ThreatQuotient

Intel 471 Reports CDF User Guide

Version 1.1.1

August 08, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

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	1.1.1
Compatible with ThreatQ Versions	>= 4.21.0
Support Tier	ThreatQ Supported

Introduction

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

The integration provides the following feeds:

- Intel 471 Reports - `https://api.intel471.com/v1/reports`
- Intel 471 Detailed Reports (Supplemental) - `https://api.intel471.com/v1/reports/:report_uid`
- Intel 471 SpotRep Detailed Reports (Supplemental) - `GET https://api.intel471.com/v1/spotReports/{uid}`

The integration ingests the following system objects:

- Adversaries
  - Adversary Attributes
- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes

Important Notes

- The supplemental feed is called for each record returned from Intel471 Reports and also for each UID in its similar_reports.
- Time constrained data fetching is possible.
- Uses basic HTTP authentication based on email address and API key.

Installation

Perform the following steps to install the integration:

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

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

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

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

You will still need to configure and then enable the feed.

Configuration

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

To configure the integration:

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

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

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

PARAMETER	DESCRIPTION
Count	The maximum number of records to retrieve from the provider per request (0-100). The default value is 10.
Report Location	Display reports related to a certain country or region. Examples: "European Union" (as a region), "United Kingdom" (as a country). The feed can only search for one location at a time.
Report Tag	Display reports related to a certain tag. Examples: "Banking & Finance", "Tools", "Airlines", "Phishing", "Spam", "Credit Card Fraud". The feed can only search for one tag at a time.
Email Address	Your Intel 471 account email address.
API Key	Your Intel 471 account API key.

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

ThreatQ Mapping

Intel 471 Reports

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

Sample Response:


```
{
    "reportTotalCount": 2,
    "reports": [
        {
            "uid":
"625bf3a87263f00e06b3cbf6cc7b6380d83fff93b7ef201d0c9e599fb6bd95bf",
            "admiraltyCode": "F4",
            "motivation": [
                "CC"
            ],
            "subject": "Possible Ukrainian actor MentoS128 (aka Silver128,
PapoKarlo) offers hacking service; Possible victims identified",
            "created": 1571659854000,
            "dateOfInformation": 1571115600000,
            "sourceCharacterization": "Information was derived from Russian-
language cybercrime forum XSS and our sensitive and reliable source.",
            "entities": [
                {
                    "type": "EmailAddress",
                    "value": "kremz@mail.ua"
                },
                {
                    "type": "EmailAddress",
                    "value": "silver_mix@ukr.net"
                },
                {
                    "type": "Handle",
                    "value": "aleksandrkremnikonov"
                }
            ],
            "locations": [
                {
                    "region": "Asia",
                    "country": "India",
                    "link": "impacts"
                },
                {
                    "region": "Asia",
                    "country": "Taiwan",
                    "link": "impacts"
```

```
                }
            ],
            "tags": [
                "Database Dumps",
                "Extortion",
                "Injects",
                "IoT (Internet of Things)",
                "Ransomware"
            ],
            "portalReportUrl": "https://titan.intel471.com/report/
10757ae14960b92e04733023130fce5e",
            "lastUpdated": 1571660657176,
            "actorSubjectsOfReport": [
                {
                    "handle": "MentoS128",
                    "aliases": [
                        "Silver128",
                        "PapoKarlo"
                    ]
                }
            ],
            "similarReports": [
                {
                    "uid":
"aa210760432ea8bf21ed3bf42068c365bf8fa34fd4c678d321ef066055625e45",
                    "admiraltyCode": "B2",
                    "motivation": [
                        "CC"
                    ],
                    "subject": "Russian actor, bulletproof hoster yalishanda's
(aka downlow, stas_vl) new control panel for fast-flux service reviewed",
                    "dateOfInformation": 1545976800000,
                    "sourceCharacterization": "Information was derived from the
Russian-language cybercrime forum Exploit, our actors' database, and our
sensitive and reliable source.",
                    "portalReportUrl": "https://titan.intel471.com/report/
4cd457bd47c42dae80f8dbf0305c3a76"
                }
            ]
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
value.uid	Report.Value	Call Intel471 Detailed Report	N/A	bfe7a5d22fe3666243085f226bc92 fb23191e8f48071f101038e6d0ba8ffb13d	N/A
value.relatedReports.uid	Report.Value	Call Intel471 Detailed Report	N/A	7e922e21655c28731812e4f15820c815	N/A

Intel 471 Detailed Reports (Supplemental)

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

Sample Response:


```
{
    "uid": "cc00f36dfd4cdb899637546cb86e1a2be4dd96e2096db0dfe7da9e2557469dbc",
    "admiraltyCode": "B4",
    "motivation": [
        "CC"
    ],
    "subject": "Possible Russian actor SOLDATKIN (aka dDonry, Hellpein, lOoOl,
Rocfor, Soldat554, 2+2=5000, Joker5218) offers to sell remote access trojan
based on remote manipulator system malware",
    "researcherComments": "<p><strong>Assessment of credibility</strong></
p>\r\n\r\n<p><strong>SOLDATKIN </strong>is a Russian-speaking ...",
    "rawText": "<p>On Oct. 1, 2019, the actor ((<strong>SOLDATKIN</strong>))
posted the following on the XSS forum:<br />\r\n---</p>\r\n\r\n....",
    "rawTextTranslated": "<p>On Oct. 1, 2019, the
actor <strong>SOLDATKIN</strong> posted the following on the XSS
forum:<br />\r.....",
    "created": 1570534310000,
    "dateOfInformation": 1569906000000,
    "sourceCharacterization": "Information was derived from the Russian-
language cybercrime forum XSS and our sensitive and reliable source.",
    "entities": [
        {
            "type": "EmailAddress",
            "value": "denis.soldatkin@bk.ru"
        },
        {
            "type": "Handle",
            "value": "2+2=5000"
        },
        {
            "type": "Handle",
            "value": "dDonry"
        },
        {
            "type": "Handle",
            "value": "Denis Soldatkin"
        },
        {
            "type": "Handle",
            "value": "GGGGG IOILA"
        }
    ],
    "locations": [
        {
```

```
            "region": "Europe",
            "country": "Russia",
            "link": "originated_from"
        }
    ],
    "tags": [
        "Crypters & Packers",
        "Malware",
        "Tools"
    ],
    "portalReportUrl": "https://titan.intel471.com/report/
08ec0068f2a36e01b8066f0e67420824",
    "lastUpdated": 1570534757790,
    "actorSubjectsOfReport": [
        {
            "handle": "SOLDATKIN",
            "aliases": [
                "dDonry",
                "Hellpein",
                "lOoOl",
                "Rocfor",
                "Soldat554",
                "2+2=5000",
                "Joker5218"
            ]
        }
    ],
    "reportAttachments": [
        {
            "fileName": "attachment-157017573009333.zip",
            "url": "https://api.intel471.com/v1/reports/
cc00f36dfd4cdb899637546cb86e1a2be4dd96e2096db0dfe7da9e2557469dbc/download/
23cc2a8b7e4eaf7fe1a982da34f24c8f/attachment-157017573009333.zip",
            "fileSize": 49680
        }
    ],
    "similarReports": [
        {
            "uid":
"aa210760432ea8bf21ed3bf42068c365bf8fa34fd4c678d321ef066055625e45",
            "admiraltyCode": "B2",
            "motivation": [
                "CC"
            ],
            "subject": "Russian actor, bulletproof hoster yalishanda's (aka
downlow, stas_vl) new control panel for fast-flux service reviewed",
            "dateOfInformation": 1545976800000,
            "sourceCharacterization": "Information was derived from the
Russian-language cybercrime forum Exploit, our actors' database, and our
sensitive and reliable source.",
```

```
            "portalReportUrl": "https://titan.intel471.com/report/
4cd457bd47c42dae80f8dbf0305c3a76"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.subject	Report.value	Value	.publishedAt	"Possible Russian actor SOLDATKIN (aka dDonry, Hellpein, lOoOl, Rocfor, Soldat554, 2+2=5000, Joker5218)...."	N/A
.researcherComments, .rawText	Report.description	Description	N/A	"Researcher Comments: **Assessment of credibility** ... Raw Text: On Oct. 1, 2019, the actor ((**SOLDATKIN**))...."	The report description will have both the .researcherComments and .rawText values concatenated. It will be limited to 32630 characters.
.created or .dateOfInformation	Report.published_at	Published At	N/A	"1570534310000"	formatted
.uid	Report.Attribute	Intel471 Report ID	.publishedAt	"cc00f36dfd4cdb899637546cb86e1a2be4dd96e2096db0dfe7da9e2557469dbc"	N/A
.sourceCharacterization	Report.Attribute	Intel471 Source	.publishedAt	"Information was derived from the Russian-language cybercrime forum XSS and our sensitive and reliable source."	N/A
.locations.region	Report.Attribute	Region	.publishedAt	"Russia"	N/A
.locations.country	Report.Attribute	Country	.publishedAt	"United States"	N/A
.portalReportURL	Report.Attribute	Intel471 Portal URL	.publishedAt	"https://titan.intel471.com/report/08ec0068f2a36e01b8066f0e67420824"	N/A
.tags	Report.Attribute	Intel471 Tags	.publishedAt	["Crypters & Packers", "Malware", "Tools"]	N/A
.admiralityCode[0]	Report.Attribute	Intel471 Admiralty Reliability	.publishedAt	"B"	N/A
.admiralityCode[1]	Report.Attribute	Intel471 Admiralty Credibility	.publishedAt	"4"	N/A
.motivation	Report.Attribute	Intel471 Motivation	.publishedAt	"CC"	N/A
.entities.value	Adversary.name	N/A	N/A	"coolcat"	if ["type"] == "Handle"
.entities.value	Indicator.value	N/A	N/A	"ch4rgui@hotmail.fr"	if ["type"] != "Handle"
.entities.type	Indicator.type	N/A	N/A	"EmailAddress"	indicator_type_map if ["type"] != "Handle"

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.actorSubjectsOfReport.aliases	Adversary.Attribute	Aliases	N/A	["dDonry", "Hellpein"]	Where actorSubjectsOfReport.handle == adversary.name

Created Indicators and Adversaries will have the same attributes as the Report objects.

Intel 471 SpotRep Detailed Reports

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

Sample Response:


```
{
    "activity": {
        "first": 1648729947000,
        "last": 1648733764000
    },
    "last_updated": 1648733764000,
    "uid": "4d2e7db6cd285a46e661ff85874e274f",
    "data": {
        "spot_report": {
            "uid": "4d2e7db6cd285a46e661ff85874e274f",
            "spot_report_data": {
                "related_reports": [
                    "3bd7fdc2d11f26c5c6185c2a3d96529e"
                ],
                "victims": [
                    {
                        "name": "Ministry of Foreign Affairs of Ukraine",
                        "urls": [
                            "https://www.mfa.gov.ua/"
                        ]
                    }
                ],
                "date_of_information": 1648684800000,
                "text": "[POSSIBLE BREACH ALERT] On March 31, 2022, the Russian
hacktivist group XakNet Team made several posts on its Telegram channel
@xaknet_team claiming to breach the Ministry of Foreign Affairs of Ukraine and
allegedly downloaded “all available documents.” The group published a portion
of the allegedly stolen documents on its Telegram channel as proof of the
claim. Our reliable source reported the attackers could have compromised a
document management system the ministry used. However, further analysis is
required to verify the attackers’ claim. Intel 471 will continue to monitor the
situation.",
                "intel_requirements": [
                    "5.5.3",
                    "6.2.4.51"
                ],
                "version": "1",
                "links": [
                    {
                        "type": "internal",
                        "url": "https://titan.intel471.com/ims_thread/
5f0ad4db43d8723d18169b2e4817a160?message_uid=e9b51b4e636b53399b4b87dabf634dff",
                        "title": "Telegram post #1"
                    },
```

```
                    {
                        "type": "internal",
                        "url": "https://titan.intel471.com/ims_thread/
5f0ad4db43d8723d18169b2e4817a160?message_uid=ac5eb7e6d53d808f1caa17eb8f731f4b",
                        "title": "Telegram post #2"
                    }
                ],
                "released_at": 1648729947000,
                "title": "Russian hacktivist group XakNet Team claims
compromise, data breach impacting Ministry of Foreign Affairs of Ukraine"
            }
        },
        "entities": [
            {
                "type": "Telegram",
                "value": "@xaknet_team"
            },
            {
                "type": "Handle",
                "value": "XakNet Team"
            }
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.spot_report.spot_report_data.title	Report.Value	N/A	.data.spot_report.spot_report_data.released_at	Threat group LAPSUS$ suggests possible involvement	Limited to 254 characters.
.data.spot_report.spot_report_data.text	Report.Description	N/A	.data.spot_report.spot_report_data.released_at	[POSSIBLE BREACH ALERT] On Jan. 9, 2022, the ..	It will be limited to 32630 characters.
.data.spot_report.spot_report_data.title	Report.Attribute	Spot Report Title	.data.spot_report.spot_report_data.released_at	Threat group LAPSUS$ suggests possible involvement in cyberattack against Vodafone Portugal	N/A
N/A	Report.Attribute	Report Type	.data.spot_report.spot_report_data.released_at	Spot Report	Hardcoded attribute
.uid	Report.Attribute	Intel 471 Spot Report Link	.data.spot_report.spot_report_data.released_at	014f7a860a14924b5cb74eeb	Formatted as `https://titan.intel471.com/spotReports/{{.alerts[].spotReport.uid}}
.data.spot_report.spot_report_data.victims[].name	Report.Attribute	Victim	.data.spot_report.spot_report_data.released_at	N/A	N/A
.data.spot_report.spot_report_data.victims[].urls[]	Report.Attribute	Victim URL	.data.spot_report.spot_report_data.released_at	N/A	N/A
.data.spot_report.spot_report_data.sensitive_source	Report.Attribute	Sensitive Source	.data.spot_report.spot_report_data.released_at	True	N/A
.data.spot_report.spot_report_data.intel_requirements[]	Report.Attribute	Intelligence Requirements	.data.spot_report.spot_report_data.released_at	1.1.3	N/A
.data.spot_report.spot_report_data.links[].title + .data.spot_report.spot_report_data.links[].url	Report.Attribute	Linked Entity	.data.spot_report.spot_report_data.released_at	Forum thread - https://titan.intel471.com/post_thread/a6bff640bf0c8d0ea31544878935e3a6	N/A
.data.entities[].value	Related Adversary.Value	N/A	.data.spot_report.spot_report_data.released_at	LAPSUS$	if ["type"] is `Handle`
.data.entities[].value	Related Indicator.Value	.alerts[].spotReport.data.entities[].type	.data.spot_report.spot_report_data.released_at	72.217.16.46	

Indicator Type Mapping

ThreatQuotient provides the following indicator type mapping:

INTEL 471	THREATQ INDICATOR
MD5	MD5
IPAddress	IP Address
ActorDomain	FQDN
ActorWebsite	URL
EmailAddress	Email Address
MaliciousURL	URL
SHA256	SHA-256
SHA1	SHA-1
URL	URL

Average Feed Run

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

Intel 471 Reports

METRIC	RESULT
Run Time	70 minutes
Indicators	1,351
Indicator Attributes	30,216
Adversaries	115
Adversary Attributes	2,216
Reports	9
Reports Attributes	163

Change Log

- **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.