

ThreatQuotient

A Securonix Company



Google Threat Intelligence Reports CDF

Version 3.0.0

May 05, 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 | 3 |
| Support | 4 |
| Integration Details | 5 |
| Introduction | 6 |
| Prerequisites | 7 |
| Installation | 8 |
| Configuration | 9 |
| ThreatQ Mapping | 15 |
| Google Threat Intelligence Reports..... | 15 |
| Google Threat Intelligence Report Related Adversaries (Supplemental)..... | 23 |
| Google Threat Intelligence Report Related Campaigns (Supplemental)..... | 26 |
| Google Threat Intelligence Report Related Attack Patterns (Supplemental) | 31 |
| Google Threat Intelligence Report Related Malware (Supplemental) | 33 |
| Google Threat Intelligence Report Related Vulnerabilities (Supplemental) | 36 |
| Related Signatures..... | 39 |
| Google Threat Intelligence Report Related Indicators (Supplemental) | 40 |
| Indicator Type Mapping..... | 42 |
| Average Feed Run | 43 |
| Known Issues / Limitations | 44 |
| Change Log | 45 |

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.

Copyright © 2026 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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 3.0.0

Compatible with ThreatQ Versions $\geq 5.12.1$

Support Tier ThreatQ Supported

Introduction

The Google Threat Intelligence Reports CDF integration enables the ingestion of curated threat intelligence reports from the Google Threat Intelligence (GTI) API into ThreatQ, replacing the legacy Mandiant Intelligence Reports workflow. This integration provides a modernized and scalable approach to collecting and operationalizing intelligence by leveraging Google's GTI platform.

The integration provides the following feeds:

- **Google Threat Intelligence Reports** - ingests GTI report collections and leverages supplemental feeds to retrieve related entities and indicators.
 - **Google Threat Intelligence Report Details (Supplemental)**
 - **Google Threat Intelligence Report Related Adversaries (Supplemental)**
 - **Google Threat Intelligence Report Related Campaigns (Supplemental)**
 - **Google Threat Intelligence Report Related Attack Patterns (Supplemental)**
 - **Google Threat Intelligence Report Related Malware (Supplemental)**
 - **Google Threat Intelligence Report Related Vulnerabilities (Supplemental)**
 - **Google Threat Intelligence Report Related Indicators (Supplemental)**

The integration ingests the following object types:

- Adversaries
- Attack Patterns
- Campaigns
- Indicators
- Malware
- Reports
- Signatures
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A Google Threat Intelligence 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 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
6. Select the individual feeds to install, when prompted and click **Install**.



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(s) 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 |
|----------------------------------|---|
| Base URL | Specify the base endpoint for the Google Threat Intelligence API. The default is <code>https://www.virustotal.com</code> . |
| API Key | Enter your Google Threat Intelligence API key. |
| Origin Filter | Filter intelligence results based on origin. Options include: <ul style="list-style-type: none"> ◦ Google Threat Intelligence (Curated) (<i>default</i>) ◦ Partner (e.g., AlienVault OTX) ◦ Crowdsourced (e.g., individual users). |
| Target Industry | Optional- specify a single target industry for filtering intelligence results. |
| Fetch Related Adversaries | Enable this parameter to retrieve related adversaries using additional API calls. This parameter is enabled by default. |





| PARAMETER | DESCRIPTION |
|------------------------------------|---|
| Adversary Context Selection | <p>Select the context to bring back with each ingested adversary. Options include:</p> <ul style="list-style-type: none"> ◦ Motivation <i>(default)</i> ◦ Target Industry <i>(default)</i> ◦ Source Region <i>(default)</i> ◦ Source Sub Region ◦ Source Country ◦ Source Country Code ◦ Target Region <i>(default)</i> ◦ Target Sub Region ◦ Target Country ◦ Target Country Code ◦ Aliases |
| Fetch Related Campaigns | <p>Enable this parameter to retrieve related campaigns via additional API calls. This parameter is enabled by default.</p> |



 Enabling this feature may significantly increase API usage and can rapidly consume your daily rate limit.

 This parameter is only accessible if you have enabled the **Fetch Related Adversaries** parameter.

 Enabling this feature may significantly increase API usage and can rapidly consume your daily rate limit.

| PARAMETER | DESCRIPTION |
|--------------------------------------|--|
| Campaign Context Selection | Select the context to bring back with each ingested campaign. Options include: |
| | <ul style="list-style-type: none"> ◦ Motivations <i>(default)</i> ◦ Source Regions Context <i>(default)</i> ◦ Targeted Regions Context <i>(default)</i> ◦ Target Sector <i>(default)</i> ◦ Last Seen <i>(default)</i> |
| | <div style="border: 1px solid #4a7ebb; border-radius: 15px; padding: 10px;">  This parameter is only accessible if you have enabled the Fetch Related Campaigns parameter. </div> |
| Fetch Related Attack Patterns | Enable this parameter to retrieve related attack patterns using additional API calls. This parameter is enabled by default. |
| | <div style="border: 1px solid #e74c3c; border-radius: 15px; padding: 10px; background-color: #f8d7da;">  Enabling this feature may significantly increase API usage and can rapidly consume your daily rate limit. </div> |
| Fetch Related Malware | Enable this parameter to retrieve related malware using additional API calls. This parameter is enabled by default. |
| | <div style="border: 1px solid #e74c3c; border-radius: 15px; padding: 10px; background-color: #f8d7da;">  Enabling this feature may significantly increase API usage and can rapidly consume your daily rate limit. </div> |
| Malware Context Selection | Select the context to bring back with each ingested malware. Options include: |
| | <ul style="list-style-type: none"> ◦ Target Operating System <i>(default)</i> ◦ Target Industry <i>(default)</i> |

| PARAMETER | DESCRIPTION |
|------------------------------|---|
| Fetch Related CVEs | <ul style="list-style-type: none"> ◦ Detection (<i>default</i>) <div data-bbox="597 331 1442 453" style="border: 1px solid #4a7ebb; border-radius: 10px; padding: 5px; margin-top: 10px;">  This parameter is only accessible if you have enabled the Fetch Related Malware parameter. </div> <p>Enable this parameter to retrieve related CVEs using additional API calls. This parameter is enabled by default.</p> <div data-bbox="597 667 1442 827" style="border: 1px solid #e74c3c; border-radius: 10px; padding: 5px; margin-top: 10px; background-color: #f8d7da;">  Enabling this feature may significantly increase API usage and can rapidly consume your daily rate limit. </div> |
| CVE Context Selection | <p>Select the context to bring back with each ingested CVE. Options include:</p> <ul style="list-style-type: none"> ◦ CVSS v2 Vector ◦ CVSS v2 Scores ◦ CVSS v3 Vector (<i>default</i>) ◦ CVSS v3 Scores (<i>default</i>) ◦ Exploitation Vectors ◦ EPSS Score (<i>default</i>) <div data-bbox="597 1373 1442 1495" style="border: 1px solid #4a7ebb; border-radius: 10px; padding: 5px; margin-top: 10px;">  This parameter is only accessible if you have enabled the Fetch Related CVEs parameter. </div> |
| Ingest CVEs As | <p>Select how CVEs are ingested into ThreatQ. Options include Indicators (CVEs) or Vulnerabilities (<i>default</i>).</p> <div data-bbox="597 1671 1442 1793" style="border: 1px solid #4a7ebb; border-radius: 10px; padding: 5px; margin-top: 10px;">  This parameter is only accessible if you have enabled the Fetch Related CVEs parameter. </div> |

| PARAMETER | DESCRIPTION |
|---|---|
| Fetch Related Indicators | <p>Enable this parameter to retrieve related indicators through additional API calls. This parameter is enabled by default.</p> <div style="border: 1px solid red; border-radius: 10px; padding: 10px; background-color: #ffe6e6;"> <p> Enabling this feature may significantly increase API usage and can rapidly consume your daily rate limit.</p> </div> |
| Ingested Indicator Types | <p>Select the related indicator types to ingest into ThreatQ. Options include:</p> <ul style="list-style-type: none"> ◦ IP Address <i>(default)</i> ◦ FQDN <i>(default)</i> ◦ URL <i>(default)</i> ◦ MD5 ◦ SHA-1 ◦ SHA-256 <i>(default)</i> <div style="border: 1px solid blue; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> This parameter is only accessible if you have enabled the Fetch Related Indicators parameter.</p> </div> |
| Ingest Crowdsourced YARA as Signatures | <p>Enable this parameter to ingest <code>crowdsourced_yara_results</code> as YARA signatures. This parameter is enabled by default.</p> |
| Enable SSL Certificate Verification | <p>Enable this parameter if the feed should validate the host-provided SSL certificate.</p> |
| Disable Proxies | <p>Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.</p> |

< Google Threat Intelligence Reports



Disabled
 Enabled

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

Overview

This feed fetches report collections from the Google Threat Intelligence API and relates associated adversaries, campaigns, attack patterns, malware, vulnerabilities, indicators, and crowdsourced Yara results.

NOTE: This feed requires a Google Threat Intelligence (Google TI) Enterprise or Enterprise Plus license.

WARNING: Running this feed historically along with fetching related objects will result in a large number of API calls (potentially thousands). Please ensure your Google TI license has sufficient API quota to accommodate this.

Connection & Authentication

Base URL

The Base URL for the Google Threat Intelligence API.

API Key

Enter your Google Threat Intelligence API Key to authenticate.

Filtering Options

Origin Filter

Filter the results based on the origin of the intelligence. We highly recommend only selecting the curated origin to ensure data quality and reduce noise/volume.

- Google Threat Intelligence (Curated)
- Partner (i.e. AlienVaultOTX)
- Crowdsourced (i.e. Individual Users)

Target Industry

Enter a single target industry to filter the intelligence by. If you need to filter by multiple industries, please use the Custom API Filter field to add this logic.

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

Google Threat Intelligence Reports

The Google Threat Intelligence Reports feed ingests GTI report collections and uses supplemental feeds to fetch related objects and indicators.

GET {base_url}/api/v3/collections?filter=collection_type:report

Sample Response (truncated):

```
{
  "data": [
    {
      "id":
"report--3994189809d809c14ff056f104fe75b920297c22114e2e1c6e11bc6d6b79c9d9",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/
report--3994189809d809c14ff05
      },
      "attributes": {
        "mitigations": [],
        "is_content_translated": false,
        "affected_systems": [],
        "detection_names": [],
        "author": "@TheHackersNews",
        "sponsor_region": "KP",
        "files_count": 0,
        "targeted_informations": [],
        "subscribers_count": 0,
        "status": "COMPUTED",
        "recent_activity_relative_change": 1.2666666666666666,
        "capabilities": [],
        "targeted_industries": [
          "Game",
          "Health",
          "Finance",
          "News - Media",
          "Government, Administration",
          "IT",
          "Automotive",
          "Retail",
          "Cryptocurrency"
        ],
        "references_count": 0,
        "name": "ThreatsDay Bulletin: $290M DeFi Hack, macOS LotL Abuse,
ProxySmart SIM Farm
        "operating_systems": [],
```

```

"private": false,
"targeted_regions": [
  "AE",
  "KW",
  "BA",
  "US",
  "GR",
  "ES",
  "BH",
  "UA",
  "QA",
  "SI",
  "OM",
  "SA",
  "GB"
],
"report_type": "OSINT Article",
"recent_activity_summary": [
  2,
  0,
  33,
  29
],
"source_region": "IR",
"targeted_industries_tree": [
  {
    "industry_group": "Media & Entertainment",
    "industry": "News - Media",
    "confidence": "crowdsourced",
    "first_seen": null,
    "last_seen": null,
    "description": null,
    "source": null
  },
  {
    "industry_group": "Media & Entertainment",
    "industry": "Game",
    "confidence": "crowdsourced",
    "first_seen": null,
    "last_seen": null,
    "description": null,
    "source": null
  },
  {
    "industry_group": "Retail",
    "industry": "Retail",
    "confidence": "crowdsourced",
    "first_seen": null,
    "last_seen": null,
    "description": null,
    "source": null
  }
],

```

```

    {
      "industry_group": "Telecommunications",
      "industry": "IT",
      "confidence": "crowdsourced",
      "first_seen": null,
      "last_seen": null,
      "description": null,
      "source": null
    },
    {
      "industry_group": "Government",
      "industry": "Government, Administration",
      "confidence": "crowdsourced",
      "first_seen": null,
      "last_seen": null,
      "description": null,
      "source": null
    },
    {
      "industry_group": "Automotive",
      "industry": "Automotive",
      "confidence": "crowdsourced",
      "first_seen": null,
      "last_seen": null,
      "description": null,
      "source": null
    },
    {
      "industry_group": "Healthcare",
      "industry": "Health",
      "confidence": "crowdsourced",
      "first_seen": null,
      "last_seen": null,
      "description": null,
      "source": null
    },
    {
      "industry_group": "Financial Services",
      "industry": "Finance",
      "confidence": "crowdsourced",
      "first_seen": null,
      "last_seen": null,
      "description": null,
      "source": null
    },
    {
      "industry_group": "Financial Services",
      "industry": "Cryptocurrency",
      "confidence": "crowdsourced",
      "first_seen": null,
      "last_seen": null,
      "description": null,

```

```

        "source": null
    }
],
"origin": "Crowdsourced",
"alt_names_details": [],
"ip_addresses_count": 0,
"malware_roles": [
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Backdoor",
        "last_seen": null
    },
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Keylogger",
        "last_seen": null
    },
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Downloader",
        "last_seen": null
    },
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Remote Control and Administration Tool",
        "last_seen": null
    },
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Ransomware",
        "last_seen": null
    },
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Backdoor - Webshell",
        "last_seen": null
    },
    {
        "description": null,
        "first_seen": null,

```

```

        "confidence": "crowdsourced",
        "value": "Dropper",
        "last_seen": null
    },
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Credential Stealer",
        "last_seen": null
    }
],
"executive_summary": "ThreatsDay Bulletin: active exploits, supply
chain attacks, AI
"tags_details": [],
"threat_scape": [],
"last_seen_details": [],
"domains_count": 1,
"counters": {
    "files": 0,
    "domains": 1,
    "ip_addresses": 0,
    "urls": 1,
    "iocs": 2,
    "subscribers": 0,
    "attack_techniques": 0
},
"urls_count": 1,
"intended_effects": [],
"collection_type": "report",
"creation_date": 1776950220,
"autogenerated_tags": [],
"source_regions_hierarchy": [
    {
        "region": "Asia",
        "sub_region": "Eastern Asia",
        "country": "Korea, Democratic People's Republic Of",
        "country_iso2": "KP",
        "confidence": "crowdsourced",
        "first_seen": null,
        "last_seen": null,
        "description": null,
        "source": null
    },
    {
        "region": "Europe",
        "sub_region": "Eastern Europe",
        "country": "Russian Federation",
        "country_iso2": "RU",
        "confidence": "crowdsourced",
        "first_seen": null,
        "last_seen": null,
    }
]

```

```

        "description": null,
        "source": null
    },
    {
        "region": "Europe",
        "sub_region": "Eastern Europe",
        "country": "Belarus",
        "country_iso2": "BY",
        "confidence": "crowdsourced",
        "first_seen": null,
        "last_seen": null,
        "description": null,
        "source": null
    },
    {
        "region": "Asia",
        "sub_region": "Southern Asia",
        "country": "Iran, Islamic Republic Of",
        "country_iso2": "IR",
        "confidence": "crowdsourced",
        "first_seen": null,
        "last_seen": null,
        "description": null,
        "source": null
    }
],
"motivations": [
    {
        "description": null,
        "first_seen": null,
        "confidence": "crowdsourced",
        "value": "Hacktivism",
        "last_seen": null
    }
],
"link": "https://thehackernews.com/2026/04/threatsday-bulletin-290m-defi-hack.html",
"top_icon_md5": [],
"collection_links": [],
"first_seen_details": [],
"alt_names": [],
"technologies": [],
"tags": [],
"last_modification_date": 1776956101,
"autogenerated_summary": "A $290 million DeFi heist occurred via RPC
infrastructure
"publisher": "thehackernews",
"aggregations": {},
"content": "# ThreatsDay Bulletin: $290M DeFi Hack, macOS LotL Abuse,
ProxySmart SIM
    },
    "context_attributes": {

```

```

    "snippet": "<b>1</b>. State-backed crypto heist North Korea
Likely ... <b>IP</b> rot
    "shared_with_me": false,
    "role": "viewer"
  }
}
]
}

```

ThreatQuotient provides the following default mapping for this feed based on each item within the `.data[]` list.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|--|--------------------|--------------------------------------|--|---|---|
| <code>.attributes.name</code> | Report.Value | Report | <code>.attributes.creation_date</code> | STX RAT: A new RAT in 2026 with Infostealer Capabilities | If <code>report_type</code> is Vulnerability Report, the primary object is ingested as a Vulnerability instead of a Report. |
| <code>.attributes.link</code> | Report.Attribute | Report Link | <code>.attributes.creation_date</code> | https://www.hendryadrian.com/stx-rat-a-new-rat-in-2026-with-infostealer-capabilities/ | N/A |
| <code>.attributes.report_type</code> | Report.Attribute | Report Type | <code>.attributes.creation_date</code> | OSINT Article | N/A |
| <code>.attributes.publisher</code> | Report.Attribute | Publisher | <code>.attributes.creation_date</code> | hendryadrian | N/A |
| <code>.attributes.author</code> | Report.Attribute | Author | <code>.attributes.creation_date</code> | Esentire @TweetThreatNews | N/A |
| <code>.attributes.origin</code> | Report.Attribute | Origin | <code>.attributes.creation_date</code> | Crowdsourced | N/A |
| <code>.attributes.targeted_industries_tree[].industry_group</code> | Report.Attribute | Target Industry | <code>.attributes.creation_date</code> | Financial Services | N/A |
| <code>.attributes.targeted_regions[]</code> | Report.Attribute | Targeted Region | <code>.attributes.creation_date</code> | US | Array value. |
| <code>.attributes.operating_systems[].value</code> | Report.Attribute | Operating System | <code>.attributes.creation_date</code> | Windows | Array value. |
| <code>.attributes.motivations[].value</code> | Report.Attribute | Motivation | <code>.attributes.creation_date</code> | Financial Gain | N/A |
| <code>.attributes.executive_summary</code> | Report.Description | N/A | N/A | N/A | Rendered into HTML in ThreatQ. |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|----------------|----------------|--------------------------------------|----------------|----------|-------|
|----------------|----------------|--------------------------------------|----------------|----------|-------|

```
+ .attribute
s.autogenerated_summary
+ .attribute
s.content
```



Supplemental related-object API calls are only made when the report indicates related data exists and the corresponding count/counter value is greater than 0.

Google Threat Intelligence Report Related Adversaries (Supplemental)

GET {base_url}/api/v3/collections/{report_id}/threat_actors

Sample Response (truncated):

```
{
  "data": [
    {
      "id": "threat-actor--50cd027f-df14-40b2-aa22-bf5de5061163",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/threat-actor--50cd027f-df14-40b2-aa22-bf5de5061163"
      },
      "attributes": {
        "summary_stats": {
          "first_submission_date": {
            "min": 0.0,
            "max": 1764641939.0,
            "avg": 1334719380.4161248
          },
          "last_submission_date": {
            "min": 0.0,
            "max": 1776844731.0,
            "avg": 1386101892.4304292
          },
          "files_detections": {
            "min": 0.0,
            "max": 64.0,
            "avg": 22.407350689127124
          },
          "urls_detections": {
            "min": 0.0,
            "max": 18.0,
            "avg": 6.534482758620692
          }
        },
        "recent_activity_relative_change": 0.05426716141001853,
        "targeted_regions_hierarchy": [
          {
            "region": "Asia",
            "sub_region": "South-eastern Asia",
            "country": "Vietnam",
            "country_iso2": "VN",
            "confidence": "crowdsourced",
            "first_seen": null,
            "last_seen": null,
            "description": null,
            "source": null
          }
        ]
      }
    }
  ]
}
```

```

    ],
    "alt_names_details": [
      {
        "last_seen": null,
        "confidence": "crowdsourced",
        "description": null,
        "first_seen": null,
        "value": "InkySquid"
      }
      {
        "last_seen": null,
        "confidence": "crowdsourced",
        "description": null,
        "first_seen": null,
        "value": "ScarCruft"
      },
      {
        "last_seen": null,
        "confidence": "crowdsourced",
        "description": null,
        "first_seen": null,
        "value": "Group 123"
      }
    ],
    "references_count": 17,
    "name": "APT37",
    "top_icon_md5": [
      "75a3c799cc431b997f76afc4dd08e479",
      "0646fde7ac29e4bde70f6e71bc4542d9",
      "b4225d8d8114854d2cdf3cb647735e73"
    ],
  ],
}

```

ThreatQuotient provides the following default mapping for this feed based on each item within the `.data[]` list.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|--|-------------------------------|--------------------------------------|---|--|--------------------|
| <code>.attributes.name</code> | Related Adversary.Value | Adversary | <code>.attributes.last_modification_date</code> | APT28 | N/A |
| <code>.attributes.alt_names_details[].value</code> | Related Adversary.Tag | N/A | N/A | APT28 (Google) | User-configurable. |
| <code>.attributes.description</code> | Related Adversary.Description | N/A | N/A | APT28 is a highly active cyber espionage group ... | N/A |
| <code>.attributes.motivations[].value</code> | Related Adversary.Attribute | Motivation | <code>.attributes.last_modification_date</code> | Espionage | User-configurable. |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|-----------------------------|--------------------------------------|------------------------------------|---------------------|--------------------|
| .attributes.targeted_industries_tree[].industry_group | Related Adversary.Attribute | Target Industry | .attributes.last_modification_date | Aerospace & Defense | User-configurable. |
| .attributes.source_regions_hierarchy[].region | Related Adversary.Attribute | Region | .attributes.last_modification_date | Europe | User-configurable. |
| .attributes.source_regions_hierarchy[].sub_region | Related Adversary.Attribute | Sub Region | .attributes.last_modification_date | Eastern Europe | User-configurable. |
| .attributes.source_regions_hierarchy[].country | Related Adversary.Attribute | Country | .attributes.last_modification_date | Russian Federation | User-configurable. |
| .attributes.source_regions_hierarchy[].country_iso2 | Related Adversary.Attribute | Country Code | .attributes.last_modification_date | RU | User-configurable. |
| .attributes.targeted_regions_hierarchy[].region | Related Adversary.Attribute | Target Region | .attributes.last_modification_date | Europe | User-configurable. |
| .attributes.targeted_regions_hierarchy[].sub_region | Related Adversary.Attribute | Target Sub Region | .attributes.last_modification_date | Western Europe | User-configurable. |
| .attributes.targeted_regions_hierarchy[].country | Related Adversary.Attribute | Target Country | .attributes.last_modification_date | Austria | User-configurable. |
| .attributes.targeted_regions_hierarchy[].country_iso2 | Related Adversary.Attribute | Target Country Code | .attributes.last_modification_date | AT | User-configurable. |

Google Threat Intelligence Report Related Campaigns (Supplemental)

GET {base_url}/api/v3/collections/{report_id}/campaigns

Sample Response:

```
{
  "data": [
    {
      "id": "campaign--06d5db6f-130f-53ed-ac1b-6076e4e4dc7b",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/campaign--06d5db6f-130f-53ed-ac1b-6076e4e4dc7b"
      },
      "attributes": {
        "alt_names_details": [
          {
            "first_seen": null,
            "confidence": "confirmed",
            "last_seen": null,
            "description": null,
            "value": "CAMP.25.067"
          }
        ],
        "files_count": 1,
        "last_seen_details": [
          {
            "first_seen": null,
            "confidence": "unconfirmed",
            "last_seen": null,
            "description": null,
            "value": "2025-10-21T00:00:00Z"
          }
        ],
        "private": false,
        "first_seen": 1741651200,
        "alt_names": [
          "CAMP.25.067"
        ],
        "domains_count": 1,
        "campaign_type": "INDIVIDUAL",
        "subscribers_count": 4,
        "targeted_industries_tree": [
          {
            "industry_group": "Construction & Engineering",
            "industry": null,
            "confidence": "confirmed",
            "first_seen": null,
            "last_seen": null,
            "description": null,

```

```

        "source": null
    },
    {
        "industry_group": "Energy & Utilities",
        "industry": null,
        "confidence": "confirmed",
        "first_seen": null,
        "last_seen": null,
        "description": null,
        "source": null
    }
],
"targeted_regions": [
    "IN",
    "US",
    "TR"
],
"collection_type": "campaign",
"tags": [],
"creation_date": 1761166941,
"merged_actors": [],
"recent_activity_relative_change": 3.5675675675675675,
"ip_addresses_count": 12,
"first_seen_details": [
    {
        "first_seen": null,
        "confidence": "unconfirmed",
        "last_seen": null,
        "description": "Mandiant Observed First Activity of Campaign",
        "value": "2025-03-11T00:00:00Z"
    }
],
"top_icon_md5": [
    "665ef003fe1bcd289f20035fedeeae280",
    "aa1c756e63d9559fd225cde44aa590f8",
    "39a349a4171759407f1aa76f9937b35f"
],
"recent_activity_summary": [
    1,
    8,
    38,
    1,
    26,
    25
],
"targeted_regions_hierarchy": [
    {
        "region": "Asia",
        "sub_region": "Southern Asia",
        "country": "India",
        "country_iso2": "IN",
        "confidence": "confirmed",
    }
]

```

```

        "first_seen": null,
        "last_seen": null,
        "description": null,
        "source": null
    }
],
"operating_systems": [],
"urls_count": 1,
"source_regions_hierarchy": [],
"summary_stats": {
    "first_submission_date": {
        "min": 0.0,
        "max": 1759859939.0,
        "avg": 879929969.5
    },
    "last_submission_date": {
        "min": 0.0,
        "max": 1759859939.0,
        "avg": 879929969.5
    },
    "files_detections": {
        "min": 0.0,
        "max": 0.0,
        "avg": 0.0
    },
    "urls_detections": {
        "min": 1.0,
        "max": 1.0,
        "avg": 1.0
    }
},
"tags_details": [],
"detection_names": [],
"last_modification_date": 1774224000,
"motivations": [],
"description": "Google Threat Intelligence Group (GTIG) has collected intelligence surrounding a campaign involving the modification of a GlobalProtect gateway to distribute a Trojanized update followed by the deployment of the SimpleHelp remote access backdoor. Based on available intelligence, targeted organizations have been located in India, Turkey, and the United States within the energy, technology, and manufacturing sectors. The campaign is being conducted by a threat actor GTIG tracks as UNC6425.",
"targeted_industries": [],
"capabilities": [],
"malware_roles": [],
"last_seen": 1761004800,
"autogenerated_tags": [],
"counters": {
    "files": 1,
    "domains": 1,
    "ip_addresses": 12,
    "urls": 1,

```

```

        "iocs": 15,
        "subscribers": 4,
        "attack_techniques": 37
    },
    "name": "Actor of Unknown Motivations Compromises GlobalProtect Gateway, Deploys SimpleHelp",
    "origin": "Google Threat Intelligence",
    "status": "COMPUTED",
    "collection_links": [],
    "references_count": 0,
    "aggregations": {}
},
"context_attributes": {
    "shared_with_me": false,
    "role": "viewer"
}
}
],
"meta": {
    "count": 1
},
"links": {
    "self": "https://www.virustotal.com/api/v3/collections/report--25-10050537/campaigns?limit=10"
}
}

```

ThreatQuotient provides the following default mapping for this feed based on each item within the `.data[]` list.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|--|------------------------------|--------------------------------------|---|--|--------------------|
| <code>.attributes.name</code> | Related Campaign.Value | Campaign | <code>.attributes.last_modification_date</code> | APT28 Conducts Credential Harvesting Campaign Targeting Multiple European Entities | N/A |
| <code>.attributes.description</code> | Related Campaign.Description | N/A | N/A | Starting in early February 2024 ... | N/A |
| <code>.attributes.motivations[].value</code> | Related Campaign.Attribute | Motivation | <code>.attributes.last_modification_date</code> | Espionage | User-configurable. |
| <code>.attributes.source_regions_hierarchy[].region</code> | Related Campaign.Attribute | Source Region | <code>.attributes.last_modification_date</code> | Europe | User-configurable. |
| <code>.attributes.source_regions_hierarchy[].sub_region</code> | Related Campaign.Attribute | Source Sub Region | <code>.attributes.last_modification_date</code> | Eastern Europe | User-configurable. |
| <code>.attributes.source_regions_hierarchy[].country</code> | Related Campaign.Attribute | Source Country | <code>.attributes.last_modification_date</code> | Russian Federation | User-configurable. |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|----------------------------|--------------------------------------|------------------------------------|----------------|-------------------------------------|
| .attributes.source_regions_hierarchy[].country_iso2 | Related Campaign.Attribute | Source Country Code | .attributes.last_modification_date | RU | User-configurable. |
| .attributes.targeted_regions_hierarchy[].region | Related Campaign.Attribute | Target Region | .attributes.last_modification_date | Europe | User-configurable. |
| .attributes.targeted_regions_hierarchy[].country | Related Campaign.Attribute | Target Country | .attributes.last_modification_date | France | User-configurable. |
| .attributes.targeted_regions_hierarchy[].sub_region | Related Campaign.Attribute | Target Sub Region | .attributes.last_modification_date | Western Europe | User-configurable. |
| .attributes.targeted_regions_hierarchy[].country_iso2 | Related Campaign.Attribute | Target Country Code | .attributes.last_modification_date | FR | User-configurable. |
| .attributes.last_seen | Related Campaign.Attribute | Last Seen | .attributes.last_modification_date | 1727913600 | User-configurable. Timestamp value. |
| .attributes.targeted_industries_tree[].industry_group | Related Campaign.Attribute | Target Sector | .attributes.last_modification_date | Government | User-configurable. |

Google Threat Intelligence Report Related Attack Patterns (Supplemental)

GET {base_url}/api/v3/collections/{report_id}/attack_techniques

Sample Response:

```
{
  "data": [
    {
      "id": "T1027",
      "type": "attack_technique",
      "links": {
        "self": "https://www.virustotal.com/api/v3/attack_techniques/T1027"
      },
      "attributes": {
        "name": "Obfuscated Files or Information",
        "last_modification_date": 1761328155,
        "description": "Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. \nPayloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and Deobfuscate/Decode Files or Information for User Execution. The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. Adversaries may also use compressed or archived scripts, such as JavaScript. \nPortions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. \nAdversaries may also abuse Command Obfuscation to obscure commands executed from payloads or directly via Command and Scripting Interpreter. Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. ",
        "revoked": false,
        "link": "https://attack.mitre.org/techniques/T1027/",
        "creation_date": 1496266232,
        "info": {
          "x_mitre_attack_spec_version": "3.2.0",
          "x_mitre_contributors": [
            "Red Canary",
            "Christiaan Beek, @ChristiaanBeek"
          ],
          "x_mitre_deprecated": false,
          "x_mitre_domains": [
            "enterprise-attack"
          ],
          "x_mitre_is_subtechnique": false,
          "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",

```

```

        "x_mitre_platforms": [
            "ESXi",
            "Linux",
            "macOS",
            "Network Devices",
            "Windows"
        ],
        "x_mitre_version": "1.7",
        "x_mitre_detection": ""
    },
    "stix_id": "attack-pattern--b3d682b6-98f2-4fb0-aa3b-b4df007ca70a"
}
}
],
"meta": {
    "count": 1
},
"links": {
    "self": "https://www.virustotal.com/api/v3/collections/report--3602a99f06e96bc189cf675fc8af90e810e9a84dc793f15b8c234f5fb46534e2/attack_techniques?limit=40"
}
}

```

ThreatQuotient provides the following default mapping for this feed based on each item within the `.data[]` list.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|--|--------------------------------------|--|---|--|
| <code>.id</code> <code>+ .attributes.name</code> | Related Attack Pattern.Value | Attack Pattern | <code>.attributes.creation_date</code> | T1003 - OS Credential Dumping | If there is a matching MITRE ATT&CK Pattern in ThreatQ, the library object is used; otherwise ID - Name is ingested. |
| <code>.attributes.description</code> | Related Attack Pattern.Description | N/A | N/A | Adversaries may attempt to dump credentials ... | N/A |

Google Threat Intelligence Report Related Malware (Supplemental)

GET {base_url}/api/v3/collections/{report_id}/malware_families

Sample Response:

```
{
  "data": [
    {
      "id": "malpedia_win_rokrat",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/malpedia_win_rokrat"
      },
      "attributes": {
        "collection_links": [],
        "targeted_industries_tree": [],
        "detection_names": [],
        "motivations": [],
        "tags": [],
        "link": "https://malpedia.caad.fkie.fraunhofer.de/details/win.rokrat",
        "origin": "Partner",
        "private": false,
        "files_count": 337,
        "description": "It is a backdoor commonly distributed as an encoded\r\nbinary file downloaded and decrypted by shellcode following the\r\nexploitation of weaponized documents. DOGCALL is capable of\r\nncapturing screenshots, logging keystrokes, evading analysis with\r\nnanti-virtual machine detections, and leveraging cloud storage APIs\r\nnsuch as Cloud, Box, Dropbox, and Yandex.",
        "subscribers_count": 2,
        "alt_names": [
          "DOGCALL"
        ],
        "recent_activity_summary": [
          407,
          371,
          319,
          304
        ],
        "source_regions_hierarchy": [],
        "summary_stats": {
          "first_submission_date": {
            "min": 0.0,
            "max": 1738167411.0,
            "avg": 1521224251.8153846
          },
          "last_submission_date": {
            "min": 0.0,
            "max": 1776794787.0,

```

```

        "avg": 1682006143.4646153
    },
    "files_detections": {
        "min": 0.0,
        "max": 70.0,
        "avg": 53.22769230769233
    }
},
"targeted_industries": [],
"tags_details": [],
"references_count": 278,
"last_seen_details": [],
"targeted_regions_hierarchy": [],
"counters": {
    "files": 337,
    "domains": 0,
    "ip_addresses": 0,
    "urls": 0,
    "iocs": 337,
    "subscribers": 2,
    "attack_techniques": 0
},
"status": "COMPUTED",
"recent_activity_relative_change": 0.19879227053140092,
"first_seen_details": [],
"last_modification_date": 1766565045,
"top_icon_md5": [
    "80890f0a8ed6b8f7644ae58033396698",
    "00ecd29321807c83650ce1e1216bc4f2",
    "fbbb78676d0ee4ddaf31a9257ebe155a"
],
"urls_count": 0,
"alt_names_details": [
    {
        "last_seen": null,
        "confidence": "crowdsourced",
        "first_seen": null,
        "value": "DOGCALL",
        "description": null
    }
],
"creation_date": 1610323200,
"malware_roles": [],
"targeted_regions": [],
"ip_addresses_count": 0,
"name": "RokRAT",
"operating_systems": [],
"autogenerated_tags": [
    "attachment",
    "cve-2002-1623",
    "themida",
    "armadillo",

```

```

        "cve-2017-0147",
        "cve-1999-0016"
    ],
    "merged_actors": [],
    "capabilities": [],
    "domains_count": 0,
    "collection_type": "malware-family",
    "aggregations": {}
  },
  "context_attributes": {
    "shared_with_me": false,
    "role": "viewer"
  }
}
],
"meta": {
  "count": 1
},
"links": {
  "self": "https://www.virustotal.com/api/v3/collections/
report--597d77f83c7e9509c476c314c7da12d6819f56171ce4e0ca39fd6d947d884569/
malware_families?limit=10"
}
}

```

ThreatQuotient provides the following default mapping for this feed based on each item within the `.data[]` list.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|--|-----------------------------|--------------------------------------|---|---------------------------------|--------------------|
| <code>.attributes.name</code> | Related Malware.Value | Malware | <code>.attributes.last_modification_date</code> | MILDMAP | N/A |
| <code>.attributes.description</code> | Related Malware.Description | N/A | N/A | MILDMAP is an APT28 dropper ... | N/A |
| <code>.attributes.operating_systems[].value</code> | Related Malware.Attribute | Target Operating System | <code>.attributes.last_modification_date</code> | Windows | User-configurable. |
| <code>.attributes.targeted_industries_tree[].industry_group</code> | Related Malware.Attribute | Industry | <code>.attributes.last_modification_date</code> | Technology | User-configurable. |
| <code>.attributes.detection_names[].value</code> | Related Malware.Attribute | Detection | <code>.attributes.last_modification_date</code> | N/A | User-configurable. |

Google Threat Intelligence Report Related Vulnerabilities (Supplemental)

GET {base_url}/api/v3/collections/{report_id}/vulnerabilities

Sample Response (truncated):

```
{
  "data": [
    {
      "id": "vulnerability--cve-2025-55182",
      "type": "collection",
      "links": {
        "self": "https://www.virustotal.com/api/v3/collections/vulnerability--cve-2025-55182"
      },
      "attributes": {
        "alt_names_details": [
          {
            "value": "React2Shell",
            "confidence": "possible",
            "last_seen": null,
            "description": null,
            "first_seen": null
          }
        ],
        "subscribers_count": 12,
        "exploitation_state": "Wide",
        "cisa_known_exploited": {
          "added_date": 1764892800,
          "ransomware_use": "Known",
          "due_date": 1765497600
        },
        "top_icon_md5": [],
        "name": "CVE-2025-55182",
        "recent_activity_relative_change": 0.09832134292565953,
        "targeted_industries_tree": [],
        "cwe": {
          "id": "CWE-502",
          "title": "Deserialization of Untrusted Data"
        },
        "recent_activity_summary": [
          30,
          26
        ],
        "exploitation_vectors": [
          "Exposed Web Application",
          "Unspecified Remote Vector"
        ],
        "exploit_availability": "Publicly Available",
        "ip_addresses_count": 0,

```

```

"creation_date": 1764778560,
"summary_stats": {
  "first_submission_date": {
    "min": 0.0,
    "max": 1771893030.0,
    "avg": 198504091.34810126
  },
  "last_submission_date": {
    "min": 0.0,
    "max": 1776700270.0,
    "avg": 201306004.92405063
  },
  "files_detections": {
    "min": 0.0,
    "max": 12.0,
    "avg": 0.14556962025316456
  }
},
"cpes": [],
"references_count": 0,
"counters": {
  "files": 204,
  "domains": 0,
  "ip_addresses": 0,
  "urls": 0,
  "iocs": 204,
  "subscribers": 12,
  "attack_techniques": 0
},
"collection_type": "vulnerability",
"origin": "Google Threat Intelligence",
"exploitation_consequence": "Code Execution",
"targeted_regions": [],
"detection_names": [],
}
}

```

ThreatQuotient provides the following default mapping for this feed based on each item within the `.data[]` list.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|--------------------------------------|---|--------------------------------------|--|---|---|
| <code>.attributes.name</code> | Related Vulnerability/Indicator.Value | CVE | <code>.attributes.creation_date</code> | CVE-2004-0210 | User-configurable. Based on Ingest CVEs As. |
| <code>.attributes.description</code> | Related Vulnerability/Indicator.Description | N/A | N/A | The National Vulnerability Database ... | N/A |

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|--|---|--------------------------------------|---------------------------|----------------------------|--------------------|
| .attributes.cvss.cvssv2_0.vector | Related Vulnerability/Indicator.Attribute | CVSS v2 Vector | .attributes.creation_date | AV:L/AC:L/Au:N/C:C/I:C/A:C | User-configurable. |
| .attributes.cvss.cvssv2_0.base_score | Related Vulnerability/Indicator.Attribute | CVSS v2 Base Score | .attributes.creation_date | 7.2 | User-configurable. |
| .attributes.cvss.cvssv2_0.temporal_score | Related Vulnerability/Indicator.Attribute | CVSS v2 Temporal Score | .attributes.creation_date | 6.0 | User-configurable. |
| .attributes.cvss.cvssv3_x.vector | Related Vulnerability/Indicator.Attribute | CVSS v3 Vector | .attributes.creation_date | CVSS:3.1/AV:L/AC:L/... | User-configurable. |
| .attributes.cvss.cvssv3_x.base_score | Related Vulnerability/Indicator.Attribute | CVSS v3 Base Score | .attributes.creation_date | 7.8 | User-configurable. |
| .attributes.cvss.cvssv3_x.temporal_score | Related Vulnerability/Indicator.Attribute | CVSS v3 Temporal Score | .attributes.creation_date | 7.8 | User-configurable. |
| .attributes.exploitation_vectors[] | Related Vulnerability/Indicator.Attribute | Exploitation Vector | .attributes.creation_date | Local Access | User-configurable. |
| .attributes.epss.score | Related Vulnerability/Indicator.Attribute | EPSS Score | .attributes.creation_date | 0.10564 | User-configurable. |

Related Signatures

No additional API call is required. Signatures are extracted from the report detail payload.

```
GET {base_url}/api/v3/collections/{report_id}
```

Sample Response:

```
{
  "data": {
    "id": "report--c81eb59b-89fe-5c73-8659-5cd10d51e2b3",
    "type": "collection",
    "attributes": {
      "aggregations": {
        "files": {
          "crowdsourced_yara_results": [
            {
              "rule_name": "STXRatLoader",
              "ruleset_name": "STXRat",
              "source": "https://github.com/kevoreilly/CAPEv2"
            }
          ]
        }
      }
    }
  }
}
```

ThreatQuotient provides the following default mapping for related signatures:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|------------------------------|--------------------------------------|----------------|--------------------------------------|---|
| .attributes.aggregations.files.crowdsourced_yara_results[].value.rule_name | Related Signature.Val ue | Yara | N/A | STXRatLoader | Ingested only when Ingest Crowdsourced Yara as Signatures is enabled. |
| .attributes.aggregations.files.crowdsourced_yara_results[].value.ruleset_name | Related Signature.Att ribute | Ruleset | N/A | STXRat | N/A |
| .attributes.aggregations.files.crowdsourced_yara_results[].value.source | Related Signature.Att ribute | Source | N/A | https://github.com/kevoreilly/CAPEv2 | N/A |

Google Threat Intelligence Report Related Indicators (Supplemental)

GET {base_url}/api/v3/collections/{report_id}/{indicator_endpoint}

Sample Response:

```
{
  "data": [
    {
      "id": "whereisitat.lucyatemysuperbox.space",
      "type": "domain",
      "attributes": {
        "last_modification_date": 1776894367
      }
    },
    {
      "id": "077d49fa708f498969d7cdf7e701eb64675baaa4968ded9bd97a4936dd56c21c",
      "type": "file",
      "attributes": {
        "md5": "150cce17d72f765217e69f36d6d6bf64",
        "sha1": "8ba3977352e5a0fb06f0ac7d774665d3dc908cce",
        "sha256": "ed97719c008422925ae21ff34448a8c35ee270a428b0478e24669396761d0790",
        "last_modification_date": 1776894367
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each item within the `.data[]` list.

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|--------------------------|--------------------------------------|---|--|------------------------------------|
| <code>.id</code> | Related Indicator.Val ue | IP Address / FQDN | <code>.attributes.last_modification_date</code> | 95.216.51.236, japanroom.com | Used for ip_addresses and domains. |
| <code>.attributes.last_final_url</code> or <code>.attributes.url</code> | Related Indicator.Val ue | URL | <code>.attributes.last_modification_date</code> | https://example.com/path | Used for urls. |
| <code>.attributes.md5</code> | Related Indicator.Val ue | MD5 | <code>.attributes.last_modification_date</code> | 5133177ac4950cf772d2f729bb0622ec | Used when MD5 is selected. |
| <code>.attributes.sha1</code> | Related Indicator.Val ue | SHA-1 | <code>.attributes.last_modification_date</code> | 042839871fa456d7d82b34a1eb85de5afe54ccd1 | Used when SHA-1 is selected. |
| <code>.attributes.sha256</code> | Related Indicator.Val ue | SHA-256 | <code>.attributes.last_modification_date</code> | 1cc7939b1a7d7462f1cf54ba88d2ab2b62a70e225d31b4883e9c42ecbd230ff3 | Used when SHA-256 is selected. |



Related indicators are currently ingested as indicator data only. No indicator attributes are mapped by default.

Indicator Type Mapping

The following table outlines the mapping between ThreatQ indicator types and Google Threat Intelligence (GTI) endpoints.

| THREATQ INDICATOR TYPE | GTI ENDPOINT |
|-------------------------------|---------------------|
| IP Address | ip_addresses |
| IPv6 Address | ip_addresses |
| FQDN | domains |
| URL | urls |
| MD5 | files |
| SHA-1 | files |
| SHA-256 | files |

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 | 15 minutes |
| Adversaries | 24 |
| Adversary Attributes | 444 |
| Attack Patterns | 253 |
| Indicators | 3,552 |
| Malware | 72 |
| Reports | 80 |
| Report Attributes | 518 |
| Signatures | 354 |
| Signature Attributes | 708 |
| Vulnerabilities | 40 |

Known Issues / Limitations

- GTI report relationships are retrieved through multiple supplemental API calls, which may result in increased API usage and rapid consumption of quota during historical feed runs.

Change Log

- **Version 3.0.0**
 - Rebranded the integration to **Google Threat Intelligence Reports CDF**.
 - Introduced the initial GTI-native reports feed and restructured report relationships into dedicated supplemental feeds for details, adversaries, campaigns, attack patterns, malware, vulnerabilities, and indicators.
 - Updated the minimum ThreatQ version to 5.12.1.
- **Version 2.0.2**
 - Renamed the **Parse for IOCs** parameter to **Parse IOCs from Content**.
 - Added a new supplemental feed, **Mandiant Report Related Indicators**, which gives users the option to ingest indicators from reports.
 - Added the following new configuration parameters:
 - **Bring Related Indicators** - enable the feed to bring in indicators related to the report.
 - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
 - **Disable Proxies** - determine if the feed should honor proxy settings set in the ThreatQ UI.
 - Resolved a YARA format issue that would occur after ingestion into ThreatQ.
- **Version 2.0.1**
 - Added the ability to parse YARA rules from reports with the new **Parse YARA** configuration parameter.
 - Resolved a `Type Error` that would occur with MITRE ATT&CK Patterns.
- **Version 2.0.0**
 - Added the ability to fetch data older than 90 days.
 - Added a new attribute: `Intended Effect`.
 - Updated the way relationships and attributes are made.
 - Added support for News Analysis Reports.
 - Added two new configuration options:
 - Ingest CVEs As
 - Parse for IoCs

-
- The IOC Parser now utilizes the built-in ThreatQ indicator parser.
 - Vulnerability Reports will now be ingested as Vulnerability objects.
 - Resolved an issue where users would encounter a `filter-mapping` error when loading MITRE Attack Patterns from the ThreatQ API.
 - **Version 1.1.4**
 - Removed the restriction on description length.
 - Resolved an issue where IOCs from report descriptions were not ingested.
 - Updated minimum ThreatQ version to 5.6.0.
 - **Version 1.1.3**
 - IP addresses, FQDNs and URLs are now ingested as indicators when parsed from a report
 - **Version 1.1.2**
 - Updated the `response_content_type` for all Mandiant API requests.
 - Updated the method for retrieving Attack Patterns from the ThreatQ API.
 - **Version 1.1.0**
 - Decreased the number of API Attack Patterns retrieved, per request, to prevent timeout errors.
 - **Version 1.0.1**
 - Fixed an issue with the `Category` field that prevented users from installing the integration on ThreatQ version 4 instances.
 - **Version 1.0.0**
 - Initial release