ThreatQuotient

Mandiant Threat Intelligence CDF

Version 1.5.0

December 10, 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	1.5.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

Mandiant is on a mission to make every organization secure from cyber threats and confident in their readiness. They deliver dynamic cyber defense solutions powered by industry-leading expertise, intelligence and innovative technology.

The Mandiant Threat Intelligence CDF provides the following feeds:

- **Mandiant Threat Intelligence** - ingests compromised Adversaries objects and any related Indicators, Malware, Vulnerabilities, Attack Patterns and Tags.
  - **Mandiant Threat Intelligence Actor Details (Supplemental)** - returns actor's details.
  - **Mandiant Threat Intelligence Malware Details (Supplemental)** - returns malware information.
  - **Mandiant Threat Intelligence Entity Attack Pattern Details (Supplemental)** - fetches related attack patterns to threat actors and / or malware.
  - **Mandiant Threat Intelligence Threat Actor Indicators (Supplemental)** - fetches related indicators to threat actors.
- **Mandiant Threat Intelligence Indicators** - ingests a list of indicators tracked by Mandiant.
- **Mandiant Vulnerability Intelligence** - ingests a list of vulnerabilities tracked by Mandiant.
- **Mandiant Threat Intelligence Malware** - ingests a list of malware tracked by Mandiant.
- **Mandiant Threat Intelligence Campaigns** - ingests a list of campaigns tracked by Mandiant.

The Mandiant Threat Intelligence CDF for ThreatQuotient ingests the following object types:

- Adversaries
  - Adversary Attributes
- Attack Patterns
- Campaigns
- Indicators
  - Indicator Attributes
- Malware
  - Malware Attributes
- Vulnerabilities
  - Vulnerability Attributes
- Tags
- Tools

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 yaml file into the dialog box
   - Select **Click to Browse** to locate the integration yaml 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.

7. The feeds will be added to the integrations page.

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

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.

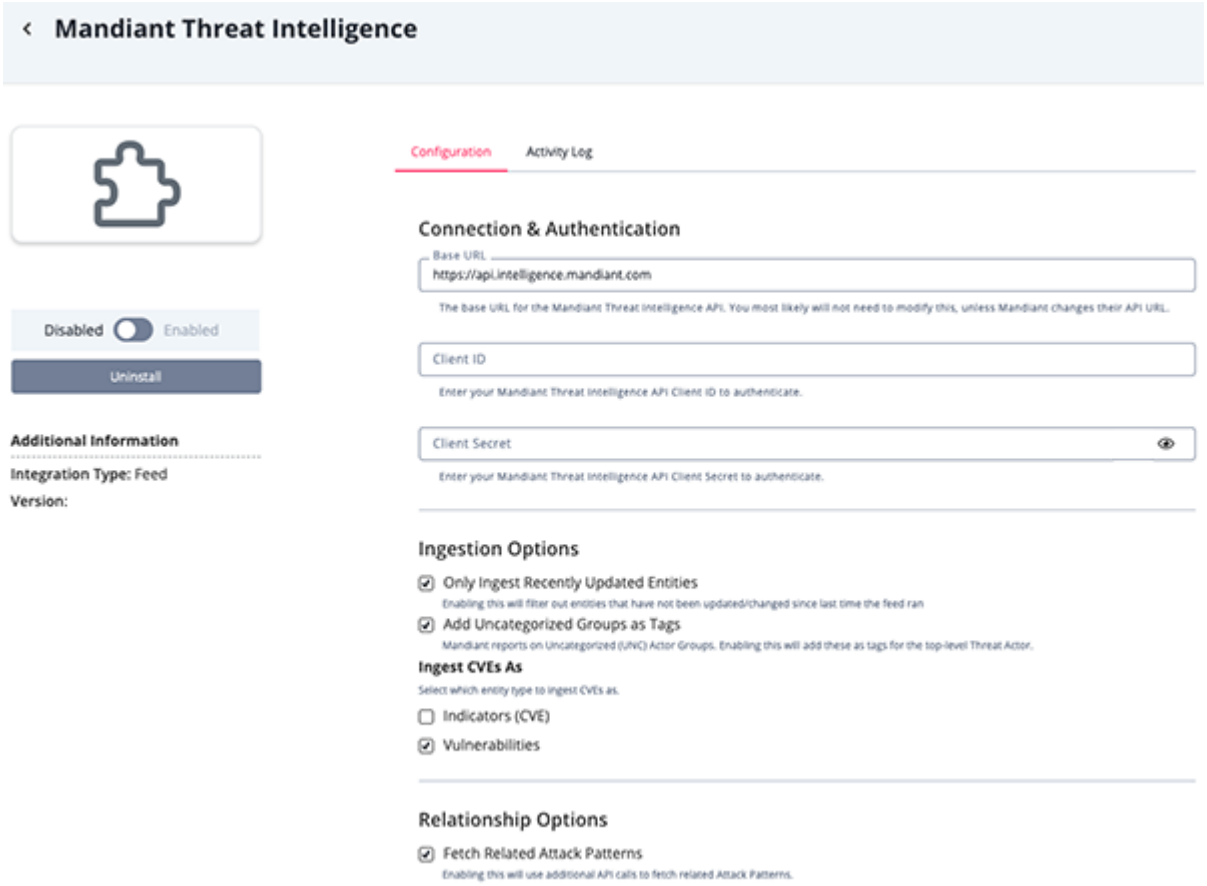
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Mandiant Threat Intelligence Parameters

PARAMETER	DESCRIPTION
Base URL	Your Mandiant base URL.
Client ID	Enter your Mandiant Client ID.
Client Secret	Enter your Mandiant Client Secret.
Only Ingest Recently Updated Entries	Enable this parameter to filter out entities that have not been updated/changed since last time the feed ran. This parameter is enabled by default.
Add Uncategorized Groups as Tags	Enabling this parameter will add Uncategorized (UNC) Actor Groups as tags to the top level Threat Actor. This parameter is enabled by default.
Save CVEs as	Select the object type(s) to ingest CVEs as into the platform. Options include ◦ Indicators (CVE) ◦ Vulnerabilities (default)

Fetch Related Attack Patterns	Enable this parameter to use additional API calls to fetch related Attack Patterns. This parameter is enabled by default.
Fetch Related Indicators	Enable this parameter to use additional API calls to fetch related Indicators. This parameter is disabled by default.
Ingested Indicator Types	Select the types of indicators you would like to ingest into ThreatQ. Options include: ◦ IP Addresses (default) ◦ URLs (default) ◦ Domains (default) ◦ Email Addresses (default) ◦ MD5 Hashes (default) ◦ SHA-1 Hashes (default) ◦ SHA-256 Hashes (default)  This parameter is only accessible if you have enabled the **Fetch Related Indicators** parameter.
Minimum Mandiant Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Malicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Malicious. The default value is 80.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Suspicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Suspicious. The default value is 60.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

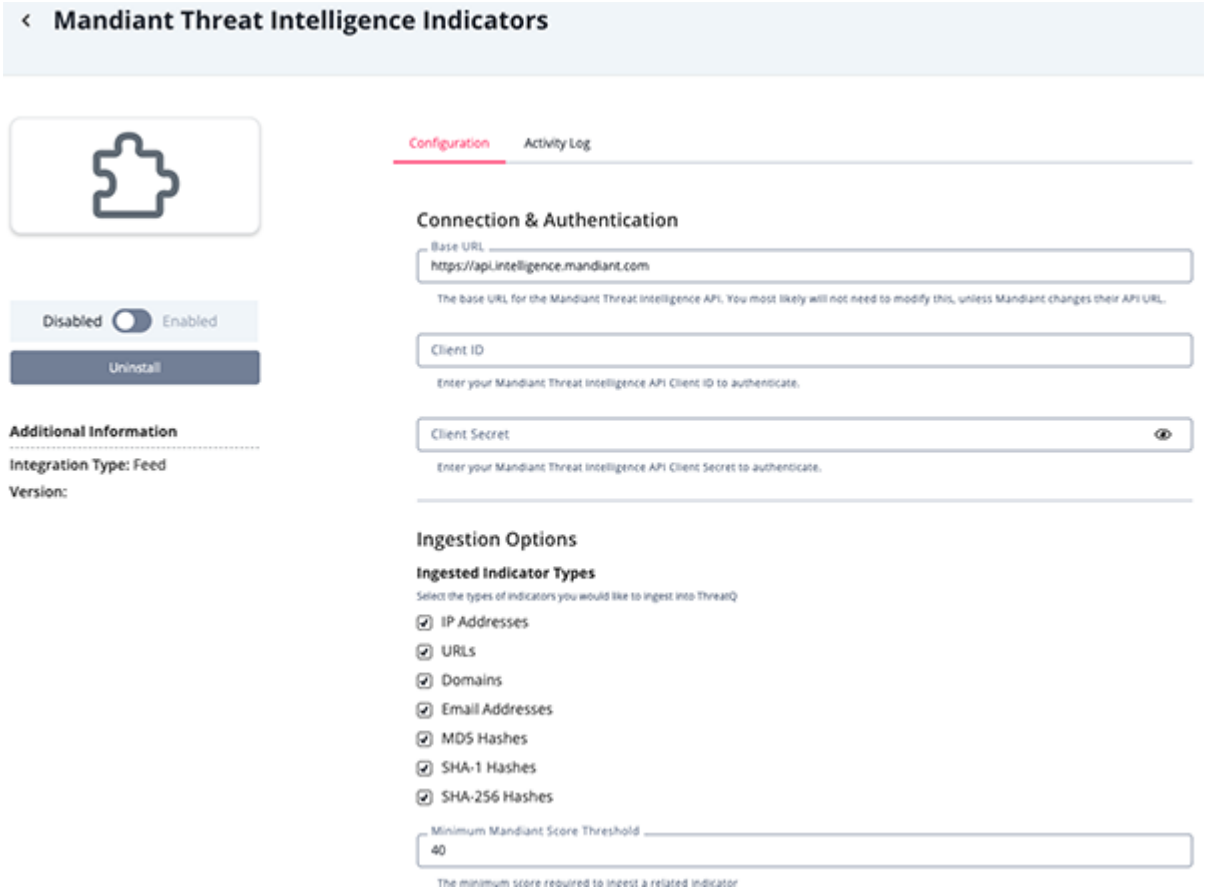
Indeterminate Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Indeterminate. The default value is 40.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Add MISP Flags to Indicator Descriptions	Enable this parameter to put the MISP flags into the description of each of the ingested indicators. This parameter is disabled by default.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Inherit Context from Indicators to Associated Hashes	Enable this parameter to inherit the context from the top-level indicators to the associated hashes. This parameter is enabled by default.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Enable SSL Verification	Enable this parameter for the feed to validate the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.


Mandiant Threat Intelligence
Disabled
Enabled
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
Connection & Authentication
Base URL
https://api.intelligence.mandiant.com
The base URL for the Mandiant Threat Intelligence API. You most likely will not need to modify this, unless Mandiant changes their API URL.
Client ID
Enter your Mandiant Threat Intelligence API Client ID to authenticate.
Client Secret
Enter your Mandiant Threat Intelligence API Client Secret to authenticate.
Ingestion Options
Only Ingest Recently Updated Entities
Enabling this will filter out entities that have not been updated/changed since last time the feed ran
Add Uncategorized Groups as Tags
Mandiant reports on Uncategorized (UNC) Actor Groups. Enabling this will add these as tags for the top-level Threat Actor.
Ingest CVEs As
Select which entity type to ingest CVEs as.
Indicators (CVE)
Vulnerabilities
Relationship Options
Fetch Related Attack Patterns
Enabling this will use additional API calls to fetch related Attack Patterns.

Mandiant Threat Intelligence Indicators

PARAMETER	DESCRIPTION
Base URL	Your Mandiant base URL.
Client ID	Enter your Mandiant Client ID.
Client Secret	Enter your Mandiant Client Secret.
Parsed Entries	Select the IOC types to automatically parse from the content. Options include: ◦ IP Addresses ◦ URLs ◦ Domains ◦ Email Addresses ◦ MD5 Hashes ◦ SHA-1 Hashes ◦ SHA-256
Minimum Mandiant Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Malicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Malicious. The default value is 80.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Suspicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Suspicious. The default value is 60.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

Indeterminate Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Indeterminate. The default value is 40.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Add MISP Flags to Indicator Descriptions	Enable this parameter to put the MISP flags into the description of each of the ingested indicators. This parameter is disabled by default.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Inherit Context from Indicators to Associated Hashes	Enable this parameter to inherit the context from the top-level indicators to the associated hashes. This parameter is enabled by default.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Enable SSL Verification	Enable this parameter for the feed to validate the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



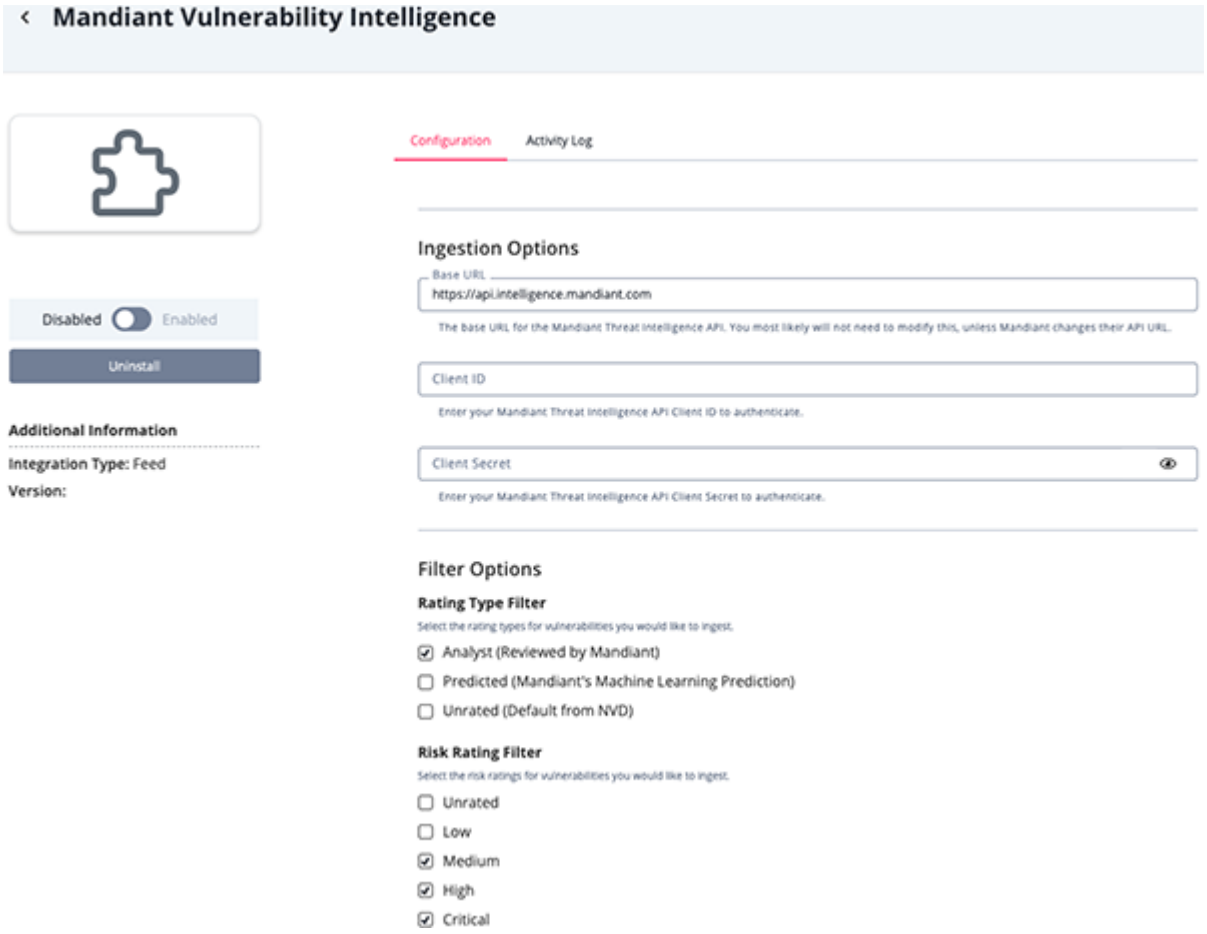
Mandiant Vulnerability Parameters

PARAMETER	DESCRIPTION
Base URL	Your Mandiant base URL.
Client ID	Enter your Mandiant Client ID.
Client Secret	Enter your Mandiant Client Secret.
Range Type Filter	Select the rating types for vulnerabilities to ingest. Options include: ◦ Analyst (Reviewed by Mandiant) *(default)* ◦ Predicted (Mandiant's Machine Learning Prediction) ◦ Unrated (Default from NVD)

Risk Rating Filter	Select the risk ratings for vulnerabilities to ingest. Options include: ◦ Unrated ◦ Low ◦ Medium *(default)* ◦ High *(default)* ◦ Critical *(default)*
Exploitation State Filter	Select the exploitation states for vulnerabilities to ingest. Options include: ◦ No Known *(default)* ◦ Available *(default)* ◦ Confirmed *(default)* ◦ Anticipated *(default)* ◦ Wide *(default)*
Exploitation Vector Filter	Select the exploitation vectors for vulnerabilities to ingest. Options include: ◦ General Network Connectivity *(default)* ◦ Web *(default)* ◦ Local Access *(default)* ◦ Email *(default)* ◦ File Share *(default)* ◦ Open Port *(default)* ◦ Local Network Access *(default)* ◦ Physical Access *(default)*
Vulnerability Must Have a Zero Day	Enabling this will filter out vulnerabilities that do not have zero days exploits. This parameter is disabled by default.
Vulnerability Must be Observed in the Wild	Enabling this will filter out vulnerabilities that have not been observed in the wild. This parameter is disabled by default.
Vulnerability Must be CISA Known Exploited	Enabling this will filter out vulnerabilities that are not CISA known exploited. This parameter is disabled by default.
Vulnerability Must Have Exploits	Enabling this will filter out vulnerabilities that have no associated exploits.

Save CVEs as	Select the object type(s) to ingest CVEs as into the platform. Options include ◦ Indicators (CVE) ◦ Vulnerabilities (default)
Vulnerability Attribute Context	Select the context for vulnerabilities to ingest.Options include: ◦ Available Mitigation *(default)* ◦ CWE *(default)* ◦ Affected Platforms (Based on CPEs) ◦ Affected Products (Based on CPEs) ◦ Affected Vendors (Based on CPEs) *(default)* ◦ Exploitation Consequence *(default)* ◦ Exploitation State *(default)* ◦ Exploitation Vector *(default)* ◦ MVE ID ◦ Observed in the Wild *(default)* ◦ Risk Rating *(default)* ◦ Has Zero Day *(default)* ◦ Is Predicted
Description Context	Select the pieces of context to include in the vulnerability's description. Options include: ◦ Analysis *(default)* ◦ Description *(default)* ◦ Executive Summary *(default)* ◦ Exploits *(default)* ◦ Sources *(default)* ◦ Vendor Fix References *(default)* ◦ Vulnerable CPEs ◦ Vulnerable Products *(default)* ◦ Workarounds *(default)* ◦ CVSS Ratings *(default)*
CVSS Attribute Context	Select the CVSS context for vulnerabilities to ingest. Options include: ◦ Attack Complexity *(default)* ◦ Attack Vector *(default)* ◦ Availability Impact *(default)* ◦ Privileges Required *(default)* ◦ Remediation Level *(default)*

	◦ Base Score *(default)* ◦ Confidentiality Impact *(default)* ◦ Exploit Code Maturity *(default)* ◦ Integrity Impact *(default)* ◦ Report Confidence *(default)* ◦ Scope *(default)* ◦ Temporal Score *(default)* ◦ User Interaction *(default)* ◦ Vector String *(default)*
Enable SSL Verification	Enable this parameter for the feed to validate the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

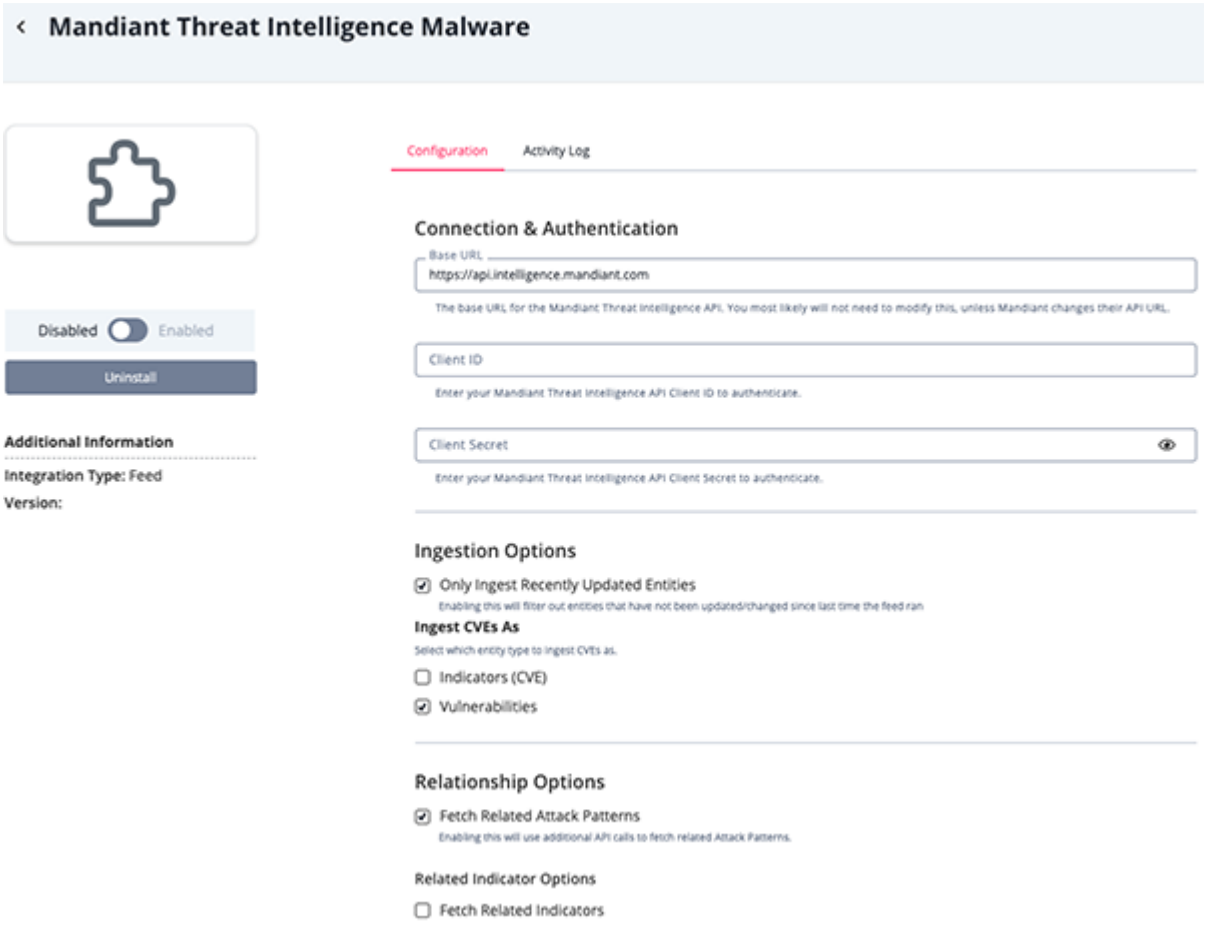


Mandiant Threat Intelligence Malware Parameters

PARAMETER	DESCRIPTION
Base URL	Your Mandiant base URL.
Client ID	Enter your Mandiant Client ID.
Client Secret	Enter your Mandiant Client Secret.
Only Ingest Recently Updated Entries	Enable this parameter to filter out entities that have not been updated/changed since last time the feed ran. This parameter is enabled by default. ⚠ Disabling this parameter will result is extremely long feed run times that may trigger a 500 Internal Server Error from Mandiant.
Save CVEs as	Select the object type(s) to ingest CVEs as into the platform. Options include ◦ Indicators (CVE) ◦ Vulnerabilities (default)
Fetch Related Attack Patterns	Enable this parameter to use additional API calls to fetch related Attack Patterns. This parameter is enabled by default.
Fetch Related Indicators	Enable this parameter to use additional API calls to fetch related Indicators. This parameter is disabled by default.
Ingested Indicator Types	Select the types of indicators you would like to ingest into ThreatQ. Options include: ◦ IP Addresses (default) ◦ URLs (default) ◦ Domains (default) ◦ Email Addresses (default) ◦ MD5 Hashes (default) ◦ SHA-1 Hashes (default) ◦ SHA-256 Hashes (default)

	This parameter is only accessible if you have enabled the **Fetch Related Indicators** parameter.
Minimum Mandiant Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Malicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Malicious. The default value is 80. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Suspicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Suspicious. The default value is 60. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Indeterminate Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Indeterminate. The default value is 40. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Add MISP Flags to Indicator Descriptions	Enable this parameter to put the MISP flags into the description of each of the ingested indicators. This parameter is disabled by default. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.

Inherit Context from Indicators to Associated Hashes	Enable this parameter to inherit the context from the top-level indicators to the associated hashes. This parameter is enabled by default. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Enable SSL Verification	Enable this parameter for the feed to validate the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

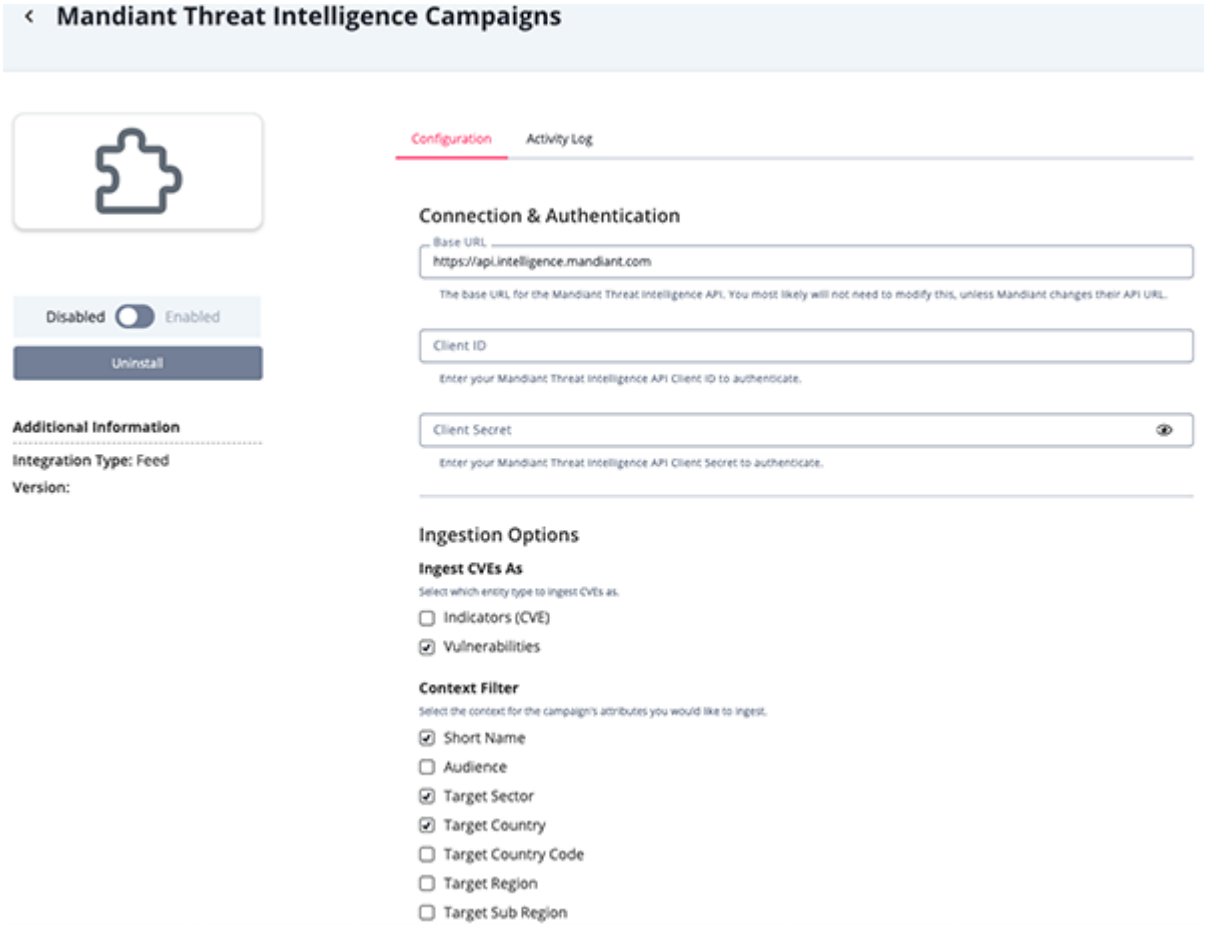


Mandiant Campaigns Parameters

PARAMETER	DESCRIPTION
Base URL	Your Mandiant base URL.
Client ID	Enter your Mandiant Client ID.
Client Secret	Enter your Mandiant Client Secret.
Save CVEs as	Select the object type(s) to ingest CVEs as into the platform. Options include ◦ Indicators (CVE) ◦ Vulnerabilities (default)
Context Filter	Select the context for the campaign's attributes to ingest. Options include: ◦ Short Name ◦ Audience ◦ Target Sector ◦ Target Country ◦ Target Country Code ◦ Target Region ◦ Target Sub Region ◦ Country ◦ Country Code ◦ Region ◦ Sub Region
Relationship Filter	Select the relationships to the campaign to ingest. Options include: ◦ Adversaries ◦ Malware ◦ Tools ◦ Vulnerabilities ◦ Attack Patterns ◦ Malicious Executable Hashes ◦ Phishing Email Addresses ◦ Phishing Email Subjects
Fetch Related Attack Patterns	Enable this parameter to use additional API calls to fetch related Attack Patterns. This parameter is enabled by default.

Fetch Related Indicators	Enable this parameter to use additional API calls to fetch related Indicators. This parameter is disabled by default.
Ingested Indicator Types	Select the types of indicators you would like to ingest into ThreatQ. Options include: ◦ IP Addresses (default) ◦ URLs (default) ◦ Domains (default) ◦ Email Addresses (default) ◦ MD5 Hashes (default) ◦ SHA-1 Hashes (default) ◦ SHA-256 Hashes (default)  This parameter is only accessible if you have enabled the **Fetch Related Indicators** parameter.
Minimum Mandiant Score Threshold	Enter the minimum score required to ingest a related indicator. The default value is 40.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Malicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Malicious. The default value is 80.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Suspicious Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Suspicious. The default value is 60.  This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Indeterminate Disposition Threshold	Enter the minimum score required to mark indicator with a Disposition of Indeterminate. The default value is 40.

	This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Add MISP Flags to Indicator Descriptions	Enable this parameter to put the MISP flags into the description of each of the ingested indicators. This parameter is disabled by default. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Inherit Context from Indicators to Associated Hashes	Enable this parameter to inherit the context from the top-level indicators to the associated hashes. This parameter is enabled by default. This parameter is only accessible if the **Fetch Related Indicators** parameter is enabled.
Enable SSL Verification	Enable this parameter for the feed to validate the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



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

Mandiant Threat Intelligence

The Mandiant Threat Intelligence feed ingests compromised Adversaries as well as any related Indicators, Malware, Vulnerabilities, Attack Patterns, and Tags.

`GET {base_url}/v4/actor`

Sample Response:


```
{
    "threat-actors": [
        {
            "last_updated": "2021-05-13T06:06:21.000Z",
            "aliases": [
                {
                    "attribution_scope": "confirmed",
                    "name": "Comment Crew (Internet)"
                },
                {
                    "attribution_scope": "confirmed",
                    "name": "Comment Crew (ThreatConnect)"
                }
            ],
            "name": "APT1",
            "description": "APT1 refers to a distinct grouping of global cyber
espionage activity with a nexus to China. Based on available data, we assess
that this is a nation-state-sponsored group located in China. Specifically, we
believe that APT1 is the 2nd Bureau of the People's Liberation Army (PLA)
General Staff Department's 3rd Department, or Unit 61398. The activity is
distinguished by the use of common infrastructure and tools and a clear intent
to collect intelligence on a number of issues that may be of interest to the
People's Republic of China (PRC).",
            "id": "threat-actor--0ac5c1db-8ad6-54b8-b4b9-c32fc738c54a",
            "intel_free": true
        },
        {
              "last_updated": "2021-05-13T05:47:03.000Z",
              "aliases": [
                  {
                      "attribution_scope": "confirmed",
                      "name": "4H"
                  },
                  {
                      "attribution_scope": "confirmed",
                      "name": "Icarus (PwC)"
                  },
```

```
                {
                    "attribution_scope": "confirmed",
                    "name": "Putter Panda (CrowdStrike)"
                }
            ],
            "name": "APT2",
            "description": "APT2 is a China-nexus cyber espionage group that
has been recorded as far back as 2010. Their activity targets several
industries, including military and aerospace. APT2 engages in cyber operations
where the goal is intellectual property theft, usually focusing on the data and
projects that make an organization competitive within its field.  ",
            "id": "threat-actor--547739f1-8168-5768-9227-91c1b19eb325",
            "intel_free": false
        }
    ]
}
```


This endpoint is used only to fetch all the `.threat-actors[].id` to be used in the Mandiant Threat Intelligence Actor Details supplemental feed.

Mandiant Threat Intelligence Actor Details (Supplemental)

The Mandiant Threat Intelligence Actor Details supplemental feed is called once per each `.threat-actors[].id` returned by the Mandiant Threat Intelligence feed.

`GET {base_url}/v4/actor/{id}`

Sample Response:


```
{
    "motivations": [
        {
            "id": "motivation--1b8ca82a-7cff-5622-bedd-965c11d38a9e",
            "name": "Espionage",
            "attribution_scope": "confirmed"
        }
    ],
    "aliases": [
        {
            "name": "Comment Crew (Internet)",
            "attribution_scope": "confirmed"
        },
        {
            "name": "Comment Crew (ThreatConnect)",
            "attribution_scope": "confirmed"
        }
    ],
    "industries": [
        {
            "id": "identity--cc593632-0c42-500c-8d0b-d38e97b90f1d",
            "name": "Aerospace & Defense",
            "attribution_scope": "confirmed"
        },
        {
            "id": "identity--a93f63bc-bbfc-52ab-88c0-794c74f5bec0",
            "name": "Chemicals & Materials",
            "attribution_scope": "confirmed"
        }
    ],
    "observed": [
        {
            "earliest": "1980-01-01T00:00:00.000Z",
            "recent": "2014-10-24T03:07:40.000Z",
            "attribution_scope": "confirmed"
        }
    ],
    "malware": [
        {
            "id": "malware--09673ebc-9fbf-5ab0-9130-7874c84cd3e4",
            "name": "AGEDMOAT",
            "attribution_scope": "confirmed"
```

```
        },
        {
            "id": "malware--7c00490d-dc79-5623-bf50-fb4b169d1b4f",
            "name": "AGEDSHOE",
            "attribution_scope": "confirmed"
        }
    ],
    "locations": {
        "source": [
            {
                "region": {
                    "id": "location--fd209e8b-e81d-52e7-956b-35aa7be87f06",
                    "name": "Asia",
                    "attribution_scope": "confirmed"
                },
                "sub_region": {
                    "id": "location--d617ba9a-eb1e-5ac5-9dee-1f3a3bd12883",
                    "name": "East Asia",
                    "attribution_scope": "confirmed"
                },
                "country": {
                    "id": "location--384b6e7c-fc6f-5bec-bfbf-1edc4b8e82de",
                    "name": "China",
                    "iso2": "cn",
                    "attribution_scope": "confirmed"
                }
            }
        ],
        "target": [
            {
                "id": "location--a509dfc8-789b-595b-a201-29c7af1dc0bb",
                "name": "Belgium",
                "iso2": "be",
                "attribution_scope": "confirmed"
            },
            {
                "id": "location--fde14246-c07b-5f3f-9ac8-8d4d50910f15",
                "name": "Canada",
                "iso2": "ca",
                "attribution_scope": "confirmed"
            }
        ]
    },
    "cve": [
      {
        "cve_id": "CVE-2021-26858"
      }
    ],
    "associated_uncs": [],
    "id": "threat-actor--0ac5c1db-8ad6-54b8-b4b9-c32fc738c54a",
```

```
    "name": "APT1",
    "description": "APT1 refers to a distinct grouping of global cyber
espionage activity with a nexus to China. Based on available data, we assess
that this is a nation-state-sponsored group located in China. Specifically, we
believe that APT1 is the 2nd Bureau of the People's Liberation Army (PLA)
General Staff Department's 3rd Department, or Unit 61398. The activity is
distinguished by the use of common infrastructure and tools and a clear intent
to collect intelligence on a number of issues that may be of interest to the
People's Republic of China (PRC).",
    "last_updated": "2021-05-13T06:06:21.000Z",
    "last_activity_time": "2014-10-24T03:07:40.000Z",
    "audience": [
        {
            "name": "intel_fusion",
            "license": "INTEL_RBI_FUS"
        },
        {
            "name": "intel_ce",
            "license": "INTEL_CYB_ESP"
        }
    ],
    "counts": {
        "reports": 58,
        "malware": 89,
        "cve": 0,
        "associated_uncs": 0,
        "aliases": 7,
        "industries": 18
    },
    "intel_free": true
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	Adversary.Value	N/A	.last_updated	APT1	N/A
.aliases[].name	Adversary.Tag	N/A	N/A	Comment Crew (Internet)	N/A
.description	Adversary.Description	N/A	N/A	APT1 refers to a	N/A
.motivations[].name + .motivations[].attribution_scope	Adversary.Attribute	Motivation	.last_updated	Espionage - confirmed	N/A
.industries[].name + .industries[].attribution_scope	Adversary.Attribute	Industry	.last_updated	Aerospace & Defense - confirmed	N/A
.locations.source[].region.name	Adversary.Attribute	Region	.last_updated	Asia	N/A
.locations.source[].sub_region.name	Adversary.Attribute	Sub Region	.last_updated	East Asia	N/A
.locations.source[].country.name	Adversary.Attribute	Country	.last_updated	China	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.locations.source[].country.iso2	Adversary.Attribute	Country Code	.last_updated	cn	N/A
.locations.target[].name	Adversary.Attribute	Target Country	.last_updated	Belgium	N/A
.locations.target[].iso2	Adversary.Attribute	Target Country Code	.last_updated	be	N/A
.audience[].name	Adversary.Attribute	Audience	.last_updated	intel_fusion	N/A
.audience[].license	Adversary.Attribute	Audience	.last_updated	INTEL_RBI_FUS	N/A
.associated_uncs[].name	Adversary.Tag	N/A	N/A	UNC235	Ingested if `Add Uncategorized Groups as Tags` option is enabled
.cve[].cve_id	Related Indicator.Value / Vulnerability.Value	N/A	.last_updated	CVE-2021-26858	N/A
.malware[].id	N/A	N/A	N/A	malware--09673ebc-9fbf-5ab0-9130-7874c84cd3e4	Will be used in `Mandiant Threat Intelligence Malware Details` Feed to get more details for the malware

Mandiant Threat Intelligence Malware Details (Supplemental)

The Mandiant Threat Intelligence Malware Details supplemental feed is called once per each `.malware[].id` returned by the Mandiant Threat Intelligence Actor Details feed.

`GET {base_url}/v4/malware/{malware.id}`

Sample Response:


```
{
    "inherently_malicious": 1,
    "operating_systems": [
        "Windows"
    ],
    "aliases": "redacted",
    "capabilities": "redacted",
    "industries": [
        {
            "id": "identity--cc593632-0c42-500c-8d0b-d38e97b90f1d",
            "name": "Aerospace & Defense"
        },
        {
            "id": "identity--93209517-b16c-5893-b55e-b7edc9b478d0",
            "name": "Telecommunications"
        }
    ],
    "detections": [
        "FE_Autopatt_Win_AGEDMOAT"
    ],
    "yara": [
        {
            "id": "signature--dc89e8a3-8f0b-56a1-a2bf-e2be22cd3e5d",
            "name": "FE_Autopatt_Win_AGEDMOAT"
        }
    ],
    "roles": "redacted",
    "malware": [
      {
            "id": "malware--228932dc-3631-5fd9-bb62-76670d8d35d0",
            "name": "AIRBREAK",
            "attribution_scope": "confirmed"
      },
      {
          "id": "malware--f901acb8-41f6-55c6-b1d7-88816d6c5a78",
          "name": "AURIGA",
          "attribution_scope": "confirmed"
      }
    ],
    "actors": [
        {
            "id": "threat-actor--0ac5c1db-8ad6-54b8-b4b9-c32fc738c54a",
```

```
            "name": "APT1",
            "country_name": "unknown",
            "iso2": "unknown"
        }
    ],
    "cve": "redacted",
    "id": "malware--09673ebc-9fbf-5ab0-9130-7874c84cd3e4",
    "name": "AGEDMOAT",
    "description": "AGEDMOAT is an HTTP-based downloader that accepts commands
embedded in a hardcoded HTML C2 file.  It is capable of downloading and
executing a file.",
    "last_updated": "2021-05-13T02:11:06.000Z",
    "last_activity_time": "2021-05-13T02:11:06.000Z",
    "audience": [
        {
            "name": "intel_fusion",
            "license": "INTEL_RBI_FUS"
        },
        {
            "name": "intel_oper",
            "license": "INTEL_RBI_OPS"
        },
        {
            "name": "tlp_marking",
            "license": "green"
        }
    ],
    "counts": {
        "reports": 0,
        "capabilities": 13,
        "malware": 0,
        "actors": 1,
        "detections": 1,
        "cve": 0,
        "aliases": 0,
        "industries": 2
    },
    "intel_free": false
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	Related Malware.Value	N/A	.last_updated	'AGEDMOAT'	N/A
.description	Related Malware.Description	N/A	.last_updated	'AGEDMOAT is an HTTP-based'	N/A
.audience[].license	Related Malware.Attribute	Audience	.last_updated	'INTEL_RBI_FUS'	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.audience[].name	Related Malware.Attribute	Audience	.last_updated	'intel_fusion'	N/A
.operating_systems[]	Related Malware.Attribute	Target Operating System	.last_updated	'Windows'	N/A
.industries[].name	Related Malware.Attribute	Industry	.last_updated	'Aerospace & Defense'	N/A
.detections[]	Related Malware.Attribute	Detection	.last_updated	'FE_Autopatt_Win_AGEDMOAT'	N/A
.malware[].name	Related Malware.Value	N/A	.last_updated	'AIRBREAK'	N/A

Mandiant Threat Intelligence Entity Attack Pattern Details (Supplemental)

Enabling the `Fetch Related Attack Patterns` configuration parameter will result in the Mandiant Threat Intelligence Entity Attack Pattern Details supplemental feed fetching related attack patterns to threat actors.

`GET {base_url}/v4/{entity}/{entity.id}`

Sample Response:


```
{
    "attack-patterns": {
        "attack-pattern--01327cde-66c4-4123-bf34-5f258d59457b": {
            "attack_pattern_identifier": "T1021.005",
            "created": "2020-02-11T18:28:44.950Z",
            "description": "Adversaries may use [Valid Accounts](https://
attack.mitre.org/techniques/T1078) to remotely control machines using Virtual
Network Computing (VNC). The adversary may then perform actions as the logged-
on user.\n\nVNC is a desktop sharing system that allows users to remotely
control another computer\u2019s display by relaying mouse and keyboard inputs
over the network. VNC does not necessarily use standard user credentials.
Instead, a VNC client and server may be configured with sets of credentials
that are used only for VNC connections.",
            "id": "attack-pattern--01327cde-66c4-4123-bf34-5f258d59457b",
            "modified": "2020-03-23T20:41:21.147Z",
            "name": "VNC",
            "x_mitre_is_subtechnique": true
        },
        "attack-pattern--0259baeb-9f63-4c69-bf10-eb038c390688": {
            "attack_pattern_identifier": "T1113",
            "created": "2017-05-31T21:31:25.060Z",
            "description": "Adversaries may attempt to take screen captures of
the desktop to gather information over the course of an operation. Screen
capturing functionality may be included as a feature of a remote access tool
used in post-compromise operations. Taking a screenshot is also typically
possible through native utilities or API calls, such as <code>CopyFromScreen</
code>, <code>xwd</code>, or <code>screencapture</code>.(Citation:
CopyFromScreen .NET)(Citation: Antiquated Mac Malware)\n",
            "id": "attack-pattern--0259baeb-9f63-4c69-bf10-eb038c390688",
            "modified": "2020-03-24T19:56:37.627Z",
            "name": "Screen Capture",
            "x_mitre_is_subtechnique": false
        }
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.[].attack_pattern_identifier - .[].name	Related AttackPattern.Value	N/A	N/A	T1113 - Screen Capture	N/A

Mandiant Threat Intelligence Threat Actor Indicators (Supplemental)

When the `Fetch Related Indicators` parameter is enabled, the Mandiant Threat Intelligence Threat Actor Indicators supplemental feed will be used to fetch related indicators to threat actors.

`GET {base_url}/v4/actor/{actor.id}/indicators`

Sample Response:


```
{
    "id": "threat-actor--0ac5c1db-8ad6-54b8-b4b9-c32fc738c54a",
    "indicator_count": {
        "email": 0,
        "fqdn": 2137,
        "hash": 35,
        "ipv4": 106,
        "total": 2281,
        "url": 3
    },
    "indicators": [
        {
            "attributed_associations": [
                {
                    "id": "threat-actor--0ac5c1db-8ad6-54b8-b4b9-c32fc738c54a",
                    "name": "APT1",
                    "type": "threat-actor"
                }
            ],
            "associated_hashes": [
                {
                    "id": "md5--16fea832-4a73-5645-911b-ba7a823947f8",
                    "type": "md5",
                    "value": "7c357e54f775f0042c2d8e36d0c38fa9"
                }
            ],
            "first_seen": "2011-09-12T12:23:13.000Z",
            "id": "fqdn--25667188-bcf5-5abc-b1cc-caabfa18e2b3",
            "is_exclusive": true,
            "is_publishable": true,
            "last_seen": "2011-09-12T12:23:13.000Z",
            "last_updated": "2022-01-16T00:26:22.080Z",
            "misp": {
                "akamai": false,
                "alexa": false,
                "alexa_1M": false,
                "amazon-aws": false,
                "apple": false,
                "automated-malware-analysis": false,
                "bank-website": false,
                "cisco_1M": true,
                "cisco_top1000": false,
```

```
            "cisco_top10k": false,
            "cisco_top20k": false,
            "cisco_top5k": false,
            "cloudflare": false,
            "common-contact-emails": false,
            "common-ioc-false-positive": false,
            "covid": false,
            "covid-19-cyber-threat-coalition-whitelist": false,
            "covid-19-krassi-whitelist": false,
            "crl-hostname": false,
            "crl-ip": false,
            "dax30": false,
            "disposable-email": false,
            "dynamic-dns": false,
            "eicar.com": false,
            "empty-hashes": false,
            "fastly": false,
            "google": false,
            "google-gcp": false,
            "google-gmail-sending-ips": false,
            "googlebot": false,
            "ipv6-linklocal": false,
            "majestic_million": false,
            "majestic_million_1M": false,
            "microsoft": false,
            "microsoft-attack-simulator": false,
            "microsoft-azure": false,
            "microsoft-azure-china": false,
            "microsoft-azure-germany": false,
            "microsoft-azure-us-gov": false,
            "microsoft-office365": false,
            "microsoft-office365-cn": false,
            "microsoft-office365-ip": false,
            "microsoft-win10-connection-endpoints": false,
            "moz-top500": false,
            "mozilla-CA": false,
            "mozilla-IntermediateCA": false,
            "multicast": false,
            "nioc-filehash": false,
            "ovh-cluster": false,
            "phone_numbers": false,
            "public-dns-hostname": false,
            "public-dns-v4": false,
            "public-dns-v6": false,
            "rfc1918": false,
            "rfc3849": false,
            "rfc5735": false,
            "rfc6598": false,
            "rfc6761": false,
            "second-level-tlds": true,
```

```
                "security-provider-blogpost": false,
                "sinkholes": false,
                "smtp-receiving-ips": false,
                "smtp-sending-ips": false,
                "stackpath": false,
                "ti-falsepositives": false,
                "tlds": true,
                "tranco": false,
                "tranco10k": false,
                "university_domains": false,
                "url-shortener": false,
                "vpn-ipv4": false,
                "vpn-ipv6": false,
                "whats-my-ip": false,
                "wikimedia": false
            },
            "mscore": 94,
            "sources": [
                {
                    "category": [],
                    "first_seen": "2011-09-12T12:23:13.000+0000",
                    "last_seen": "2011-09-12T12:23:13.000+0000",
                    "osint": false,
                    "source_name": "Mandiant"
                }
            ],
            "type": "fqdn",
            "value": "agru.qpoe.com"
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].value	Indicator.Value	Mapped: `.type`	.first_seen	agru.qpoe.com	See Indicator Type mapping table below
.indicators[].mscore	Indicator.Attribute	Mandiant Score	.first_seen	94	N/A
.indicators[].mscore	Indicator.Attribute	Mandiant Confidence	.first_seen	Malicious	Benign,Indeterminate, or Malicious
.indicators[].sources[].category[]	Indicator.Attribute	Category	.first_seen	94	N/A
.indicators[].misp	Indicator.Description	N/A	N/A	N/A	Json format of `misp` field
.indicators[].attributed_associations[].name	Related Adversary.Value	N/A	.first_seen	APT1	Ingested if `type` is `threat-actor`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].associated_hashes[].value	Related Indicator.Value	Mapped: `.type`	.first_seen	7c357e54f775f0042c2d8e36d0c38fa9	See Indicator Type mapping table below

Indicator Type Mapping

MANDIANT TYPE	THREATQ INDICATOR TYPE
fqdn	FQDN
ip	IP Address
ipv4	IP Address
email	Email Address
ipv6	IPv6 Address
url	URL
domain	FQDN
sha1	SHA-1
md5	MD5
sha256	SHA-256
sha512	SHA-512
sha386	SHA-386

Mandiant Threat Intelligence Indicators

The Mandiant Threat Intelligence Indicators feed ingests a list of Indicators tracked by Mandiant.

`GET {base_url}/v4/indicator`

Sample Response:


```
{
    "indicators": [
        {
            "id": "ipv4--5d6fe061-0735-5f94-9f34-666fb4ddcdb8",
            "mscore": 19,
            "type": "ipv4",
            "value": "208.109.67.112",
            "is_publishable": true,
            "sources": [
                {
                    "first_seen": "2022-04-26T22:10:00.678+0000",
                    "last_seen": "2022-09-25T22:10:00.929+0000",
                    "osint": true,
                    "category": [
                        "phishing",
                        "malware"
                    ],
                    "source_name": "phishstats"
                },
                {
                    "first_seen": "2022-08-12T03:10:58.820+0000",
                    "last_seen": "2022-08-12T03:10:58.820+0000",
                    "osint": false,
                    "category": [],
                    "source_name": "Mandiant"
                }
            ],
            "misp": {
                "akamai": false,
                "alexa": false,
                "alexa_1M": false,
                "amazon-aws": false,
                "apple": false,
                "automated-malware-analysis": false,
                "bank-website": false,
                "cisco_1M": false,
                "cisco_top1000": false,
                "cisco_top10k": false,
                "cisco_top20k": false,
                "cisco_top5k": false,
                "cloudflare": false,
                "common-contact-emails": false,
```

```
            "common-ioc-false-positive": false,
            "covid": false,
            "covid-19-cyber-threat-coalition-whitelist": false,
            "covid-19-krassi-whitelist": false,
            "crl-hostname": false,
            "crl-ip": false,
            "dax30": false,
            "disposable-email": false,
            "dynamic-dns": false,
            "eicar.com": false,
            "empty-hashes": false,
            "fastly": false,
            "google": false,
            "google-gcp": false,
            "google-gmail-sending-ips": false,
            "googlebot": false,
            "ipv6-linklocal": false,
            "majestic_million": false,
            "majestic_million_1M": false,
            "microsoft": false,
            "microsoft-attack-simulator": false,
            "microsoft-azure": false,
            "microsoft-azure-china": false,
            "microsoft-azure-germany": false,
            "microsoft-azure-us-gov": false,
            "microsoft-office365": false,
            "microsoft-office365-cn": false,
            "microsoft-office365-ip": false,
            "microsoft-win10-connection-endpoints": false,
            "moz-top500": false,
            "mozilla-CA": false,
            "mozilla-IntermediateCA": false,
            "multicast": false,
            "nioc-filehash": false,
            "ovh-cluster": false,
            "phone_numbers": false,
            "public-dns-hostname": false,
            "public-dns-v4": false,
            "public-dns-v6": false,
            "rfc1918": false,
            "rfc3849": false,
            "rfc5735": false,
            "rfc6598": false,
            "rfc6761": false,
            "second-level-tlds": false,
            "security-provider-blogpost": false,
            "sinkholes": false,
            "smtp-receiving-ips": false,
            "smtp-sending-ips": false,
            "stackpath": false,
```

```
                "tenable-cloud-ipv4": false,
                "tenable-cloud-ipv6": false,
                "ti-falsepositives": false,
                "tlds": false,
                "tranco": false,
                "tranco10k": false,
                "university_domains": false,
                "url-shortener": false,
                "vpn-ipv4": true,
                "vpn-ipv6": false,
                "whats-my-ip": false,
                "wikimedia": false
            },
            "last_updated": "2022-10-26T02:34:33.008Z",
            "first_seen": "2022-04-26T22:10:00.000Z",
            "last_seen": "2022-09-25T22:10:00.000Z"
        }
    ],
    "next":
"FGluY2x1ZGVfY29udGV4dF91dWlkDnF1ZXJ5VGhlbkZldGNoKhZ5NzZIQ3hES1J5YTcxdzFuV0QyT2
p3AAAAAAH5b
oQWTVFPRUpvOGdUV0tQZ1FPMzFKUWduQRZXRVpGZldhY1FUbUFfdDA4ZW9uTVd3AAAAAAHdrksWUmdp
aFJUbkVUbnl
ydm16bVh4d3lxURY0aGlYNVo5TFJWS0o2ek5VcVVnSzBRAAAAAAImtYYWTGRKREd5TUNRckNFWXJhc3
hRbnBKZxZ2V
m9tR2lrYVNHYV8wUm9kRU1mS053AAAAAAIQSywWZWpobmJSbFRTRGUtRjJoMEpESFBlZxZZeXVoRFZw
WVFXeUxxU0l
xUXNSQUxBAAAAAAIDHrcWWWZGOTJLTGlRMjJhWXlZRzh4U3ZsdxZTWld2Uk14UFRmdURxMlMtazRHcj
NnAAAAAAHnK
5gWa1pRNklpaERRekN6Y1JyM193M2NOURZUeVRhODMyU1J5R2lBVHdfalM4cWpBAAAAAAIKTa8WZkZI
NDZIUktSc2U
2ZzlJdmZ5cmVXZxYyLTI1ZXd4ZVJZMlF2eFZzcTdyc193AAAAAAI0JZIWSWlBalNDc2hRYWFiN3VlZW
hWNWdPZxZXU
0R3NzdDWVRyLWo2emhLUzd4MnNnAAAAAAIM9vkWLTdpbXB1S3JSRkNEYzdYZ0pWWEs3ZxZZeXVoRFZw
WVFXeUxxU0l
xUXNSQUxBAAAAAAIDHrYWWWZGOTJLTGlRMjJhWXlZRzh4U3ZsdxYyLTI1ZXd4ZVJZMlF2eFZzcTdyc1
93AAAAAAI0J
ZEWSWlBalNDc2hRYWFiN3VlZWhWNWdPZxY0aGlYNVo5TFJWS0o2ek5VcVVnSzBRAAAAAAImtYUWTGRK
REd5TUNRckN
FWXJhc3hRbnBKZxZ5NzZIQ3hES1J5YTcxdzFuV0QyT2p3AAAAAAH5boUWTVFPRUpvOGdUV0tQZ1FPMz
FKUWduQRZ2V
m9tR2lrYVNHYV8wUm9kRU1mS053AAAAAAIQSysWZWpobmJSbFRTRGUtRjJoMEpESFBlZxY4MU01M3ZY
bVFPNldmZ3p
hRXhEMnh3AAAAAAHwOkQWWkVBb3BKLUFRSmUxbjhHUFp2Sm44URYyLTI1ZXd4ZVJZMlF2eFZzcTdyc1
93AAAAAAI0J
ZAWSWlBalNDc2hRYWFiN3VlZWhWNWdPZxZERno0UFFCRFM5eW5FNVlUaHpjczJRAAAAAAH1GhwWUU9N
TTVqYWpTeEN
GWnF0VTd0Q0VhdxZERno0UFFCRFM5eW5FNVlUaHpjczJRAAAAAAH1GhsWUU9NTTVqYWpTeENGWnF0VT
d0Q0VhdxZ2V
m9tR2lrYVNHYV8wUm9kRU1mS053AAAAAAIQSy0WZWpobmJSbFRTRGUtRjJoMEpESFBlZxZ5NzZIQ3hE
```

```
S1J5YTcxdzF
uV0QyT2p3AAAAAAH5boMWTVFPRUpvOGdUV0tQZ1FPMzFKUWduQRZXU0R3NzdDWVRyLWo2emhLUzd4Mn
NnAAAAAAIM9
voWLTdpbXB1S3JSRkNEYzdYZ0pWWEs3ZxZERno0UFFCRFM5eW5FNVlUaHpjczJRAAAAAAH1Gh0WUU9N
TTVqYWpTeEN
GWnF0VTd0Q0VhdxZXRVpGZldhY1FUbUFfdDA4ZW9uTVd3AAAAAAHdrkwWUmdpaFJUbkVUbnlydm16bV
h4d3lxURZUe
VRhODMyU1J5R2lBVHdfalM4cWpBAAAAAAIKTbEWZkZINDZIUktSc2U2ZzlJdmZ5cmVXZxZUeVRhODMy
U1J5R2lBVHd
falM4cWpBAAAAAAIKTbAWZkZINDZIUktSc2U2ZzlJdmZ5cmVXZxZUeVRhODMyU1J5R2lBVHdfalM4cW
pBAAAAAAIKT
bIWZkZINDZIUktSc2U2ZzlJdmZ5cmVXZxZXU0R3NzdDWVRyLWo2emhLUzd4MnNnAAAAAAIM9vsWLTdp
bXB1S3JSRkN
EYzdYZ0pWWEs3ZxZjWTFieVZsZlR5ZUx1ek50QzQ3MzdnAAAAAAHgFz8WSklEcml3WThRbWFKZEdzaz
Rsam9vdxZZe
XVoRFZwWVFXeUxxU0lxUXNSQUxBAAAAAAIDHrkWWWZGOTJLTGlRMjJhWXlZRzh4U3ZsdxZjWTFieVZs
ZlR5ZUx1ek5
0QzQ3MzdnAAAAAAHgFz4WSklEcml3WThRbWFKZEdzazRsam9vdxY0aGlYNVo5TFJWS0o2ek5VcVVnSz
BRAAAAAAImt
YcWTGRKREd5TUNRckNFWXJhc3hRbnBKZxZXRVpGZldhY1FUbUFfdDA4ZW9uTVd3AAAAAAHdrkoWUmdp
aFJUbkVUbnl
ydm16bVh4d3lxURZjWTFieVZsZlR5ZUx1ek50QzQ3MzdnAAAAAAHgF0AWSklEcml3WThRbWFKZEdzaz
Rsam9vdxZTW
ld2Uk14UFRmdURxMlMtazRHcjNnAAAAAAHnK5kWa1pRNklpaERRekN6Y1JyM193M2NOURZTWld2Uk14
UFRmdURxMlM
tazRHcjNnAAAAAAHnK5oWa1pRNklpaERRekN6Y1JyM193M2NOURZTWld2Uk14UFRmdURxMlMtazRHcj
NnAAAAAAHnK
5sWa1pRNklpaERRekN6Y1JyM193M2NOURZXU0R3NzdDWVRyLWo2emhLUzd4MnNnAAAAAAIM9v0WLTdp
bXB1S3JSRkN
EYzdYZ0pWWEs3ZxZZeXVoRFZwWVFXeUxxU0lxUXNSQUxBAAAAAAIDHrsWWWZGOTJLTGlRMjJhWXlZRz
h4U3ZsdxY4M
U01M3ZYbVFPNldmZ3phRXhEMnh3AAAAAAHwOkgWWkVBb3BKLUFRSmUxbjhHUFp2Sm44URY4MU01M3ZY
bVFPNldmZ3p
hRXhEMnh3AAAAAAHwOkkWWkVBb3BKLUFRSmUxbjhHUFp2Sm44URYyLTI1ZXd4ZVJZMlF2eFZzcTdyc1
93AAAAAAI0J
ZQWSWlBalNDc2hRYWFiN3VlZWhWNWdPZxY0aGlYNVo5TFJWS0o2ek5VcVVnSzBRAAAAAAImtYsWTGRK
REd5TUNRckN
FWXJhc3hRbnBKZw=="
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].value	Indicator.Value	Mapped: `.type`	.first_seen	agru.qpoe.com	See Indicator Type Mapping Table above
.indicators[].mscore	Indicator.Attribute	Mandiant Score	.first_seen	94	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.indicators[].mscore	Indicator.Attribute	Mandiant Confidence	.first_seen	Malicious	Benign,Indeterminate, or Malicious
.indicators[].sources[].category[]	Indicator.Attribute	Category	.first_seen	94	N/A
.indicators[].misp	Indicator.Description	N/A	N/A	N/A	N/A
.indicators[].attributed_associations[].name	Related Adversary.Value	N/A	.first_seen	APT1	Ingested if `type` is `threat-actor`
.indicators[].associated_hashes[].value	Related Indicator.Value	Mapped: `.type`	.first_seen	7c357e54f775f0042c2d8e36d0c38fa9	See Indicator Type Mapping Table above

Mandiant Vulnerability Intelligence

The Mandiant Vulnerability Intelligence feed ingests a list of Vulnerabilities tracked by Mandiant.

`GET {base_url}/v4/vulnerability`

Sample Response:


```
{
  "vulnerability": [
    {
      "analysis": "<p>An attacker could exploit this vulnerability to execute
arbitrary code. An attacker would need to craft malicious webpage and lure a
user to visit it.</p>\n<p>On Sept. 21, 2023, Apple reported three
vulnerabilities <a href=\"https://advantage.mandiant.com/vulnerabilities/
CVE-2023-41991\">(CVE-2023-41991</a>, <a href=\"https://advantage.mandiant.com/
vulnerabilities/CVE-2023-41992\">CVE-2023-41992</a>, and <a href=\"https://
advantage.mandiant.com/vulnerabilities/CVE-2023-41993\">CVE-2023-41993)</a>
were being exploited in the wild against versions of iOS before iOS 16.7
crediting the partnership of The Citizen Lab and Google's Threat Analysis
Group.</p>\n<p>On Sept. 22, 2023, Google Threat Analysis Group (TAG) and
Citizen Lab published individual blogs detailing their observations on the
zero-day exploit chain which was used to install Predator spyware on at least
one victim&rsquo;s device. In the iOS exploit chain, <a href=\"https://
advantage.mandiant.com/vulnerabilities/CVE-2023-41993\">(CVE-2023-41993</a>)
was exploited to gain initial access, followed by <a href=\"https://
advantage.mandiant.com/vulnerabilities/CVE-2023-41993\">(CVE-2023-41993</a>)
and (<a href=\"https://advantage.mandiant.com/vulnerabilities/
CVE-2023-41991\">CVE-2023-41991)</a>, to escalate privileges and maintain
persistence on exploited devices. Google observed the attacker also possessed
an exploit chain to install Predator on Android devices using <a
href=\"https://advantage.mandiant.com/vulnerabilities/
CVE-2023-4762\">(CVE-2023-4762)</a> to gain initial access. For more
information, please see Google TAG's blog,&amp;nbsp;<a href=\"https://blog.google/
threat-analysis-group/0-days-exploited-by-commercial-surveillance-vendor-in-
egypt/\">\"0-days exploited by commercial surveillance vendor in Egypt,\"</a>
and Citizen's Lab blog,&amp;nbsp;<a href=\"https://citizenlab.ca/2023/09/predator-
in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-
presidential-ambitions/\">\"PREDATOR IN THE WIRES.\"</a></p>\n<p>While this
vulnerability was initially reported as a zero day vulnerability, further
analysis revealed that it was exploited after a patch for chromium was made
available. Exploitation occurred on iOS devices where the patch had yet to be
deployed by the vendor. This is commonly referred to as \"patch-gapping\" and
does not meet Mandiant's definition of a zero day vulnerability.</
p>\n<p>Mandiant Intelligence considers this a Medium-risk vulnerability due to
the potential for a remote attacker to execute arbitrary code offset by the
requirement for user interaction.</p>",
      "available_mitigation": ["Patch"],
      "common_vulnerability_scores": {
        "v3.1": {
```

```
          "attack_complexity": "LOW",
          "attack_vector": "NETWORK",
          "availability_impact": "HIGH",
          "base_score": 8.8,
          "confidentiality_impact": "HIGH",
          "exploit_code_maturity": "UNPROVEN",
          "integrity_impact": "HIGH",
          "privileges_required": "NONE",
          "remediation_level": "NOT_DEFINED",
          "report_confidence": "CONFIRMED",
          "scope": "UNCHANGED",
          "temporal_score": 8.8,
          "user_interaction": "REQUIRED",
          "vector_string": "CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H"
        }
      },
      "cve_id": "CVE-2023-4762",
      "cwe": "Access of Resource Using Incompatible Type ('Type Confusion')",
      "description": "<p>Type Confusion in V8 in Google Chrome prior to
116.0.5845.179 allowed a remote attacker to execute arbitrary code via a
crafted HTML page.</p>",
      "executive_summary": "<ul><li>An Access of Resource Using Incompatible
Type ('Type Confusion') vulnerability exists that, when exploited, allows a
remote attacker to execute arbitrary code.</li><li>This vulnerability has been
confirmed to be exploited in the wild, and proof-of-concept code is publicly
available.</li><li>Mandiant Intelligence considers this a Medium-risk
vulnerability due to the potential for arbitrary code execution, offset by user
interaction requirements.</li><li>Mitigation options include a patch.</li></
ul>",
      "exploitation_consequence": "Code Execution",
      "exploitation_state": "Confirmed",
      "exploitation_vectors": ["Web"],
      "exploits": [
        {
          "description": "<p>This PoC takes the form of a write-up and
JavaScript which can trigger this vulnerability.</p>",
          "exploit_url": "https://github.com/buptsb/CVE-2023-4762/blob/main/
poc.js",
          "file_size": 4981,
          "grade": "Proof-of-concept",
          "hashes": {
            "md5": "7F88CF7D9E3913A8AF703780288A4C65",
            "sha1": "F188DB78C65336DBB87F0C9643838C4F65CCB51E",
            "sha256":
"9E042FAD9611C297C90E3E5917A31CCB3C2082CEC04239A5466CB5D1D323E9BF"
          },
          "md5": "7F88CF7D9E3913A8AF703780288A4C65",
          "name": "CVE-2023-4762_buptsb",
          "release_date": "2023-09-27T00:00:00Z",
          "reliability": "Reviewed",
```

```
          "replication_urls": []
        }
      ],
      "intel_free": false,
      "is_predicted": false,
      "mve_id": "MVE-2023-15073",
      "observed_in_the_wild": true,
      "publish_date": "2023-10-18T16:16:14.000Z",
      "risk_rating": "MEDIUM",
      "sources": [
        {
          "date": "2023-09-07T16:03:38.000Z",
          "is_vendor_fix": true,
          "source_name": "Microsoft Corp.",
          "title": "Chromium: CVE-2023-4762 Type Confusion in V8",
          "url": "https://msrc.microsoft.com/update-guide/en-US/vulnerability/
CVE-2023-4762"
        },
        {
          "date": "2023-09-05T22:15:09.000Z",
          "is_vendor_fix": false,
          "source_name": "National Vulnerability Database",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2023-4762"
        },
        {
          "date": "2023-09-05T12:00:00.000Z",
          "is_vendor_fix": false,
          "source_description": "Red Hat Bugzilla bug",
          "source_name": "Red Hat Inc.",
          "title": "2237506 â€“ (CVE-2023-4762) CVE-2023-4762 chromium-browser:
Type Confusion in V8",
          "unique_id": "2237506",
          "url": "https://bugzilla.redhat.com/show_bug.cgi?id=2237506"
        }
      ],
      "title": "Google Chrome Prior to 116.0.5845.179 Type Confusion
Vulnerability",
      "vendor_fix_references": [
        {
          "name": "Microsoft Corp.",
          "published_date": "2023-09-07T16:03:38Z",
          "unique_id": "",
          "url": "https://msrc.microsoft.com/update-guide/en-US/vulnerability/
CVE-2023-4762"
        },
        {
          "name": "Debian Project",
          "published_date": "2023-09-07T00:00:00Z",
          "unique_id": "DSA-5491-1",
          "url": "https://www.debian.org/security/2023/dsa-5491"
```

```
        }
      ],
      "vulnerable_cpes": [
        {
          "cpe": "cpe:2.3:a:northgrid:proself:5.62:*:*:*:standard:*:*:*",
          "cpe_title": "Northgrid Proself 5.62 Standard",
          "technology_name": "Proself",
          "vendor_name": "Northgrid"
        },
        {
          "cpe": "cpe:2.3:a:northgrid:proself:5.62:*:*:*:enterprise:*:*:*",
          "cpe_title": "Northgrid Proself 5.62 EE",
          "technology_name": "Proself",
          "vendor_name": "Northgrid"
        }
      ],
      "vulnerable_products": "<p>The following vendors/products have been
reported as vulnerable:<br /><ul><li>Debian Project: Debian Linux (OS) 11.0,
12.0</li><br /><li>Fedora Project: Fedora (OS) 37, 38</li><br /><li>FreeBSD
Project: Freebsd (OS) 13.1</li><br /><li>Freebsd: Freebsd 12.4, 13.2</li><br /
><li>Google: Chrome prior to 116.0.5845.179</li><br /><li>Microsoft: Edge prior
to 116.0.1938.76</li><br /><li>Opensuse: Backports sle-15 Sp5</li><br /
><li>openSUSE: Backports SLE-15 Service Pack 4</li><br /></ul></p>",
      "was_zero_day": false,
      "workarounds": null
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Vulnerability.Value	N/A	`.publish_date`	`Google Chrome Prior to 116.0.5845.179 Type Confusion Vulnerability`	N/A
`.executive_summary`, `.analysis`, `.description`, `.common_vulnerability_scores.*`, `.vulnerable_products[]`, `.workarounds[]`, `.exploits[]`, `.sources[]`, `.vendor_fix_references[]`, `.vulnerable_cpes[]`	Vulnerability.Description	N/A	`.publish_date`	N/A	All fields are optional; Fields are concatenated into HTML when enabled.
`.cve_id`	Vulnerability.Value	N/A	`.publish_date`	CVE-2019-8921	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.risk_rating	Vulnerability.Attribute	Risk Rating	.publish_date	MEDIUM	Optional
.available_mitigation	Vulnerability.Attribute	Available Mitigation	.publish_date	Patch	Optional
.cwe	Vulnerability.Attribute	CWE	.publish_date	Improper Restriction of XML External Entity Reference	Optional
.exploitation_state	Vulnerability.Attribute	Exploitation State	.publish_date	Confirmed	Optional
.exploitation_vectors	Vulnerability.Attribute	Exploitation Vector	.publish_date	Web	Optional
.mve_id	Vulnerability.Attribute	MVE ID	.publish_date	MVE-2023-15073	Optional
.observed_in_the_wild	Vulnerability.Attribute	Observed in the Wild	.publish_date	true	Optional
.was_zero_day	Vulnerability.Attribute	Has Zero Day	.publish_date	true	Optional
.is_predicted	Vulnerability.Attribute	Is Predicted	.publish_date	false	Optional
.vulnerable_cpes[].cpe	Vulnerability.Attribute	Affected Vendor	.publish_date	northgrid	Optional
.vulnerable_cpes[].cpe	Vulnerability.Attribute	Affected Product	.publish_date	proself	Optional
.vulnerable_cpes[].cpe	Vulnerability.Attribute	Affected Platform	.publish_date	windows	Optional
.common_vulnerability_scores[{cve_version}].attack_complexity	Vulnerability.Attribute	CVSS Attack Complexity	.publish_date	LOW	Optional
.common_vulnerability_scores[{cve_version}].attack_vector	Vulnerability.Attribute	CVSS Attack Vector	.publish_date	NETWORK	Optional
.common_vulnerability_scores[{cve_version}].availability_impact	Vulnerability.Attribute	CVSS Availability Impact	.publish_date	HIGH	Optional
.common_vulnerability_scores[{cve_version}].base_score	Vulnerability.Attribute	CVSS Base Score	.publish_date	8.8	Optional
.common_vulnerability_scores[{cve_version}].	Vulnerability.Attribute	CVSS Confidentiality Impact	.publish_date	HIGH	Optional

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`confidentiality_impact`					
`.common_vulnerability_scores[{cve_version}].exploit_code_maturity`	Vulnerability.Attribute	CVSS Exploiot Code Maturity	`.publish_date`	`UNPROVEN`	Optional
`.common_vulnerability_scores[{cve_version}].integrity_impact`	Vulnerability.Attribute	CVSS Integrity Impact	`.publish_date`	`HIGH`	Optional
`.common_vulnerability_scores[{cve_version}].privileges_required`	Vulnerability.Attribute	CVSS Privileges Required	`.publish_date`	`NONE`	Optional
`.common_vulnerability_scores[{cve_version}].remediation_level`	Vulnerability.Attribute	CVSS Remediation Level	`.publish_date`	`NOT_DEFINED`	Optional
`.common_vulnerability_scores[{cve_version}].report_confidence`	Vulnerability.Attribute	CVSS Report Confidence	`.publish_date`	`CONFIRMED`	Optional
`.common_vulnerability_scores[{cve_version}].scope`	Vulnerability.Attribute	CVSS Scope	`.publish_date`	`UNCHANGED`	Optional
`.common_vulnerability_scores[{cve_version}].temporal_score`	Vulnerability.Attribute	CVSS Temporal Score	`.publish_date`	`8.8`	Optional
`.common_vulnerability_scores[{cve_version}].user_interaction`	Vulnerability.Attribute	CVSS User Interaction	`.publish_date`	`REQUIRED`	Optional
`.common_vulnerability_scores[{cve_version}].vector_string`	Vulnerability.Attribute	CVSS Vector String	`.publish_date`	`MECVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:HDIUM`	Optional

Mandiant Threat Intelligence Campaigns

The Mandiant Threat Intelligence Campaign feed ingests campaigns tracked by Mandiant. The feed also ingests any related indicators, malware, threat actors, vulnerabilities, and attack patterns,

revelant to the campaign. In addition, the campaign overview and timeline will be added to each campaign object's description.

`GET {base_url}/v4/campaign`

Sample Reponse:


```
{
  "campaigns": [
    {
      "id": "campaign--ea9e3c86-50db-55ac-869e-f60c29fd5d3b",
      "name": "APT19 Exploits CVE-2021-44228 to Deploy COLDSTEEL Backdoor at
Primarily Asian-Based Organizations",
      "profile_updated": "2024-02-01T07:05:51.712Z",
      "short_name": "CAMP.22.009"
    },
    {
      "id": "campaign--8d6e7115-c792-5ded-b0a9-81d10027a943",
      "name": "APT29 Conducts Phishing Campaign Targeting Multiple Ministries
of Foreign Affairs",
      "profile_updated": "2024-02-01T07:07:02.741Z",
      "short_name": "CAMP.22.005"
    }
  ]
}
```


For each of the campaigns, the feed will invoke the **Mandiant SecOps Intelligence - Get Entity by ID supplemental feed** to retrieve the campaign details.

`GET {base_url}/v4/campaign/{campaign_id}`

Sample Response:


```
{
  "type": "campaign",
  "id": "campaign--ea9e3c86-50db-55ac-869e-f60c29fd5d3b",
  "name": "APT19 Exploits CVE-2021-44228 to Deploy COLDSTEEL Backdoor at
Primarily Asian-Based Organizations",
  "description": "This campaign tracks APT19 activities against multiple public
and private companies in the U.S. as well as foreign subsidiaries of Japanese
corporations in early 2022.\n\nBeginning in February 2022,  Mandiant detected
suspicious network traffic going from US state government organizations to
known COLDSTEEL command-and-control (CnC) IP addresses. During the same period,
two foreign subsidiaries of Japanese corporations were also observed
communicating with the same IP addresses. COLDSTEEL, also publicly reported as
\"Derusbi\", is fully featured backdoor that can capture screenshots, enumerate
files and sessions, execute files, create a reverse shell, and simulate
keystrokes and mouse clicks. This APT19 activity marks the return of a prolific
Chinese MSS operator which was last observed in 2018.",
  "releasable": true,
  "counts": {
    "actors": 1,
    "reports": 1,
    "malware": 1,
```

```
    "campaigns": 0,
    "industries": 4,
    "timeline": 13,
    "vulnerabilities": 1,
    "actor_collaborations": 0,
    "tools": 0
  },
  "audience": [
    {
      "name": "intel_fusion",
      "license": "INTEL_RBI_FUS"
    },
    {
      "name": "intel_oper",
      "license": "INTEL_RBI_OPS"
    },
    {
      "name": "tlp_marking",
      "license": "white"
    }
  ],
  "aliases": {
    "releasable": true,
    "malware": [],
    "campaign": [],
    "actor": []
  },
  "profile_updated": "2024-02-01T07:05:51.712Z",
  "campaign_type": "Individual",
  "short_name": "CAMP.12.1234",
  "last_activity_time": "2022-08-19T00:00:00.000Z",
  "timeline": [
    {
      "name": "First Observed",
      "description": "Mandiant Observed First Activity of Campaign",
      "releasable": true,
      "event_type": "first_observed",
      "timestamp": "2021-12-08T00:00:00.000Z"
    },
    {
      "brief": "Vulnerability Disclosed",
      "name": "Event",
      "description": "Key Event",
      "releasable": true,
      "event_type": "key_event",
      "timestamp": "2021-12-08T00:00:00.000Z",
      "attributions": {
        "vulnerabilities": [
          {
            "type": "vulnerability",
```

```
          "id": "vulnerability--3f6bf43b-e5b6-5f24-ba3e-a519e941f8bf",
          "attribution_scope": "confirmed",
          "releasable": true,
          "cve_id": "CVE-2024-12345"
        }
      ],
      "releasable": true
    },
    "analyst_brief": "CVE-2024-12345 Date of Disclosure"
  },
  {
    "brief": "Vulnerability Scanning",
    "name": "Event",
    "description": "Key Event",
    "releasable": true,
    "event_type": "key_event",
    "timestamp": "2021-12-20T00:00:00.000Z",
    "attributions": {
      "mandiant_techniques": [
        {
          "type": "attack-pattern",
          "id": "attack-pattern--30af7d5b-b808-5132-abb9-58297661a14c",
          "name": "Vulnerability Scanning",
          "attribution_scope": "confirmed",
          "releasable": true,
          "mitre_techniques": [
            {
              "type": "attack-pattern",
              "id": "attack-pattern--67073dde-d720-45ae-83da-b12d5e73ca3b",
              "name": "Active Scanning",
              "attribution_scope": "confirmed",
              "releasable": true,
              "mitre_id": "T1234",
              "tactics": ["Reconnaissance"]
            }
          ]
        },
        {
          "type": "attack-pattern",
          "id": "attack-pattern--54389604-ada5-554f-b339-9e7f9dfbc130",
          "name": "Access attempt via an exploit.",
          "attribution_scope": "confirmed",
          "releasable": true,
          "mitre_techniques": [
            {
              "type": "attack-pattern",
              "id": "attack-pattern--3f886f2a-874f-4333-b794-aa6075009b1c",
              "name": "Exploit Public-Facing Application",
              "attribution_scope": "confirmed",
              "releasable": true,
```

```
              "mitre_id": "T4567",
              "tactics": ["Initial Access"]
            }
          ]
        }
      ],
      "vulnerabilities": [
        {
          "type": "vulnerability",
          "id": "vulnerability--3f6bf43b-e5b6-5f24-ba3e-a519e941f8bf",
          "attribution_scope": "confirmed",
          "releasable": true,
          "cve_id": "CVE-2023-1234"
        }
      ],
      "actors": [
        {
          "type": "threat-actor",
          "id": "threat-actor--792d3d19-4a05-5f1b-a449-bdaa351773c7",
          "name": "ACME ACTOR",
          "attribution_scope": "confirmed",
          "releasable": true
        }
      ],
      "events": [
        {
          "type": "event",
          "id": "event--80b56253-5679-50be-9ae3-fbd3feddb182",
          "name": "C:\\Log4jSherlock\\log4jsherlock 2021-12-20_09-13-39.txt",
          "attribution_scope": "confirmed",
          "releasable": true
        }
      ],
      "releasable": true
    },
    "analyst_brief": "The output of a CVE-2023-1234 (\"Log4Shell\") ..."
  }
],
"campaigns": [],
"actors": [
  {
    "type": "threat-actor",
    "id": "threat-actor--792d3d19-4a05-5f1b-a449-bdaa351773c7",
    "name": "ACME ACTOR",
    "attribution_scope": "confirmed",
    "releasable": true,
    "motivations": [
      {
        "type": "motivation",
        "id": "motivation--1b8ca82a-7cff-5622-bedd-965c11d38a9e",
```

```
        "name": "Espionage",
        "attribution_scope": "confirmed",
        "releasable": true
      }
    ],
    "source_locations": [
      {
        "releasable": true,
        "country": {
          "type": "location",
          "id": "location--740e7e5f-f2a0-55e0-98a3-88872c55b581",
          "name": "United Kingdom",
          "attribution_scope": "confirmed",
          "iso2": "UK",
          "releasable": true
        },
        "region": {
          "type": "location",
          "id": "location--8fc231f3-4e62-57e7-b734-eaee0a734612",
          "name": "Europe",
          "attribution_scope": "confirmed",
          "releasable": true
        },
        "sub_region": {
          "type": "location",
          "id": "location--7b33370b-da4b-5c48-9741-b69f69febb77",
          "name": "North Europe",
          "attribution_scope": "confirmed",
          "releasable": true
        }
      }
    ]
  }
],
"malware": [
  {
    "type": "malware",
    "id": "malware--9fed1d76-f7a1-5705-85f5-766796d0bcfc",
    "name": "Lockbit 10.0",
    "attribution_scope": "confirmed",
    "releasable": true,
    "inherently_malicious": 1
  }
],
"tools": [],
"vulnerabilities": [
  {
    "type": "vulnerability",
    "id": "vulnerability--3f6bf43b-e5b6-5f24-ba3e-a519e941f8bf",
    "attribution_scope": "confirmed",
```

```
      "cve_id": "CVE-2023-1234",
      "releasable": true
    }
  ],
  "industries": [
    {
      "type": "identity",
      "id": "identity--5b3cb2f9-14d8-5e48-bc4e-3ef3cd477ce1",
      "name": "Construction n Engineering",
      "attribution_scope": "confirmed",
      "releasable": true
    },
    {
      "type": "identity",
      "id": "identity--8d0881d8-d199-5e5a-bef9-be3ca6bb8f0d",
      "name": "Governments",
      "attribution_scope": "confirmed",
      "releasable": true
    }
  ],
  "target_locations": {
    "releasable": true,
    "countries": [
      {
        "id": "location--a33aa965-eb02-515e-8111-dab455b4a749",
        "name": "Japan",
        "attribution_scope": "confirmed",
        "releasable": true,
        "type": "location",
        "count": 2,
        "iso2": "JP",
        "sub_region": "location--7b33370b-da4b-5c48-9741-b69f69febb77",
        "region": "location--8fc231f3-4e62-57e7-b734-eaee0a734612"
      },
      {
        "id": "location--5c5b39aa-9308-52a6-9daf-0547d5aaa160",
        "name": "United States of America",
        "attribution_scope": "confirmed",
        "releasable": true,
        "type": "location",
        "count": 1,
        "iso2": "US",
        "sub_region": "location--0daadcfb-ad23-5f16-b53b-6c5b09bf20de",
        "region": "location--6d65522f-0166-5e7e-973c-35cf7973e4e3"
      }
    ],
    "regions": [
      {
        "id": "location--6d65522f-0166-5e7e-973c-35cf7973e4e3",
        "name": "Americas",
```

```
        "attribution_scope": "confirmed",
        "releasable": true,
        "type": "location",
        "count": 1
      },
      {
        "id": "location--8fc231f3-4e62-57e7-b734-eaee0a734612",
        "name": "Asia",
        "attribution_scope": "confirmed",
        "releasable": true,
        "type": "location",
        "count": 2
      }
    ],
    "sub_regions": [
      {
        "id": "location--7b33370b-da4b-5c48-9741-b69f69febb77",
        "name": "East Asia",
        "attribution_scope": "confirmed",
        "releasable": true,
        "type": "location",
        "count": 2,
        "region": "location--8fc231f3-4e62-57e7-b734-eaee0a734612"
      },
      {
        "id": "location--0daadcfb-ad23-5f16-b53b-6c5b09bf20de",
        "name": "North America",
        "attribution_scope": "confirmed",
        "releasable": true,
        "type": "location",
        "count": 1,
        "region": "location--6d65522f-0166-5e7e-973c-35cf7973e4e3"
      }
    ]
  },
  "actor_collaborations": [],
  "is_publishable": true,
  "intel_free": false
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.short_name`, `.name`	Campaign Value	N/A	`.profile_updated`	`APT29 Conducts Phishing Campaign Targeting Multiple Ministries of Foreign Affairs`	Short Name & Name are concatenated together
`.audience[]`	Attribute	Audience	`.profile_updated`	`INTEL_RBI_OPS`	Optional; When `name != tlp_marking`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.actor[].name`	Adversary Name	N/A	N/A	`APT26`	Optional
`.actors[].source_locations[].country.name`	Attribute	Country	N/A	`United States`	Optional; Applied to the relevant actor only
`.actors[].source_locations[].country.iso2`	Attribute	Country Code	N/A	`US`	Optional; Applied to the relevant actor only
`.actors[].source_locations[].region.name`	Attribute	Region	N/A	`Asia`	Optional; Applied to the relevant actor only
`.actors[].source_locations[].sub_region.name`	Attribute	Sub Region	N/A	`East Asia`	Optional; Applied to the relevant actor only
`.actors[].motivations[].name`	Attribute	Motivation	N/A	`Espionage`	Optional; Applied to the relevant actor only
`.malware[].name`	Malware Value	N/A	N/A	`COLDSTEEL`	Optional
`.tools[].name`	Tool Value	N/A	N/A	`Cobalt Strike`	Optional
`.industries[].name`	Attribute	Target Sector	N/A	`Governments`	Optional
`.vulnerabilities[].cve_id`	Vulnerability Value, Indicator Value	CVE	N/A	`CVE-2024-12345`	Optional; Ingested object is based on user-field selection
`.target_locations.countries[].name`	Attribute	Target Country	`.profile_updated`	`Japan`	Optional
`.target_locations.countries[].iso2`	Attribute	Target Country Code	`.profile_updated`	`JP`	Optional
`.target_locations.regions[].name`	Attribute	Target Region	`.profile_updated`	`Asia`	Optional
`.target_locations.regions[].sub_region.name`	Attribute	Target Sub Region	`.profile_updated`	`East Asia`	Optional
`.timeline[].attributions.files[].associated_hashes[].value`	Indicator	MD5, SHA-1	N/A	N/A	Optional; When `.timeline[].name` == `Malicious Executable`
`.timeline[].attributions.emails[].from.value`	Indicator	Email Address	N/A	`john.doe@gmail.com`	Optional; When `.timeline[].name` == `Phishing Email`
`.timeline[].attributions.emails[].subject`	Indicator	Email Subject	N/A	N/A	Optional; When `.timeline[].name` == `Phishing Email`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Indicator.Attribute	Threat Type	N/A	Phishing	N/A

Additional Calls - Fetch Related Indicators

The feed makes an additional API call (if enabled) to fetch related indicators, using the Mandiant SecOps Intelligence - Get Entity Relationships supplemental feed.

```
GET {base_url}/v4/campaign/{campaign_id}/indicators
```

Sample data and mapping can be found in the Mandiant Threat Intelligence Threat Actor Indicators (Supplemental) feed section.

Additional API Calls - Fetch Related Attack Patterns

The feed makes an additional API call (if enabled) to fetch related attack patterns.

```
GET {base_url}/v4/campaign/{campaign_id}/attack-pattern
```

Sample data and mapping can be found in the Mandiant Threat Intelligence Entity Attack Pattern Details (Supplemental) feed mapping section.

Mandiant Threat Intelligence Malware

The Mandiant Threat Intelligence Malware feed ingests malware tracked by Mandiant. The feed also ingests any related indicators, threat actors, vulnerabilities, and attack patterns, relevant to the malware.

```
GET {base_url}/v4/malware
```

Sample Response:


```
{
  "malware": [
    {
      "last_updated": "2022-12-05T16:05:33.521Z",
      "aliases": [
        {
          "name": "008s"
        },
        {
          "name": "Ddkong (Palo Alto Networks)"
        }
      ],
      "name": "008S",
      "description": "The 008S malware family is modular. Upon initial
infection, 008S will call out to the configured CnC to determine what plugins
should be downloaded and loaded into the malicious process. The additional
plugins extend functionality of the malware.",
      "id": "malware--81f821d1-4ec9-534d-8dc7-53da47e5074a",
```

```
      "inherently_malicious": 1,
      "intel_free": false,
      "has_yara": true
    },
    {
      "last_updated": "2022-12-05T16:25:47.924Z",
      "aliases": [],
      "name": "1487SHELL",
      "description": "1487 Shell is a webshell. It is capable of using
authentication, file upload and download, file modification, file system
enumeration, and command line command execution.",
      "id": "malware--bf69c98d-74a5-5a37-92c6-1fb5a4bc8cb9",
      "inherently_malicious": 1,
      "intel_free": false,
      "has_yara": false
    }
  ]
}
```


For each of the campaigns, the feed will invoke the `Mandiant SecOps Intelligence - Get Entity by ID` supplemental feed to retrieve the campaign details.

`GET {base_url}/v4/campaign/{campaign_id}`

Sample Response:


```
{
  "actors": [
    {
      "id": "threat-actor--14e31117-b933-5349-9d9b-0a3b395380e9",
      "name": "FIN12",
      "country_name": "unknown",
      "iso2": "unknown",
      "last_updated": "2024-03-21T06:08:36Z"
    },
    {
      "id": "threat-actor--aee7efe3-a260-574c-8ee0-e5b100077197",
      "name": "TEMP.Zagros",
      "country_name": "Iran",
      "iso2": "IR",
      "last_updated": "2024-03-21T03:55:12Z"
    }
  ],
  "aliases": [
    {
      "name": "LockBit 3.0 (DuskRise Inc.)"
    },
    {
      "name": "Lockbit 3.0 (Infinitum IT)"
    },
    {
      "name": "Lockbitblack (Sophos)"
```

```
    }
  ],
  "audience": [
    {
      "name": "intel_fusion",
      "license": "INTEL_RBI_FUS"
    },
    {
      "name": "intel_oper",
      "license": "INTEL_RBI_OPS"
    },
    {
      "name": "tlp_marking",
      "license": "amber"
    }
  ],
  "capabilities": [
    {
      "name": "Anti-VM capabilities",
      "description": "Capabilities associated with detecting or evading virtual
machine or \"sandbox\" programs. \"Parent\" aspect used to contain specific
sub-aspects."
    },
    {
      "name": "Anti-VM: VMware",
      "description": "Capable of detecting or evading VMWare virtual machines."
    }
  ],
  "cve": [],
  "description": "LOCKBIT is a ransomware written in C that encrypts files
stored locally and on network shares. LOCKBIT can also identify additional
systems on a network and propagate via SMB. Prior to encrypting files, LOCKBIT
clears event logs, deletes volume shadow copies, and terminates processes and
services that may impact its ability to encrypt files. LOCKBIT has been
observed using the file extension \".lockbit\" for encrypted files.",
  "detections": [
    "(http_inspect) unknown Content-Encoding used (Cisco Firepower)",
    "ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood
of being hostile (ET OPEN)",
    "ET INFO Executable Download from dotted-quad Host (ET OPEN)"
  ],
  "id": "malware--4e596360-8a5c-5c36-ae0d-20ffb5f2ffb5",
  "industries": [
    {
      "id": "identity--cc593632-0c42-500c-8d0b-d38e97b90f1d",
      "name": "Aerospace n Defense"
    },
    {
      "id": "identity--41930e54-396f-508e-8f65-418dd09f935d",
      "name": "Automotive"
```

```
    }
  ],
  "inherently_malicious": 1,
  "last_activity_time": "2024-03-11T18:07:33.000Z",
  "last_updated": "2024-03-11T16:10:46.435Z",
  "malware": [
    {
      "id": "malware--cc1d563a-cf32-55e8-bae3-cbdf8266c794",
      "name": "AMADEY"
    },
    {
      "id": "malware--e6810cc5-2759-52cc-bf57-9b2ffc381760",
      "name": "ASYNCRAT"
    }
  ],
  "name": "LOCKBIT",
  "operating_systems": ["Windows"],
  "roles": ["Ransomware"],
  "type": "malware",
  "yara": [
    {
      "id": "signature--4ac9a4c2-0ba9-532b-8f2a-fd2b381f8ab2",
      "name": "FE_Ransomware_Win32_LOCKBIT_1"
    }
  ],
  "is_publishable": true,
  "intel_free": false,
  "counts": {
    "reports": 244,
    "capabilities": 96,
    "malware": 7,
    "actors": 12,
    "detections": 42,
    "cve": 0,
    "aliases": 3,
    "industries": 15,
    "attack_patterns": 68
  }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.name`	Malware Value	N/A	`.last_updated`	`LOCKBIT`	Short Name & Name are concatenated together
`.description`	Malware Description	N/A	`.last_updated`	`LOCKBIT is a ransomware written in C...`	N/A
`.aliases[].name`	Attribute	`Alias`	`.last_updated`	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.capabilities[].name`	Attribute	`Capability`	`.last_updated`	N/A	N/A
`.industries[].name`	Attribute	`Target Sector`	`.last_updated`	N/A	N/A
`.last_activity_time`	Attribute	`Last Active`	`.last_updated`	N/A	Updatable
`.operating_systems[]`	Attribute	`Target Operating System`	`.last_updated`	N/A	N/A
`.roles[]`	Attribute	`Role`	`.last_updated`	N/A	N/A
`.type`	Attribute	`Type`	`.last_updated`	N/A	N/A
`.inherently_malicious`	Attribute	`Inherently Malicious`	`.last_updated`	N/A	Converted from integer to boolean
`.actors[].name`	Adversary Name	`APT28`	`.last_updated`	N/A	N/A
`.cve[]`	Indicator Value, Vulnerability Value	CVE	`.last_updated`	N/A	Ingested as an Indicator or Vulnerability based on user-field selection

Additional Calls - Fetch Related Indicators

The feed makes an additional API call (if enabled) to fetch related indicators, using the Mandiant SecOps Intelligence - Get Entity Relationships supplemental feed.

`GET {base_url}/v4/campaign/{campaign_id}/indicators`

Sample data and mapping can be found in the Mandiant Threat Intelligence Threat Actor Indicators (Supplemental) feed section.

Additional API Calls - Fetch Related Attack Patterns

The feed makes an additional API call (if enabled) to fetch related attack patterns.

`GET {base_url}/v4/campaign/{campaign_id}/attack-pattern`

Sample data and mapping can be found in the Mandiant Threat Intelligence Entity Attack Pattern Details (Supplemental) feed mapping section.

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.

Mandiant Threat Intelligence

METRIC	RESULT
Run Time	23 minutes
Adversaries	253
Adversary Attributes	7,520
Attack Patterns	263
Indicators	2,257
Indicator Attributes	2,390
Malware	630
Malware Attributes	8,340
Vulnerabilities	46

Mandiant Threat Intelligence Indicators

METRIC	RESULT
Run Time	48 minutes
Adversaries	41
Indicators	159,178
Indicator Attributes	142,805

Mandiant Threat Vulnerability Intelligence

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	363
Vulnerability Attributes	6,194
Indicators	207
Indicator Attributes	4,731

Known Issues / Limitations

- Mandiant's API requires that query ranges have a maximum of 90 days. In the case that the data range selected for manual run is greater than 90 days, the end date of the interval will be updated to be 90 days after the start date.
- Users will have to reconfigure and reenable their feeds when upgrading the integration to version 1.5.0 or later from a previous version (<1.5.0).
- Mandiant Threat Intelligence Malware feed - disabling the `Only Ingest Recently Updated Entities` will result is extremely long feed run times and could possible trigger a 500 internal server error from Mandiant.

Change Log

- **Version 1.5.0**
  - Added the following new feeds:
    - Mandiant Threat Intelligence Campaigns
    - Mandiant Threat Intelligence Malware
  - The **Mandiant Threat Intelligence** (actors) feed no longer will fetch attack patterns related to *related malware* as this fetch will be handled by the dedicated **Mandiant Threat Intelligence Malware** feed.
  - Added a new configuration parameter, **Ingest CVEs As**, to the Mandiant Vulnerability Intelligence feed.
  - Performed the following updates regarding Mandiant Score Mapping:
    - Mandiant Score now normalizes to an attribute called `Disposition`. It was previously called `Mandiant Confidence.` Users should adjust their scoring policy to account for this change.
    - Score thresholds are now inclusive (previously exclusive).
    - Added the ability to map to a Disposition of `Suspicious.`
    - Modified the default score thresholds based on Mandiant's recommendations:
      - 0-39: Unknown
      - 40-59: Indeterminate
      - 60-79: Suspicious
      - 80-100: Malicious
    - Indicators are no longer marked as `Benign` if their score does not reach the Indeterminate threshold. Instead, they will be marked as `Unknown`, per Mandiant's recommendations
  - Added TLP mapping Support.
  - Added the ability to have associated hashes (to indicators) inherit attributes from the top-level indicator
  - Added `Category` attribute for indicators based on the reporting sources.
  - Added the ability to ingest MISP flags into the description of each indicator (Indicators feed only).
  - Removed the redundant `Audience Name` attribute from the `Mandiant Threat Intelligence` feed and renamed the `Audience License` attribute to `Audience.`
  - Resolved a pagination issue where the supplemental feed may error out when relationships exceed 10k.
  - Renamed the `Operating System` attribute for Malware to `Target Operation System`
  - The default selection for how CVEs will be ingested is now set to `Vulnerabilities.`
  - The default MScore threshold is now 40 to prevent ingestion of unrated indicators.
  - Added the ability to enable/disable SSL Verification.
  - Added the ability to enable/disable Proxies.
  - Added two new known issues / limitation entries:
    - Users upgrading from an integration version <1.5.0 will have to reconfigure and reenable their feeds upon upgrade to 1.5.0 or later.

        - Disabling the **Only Ingest Recently Updated Entities** configuration parameter for the Mandiant Threat Intelligence Malware feed will result in extremely long run times and may trigger a 500 internal server error from Mandiant.
    - Updated the minimum ThreatQ version to 5.12.1.
- **Version 1.4.0**
    - Updated the minimum ThreatQ version to 5.6.0.
    - The **Mandiant Threat Intelligence Vulnerabilities** feed has been renamed to the **Mandiant Vulnerability Intelligence** feed.
        - The feed can now parse and return more context and details regarding vulnerabilities.
        - Added the following parameters:
            - **Range Type Filter** - select the rating types for vulnerabilities to ingest.
            - **Risk Rating Filter** - select the risk ratings for vulnerabilities to ingest.
            - **Exploitation State Filter** - select the exploitation states for vulnerabilities to ingest.
            - **Exploitation Vector Filter** - select the exploitation vectors for vulnerabilities to ingest.
            - **Vulnerability Must Have a Zero Day** - filter out vulnerabilities that do not have zero days exploits.
            - **Vulnerability Must be Observed in the Wild** - filter out vulnerabilities that have not been observed in the wild.
            - **Vulnerability Must be CISA Known Exploited** - filter out vulnerabilities that are not CISA known exploited.
            - **Vulnerability Must Have Exploits** - filter out vulnerabilities that have no associated exploits.
            - **Vulnerability Attribute Context** - select the context for vulnerabilities to ingest.
            - **Description Context** - select the pieces of context to include in the vulnerability's description.
            - **CVSS Attribute Context** - select the CVSS context for vulnerabilities to ingest.
        - Removed the **Save CVE Data As** parameter from the feed.
    - Added the following parameters to the Intelligence and Indicator Intelligence feeds:
        - **Inherit Attributes from Indicators to Associated Hashes** - adds the ability to inherit attribution from top-level indicators to the associated hashes.
        - **Add MISP Flags to Indicator Descriptions** - adds the ability to ingest the MISP flags into the description of each indicator.
    - Added the **Parsing Entities** parameter field to the Mandiant Threat Intelligence feed.
    - Resolved an issue where the Confidence mapping was not an inclusive threshold.
- **Version 1.3.4**
    - Added a new configuration parameter, **Parsed Entries**, that allows you to select the IOC types to automatically parse from the content.
    - Added ingestion rules for certain attributes.
    - Updated the **Save CVE Data** default setting. The Vulnerabilities option will now be selected by default.
- **Version 1.3.3**
    - Added new configuration option: **Base URL**, that allows you set the Mandiant Base URL for the feeds.

  - New Known Issue / Limitation chapter entry added to the user guide regarding data ranges.
- **Version 1.3.2**
  - Resolved an issue where feed requests would fail with a 400 Bad Request message when the epoch value was empty.
- **Version 1.3.1**
  - Added the following new configuration options for the **Mandiant Threat Intelligence** and **Mandiant Threat Intelligence Indicators** feeds:
    - Mandiant Score Confidence Indeterminate Threshold
    - Mandiant Score Confidence Malicious Threshold
  - Added additional attribute, **Mandiant Classification**, that is derived from the Mandiant Score.
- **Version 1.3.0**
  - Added two new feeds: **Mandiant Threat Intelligence Indicators** and **Mandiant Threat Intelligence Vulnerabilities**.
- **Version 1.2.1**
  - Updated integration authentication method to use **API ID** and **Secret Key** opposed to Username and Password.
- **Version 1.2.0**
  - Added the ability to:
    - Include uncategorized groups as tags.
    - Filter data by recently updated entities.
    - Fetch related attack patterns to the threat actors.
    - Fetch related indicators to the threat actors.
    - Fetch related attack patterns to the related malware.
  - Fixed an issue where the feed attempted to ingest related malware as Indicators
- **Version 1.1.1**
  - Fixed an issue where the integration would attempt to ingest related malware as indicators.
  - Added the following configuration parameters:
    - **Only Ingest Recently Updated Threat Actors -** Adds ability to filter data by recently updated entities.
    - **Add Uncategorized Groups as Tags -** Adds ability to include uncategorized groups as tags.
    - **Fetch Attack Patterns Related to Threat Actors -** Adds ability to fetch related attack patterns to the threat actors.
    - **Fetch Indicators Related to Threat Actors -** Adds ability to fetch related indicators to the threat actors.
    - **Fetch Indicators Related to Malware -** Adds ability to fetch related attack patterns to the related malware.
- **Version 1.1.0**
  - Added X-App-Name as a header.
  - Performed internal refactoring.
- **Version 1.0.0**
  - Initial release