ThreatQuotient

PwC Threat Intelligence CDF

Version 1.0.0

March 19, 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	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The PwC Threat Intelligence integration allows you to ingest the latest intelligence reports and Indicators. The integration also provides you with the ability to download and ingest intelligence reports as PDFs.

The integration provides the following feeds:

- **PwC Threat Intelligence Indicators -** retrieves from PwC IOCs of type domain, hash, IP Address, and URL, and saves them to ThreatQ.
- **PwC Threat Intelligence Reports -** retrieves intelligence reports from PwC and saves them in ThreatQ as PDFs.
- **PwC Threat Intelligence News -** retrieves latest intelligence reports and ingests them into ThreatQ.
- **PwC Threat Intelligence Actors -** retrieves all PwC Actors created in the given time range.

The integration ingests the following system objects:

- Adversaries
- Campaigns
- Files
- Indicators
    - Indicator Attributes
- Reports

Prerequisites

The integration requires the following:

- PwC Client ID
- PwC 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 yaml integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the yaml 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.

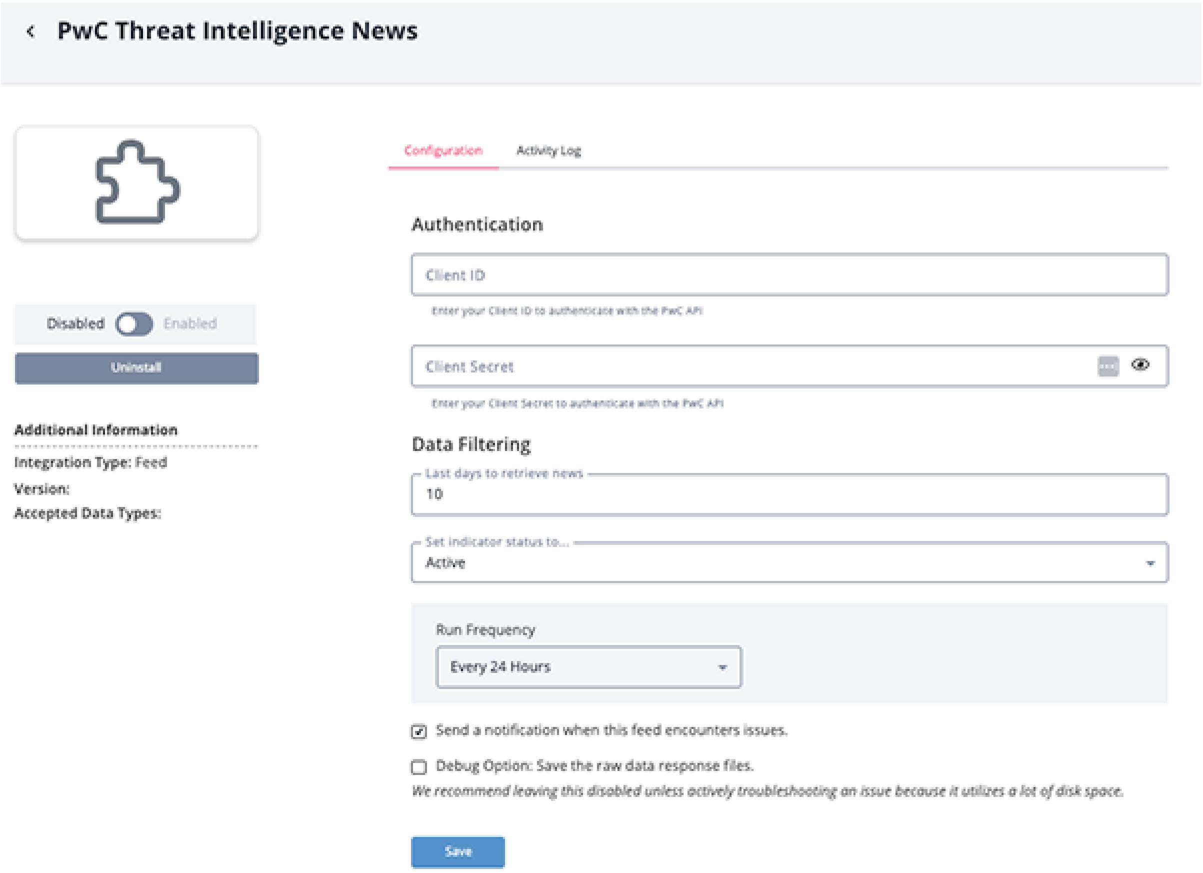
To configure the integration:

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
Client ID	Your Client ID used to authenticate with the PwC API.
Client Secret	Your Client Secret used to authenticate with the PwC API.
Lays Days to Retrieve News *(PwC Threat Intelligence News feed only)*	Select the number of days back to start the query. The default value is 10. The maximum number of days back allowed is 99. Using a greater value than 99 will result in a 404 error from the PwC API.



‹ PwC Threat Intelligence News

Configuration | Activity Log

Disabled ○ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Authentication

Client ID

Enter your Client ID to authenticate with the PwC API

Client Secret

Enter your Client Secret to authenticate with the PwC API

Data Filtering

Last days to retrieve news: 10

Set indicator status to...: Active

Run Frequency: Every 24 Hours

☑ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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

PwC Threat Intelligence Indicators

The PwC Threat Intelligence Indicators feed ingests IOCs of type domain, hash, IP Address, and URL into ThreatQ.

Get Domains

`GET https://api.threatintel.io/v1/domains/filter/range`

Sample Response:

```
{
  "total_pages": 1,
  "total_rows": 18,
  "data": [
    {
      "domain": "service-lew09ujr-1307700818.sh.apigw.tencentcs.com",
      "create_time": "2023-12-04T12:24:46.952886+00:00",
      "uid": "664ebef9-38d7-4f70-acbf-b7087f9846c0",
      "campaign_name": null,
      "threat_actor": [
        "Heuristic and General"
      ],
      "report_id": null,
      "threat_status": "{malicious}",
      "tlp": [
        "amber"
      ],
      "source": [
        "hendrix"
      ],
      "confidence": null
    }
    ]
    }
```

Get IPs

`GET https://api.threatintel.io/v1/ip/filter/range`

Sample Response:

```
{
  "total_pages": 4,
  "total_rows": 115,
  "data": [
    {
      "create_time": "2023-12-03T01:00:39.832426+00:00",
      "uid": "56bbb193-a51d-4e2c-b4e7-72161629f91c",
      "campaign_name": [
        "Automated infrastructure tracking: ShadowPad"
      ],
      "threat_actor": null,
      "report_id": null,
      "ip": "208.76.222.168",
      "threat_status": null,
      "tlp": [
        "AMBER"
      ],
      "source": [
        "infrastructure-tracking"
      ]
    }
    ]
    }
```

Get URLs

`GET https://api.threatintel.io/v1/urls/filter/range`

Sample Response:

```
{
  "total_pages": 8,
  "total_rows": 223,
  "data": [
    {
      "uid": "c0b7181a-eceb-4ca2-8a3c-a8ec5b6e85b7",
      "threat_actor": [
        "teal kurma"
      ],
      "url": "http://108.61.103.186/sy.php",
      "confidence": "HIGH",
      "create_time": "2023-12-04T14:39:27.899000+00:00",
      "tlp": [
        "AMBER"
      ],
      "report_id": "CTO-TIB-20231204-01A"
    }
    ]
    }
```

Get Hashes

`GET https://api.threatintel.io/v1/hashes/filter/range`

Sample Response:

```
{
  "total_pages": 3,
  "total_rows": 61,
  "data": [
    {
      "create_time": "2023-12-04T08:42:54.035000+00:00",
      "uid": "49f89038-a852-43d0-924a-92a5d020d212",
      "tlp": [
        "AMBER"
      ],
      "sha1": "ADF7DA29F70F6A4C62EC88DA1841752CE13941A7",
      "sha256":
"3CAEABD7CBEB5E305C627FA501F19F91F21E3D31EEE2E289DC43C6A669F069DB",
      "md5": "DEA5C8F4ACAC0391F5EE7713E76FD043",
      "threat_actor": [
        "Red Icarus"
      ],
      "report_id": null,
      "source": [
        "maltego",
        "yara"
      ],
      "campaign_name": "Red Icarus"
    }
    ]
    }
```

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[].domain	Indicator Value	FQDN	`data[].create_time`	service-lew09ujr-1307700818.sh.apigw.tencentcs.com	N/A
data[].ip	Indicator Value	IP Address	`data[].create_time`	208.76.222.168	N/A
data[].url	Indicator Value	URL	`data[].create_time`	https://swissborg.blog/tx/10299301992/hash	N/A
data[].md5	Indicator Value	MD5	`data[].create_time`	DEA5C8F4ACAC0391F5EE7713E76FD043	N/A
data[].sha1	Indicator Value	SHA-1	`data[].create_time`	ADF7DA29F70F6A4C62EC88DA1841752CE13941A7	N/A
data[].sha256	Indicator Value	SHA-256	`data[].create_time`	3CAEABD7CBEB5E305C627FA501F19F91F21E3D31EEE2E289DC43C6A669F069DB	N/A
data[].tlp	Indicator TLP	N/A	`data[].create_time`	AMBER	N/A
data[].confidence	Indicator Attribute	Confidence	`data[].create_time`	HIGH	Updated at ingestion time
data[].uid	Indicator Attribute	Indicator UID	`data[].create_time`	56bbb193-a51d-4e2c-b4e7-72161629f91c	N/A
data[].report_id	Indicator Attribute	Report ID	`data[].create_time`	N/A	n/A
data[].source[]	Indicator Attribute	Source	`data[].create_time`	infrastructure-tracking	Source list values joined by ','.
data[].threat_status	Indicator Attribute	Threat Status	`data[].create_time`	N/A	N/A
data[].threat_actor	Adversary Value	N/A	`data[].create_time`	Red Icarus	N/A
data[].campaign_name	Campaign Value	N/A	`data[].create_time`	Automated infrastructure tracking: ShadowPad	N/A

PwC Threat Intelligence Reports

The PwC Threat Intelligence Reports feed ingests intelligence reports from PwC into ThreatQ as PDFs.

`GET https://api.threatintel.io/v1/reports/filter/range`

Sample Response:

```
{
  "total_pages": 1,
  "total_rows": 16,
  "data": [
    "CTO-UTL-20221221-01A",
    "CTO-UTL-20221202-01A",
    "CTO-UTL-20221010-01A",
    "CTO-UTL-20220701-01A"
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`Report_`+data[]	File Title	File	N/A	Report_CTO-UTL-20221221-01A	Data items are used to create File title and to request PDF generation and after that to download PDF content and update the file with it.

> Data items are used to create File title in the format: `Report_{report_id}` and is sent to `PwC Schedule Report` for PDF generation.

PwC Schedule Report (Supplemental)

```
GET https://api.threatintel.io/v1/reports/pdf/schedule/{report_id}
```

Sample Response:

```
{
  "link": "/reports/pdf/2Zq88v0UeH39XCpOVUrA1zeQEqB/download/CTO-
UTL-20221221-01A",
  "message": "Report is being processed. Please visit the following link in 5
seconds.The link is valid for a day."
}
```

> The `link` is used to download the content of the PDF and ingest it in ThreatQ File object.

PwC Download PDF (Supplemental)

```
GET https://api.threatintel.io/v1{report_link}
```

PwC Threat Intelligence News

The PwC Threat Intelligence News feed retrieves intelligence reports for the last user-specified amount of days and ingests them into the ThreatQ platform.

`GET https://api.threatintel.io/v1/news/{days}`

Sample Response:

```
{
  "data": [
    {
      "create_time": "2023-11-22T17:45:54.637617+00:00",
      "title": "Ongoing CyberLink supply chain attack attributed to Black
Artemis (Diamond Sleet, Labyrinth Chollima)",
      "bullets": [
        "We are aware of an ongoing supply chain attack using a trojanised
version of CyberLink software. Microsoft has linked the attack to the North
Korea-based Black Artemis subgroup known as Diamond Sleet (formerly ZINC) /
Labyrinth Chollima.",
        "Microsoft has reported that the supply chain attack has been ongoing
since at least 20th October 2023. The threat actor is staging the malicious
files on compromised CyberLink update infrastructure, and has signed the
malicious versions of CyberLink software with a valid certificate issued to
CyberLink Corp.",
        "The compromised CyberLink installers, dubbed LambLoad, are being used
as downloaders for an encrypted payload that masquerades as a PNG file.",
        "We are working on an intelligence product on this topic; in the
meantime, if you use CyberLink software, consider threat hunting in your
environment for the activity highlighted in this post: https://
www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-
compromise-distributes-a-modified-cyberlink-installer/"
      ],
      "tlp": "GREEN"
    }
  ]
}
```

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[].title	Report Title	N/A	data[].create_time	Ongoing CyberLink supply chain attack attributed to Black Artemis (Diamond Sleet, Labyrinth Chollima)	N/A
data[].bullets	Report Description	N/A	data[].create_time	We are aware of an ongoing supply chain attack using a trojanised version of CyberLink software...	Constructed by joining bullets by <br />
data[].tlp	Report TLP	N/A	data[].create_time	GREEN	N/A

PwC Threat Intelligence Actors

The PwC Threat Intelligence Actors feed retrieves all PwC Actors created in the given time range.

`GET https://api.threatintel.io/v1/actors/all`

Sample Response:

```
{
  "total_pages": 3,
  "total_rows": 219,
  "data": [
    {
      "create_time": "2022-08-29T17:53:32.734032+00:00",
      "uid": "07a3bc63-199d-4dbf-b0e1-e1b71db2ab29",
      "name": "White Dev 115",
      "type": "White",
      "aliases": [
        "Black Basta"
      ],
      "country_origin": [
        "unknown"
      ],
      "country_origin_iso": [
        "UNKNOWN"
      ],
      "country_targets": [
        "Switzerland",
        "United States",
        "Germany",
        "France",
        "Netherlands"
      ],
      "country_targets_iso": [
        "CH",
        "US",
        "DE",
        "FR",
        "NL"
      ],
      "sector_targets": [
        "Construction",
        "Financial Services",
        "Legal",
        "Manufacturing",
        "Professional Services",
        "Retail",
        "Utilities"
      ],
      "threat_category": [
        "Cyber Crime"
      ],
      "ti_teams": [
        "CRIME"
      ],
      "pwc_projects": [],
      "byline": "White Dev 115 is the PwC name given to the operator behind the
Ransomware-as-a-Service (RaaS) programme known in open source as Black Basta.
This is an operation that first appeared in April 2022, and has since gathered
traction amongst the RaaS marketplace, attracting affiliates to conduct
multiple ransomware intrusions against victims based in either the United
States or central Europe. \r\n\r\nDue to the timing of the Black Basta RaaS
appearing on the scene, which was in-line with an initial reduction in activity
of the Conti RaaS (operated by a threat actor PwC tracks as Blue Cronus), there
has been much speculation in regards to whether Black Basta is infact a rebrand
of Conti, engineered by Blue Cronus. PwC's threat intelligence team is
unwilling to make such attribution claims at this time, instead choosing to
track Black Basta's operator as its own entity. This decision is based on our
analysis of both Black Basta and Conti ransomware binaries, with little in the
way of codebase overlaps for us to make any firm attribution assessment.",
      "last_edited_guid": "2EyitwtA0rHdCJGPidSycKkToCs",
      "pk": "2GXMr21G2wOI1kFEfrBspdEBgIf"
    }
]
}
```

ThreatQuotient provides the following mapping for this feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].name	Adversary Name	N/A	data[].create_time	White Dev 115	N/A
data[].byline	Adversary Description	N/A	data[].create_time	White Dev 115 is the PwC name given to the operator behind the Ransomware-as-a-Service (RaaS) programme known in open source...	N/A
data[].uid	Adversary Attribute	UID	data[].create_time	07a3bc63-199d-4dbf-b0e1-e1b71db2ab29	N/A
data[].threat_category	Adversary Attribute	Category	data[].create_time	Cyber Crime	Updated at ingestion. If there are multiple values, they will ve joined by ', '
data[].country_targets_iso	Adversary Attribute	Target Country Code	data[].create_time	"CH","US","DE","FR","NL"	Updated at ingestion. If there are multiple values, they will ve joined by ', '
data[].country_origin_iso	Adversary Attribute	Origin Country Code	data[].create_time	unknown	Updated at ingestion. If

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					there are multiple values, they will ve joined by ', '
data[].aliases	Adversary Attribute	Adversary Alias	data[].create_time	Black Basta	Updated at ingestion. If there are multiple values, they will ve joined by ', '

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.

PwC Threat Intelligence Indicators

METRIC	RESULT
Run Time	3 min
Indicators	1257
Indicator Attributes	2864
Adversaries	7
Campaign	146

PwC Threat Intelligence Reports

METRIC	RESULT
Run Time	1 min
Files	13

PwC Threat Intelligence News

METRIC	RESULT
Run Time	1 min
Reports	6

PwC Threat Intelligence Actors

METRIC	RESULT
Run Time	1 min
Adversaries	100
Adversary Attributes	479

Known Issues / Limitations

- The maximum days for **PwC Threat Intelligence News** in 99. For any higher number of days, the API returns 404 Error.

Change Log

- **Version 1.0.0**
    - Initial release