ThreatQuotient

Adversary Reader CDF

Version 1.0.0 rev-a

September 05, 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	>= 5.26.0
Support Tier	ThreatQ Supported

Introduction

The Adversary Reader CDF retrieves and parses adversary and related information from the APT Groups and Operations Google spreadsheet and ingests the threat data into the ThreatQ platform.

The integration provides the following feed:

- **Adversary Reader CDF** - captures and parses adversary information from the APT Groups and Operations Google sheet.

The integration ingests the following system objects:

- Adversaries
  - Adversary Attributes
- Files (Attachments)

Prerequisites

The following is required to run the integration:

- The Google Sheets API must be enabled - see **Enable and Disable APIs** Google Answer topic: https://support.google.com/googleapi/answer/6158841?hl=en&ref_topic=7013279&sjid=10854679303228498060-NA
- Google API Key - see the **Setting up API Keys** Google Answer topic: https://support.google.com/googleapi/answer/6158862?hl=en.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the 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 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.

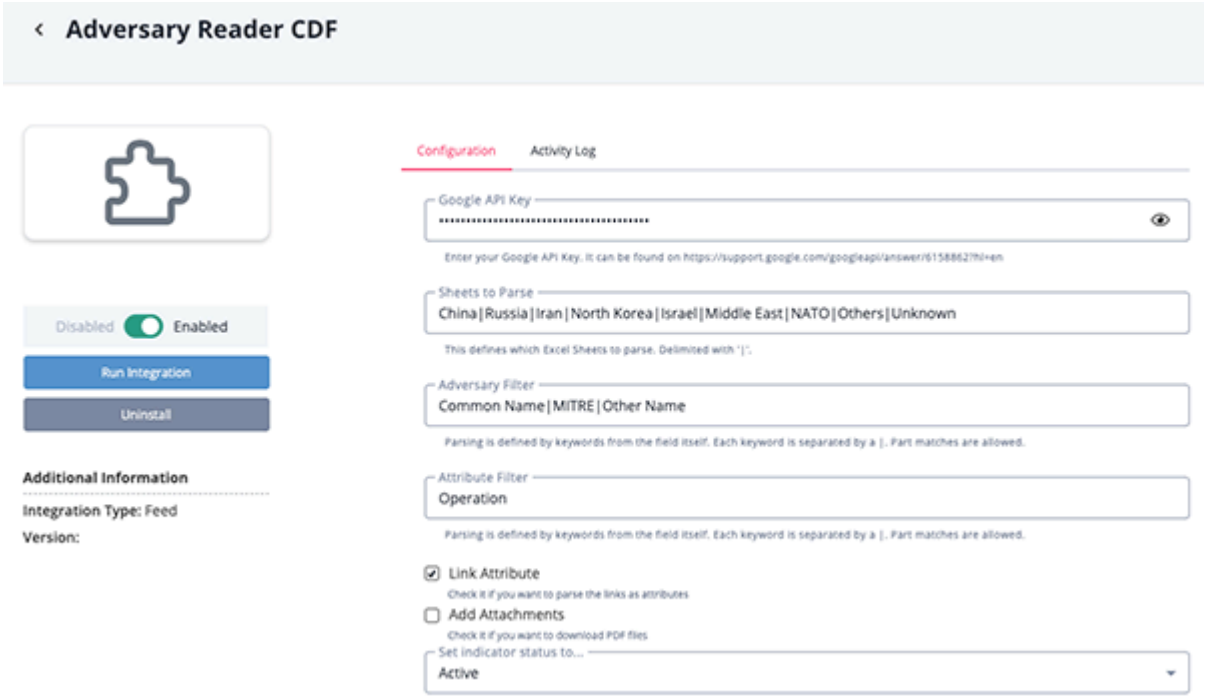
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** 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
Google API Key	Your Google API Key. See the following Google Answer topic for more information: https://support.google.com/googleapi/answer/6158862?hl=en.
Sheets to Parse	Define the google sheets to parse. Delimit sheets with `|` . The default is `China|Russia|Iran|North Korea|Israel|Middle East|NATO|Others|Unknown`.
Adversary Filter	Filter adversaries by parsing via keywords. Each keyword should be separated by a `|`. Partial matches are allowed.
Attribute Filter	Filter attributes by parsing via keywords. Each keyword should be separated by a `|`. Partial matches are allowed.
Link Attribute	Enable this option to parse links as attributes.
Add Attachments	Enable this option to download PDF files.



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

Adversary Reader CDF

The Adversary Reader feed captures and parses adversary information from the APT Groups and Operations Google sheet.

`GET https://sheets.googleapis.com/v4/spreadsheets/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/values/{sheet}`

Sample Response:


```
{
    "range": "China!A1:BY1008",
    "majorDimension": "ROWS",
    "values": [
        [
            "China"
        ],
        [
            "Common Name",
            "CrowdStrike",
            "IRL",
            "Kaspersky",
            "Secureworks",
            "Mandiant",
            "FireEye",
            "Symantec",
            "iSight",
            "Cisco (Sourcefire/VRT > Talos)",
            "Palo Alto Unit 42",
            "Other Names",
            "MITRE ATTCK",
            "Operation 1",
            "Operation 2",
            "Operation 3",
            "Operation 4",
            "Toolset / Malware",
            "Targets",
            "Modus Operandi",
            "Overlaps to",
            "Comment",
            "Link 1",
            "Link 2",
            "Link 3",
            "Link 4",
            "Link 5",
            "Link 6",
```

```
            "Link 7",
            "Link 8",
            "Link 9",
            "Link 10",
            "Link 11",
            "Link 12",
            "Link 13",
            "Link 14",
            "Link 15",
            "Link 16",
            "Link 17",
            "Link 18",
            "Link 19",
            "Link 20",
            "Link 21",
            "Link 22",
            "Link 23",
            "Link 24",
            "Link 25"
        ],
        [
            "Comment Crew",
            "Comment Panda",
            "PLA Unit 61398",
            "",
            "TG-8223",
            "APT1",
            "",
            "",
            "BrownFox",
            "Group 3",
            "",
            "GIF89a, ShadyRAT, Shanghai Group, Byzantine Candor",
            "G0006",
            "Shady RAT",
            "GhostNet",
            "",
            "",
            "WEBC2, BISCUIT and many others",
            "U.S. cybersecurity firm Mandiant, later purchased by FireEye,
released a report in February 2013 that exposed one of China's cyber espionage
units, Unit 61398. The group, which FireEye called APT1, is a unit within
China's People's Liberation Army (PLA) that has been linked to a wide range of
cyber operations targeting U.S. private sector entities for espionage purposes.
The comprehensive report detailed evidence connecting APT1 and the PLA, offered
insight into APT1's operational malware and methodologies, and provided
timelines of the espionage it conducted.",
            "",
            "",
            "",
```

```
            "http://www.mcafee.com/us/resources/white-papers/wp-operation-
shady-rat.pdf",
            "http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-
as-tied-to-hacking-against-us.html?emc=na_r=2",
            "https://www.secureworks.com/research/analysis-of-dhs-nccic-
indicators",
            "https://www.scribd.com/doc/13731776/Tracking-GhostNet-
Investigating-a-Cyber-Espionage-Network",
            "http://www.nartv.org/mirror/ghostnet.pdf"
        ],
        [
            "APT2",
            "Putter Panda",
            "PLA Unit 61486",
            "",
            "TG-6952",
            "APT2",
            "",
            "",
            "",
            "Group 36",
            "",
            "SearchFire",
            "G0024",
            "",
            "",
            "",
            "",
            "Their activities are commonly known to be exploiting CVE-2012-0158
(MSOffice vulnerability in MSCOMCTL.OCX) in SpearPhising operations. Related
malware: Moose, Warp, MSUpdater",
            "This threat actor targets firms in the technology (communications,
space, aerospace), research, defense, and government sectors in the United
States for espionage purposes. The tools and infrastructure it uses overlap
with PLA Unit 61398.",
            "",
            "",
            "",
            "http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-
report-putter-panda.original.pdf",
            "http://icitech.org/icit-brief-chinas-espionage-dynasty-economic-
death-by-a-thousand-cuts/"
        ]
    ]
}
```

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[]`	Adversary.Name	N/A	`N/A`	`PLA Unit 61398`	Adversary Name is fetched using the values stated on the user field
`value[]`	Adversary.Attribute	N/A	`N/A`	`WEBC2, BISCUIT and many others`	Adversary Attributes are fetched using the values stated on the user field
`value[]`	Attachment.Name	N/A	`N/A`	`ghostnet`	Attachment are fetch from the links if it's a PDF file

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.

METRIC	RESULT
Run Time	2 minutes
Adversaries	285
Adversary Attributes	2,995
Files	46

Known Issues / Limitations

- Some PDF links may not direct to an actual PDF file. In such instances, an attachment will be created, but it will lack content.
- Due to the substantial amount of data in the spreadsheet and the fields populated on the configuration page, a timeout error may occur. In such cases, it is recommended to split the process into multiple runs.
- As of this publication, this feed cannot execute all the functions of its custom connector counterpart due to platform limitations.

Change Log

- **Version 1.0.0 rev-a**
  - Added link to steps to enable Google Sheets API.
- **Version 1.0.0**
  - Initial release