ThreatQuotient

Bambenek Feeds CDF

Version 2.1.4

October 01, 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	2.1.4
Compatible with ThreatQ Versions	>= 5.25.0
Support Tier	ThreatQ Supported

Introduction

Bambenek Consulting is a cybersecurity investigation and intelligence consulting firm focusing on tackling major criminal threats. ThreatQ integrates with all the feeds provided by Bambenek Consulting:

- Bambenek Consulting - C2 IP
- Bambenek Consulting - C2 Domain
- Bambenek Consulting - C2 All Indicators
- Bambenek Consulting - DGA Domain
- Bambenek Consulting - High-Confidence C2 IP
- Bambenek Consulting - High-Confidence C2 Domain
- Bambenek Consulting - High-Confidence C2 All Indicators
- Bambenek Consulting - High-Confidence DGA Domain
- Bambenek Consulting - Bamital Master
- Bambenek Consulting - Banjori Master
- Bambenek Consulting - Bebloh/URLZone Master
- Bambenek Consulting - Bedep Master
- Bambenek Consulting - Beebone Master
- Bambenek Consulting - Chinad Master
- Bambenek Consulting - Corebot Master
- Bambenek Consulting - Cryptolocker Master
- Bambenek Consulting - Dircrypt Master
- Bambenek Consulting - Dromedan Master
- Bambenek Consulting - Dyre Master
- Bambenek Consulting - Fobber Master
- Bambenek Consulting - G01 Master
- Bambenek Consulting - Geodo Master
- Bambenek Consulting - Gozi Master
- Bambenek Consulting - Hesperbot Master
- Bambenek Consulting - Kraken Master
- Bambenek Consulting - Locky Master
- Bambenek Consulting - Madmax Master
- Bambenek Consulting - Matsnu Master
- Bambenek Consulting - Mirai Master
- Bambenek Consulting - Murofet Master
- Bambenek Consulting - Necurs Master
- Bambenek Consulting - Nymaim Master
- Bambenek Consulting - P2P GOZ Master
- Bambenek Consulting - Pandabanker Master
- Bambenek Consulting - PT GOZ / New GOZ Master
- Bambenek Consulting - Padcrypt Master
- Bambenek Consulting - Pizd Master
- Bambenek Consulting - Proslikefan Master
- Bambenek Consulting - Pushdo Master
- Bambenek Consulting - Pykspa Master
- Bambenek Consulting - Qadars Master
- Bambenek Consulting - Qakbot Master
- Bambenek Consulting - Ramdo Master
- Bambenek Consulting - Ramnit Master
- Bambenek Consulting - Ranbyus Master
- Bambenek Consulting - Shifu Master
- Bambenek Consulting - Simda Master
- Bambenek Consulting - Sisron Master
- Bambenek Consulting - Sphinx Master
- Bambenek Consulting - Suppobox Master
- Bambenek Consulting - Symmi Master
- Bambenek Consulting - Tempedreve Master
- Bambenek Consulting - Tinba / TinyBanker Master
- Bambenek Consulting - Tinynuke Master
- Bambenek Consulting - Tofsee Master
- Bambenek Consulting - Unknowndropper Master
- Bambenek Consulting - Unknownjs Master
- Bambenek Consulting - Vawtrak Master
- Bambenek Consulting - Vidro Master
- Bambenek Consulting - Virut Master
- Bambenek Consulting - Volatile Cedar / Explosive Master

The integration ingests indicators and indicator attributes object types.

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. Select the individual feeds to install, when prompted, and click **Install**. The feed(s) 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
Username	Your Bambenek Consulting Username.
Password	Your Bambenek Consulting Password.
URL	The Bambenek Consulting URL. This is for UI display purposes only.

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

Master or All Indicators

This mapping is for feeds containing 'Master' or 'All Indicators' in their name mapping. The response is in text format with comma separated values.

Sample Response:

```
aakamen.com,78.24.9.52,ns2.vshosting.cz|ns.aakamen.com|
poski.vshosting.cz,78.24.9.52|89.235.0.2,Master Indicator Feed for banjori non-
sinkholed domains,https://osint.bambenekconsulting.com/manual/banjori.txt
aaskmen.com,103.224.212.222,ns15.above.com|ns16.above.com,103.224.212.5|
103.224.212.6,Master Indicator Feed for banjori non-sinkholed domains,https://
osint.bambenekconsulting.com/manual/banjori.txt
aifamen.com,157.52.223.233,juming.dnsdun.com|juming.dnsdun.net|v1.dnsdun.com|
v1.dnsdun.net,47.96.179.127|104.152.45.130|104.152.45.131|116.1.237.4|
122.228.80.247|172.247.255.190,Master Indicator Feed for banjori non-sinkholed
domains,https://osint.bambenekconsulting.com/manual/banjori.txt
```

ThreatQuotient provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
1 (first token)	indicator.value	FQDN	aakamen.com
2 (second token)	indicator.value	IP Address	78.24.9.52
3 (third token)	indicator.value	FQDN	[vshosting.cz, ns.aakamen.com, poski.vshosting.cz]
4 (forth token)	indicator.value	IP Address	[78.24.9.52, 89.235.0.2]
5 (fifth token)	indicator.description	N/A	Master Indicator Feed for banjori non-sinkholed domains
6 (sixth token)	indicator.attribute	Source	https://osint.bambenekconsulting.com/manual/banjori.txt

IP

This mapping is for feeds containing 'IP' in their name mapping. The response will be in text format with comma separated values.

Sample Response:

```
5.79.79.209,IP used by banjori C&C,2019-11-20 19:03,https://
osint.bambenekconsulting.com/manual/banjori.txt
14.192.4.35,IP used by banjori C&C,2019-11-20 19:03,https://
osint.bambenekconsulting.com/manual/banjori.txt
18.213.250.117,IP used by banjori C&C,2019-11-20 19:03,https://
osint.bambenekconsulting.com/manual/banjori.txt
```

ThreatQuotient provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
1 (first token)	indicator.value	IP Address	5.79.79.209
2 (second token)	indicator.description	N/A	IP used by banjori C&C
3 (third token)	indicator.published_at	Published At	2019-11-20 19:03
4 (forth token)	indicator.attribute	Source	https://osint.bambenekconsulting.com/manual/banjori.txt

Domains

This mapping is for feeds containing 'Domain' in their name mapping. The response will be in text format with comma separated values.

Sample Response:

```
jaxwolcxabjzcexx0p.com,Domain used by bedep,2019-11-20 19:08,https://
osint.bambenekconsulting.com/manual/bedep.txt
llyamcjgytzaw5n.com,Domain used by bedep,2019-11-20 19:08,https://
osint.bambenekconsulting.com/manual/bedep.txt
yjkcbwknkzqdnirl.com,Domain used by bedep,2019-11-20 19:08,https://
osint.bambenekconsulting.com/manual/bedep.txt
```

ThreatQuotient provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
1 (first token)	indicator.value	FQDN	jaxwolcxabjzcexx0p.com
2 (second token)	indicator.description	N/A	Domain used by bedep
3 (third token)	indicator.published_at	Published At	2019-11-20 19:08
4 (forth token)	indicator.attribute	Source	https://osint.bambenekconsulting.com/manual/bedep.txt

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.

Master or All Indicators

Feeds containing 'Master' or 'All Indicators' in their Name.

METRIC	RESULT
Run Time	1 minute
Indicators	727
Indicator Attributes	727

IP

Feeds containing 'IP' in their Name.

METRIC	RESULT
Run Time	1 minute
Indicators	47
Indicator Attributes	55

Domain

Feeds containing 'Domain' in their Name.

METRIC	RESULT
Run Time	1minute
Indicators	154
Indicator Attributes	154

Change Log

- **Version 2.1.4**
  - The description attribute has been removed. The threat data that previously populated this attribute will be ingested as an IoC description.
  - Updated minimum ThreatQ version to 5.25.0.
- **Version 2.1.3**
  - Removed the use of the inter-related flag.
- **Version 2.1.2**
  - Updated URLs to use https protocol.
- **Version 2.1.1**
  - Changed Category from **OSINT** to **Commercial.**
- **Version 2.1.0**
  - Updated Nameserver from Attribute to Indicator.
- **Version 2.0.0**
  - Initial release