ThreatQuotient

BitDefender Advanced Threat Intelligence CDF Guide

Version 1.0.0

July 23, 2021

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

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.

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.20.0`

Introduction

BitDefender Advanced Threat Intelligence gives users direct access to actionable, near-real-time insights into the latest active threats.

With over 1,600 employees and a team of 800+ engineers and researchers, BitDefender is one of the most innovative IT security software vendors in the world today. BitDefender Labs correlate hundreds of thousands of Indicators of Compromise (IoCs) collected through hundreds of millions of endpoints deployed globally to deliver first-hand threat intelligence.

Subscribe to gain access to permanently updated IoCs, coming either from opportunistic threats such as Malicious domains, IPs, URLs, phishing-domains, file-hashes and C&C IPs or from APTs (Advanced Persistent Threats) such as domains, IPs and file hashes.

The threats’ IoCs and related information is permanently verified and extended to strengthen your security posture. Depending on your use case, it can either prevent infiltration by updating automated tools rules or ensure you understand more when under attack and know what to expect next.

> The BitDefender Advanced Threat Intelligence CDF is a partner-submitted integration.

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
API Key	The API key to be used when authenticating to BitDefender Threat Intelligence service.

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

BitDefender CNC IPs Feed

The data is returned in a CSV format, where each column represents the following:

COLUMN	DETAILS
ip	The indicator.
threat_name	The threat name associated to the indicator (e.g. trojan).
threat_family	The threat family associated with the indicator. This defaults to *cnc.*
updated_at	Timestamp indicating when the indicator was last updated.

Example of CSV data can be observed below

```
ip,threat_name,threat_family,updated_at
182.33.88.21,Android.Trojan.Banker.NN,cnc,1571318161468
69.64.3.121,Android.Trojan.Banker.NN,cnc,1571318161468
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator	IP Address	4 (fourth token)	182.33.88.21	
1 (second token)	Malware	N/A	4 (fourth token)	Android.Trojan.Banker.NN	The value "phishing-unknown" is dropped and not created as a Malware object
1 (second token)	Attribute	Threat Name	4 (fourth token)	Android.Trojan.Banker.NN	Values mapped as Malware objects are not included as attributes. The value "malware" is also dropped and not created as an Attribute
3 (third token)	Attribute	Threat Family	4 (fourth token)	cnc	
4 (fourth token)	N/A	N/A	N/A	1571318161468	

BitDefender Phishing Domain Feed

The data is returned in a CSV format, where each column represents the following:

COLUMN	DETAILS
domain	The indicator.
threat_name	The threat name associated to the indicator (e.g. trojan).
threat_family	The threat family associated with the indicator. This defaults to *cnc.*
updated_at	Timestamp indicating when the indicator was last updated.

Example of CSV data can be observed below

```
ip,threat_name,threat_family,updated_at
001saf.eu,trojan,malware,1571318161468
001ddf.eu,trojan,phishing,1571318161468
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator	FQDN	4 (fourth token)	001saf.eu	
1 (second token)	Malware	N/A	4 (fourth token)	trojan	The value "phishing-unknown" is dropped and not created as a Malware object
1 (second token)	Attribute	Threat Name	4 (fourth token)	trojan	Values mapped as Malware objects are not included as attributes. The value "malware" is also dropped and not created as an Attribute
3 (third token)	Attribute	Threat Family	4 (fourth token)	phishing	
4 (fourth token)	N/A	N/A	N/A	1571318161468	

BitDefender URL Reputations Feed

The data is returned in a CSV format, where each column represents the following:

COLUMN	DETAILS
rank	The reputational rank of the indicator.
url	The indicator value.
threat_types	Comma-separated list of threat types.

Example of CSV data can be observed below

```
5,"http://fifa2018start.info/panel/tasks.php","malware"
5,"http://4dexports.com","malware,phishing"
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Attribute	Rank	N/A	5	
1 (second token)	Indicator	URL	N/A	`http://4dexports.com`	N/A
3 (third token)	Attribute	Threat Type	N/A	phishing	

BitDefender Domain Reputations Feed

The data is returned in a CSV format, where each column represents the following:

COLUMN	DETAILS
rank	The reputational rank of the indicator.
domain	The indicator value.
threat_types	Comma-separated list of threat types.

Example of CSV data can be observed below

```
5,"5zgmu7o20kt5d8yq.com","malware"
5,"adult.contents.fc2.com,"spam,untrusted"
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Attribute	Rank	N/A	5	
1 (second token)	Indicator	FQDN	N/A	`5zgmu7o20kt5d8yq.com`	N/A
3 (third token)	Attribute	Threat Type	N/A	phishing	

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.

BitDefender CNC IPs Feed

METRIC	RESULT
Run Time	2 minutes
Indicators	491
Indicator Attributes	490
Malware	215

BitDefender Phishing Domain Feed

METRIC	RESULT
Run Time	32 minutes
Indicators	93989
Indicator Attributes	93989
Malware	117

BitDefender URL Reputations Feed

METRIC	RESULT
Run Time	72 minutes
Indicators	112,858
Indicator Attributes	485,820

BitDefender Domain Reputations Feed

METRIC	RESULT
Run Time	30 minutes
Indicators	99,998
Indicator Attributes	195,094

Change Log

- **Version 1.0.0**
    - Initial Release