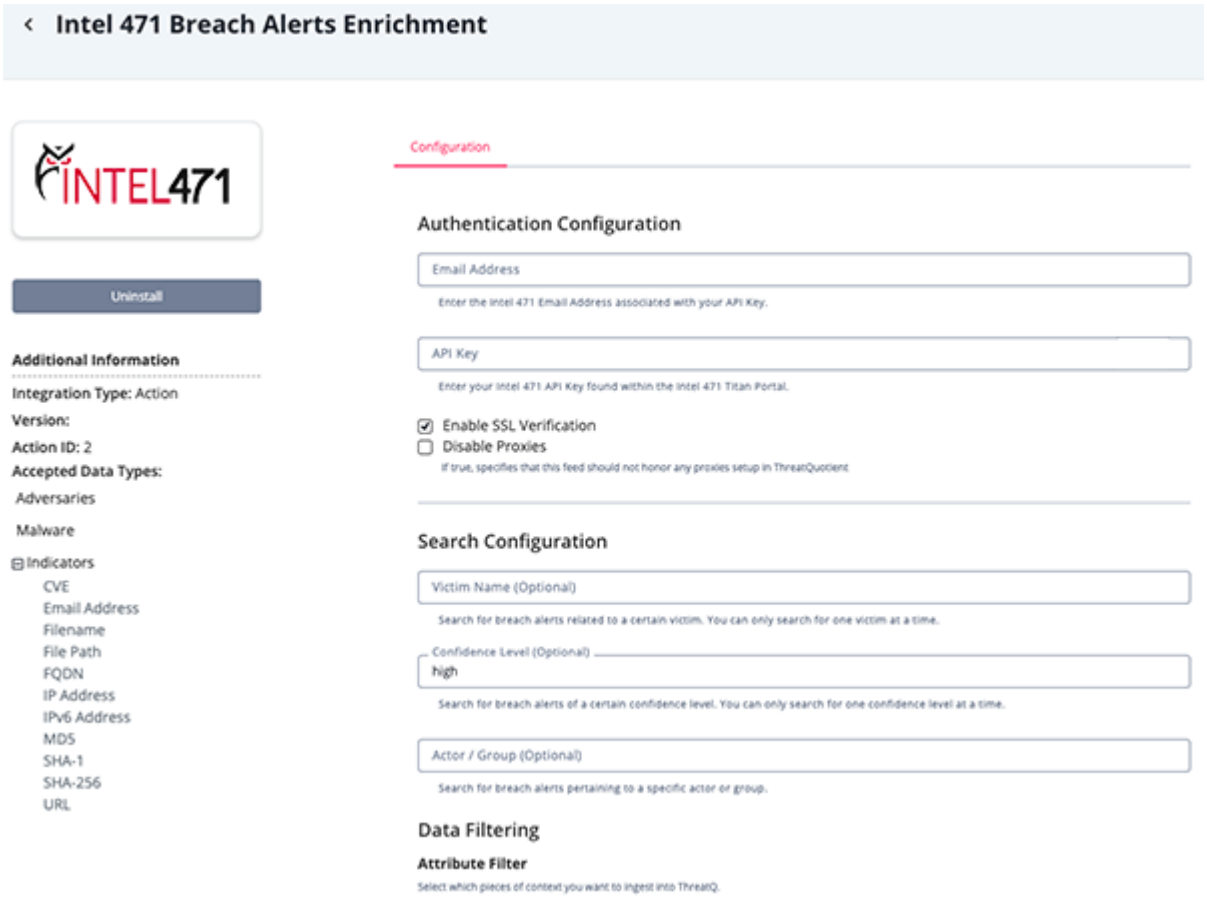


Breach Alerts Enrichment Parameters

PARAMETER	DESCRIPTION
Email Address	Enter the Intel 471 Email Address associated with your API Key.
API Key	Enter your Intel 471 API Key found within the Intel 471 Titan Portal.
Enable SSL Verification	Enable or Disable Host SSL certificate verification.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Victim Name	Optional - Search for breach alerts related to a certain victim.  You can only search for one victim at a time.
Confidence Level	Optional - Search for breach alerts of a certain confidence level.  You can only search for one confidence level at a time.
Actor / Group	Optional - Search for breach alerts pertaining to a specific actor or group.
Attribute Filter	Select which pieces of context to ingest into ThreatQ. Options include: ◦ GIRs ◦ Victims ◦ Victim Industries ◦ Victim Countries ◦ Confidence Level ◦ First Activity Date ◦ Last Activity Date
Fetch GIR Names	When enabled, GIR names will be fetched and used. **Example**: 5.2.1 - Initial Access Tactic.

PARAMETER	DESCRIPTION
	When disabled, GIRs names will be left in their raw format. **Example**: 3.1.1.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report ◦ Actor or Group ◦ Handles (Adversaries) ◦ Malware Families
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include: ◦ Malicious URLs ◦ Malicious Domains ◦ IP Addresses ◦ CVE IDs ◦ MD5 Hashes ◦ SHA-1 Hashes ◦ SHA-256 Hashes ◦ Actor Domains ◦ Actor Websites ◦ URLs ◦ File Paths ◦ Filenames ◦ 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 Indirect option is selected by default because the URLs are typically not malicious.
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted The Indirect option is selected by default because the actor domains are typically not malicious.

PARAMETER	DESCRIPTION
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted The Indirect option is selected by default because the actor websites are typically not malicious.
Objects Per Run	The number of objects to process per run of the workflow.

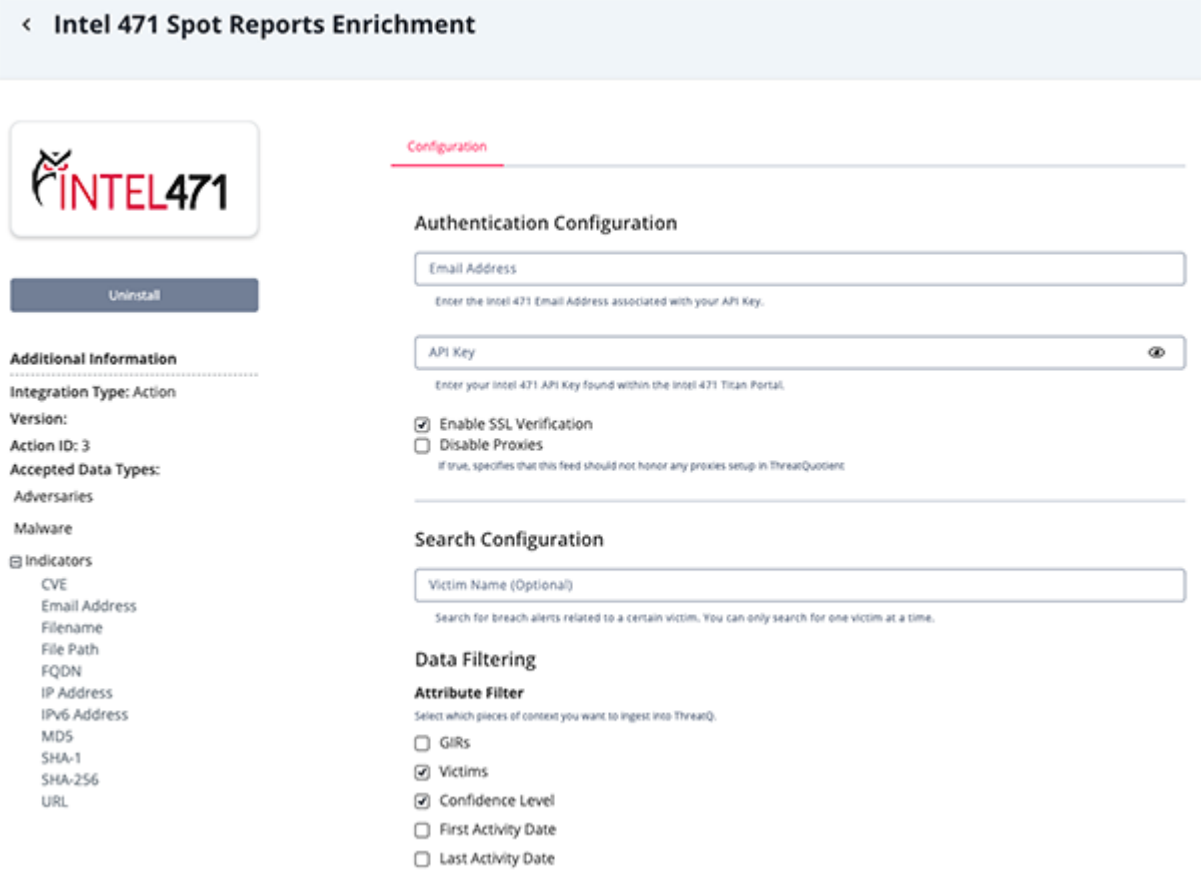


Spot Reports Enrichment Parameters

PARAMETER	DESCRIPTION
Email Address	Enter the Intel 471 Email Address associated with your API Key.
API Key	Enter your Intel 471 API Key found within the Intel 471 Titan Portal.
Enable SSL Verification	Enable or Disable Host SSL certificate verification.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Victim Name	Optional - Search for breach alerts related to a certain victim. You can only search for one victim at a time.
Attribute Filter	Select which pieces of context to ingest into ThreatQ. Options include: ◦ GIRs ◦ Victims ◦ Confidence Level ◦ First Activity Date ◦ Last Activity Date
Fetch GIR Names	When enabled, GIR names will be fetched and used. **Example**: 5.2.1 - Initial Access Tactic. When disabled, GIRs names will be left in their raw format. **Example**: 3.1.1.
Relationship Filter	Select which relationship context to ingest into ThreatQ. Options include: ◦ Actors Subject of Report ◦ Actor or Group ◦ Handles (Adversaries) ◦ Malware Families
Indicator Filter	Select which indicators to ingest into ThreatQ. Options include:

PARAMETER	DESCRIPTION
	◦ Malicious URLs ◦ Malicious Domains ◦ IP Addresses ◦ CVE IDs ◦ MD5 Hashes ◦ SHA-1 Hashes ◦ SHA-256 Hashes ◦ Actor Domains ◦ Actor Websites ◦ URLs ◦ File Paths ◦ Filenames ◦ 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 Indirect option is selected by default because the URLs are typically not malicious.
Actor Domain Status	Select the status to use for actor domains. Options include: ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted  The Indirect option is selected by default because the actor domains are typically not malicious.
Actor Website Status	Select the status to use for actor websites. Options include: ◦ Indirect (default) ◦ Active ◦ Review ◦ Whitelisted  The Indirect option is selected by default because the actor websites are typically not malicious.

PARAMETER	DESCRIPTION
Objects Per Run	The number of objects to process per run of the workflow.



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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Intel 471 Reports Enrichment	Queries data against Intel 471 Reports.	Indicator, Adversary, Malware	Indicators - CVE, Email Address, Filename, File Path, FQDN, IP Address, IPv6 Address, MD5, SHA-1, SHA-256, URL
Intel 471 Breach Alerts Enrichment	Queries data against Intel 471 Breach Alerts.	Indicator, Adversary, Malware	Indicators - CVE, Email Address, Filename, File Path, FQDN, IP Address, IPv6 Address, MD5, SHA-1, SHA-256, URL
Intel 471 Spot Reports Enrichment	Queries data against Intel 471 Spot Reports.	Indicator, Adversary, Malware	Indicators - CVE, Email Address, Filename, File Path, FQDN, IP Address, IPv6 Address, MD5, SHA-1, SHA-256, URL

Intel 471 Reports Enrichment

The Intel 471 Reports Enrichment action queries ThreatQ objects against Intel 471 Reports 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 action also will ingest related reports, if enabled via the **Fetch Related Reports** configuration parameter. These reports may also include Sport Reports.

The mapping for this action is defined in the Shared Data Mapping section.

`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 actorâ€™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, JuneÂ 16, 2023, the actor
<strong>yalishandaâ€™sÂ </strong>fast-flux network stands at 250Â total hosts.
There wereÂ 12Â hosts added to the network in the lastÂ 24 hours, whileÂ 15
hosts were dropped during this period.</p><p>The actor hosted phishing
campaigns targeting Amazon andÂ National Australia BankÂ (NAB) customers, and
PrivateLoader malware samples.</p>"
}
```

Intel 471 Breach Alerts Enrichment

The Intel 471 Breach Alerts Enrichment action queries ThreatQ objects against Intel 471 Breach Alerts intelligence stream.

> The mapping for this action is defined in the Shared Data Mapping section, after selecting the data within the `breach_alert` key.

`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 ransomwareÂ with theÂ
57e4a5c937bc58b01622997ca2acaa91cea2ff5cc9e7f9c4c8bf82349c23e0a9Â SHA-256. Our
monitoring of ransomware attacker communication revealed the sample likely was
used in an attack againstÂ the Ohio, U.S.-basedÂ Akron-Summit County Public
Library at theÂ akronlibrary.org website. The perpetrators allegedly deployed
the ransomware on or about May 30, 2023, exfiltrated about 71.2 GB of data and
demanded USÂ $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"
      }
    ]
  }
}
```

Intel 471 Spot Reports Enrichment

The Intel 471 Spot Reports Enrichment action queries ThreatQ objects against Intel 471 Spot Reports intelligence stream.

> The mapping for this action is defined in the Shared Data Mapping section, after selecting the data within the `spot_report` key.

`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"
      }
    ]
  }
}
```

Shared Data Mapping

ThreatQuotient provides the following default mapping for this action:

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	Updatable
`.activity.last`	Report Attribute	Last Activity	N/A	N/A	Updatable
`.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	`bc1ql5f3m75qx3ueu2pz5eeveyqsw6pdjs3ufk8r20`	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`
`.entities[]`	Related Indicator	IP Address	`.published_at`	N/A	When `type` == `IPAddress`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.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`	Updatable
`.sensitiveSource`	Report Attribute	Sensitive Source	N/A	`true`	N/A
`.admiraltyCode[0]`	Report Attribute	Admiralty Reliability	N/A	`A`	Updatable
`.admiraltyCode[1]`	Report Attribute	Admiralty Credibility	N/A	`1`	Updatable
`Telegram/Jabber`	Indicator Attribute	Platform	N/A	N/A	`Telegram` or `Jabber` based on indicator type and if `Telegram Usernames` or `Jabber Usernames` is

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

Enriched Data

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

Intel 471 Reports Enrichment

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 Breach Alerts Enrichment

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

Intel 471 Spot Reports Enrichment

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

Use Case Example

Intel 471 Reports Enrichment

1. A Threat Analyst identifies a collection of indicators they would like to enrich with Intel 471 Reports data.
2. The Threat Analyst configures the action with the desired parameters and enables the workflow.
3. The workflow executes the action and ingests all the reports found for the input values.

Intel 471 Breach Alerts Enrichment

1. A Threat Analyst identifies a collection of indicators they would like to enrich with Intel 471 Reports Breach Alerts.
2. The Threat Analyst configures the action with the desired parameters and enables the workflow.
3. The workflow executes the actions and ingests all the reports found for the input values.

Intel 471 Spot Reports Enrichment

1. A Threat Analyst identifies a collection of indicators they would like to enrich with Intel 471 Spot Reports data.
2. The Threat Analyst configures the action with the desired parameters and enables the workflow.
3. The workflow executes the action and ingests all the reports found for the input values.

Known Issues / Limitations

- API usage is limited to your Intel 471 rate limit. Be conscious of that limit and adjust the **Objects Per Run** configurations accordingly. An API call is made for each object.
- Images will be removed if the description is too long. This is due to a ThreatQ platform limitation.
- MITRE ATT&CK data is loaded from the cache memory that is refreshed every 24 hours.

Change Log

- **Version 1.0.0**
  - Initial release