ThreatQuotient

Mandiant Threat Intelligence CDF User Guide

Version 1.3.4

January 23, 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	1.3.4
Compatible with ThreatQ Versions	>= 4.45.0
Support Tier	ThreatQ Supported

Introduction

Mandiant, formerly known as FireEye, provides solutions that protect and defend organizations against cyber security attacks, globally leveraging innovative technology and expertise from the front lines to deliver a broad portfolio of world-class consulting, innovative software-as-a-service (SaaS) solutions and managed security services.

The Mandiant Threat Intelligence CDF provides the following endpoints:

- **Mandiant Threat Intelligence** - ingests compromised Adversaries and any related Indicators, Malware, Vulnerabilities, Attack Patterns, and Tags.
- **Mandiant Threat Intelligence Indicators** - ingests a list of indicators tracked by Mandiant.
- **Mandiant Threat Intelligence Vulnerabilities** - ingests a list of vulnerabilities tracked by Mandiant.
- **Mandiant Threat Intelligence Malware Details (Supplemental)** - called once per each `.malware[].id` returned by the Mandiant Threat Intelligence Actor Details feed.
- **Mandiant Threat Intelligence Entity Attack Pattern Details (Supplemental)** - used to fetch related attack patterns to both threat actors and malware.
- **Mandiant Threat Intelligence Actor Details (Supplemental)** - called once per each `.threat-actors[].id` returned by the Mandiant Threat Intelligence feed.
- **Mandiant Threat Actor Indicators (Supplemental)** - used to fetch related attack patterns to both threat actors and malware.

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

- Adversaries
  - Adversary Attributes
- Attack Patterns
- Indicators
  - Indicator Attributes
- Malware
  - Malware Attributes
- Vulnerabilities
- Tags

Installation

Perform the following steps to install the integration:

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

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

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

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

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

Configuration

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

To configure the integration:

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

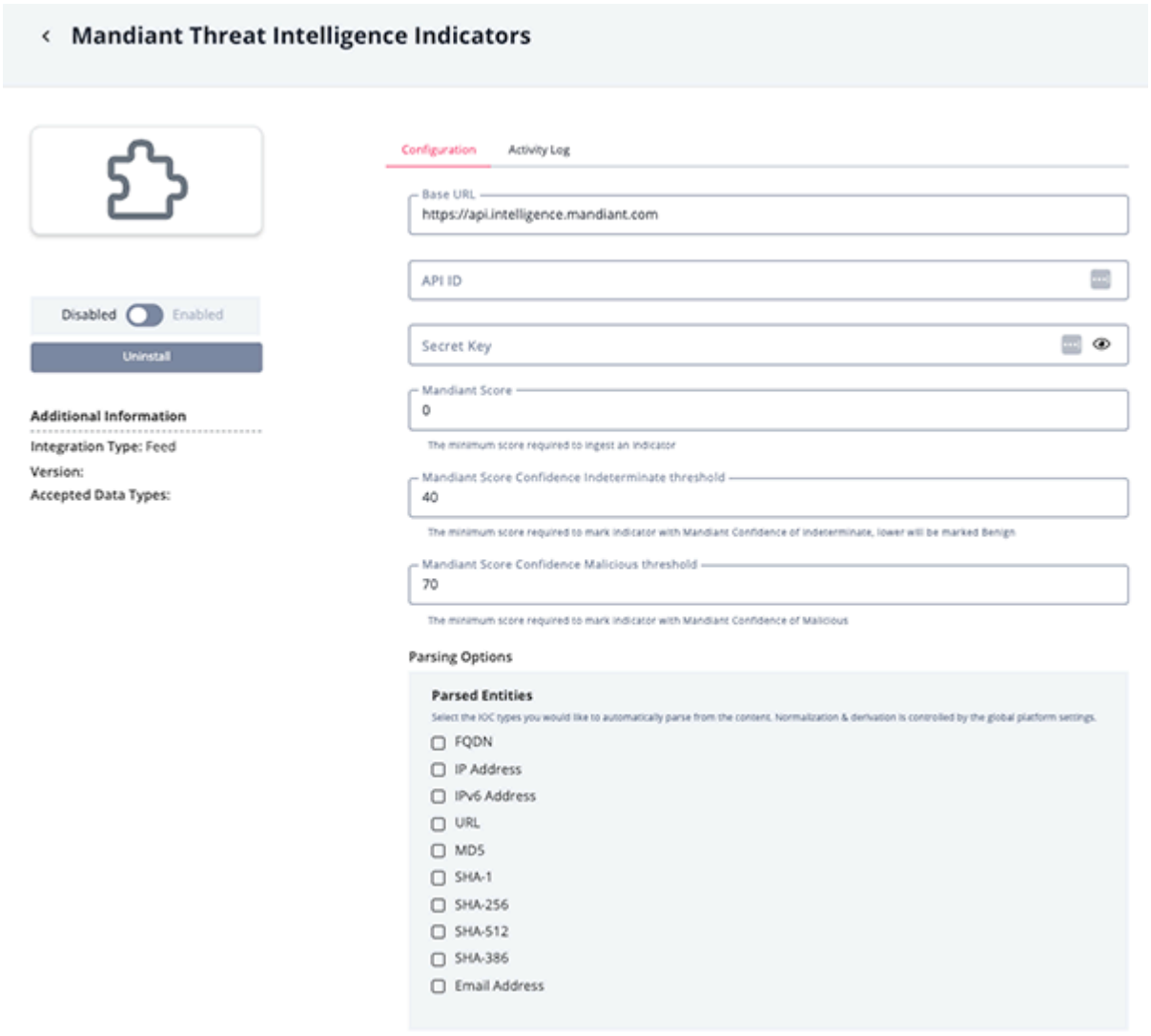
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

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

PARAMETER	DESCRIPTION
Base URL	Your Mandiant base URL.
API ID	Enter your Mandiant API ID.
Secret Key	Enter your Mandiant Secret Key.
Save CVE Data as *(Mandiant Threat Intelligence Feed only)*	Select the object type(s) to ingest CVEs as into the platform. Options include ◦ Indicators ◦ Vulnerabilities (default)
Only Ingest Recently Updated Threat Actors *(Mandiant Threat Intelligence Feed only)*	Enabling this option will filter out Threat Actors that have not been updated since the last time the feed ran. This option is not selected by default.
Add Uncategorized Groups as Tags *(Mandiant Threat Intelligence Feed only)*	Mandiant reports on Uncategorized (UNC) Actor Groups. Enabling this will add these as tags for the top-level Threat Actor. This option is selected by default.

Fetch Attack Patterns Related to Threat Actors *(Mandiant Threat Intelligence Feed only)*	Enable this option to use additional API calls to fetch related Attack Patterns for the given Threat Actor. This option is selected by default.
Fetch Indicators Related to Threat Actors *(Mandiant Threat Intelligence Feed only)*	Enable this option to use additional API calls to fetch related indicators for the given Threat Actor. This option is not selected by default.
Fetch Indicators Related to Malware *(Mandiant Threat Intelligence Feed only)*	Enable this option to use additional API calls to fetch related indicators for the given related Malware. This option is not selected by default.
Mandiant Score *(Mandiant Intelligence and and Indicator feeds only)*	The minimum score required to ingest an indicator. The default value is 0.
Mandiant Score Confidence Indeterminate Threshold *(Mandiant Intelligence and Indicator feeds only)*	The minimum score required to mark indicator with Mandiant Confidence of **Indeterminate**. Indicators with lower scores will be marked **Benign**.
Mandiant Score Confidence Malicious Threshold *(Mandiant Intelligence and Indicator feeds only)*	The minimum score required to mark indicator with Mandiant Confidence of **Malicious**.
Parsed Entries *(Mandiant Intelligence and Indicator feeds only)*	Select the IOC types to automatically parse from the content. Options include: ◦ FQDN ◦ SHA-1

- IP Address
- IPv6 Address
- URL
- MD5
- SHA-256
- SHA-512
- SHA-386
- Email Address



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 and 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	
.aliases[].name	Adversary.Tag	N/A	N/A	Comment Crew (Internet)	
.description	Adversary.Description	N/A	N/A	APT1 refers to a	
.motivations[].name + .motivations[].attribution_scope	Adversary.Attribute	Motivation	.last_updated	Espionage - confirmed	
.industries[].name + .industries[].attribution_scope	Adversary.Attribute	Industry	.last_updated	Aerospace & Defense - confirmed	
.locations.source[].region.name	Adversary.Attribute	Region	.last_updated	Asia	
.locations.source[].sub_region.name	Adversary.Attribute	Sub Region	.last_updated	East Asia	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.locations.source[].country.name	Adversary.Attribute	Country	.last_updated	China	
.locations.source[].country.iso2	Adversary.Attribute	Country Code	.last_updated	cn	
.locations.target[].name	Adversary.Attribute	Target Country	.last_updated	Belgium	
.locations.target[].iso2	Adversary.Attribute	Target Country Code	.last_updated	be	
.audience[].name	Adversary.Attribute	Audience Name	.last_updated	intel_fusion	
.audience[].license	Adversary.Attribute	Audience License	.last_updated	INTEL_RBI_FUS	
.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	
.malware[].id	N/A	N/A	N/A	malware--09673ebc-9fbf-5ab0-9130-7874c84cd3e4	Will be used 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'	
.description	Related Malware.Description	N/A	.last_updated	'AGEDMOAT is an HTTP-based'	

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

Mandiant Threat Intelligence Entity Attack Pattern Details (Supplemental)

When enabled, the Mandiant Threat Intelligence Entity Attack Pattern Details supplemental feed will be used to fetch related attack patterns to both threat actors and malware.

`GET {base_url}/v4/malware/{malware.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 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 mapping table below
.indicators[].mscore	Indicator.Attribute	Mandiant Score	.first_seen	94	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 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
.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 above

Mandiant Threat Intelligence Vulnerabilities

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

```
GET {base_url}/v4/vulnerability
```

Sample Response:


```
{
    "total_count": 219,
    "next":
"FGluY2x1ZGVfY29udGV4dF91dWlkDnF1ZXJ5VGhlbkZldGNoBRZ5NzZIQ3hES1J5YTcxdzFuV0QyT2
p3AAAAAAH7Z
jQWTVFPRUpvOGdUV0tQZ1FPMzFKUWduQRZUeVRhODMyU1J5R2lBVHdfalM4cWpBAAAAAAIMcE4WZkZI
NDZIUktSc2U
2ZzlJdmZ5cmVXZxZZeXVoRFZwWVFXeUxxU0lxUXNSQUxBAAAAAAIFRBoWWWZGOTJLTGlRMjJhWXlZRz
h4U3ZsdxY4M
U01M3ZYbVFPNldmZ3phRXhEMnh3AAAAAAHyNxkWWkVBb3BKLUFRSmUxbjhHUFp2Sm44URYyLTI1ZXd4
ZVJZMlF2eFZ
zcTdyc193AAAAAAI2cTgWSWlBalNDc2hRYWFiN3VlZWhWNWdPZw==",
    "vulnerability": [
        {
            "common_vulnerability_scores": {
                "v3.1": {
                    "attack_complexity": "LOW",
                    "base_score": 6.5,
                    "vector_string": "redacted",
                    "integrity_impact": "NONE",
                    "report_confidence": "redacted",
                    "attack_vector": "ADJACENT_NETWORK",
                    "privileges_required": "NONE",
                    "availability_impact": "NONE",
                    "temporal_score": 5.7,
                    "exploit_code_maturity": "redacted",
                    "user_interaction": "NONE",
                    "scope": "UNCHANGED",
                    "confidentiality_impact": "HIGH",
                    "remediation_level": "redacted"
                },
                "v2.0": {
                    "availability_impact": "NONE",
                    "temporal_score": 2.4,
                    "base_score": 3.3,
                    "vector_string": "redacted",
                    "integrity_impact": "NONE",
                    "report_confidence": "redacted",
                    "confidentiality_impact": "PARTIAL",
                    "access_vector": "ADJACENT_NETWORK",
                    "remediation_level": "redacted",
```

```
                    "exploitability": "redacted",
                    "access_complexity": "LOW",
                    "authentication": "NONE"
                }
            },
            "exploitation_state": "redacted",
            "sources": [
                {
                    "date": "2021-11-29T12:00:00.000Z",
                    "unique_id": "2027458",
                    "source_name": "Red Hat Inc.",
                    "url": "https://bugzilla.redhat.com/show_bug.cgi?
id=2027458",
                    "source_description": "2027458"
                },
                {
                    "date": "2021-11-30T12:00:00.000Z",
                    "unique_id": "1193237",
                    "source_name": "SUSE Inc.",
                    "url": "https://bugzilla.suse.com/show_bug.cgi?id=1193237",
                    "source_description": "1193237"
                },
                {
                    "date": "2021-11-29T12:00:00.000Z",
                    "unique_id": "CVE-2019-8921",
                    "source_name": "National Vulnerability Database",
                    "url": "https://nvd.nist.gov/vuln/detail/CVE-2019-8921",
                    "source_description": "CVE-2019-8921"
                },
                {
                    "url": "https://ssd-disclosure.com/ssd-advisory-linux-
bluez-information-leak-and-heap-overflow/",
                    "source_name": "NVD Reference #1",
                    "source_description": "This url was provided by NVD."
                },
                {
                    "url": "https://security.netapp.com/advisory/
ntap-20211203-0002/",
                    "source_name": "NVD Reference #2",
                    "source_description": "This url was provided by NVD."
                },
                {
                    "date": "2022-10-21T17:00:00.000Z",
                    "unique_id": "SUSE-SU-2022:3687-1",
                    "source_name": "SUSE Inc.",
                    "url": "https://www.suse.com/support/update/announcement/
2022/suse-su-20223687-1/",
                    "source_description": "SUSE-SU-2022:3687-1"
                },
                {
```

```
                    "date": "2022-10-21T17:00:00.000Z",
                    "unique_id": "SUSE-SU-2022:3691-1",
                    "source_name": "SUSE Inc.",
                    "url": "https://www.suse.com/support/update/announcement/
2022/suse-su-20223691-1/",
                    "source_description": "SUSE-SU-2022:3691-1"
                },
                {
                    "date": "2022-10-25T17:00:00.000Z",
                    "unique_id": "SUSE-SU-2022:3718-1",
                    "source_name": "SUSE Inc.",
                    "url": "https://www.suse.com/support/update/announcement/
2022/suse-su-20223718-1/",
                    "source_description": "SUSE-SU-2022:3718-1"
                },
                {
                    "url": "https://lists.debian.org/debian-lts-announce/
2022/10/msg00026.html",
                    "source_name": "NVD Reference #3",
                    "source_description": "This url was provided by NVD."
                }
            ],
            "risk_rating": "redacted",
            "cve_id": "CVE-2019-8921",
            "observed_in_the_wild": "redacted",
            "description": "<p>The National Vulnerability Database (NVD) has
provided the following description:<br /><em>An issue was discovered in
bluetoothd in BlueZ through 5.48. The vulnerability lies in the handling of a
SVC_ATTR_REQ by the SDP implementation. By crafting a malicious CSTATE, it is
possible to trick the server into returning more bytes than the buffer actually
holds, resulting in leaking arbitrary heap data. The root cause can be found in
the function service_attr_req of sdpd-request.c. The server does not check
whether the CSTATE data is the same in consecutive requests, and instead simply
trusts that it is the same.</em></p>",
            "id": "vulnerability--04d29534-4d5c-53e6-9592-8bafc3765cda",
            "vulnerable_cpes": "redacted",
            "publish_date": "2022-10-25T22:51:00.000Z",
            "was_zero_day": "redacted",
            "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
.vulnerability[].value	Indicator.Value	CVE	.vulnerability[].publish_date	CVE-2019-8921	N/A

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 Intelligence Vulnerabilities

METRIC	RESULT
Run Time	19 minutes
Vulnerabilities	95,145

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.

Change Log

- **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