ThreatQuotient

Mandiant Threat Intelligence CDF Guide

Version 1.0.0

November 01, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.45.0`

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 for ThreatQuotient ingests the following object types:

- Adversaries
- Indicators
    - CVEs
- Malware
- Vulnerabilities

See the ThreatQ Mapping chapter for more information.

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Username	Your Mandiant username.
Password	Your Mandiant password.
Save CVE Data as	Select the object type(s) to ingest CVEs as into the platform.

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

`GET https://api.intelligence.fireeye.com/v4/actor`

This feed ingests compromised Adversaries objects and any related Indicators, Malware, and Vulnerabilities.


```
{
    "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
          }
    ]
}
```


Endpoint use only to fetch all the `.threat-actors[].id` that would further on be used in the Mandiant Actor Details supplemental feed.

Mandiant Actor Details (Supplemental)

`GET https://api.intelligence.fireeye.com/v4/actor/{id}`

Supplemental feed called once per each `.threat-actors[].id` returned by the Mandiant Threat Intelligence feed.


```
{
    "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
}
```


ThreatQ 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	
.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	
.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 Malware Details (Supplemental)

`GET https://api.intelligence.fireeye.com/v4/malware/{malware.id}`

Supplemental feed called once per each `.malware[].id` returned by the Mandiant Threat Intelligence Actor Details feed.


```
{
    "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
}
```


ThreatQ 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	'AGEDMOAT'	
.description	Malware.Description	N/A	.last_updated	'AGEDMOAT is an HTTP-based'	
.audience[].license	Malware.Attribute	Audience License	.last_updated	'INTEL_RBI_FUS'	
.audience[].name	Malware.Attribute	Audience Name	.last_updated	'intel_fusion'	
.operating_systems[]	Malware.Attribute	Operating System	.last_updated	'Windows'	
.industries[].name	Malware.Attribute	Industry	.last_updated	'Aerospace & Defense'	
.detections[]	Malware.Attribute	Detection	.last_updated	'FE_Autopatt_Win_AGEDMOAT'	
.malware[].name	Related Malware.Value	N/A	.last_updated	'AIRBREAK'	

Average Feed Run

METRIC	RESULT
Run Time	2 minutes
Adversaries	10
Adversary Attributes	599
Indicators	33
Malware	308
Malware Attributes	5,686
Vulnerabilities	33

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.

Change Log

- **Version 1.0.0**
  - Initial release