

ThreatQuotient



Mandiant Intelligence Reports CDF Guide

Version 1.1.0

March 13, 2023

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

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.

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 © 2023 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.

Contents

- Integration Details..... 5
- Introduction 6
- Installation..... 7
- Configuration 8
- ThreatQ Mapping 10
 - Mandiant Intelligence Reports 10
 - Mandiant Report Download (Supplemental) 11
- Average Feed Run..... 16
 - Mandiant Intelligence Reports 16
- Known Issues / Limitations 17
- Change Log..... 18

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 4.34.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https:// marketplace.threatq.com/ details/mandiant- intelligence-reports-cdf

Introduction

The Mandiant Intelligence Reports integration allows a user to ingest threat intelligence reports from Mandiant's API.

The integration provides the following feeds:

- **Mandiant Intelligence Reports** - returns a list of finished intelligence reports created by Mandiant.
- **Mandiant Report Download** (Supplemental) - returns details of a Mandiant report.

The integration ingests the following system object types:

- Adversaries
 - Adversary Attributes
- Indicators
 - Indicator Attributes
- Malware
 - Malware Attributes
- Reports
 - Report Attributes



This integration, Mandiant Intelligence Reports CDF, replaces the FireEye Intelligence Reports CDF.

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
API ID	Your Mandiant API ID used for authentication.
API Key	Your Mandiant API key used for authentication.

Disabled ☐ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version: 1.0.0

Configuration

Activity Log

API ID

API Key

Set indicator status to...
Active

Run Frequency
Every 24 Hours

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.
We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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 Intelligence Reports

Retrieves a list of reports from Mandiant. Additionally, the `objects[].report_id` is used as a parameter in the Mandiant Report Download supplemental feed call.

GET `https://api.intelligence.mandiant.com/v4/reports`

Sample Response:

```
{
  "next":
  "DnF1ZXJ5VGhlbkZldGNoAwAAAAAfysFdFkxkSkRHeU1DUXJDRVlyYXN4UW5wSmcAAAAAGnyQvBZSZ21oU1RuVRueXJ2bXptWHh3eXFRAAAAAB0MHPUWUU9NTTVqYWpTeENGWnF0VTd0Q0Vhdw==",
  "objects": [
    {
      "audience": [
        "Media Highlights"
      ],
      "id": "report--82f90aa8-2f51-5aa6-83aa-ffd31b93f9cf",
      "intelligence_type": "tmh",
      "publish_date": "2022-06-30T19:24:27.562Z",
      "report_id": "22-00015388",
      "report_link": "https://advantage.mandiant.com/reports/22-00015388",
      "report_type": "News Analysis",
      "title": "FCC Commissioner Urges Google, Apple to Drop TikTok App",
      "version": "1",
      "version_one_publish_date": "2022-06-30T19:24:27.562Z"
    }
  ],
  "total_count": 3054
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.objects[].report_link</code>	report.attribute	Report Link	<code>.publish_date</code>	<code>https://advantage.mandiant.com/reports/22-00015388</code>	N/A

Mandiant Report Download (Supplemental)

The supplemental feed uses the `objects[].report_id` retrieved from the Mandiant Intelligence Reports as the `reportId` parameter in order to fetch the detailed report.

GET `https://api.intelligence.mandiant.com/v4/report/{reportId}`

Sample Response:

```
{
  "audience": [
    "cyber espionage"
  ],
  "cvss_base_score": "0",
  "cvss_temporal_score": "0",
  "executive_summary": "<ul style='margin-bottom: 0in; font-family: 'open sans', sans-serif; font-size: 12pt;'>\n<li><span style='font-size: 12.0pt;'>Mandiant assesses with high confidence that APT42 is an Iranian state-sponsored cyber espionage group tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian Government. We further estimate with moderate confidence that APT42 operates on behalf of the Islamic Revolutionary Guard Corps (IRGC) based on targeting patterns that align with the IRGC's operational mandates and priorities.</span></li>\n<li><span style='font-size: 12.0pt;'>Active since at least 2015, APT42 is characterized by highly targeted spear-phishing and surveillance operations against individuals and organizations of strategic interest to Iran. The group's operations, which are designed to build trust and rapport with their victims, have included accessing the personal and corporate email accounts of government officials, former Iranian policymakers or political figures, members of the Iranian diaspora and opposition groups, journalists, and academics who are involved in research on Iran. The group has also deployed mobile malware capable of tracking victim locations, recording phone conversations, accessing videos and images, and extracting entire SMS inboxes.</span></li>\n<li><span style='font-size: 12.0pt;'>APT42 has a demonstrated ability to alter its operational focus as Iran's priorities evolve over time. We anticipate that APT42 will continue to conduct cyber espionage operations in support of Iran's strategic priorities in the long term based on their extensive operational history and imperviousness to public reporting and infrastructure takedowns.</span></li>\n</ul>",
  "files": [
    {
      "actor": "APT42",
      "identifier": "Attacker",
      "malwareFamily": "MAGICDROP",
      "md5": "9d0e761f3803889dc83c180901dc7b22",
      "name": "flashplayer.exe",
      "sha1": "ecf9b7283fda023fa37ad7fdb15be4eadded4e06",
      "sha256": "d4375a22c0f3fb36ab788c0a9d6e0479bd19f48349f6e192b10d83047a74c9d7",
      "size": "2871296",
      "type": "application/x-dosexec"
    }
  ],
  "id": "report--d5a62569-3935-572a-882e-25d40c63e4c1",
  "in_the_wild": false,
  "previous_versions": [
    {
      "publish_date": "2022-08-01T16:33:59.053Z",
      "report_id": "22-00018039",
      "version_number": 1
    }
  ]
}
```

```
}
],
"publish_date": "2022-08-01T16:33:59.053Z",
"relations": {},
"report_confidence": "ND",
"report_id": "22-00018039",
"report_type": "Actor Profile",
"requester_org_id": "FireEye",
"tags": {
  "actors": [
    {
      "aliases": [
        "APT 42"
      ],
      "id": "threat-actor--f7fdbf0c-4b5b-5b95-b005-702afffe4a72",
      "name": "APT42"
    }
  ],
  "affected_industries": [
    "Civil Society & Non-profits"
  ],
  "affected_systems": [
    "Users/Application and Software"
  ],
  "intended_effects": [
    "Political Advantage"
  ],
  "malware_families": [
    {
      "aliases": [
        "TABBYCAT"
      ],
      "id": "malware--a27fdd81-afcc-563d-add9-2ebf1138aaeb",
      "name": "TABBYCAT"
    }
  ],
  "motivations": [
    "Military/Security/Diplomatic"
  ],
  "source_geographies": [
    "Iran"
  ],
  "target_geographies": [
    "Australia"
  ],
  "targeted_information": [
    "Government Information"
  ],
  "ttps": [
    "Social Engineering"
  ]
},
"threat_detail": "threat detail",
"threat_scape": [
  "Cyber Espionage"
],
"title": "APT42: Crooked Charms, Cons, and Compromises",
"version": 1,
"version_one_publish_date": "2022-08-01T16:33:59.053Z",
```

```
"zero_day": 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
.title	report.value	N/A	.publish_date	APT42: Crooked Charms, Cons, and Compromises	N/A
.report_type + .publish_date + .executive_summary + .threat_detail	report.description	N/A	N/A	Report Type: Actor Profile Published At: 2022-08-01T16:33:59.053Z Executive Summary Mandiant (IR. ...[Truncated - see full report] will be appended to the description.	N/A
.executive_summary	report.attribute	Executive Summary	.publish_date	Mandiant assesses with high confidence that APT42 is an Iranian state-sponsored cyber espionage group tasked with conducting information collection and	N/A
.executive_summary	attack_pattern.value	N/A	N/A	T1055.001 - Dynamic-link Library Injection	N/A
.audience	report.attribute	Audience	.publish_date	cyber espionage	N/A
.version	report.attribute	Version	.publish_date	1	N/A
.report_type	report.attribute	Report Type	.publish_date	Actor Profile	N/A
.report_id	report.attribute	Report ID	.publish_date	22-00018039	N/A
.previous_versions[].version_number	report.attribute	Previous Version Number	.publish_date	1	If multiple previous_version objects exist, only the most recent previous_version object is reported.
.previous_versions[].publish_date	report.attribute	Previous Version Date	.publish_date	2022-10-13 15:04:24-00:00	If multiple previous_version objects exist, only the most recent previous_version object is reported.
.tags.affected_industries[]	report.attribute / adversary.attribute / malware.attribute	Affected Industry	.publish_date	Civil Society & Non-profits	N/A
.tags.affected_systems[]	report.attribute / adversary.attribute / malware.attribute	Affected System	.publish_date	Users/Application and Software	N/A
.tags.motivations[]	report.attribute / adversary.attribute / malware.attribute	Motivation	.publish_date	Military/Security/Diplomatic	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.tags.source_geographies[]	report.attribute / adversary.attribute / malware.attribute	Source Geography	.publish_date	Iran	N/A
.tags.target_geographies[]	report.attribute / adversary.attribute / malware.attribute	Target Geography	.publish_date	Australia	N/A
.tags.targeted_informations[]	report.attribute / adversary.attribute / malware.attribute	Targeted Information	.publish_date	Government Information	N/A
.tags.ttps[]	report.attribute / adversary.attribute / malware.attribute	TTP	.publish_date	Social Engineering	N/A
.tags.actors[].name	adversary.name	N/A	.publish_date	APT42	Adversary objects are related to the primary Report object.
.tags.actors[].id	adversary.attribute	ID	.publish_date	threat-actor--f7fdbf0c-4b5b-5b95-b005-702afffe4a72	N/A
.tags.malware_families[].name	malware.value	N/A	.publish_date	TABBYCAT	Malware objects are related to the primary Report object and all other Adversary, Malware, and Indicator objects parsed from the Report object.
.tags.malware_families[].id	malware.attribute	ID	.publish_date	malware--a27fdd81-afcc-563d-add9-2ebf1138aaeb	N/A
.tags.malware_families[].aliases[]	malware.attribute	Alias	.publish_date	TABBYCAT	N/A
.files[].name	indicator.value	N/A	.publish_date	flashplayer.exe	Indicator type is Filename. Indicator objects are related to the primary Report object.
.files[].sha1	indicator.value	N/A	.publish_date	ecf9b7283fda023fa37ad7fdb15be4eadded4e06	Indicator type is SHA-1. Indicator objects are related to the primary Report object.
.files[].sha256	indicator.value	N/A	.publish_date	d4375a22c0f3fb36ab788c0a9d6e0479bd19f48349f6e192b10d83047a74c9d7	Indicator type is SHA-256. Indicator objects are related to the

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					primary Report object
.files[].md5	indicator.value	N/A	.publish_date	9d0e761f3803889dc83c180901dc7b22	Indicator type is MD5. Indicator objects are related to the primary Report object
.files[].size	indicator.attribute	File Size	.publish_date	2871296	N/A
.files[].identifier	indicator.attribute	Identifier	.publish_date	Attacker	N/A
.files[].type	indicator.attribute	File Type	.publish_date	application/x-dosexec	N/A
.files[].malwareFamily	indicator.attribute	Malware Family	.publish_date	MAGICDROP	N/A
.files[].actor	indicator.attribute	Actor	.publish_date	APT42	N/A
.threat_scape	indicator.attribute	Threat Scape	.publish_date	Cyber Espionage	N/A
.cvss_base_score	report.attribute / adversary.attribute / malware.attribute	CVSS Base Score	.publish_date	0	N/A
.cvss_temporal_score	report.attribute / adversary.attribute / malware.attribute	CVSS Temporal Score	.publish_date	0	N/A
.report_confidence	report.attribute / adversary.attribute / malware.attribute	Report Confidence	.publish_date	ND	N/A
.in_the_wild	report.attribute / adversary.attribute / malware.attribute	Exploitation: In the Wild	.publish_date	false	N/A
.zero_day	report.attribute / adversary.attribute / malware.attribute	Exploitation: Zero Day	.publish_date	false	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 Intelligence Reports

METRIC	RESULT
Run Time	5 minutes
Reports	480
Report Attributes	6,950
Adversaries	53
Adversary Attributes	1,860
Indicators	1,355
Indicator Attributes	6,348
Malware	149
Malware Attributes	5,945

Known Issues / Limitations

- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns extracted from a report's Executive Summary to be related to the report. MITRE ATT&CK attack patterns are ingested from the following feeds:
 - MITRE Enterprise ATT&CK
 - MITRE Mobile ATT&CK
 - MITRE PRE-ATT&CK

Change Log

- **Version 1.1.0**
 - Decreased the number of API Attack Patterns retrieved, per request, to prevent timeout errors.
- **Version 1.0.1**
 - Fixed an issue with the category field that prevented users from installing the integration on ThreatQ version 4 instances.
- **Version 1.0.0**
 - Initial release