ThreatQuotient

Mandiant Threat Intelligence CDF Guide

Version 1.1.1

February 22, 2022

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.

Copyright © 2022 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: 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: `1.1.1`
- 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 provides the following endpoints:

- **Mandiant Threat Intelligence** - ingests compromised Adversaries objects and any related Indicators, Malware, and Vulnerabilities.
- **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 Patterns (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

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:

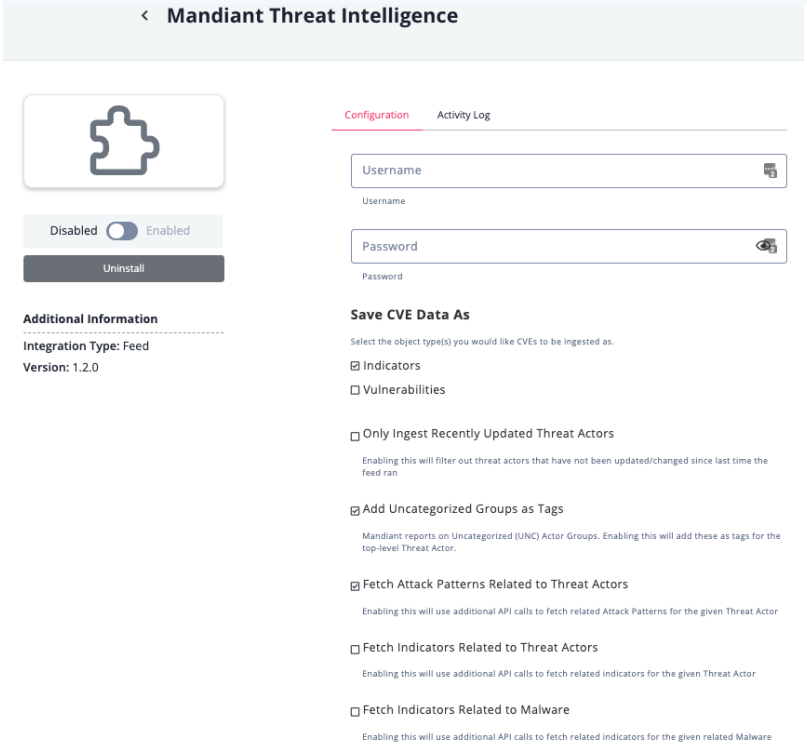
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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	Enter your Mandiant username.
Password	Enter your Mandiant password.
Save CVE Data as	Select the object type(s) to ingest CVEs as into the platform. Options include ◦ Indicators (default) ◦ Vulnerabilities
Only Ingest Recently Updated Threat Actors	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.

PARAMETER	DESCRIPTION
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. This option is selected by default.
Fetch Attack Patterns Related to Threat Actors	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	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	Enable this option to use additional API calls to fetch related indicators for the given related Malware. This option is not selected by default.



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 objects and any related Indicators, Malware, and Vulnerabilities.

`GET https://api.intelligence.fireeye.com/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
          }
    ]
}
```

Endpoint use only to fetch all the `.threat-actors[].id` that would further on 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 https://api.intelligence.fireeye.com/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
}
```

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	
.associated_uncs[].name	Adversary.Tag	N/A	N/A	UNC235	
.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 https://api.intelligence.fireeye.com/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
}
```


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'	

Mandiant Threat Intelligence Entity Attack Patterns (Supplemental)

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

```
GET https://api.intelligence.fireeye.com/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
        },
        "attack-pattern--03d7999c-1f4c-42cc-8373-e7690d318104": {
            "attack_pattern_identifier": "T1033",
            "created": "2017-05-31T21:30:35.733Z",
            "description": "Adversaries may attempt to identify the primary user, currently logged in user, set of
users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by
retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The
information may be collected in a number of different ways using other Discovery techniques, because user and
username details are prevalent throughout a system and include running process ownership, file/directory ownership,
session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://
attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not
the adversary fully infects the target and/or attempts specific actions.\n\nUtilities and commands that acquire this
information include <code>whoami</code>. In Mac and Linux, the currently logged in user can be identified with
<code>w</code> and <code>who</code>.",
            "id": "attack-pattern--03d7999c-1f4c-42cc-8373-e7690d318104",
            "modified": "2020-03-15T01:03:47.866Z",
```

```
            "name": "System Owner/User Discovery",
            "x_mitre_is_subtechnique": false
        },
        "attack-pattern--0458aab9-ad42-4eac-9e22-706a95bafee2": {
            "attack_pattern_identifier": "T1583",
            "created": "2020-09-30T16:37:40.271Z",
            "description": "Before compromising a victim, adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase.\n\nUse of these infrastructure solutions allows an adversary to stage, launch, and execute an operation. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contact to third-party web services. Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.",
            "id": "attack-pattern--0458aab9-ad42-4eac-9e22-706a95bafee2",
            "modified": "2020-10-22T17:59:17.606Z",
            "name": "Acquire Infrastructure",
            "x_mitre_is_subtechnique": false
        },
        "attack-pattern--09a60ea3-a8d1-4ae5-976e-5783248b72a4": {
            "attack_pattern_identifier": "T1056.001",
            "created": "2020-02-11T18:58:11.791Z",
            "description": "Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. \n\nKeylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes. (Citation: Adventures of a Keystroke) Some methods include:\n\n* Hooking API callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data.\n* Reading raw keystroke data from the hardware buffer.\n* Windows Registry modifications.\n* Custom drivers.\n* [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks) ",
            "id": "attack-pattern--09a60ea3-a8d1-4ae5-976e-5783248b72a4",
            "modified": "2020-10-21T01:30:56.227Z",
            "name": "Keylogging",
            "x_mitre_is_subtechnique": true
        },
        "attack-pattern--0a3ead4e-6d47-4ccb-854c-a6a4f9d96b22": {
            "attack_pattern_identifier": "T1003",
            "created": "2017-05-31T21:30:19.735Z",
            "description": "Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information.\n\nSeveral of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.\n",
            "id": "attack-pattern--0a3ead4e-6d47-4ccb-854c-a6a4f9d96b22",
            "modified": "2020-06-09T20:46:00.758Z",
            "name": "OS Credential Dumping",
            "x_mitre_is_subtechnique": false
        },
        "attack-pattern--1035cdf2-3e5f-446f-a7a7-e8f6d7925967": {
            "attack_pattern_identifier": "T1123",
            "created": "2017-05-31T21:31:34.528Z",
            "description": "An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.\n\nMalware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.",
            "id": "attack-pattern--1035cdf2-3e5f-446f-a7a7-e8f6d7925967",
            "modified": "2020-07-14T19:42:10.235Z",
```

```
            "name": "Audio Capture",
            "x_mitre_is_subtechnique": false
        },
        "attack-pattern--106c0cf6-bf73-4601-9aa8-0945c2715ec5": {
            "attack_pattern_identifier": "T1543",
            "created": "2020-01-10T16:03:18.865Z",
            "description": "Adversaries may create or modify system-level processes to repeatedly execute malicious
payloads as part of persistence. When operating systems boot up, they can start processes that perform background
system functions. On Windows and Linux, these system processes are referred to as services. (Citation: TechNet
Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and
[Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user
specific parameters.(Citation: AppleDocs Launch Agent Daemons) \n\nAdversaries may install new services, daemons, or
agents that can be configured to execute at startup or a repeatable interval in order to establish persistence.
Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect.  \n\nServices,
daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges.
Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.
(Citation: OSX Malware Detection).  ",
            "id": "attack-pattern--106c0cf6-bf73-4601-9aa8-0945c2715ec5",
            "modified": "2020-10-09T13:46:29.922Z",
            "name": "Create or Modify System Process",
            "x_mitre_is_subtechnique": false
        },
        "attack-pattern--10d51417-ee35-4589-b1ff-b6df1c334e8d": {
            "attack_pattern_identifier": "T1133",
            "created": "2017-05-31T21:31:44.421Z",
            "description": "Adversaries may leverage external-facing remote services to initially access and/or
persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to
internal enterprise network resources from external locations. There are often remote service gateways that manage
connections and credential authentication for these services. Services such as [Windows Remote Management](https://
attack.mitre.org/techniques/T1021/006) can also be used externally.\n\nAccess to [Valid Accounts](https://
attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through
credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation:
Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access
mechanism during an operation.",
            "id": "attack-pattern--10d51417-ee35-4589-b1ff-b6df1c334e8d",
            "modified": "2020-06-19T20:07:09.600Z",
            "name": "External Remote Services",
            "x_mitre_is_subtechnique": false
        },
        "attack-pattern--1608f3e1-598a-42f4-a01a-2e252e81728f": {
            "attack_pattern_identifier": "T1114",
            "created": "2017-05-31T21:31:25.454Z",
            "description": "Adversaries may target user email to collect sensitive information. Emails may contain
sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries
can collect or forward email from mail servers or clients. ",
            "id": "attack-pattern--1608f3e1-598a-42f4-a01a-2e252e81728f",
            "modified": "2020-03-24T18:31:06.417Z",
            "name": "Email Collection",
            "x_mitre_is_subtechnique": 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
.attack-patterns[id] [attack_pattern_identifier|name]	AttackPattern.Value	N/A	N/A	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 attack patterns to both threat actors and malware

```
GET https://api.intelligence.fireeye.com/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"
                }
            ],
            "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"
    },
    {
        "attributed_associations": [
            {
                "id": "threat-actor--0ac5c1db-8ad6-54b8-b4b9-c32fc738c54a",
                "name": "APT1",
                "type": "threat-actor"
            }
        ],
        "first_seen": "2011-09-12T12:23:13.000Z",
        "id": "fqdn--b31f40c6-dda2-5526-b844-c54716a73620",
        "is_exclusive": true,
        "is_publishable": true,
        "last_seen": "2011-09-12T12:23:13.000Z",
        "last_updated": "2022-01-22T19:59:44.920Z",
        "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": true,
            "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": 88,
            "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": "sunnysaf.allowed.org"
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value`	Indicator.Value	Mapped: `.type`	.first_seen	N/A	
`.mscore`	Indicator.Attribute	Mandiant Score	N/A	N/A	
`.attributed_associations[].name`	Indicator.Adversary	N/A	N/A	N/A	Skipped if `type` != `threat-actor`

Average Feed Run

METRIC	RESULT
Run Time	26 minutes
Adversaries	566
Adversary Attributes	7,731
Attack Patterns	317
Indicators	9,541
Indicator Attributes	5,584
Malware	2,069
Malware Attributes	30,208

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 1.1.1**
  - 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