ThreatQuotient

A Securonix Company

MalBeacon CDF

Version 1.0.0

October 20, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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 © 2025 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: tq-support@securonix.com
Support Web: https://ts.securonix.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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The MalBeacon CDF integration enables organizations to leverage deception-based threat intelligence to enhance their security posture. By ingesting IPs, hostnames, emails, and hashes associated with malicious activity, the feed provides actionable insights into real-world attacker behavior. MalBeacon uses decoy systems to lure and observe attackers, allowing security teams to analyze their tactics, techniques, and procedures (TTPs) and proactively strengthen defenses.

The integration provides the following feeds:

- **MalBeacon Actor Beacons** - ingests IPs and hostnames associated with threat actors and their command-and-control (C2) beacons.
- **MalBeacon Malware C2** - ingests IPs and hostnames gathered from IPv4 scans identifying malware C2 infrastructure.
- **MalBeacon Email Beacons** - ingests emails, IPs, and hostnames from attacker-controlled email accounts.
- **MalBeacon Document Beacons** - ingests IPs and hostnames extracted from malware sandbox–based document beacons.

The integration ingests the following object types:

- Indicators
  - Indicator Attributes
- Malware

Prerequisites

The following is required to install and operate the integration:

- MalBeacon API Key from your MalBeacon Portal: https://portal.malbeacon.com/profile.

Installation

Perform the following steps to install the integration:

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration YAML file.
3. Navigate to the integrations management page in your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration YAML file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the file
6. Select the individual feeds to install when prompted, then click **Install**.

> 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.

The feed(s) will be added to the integrations page. You will still need to configure and enable the feeds.

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).

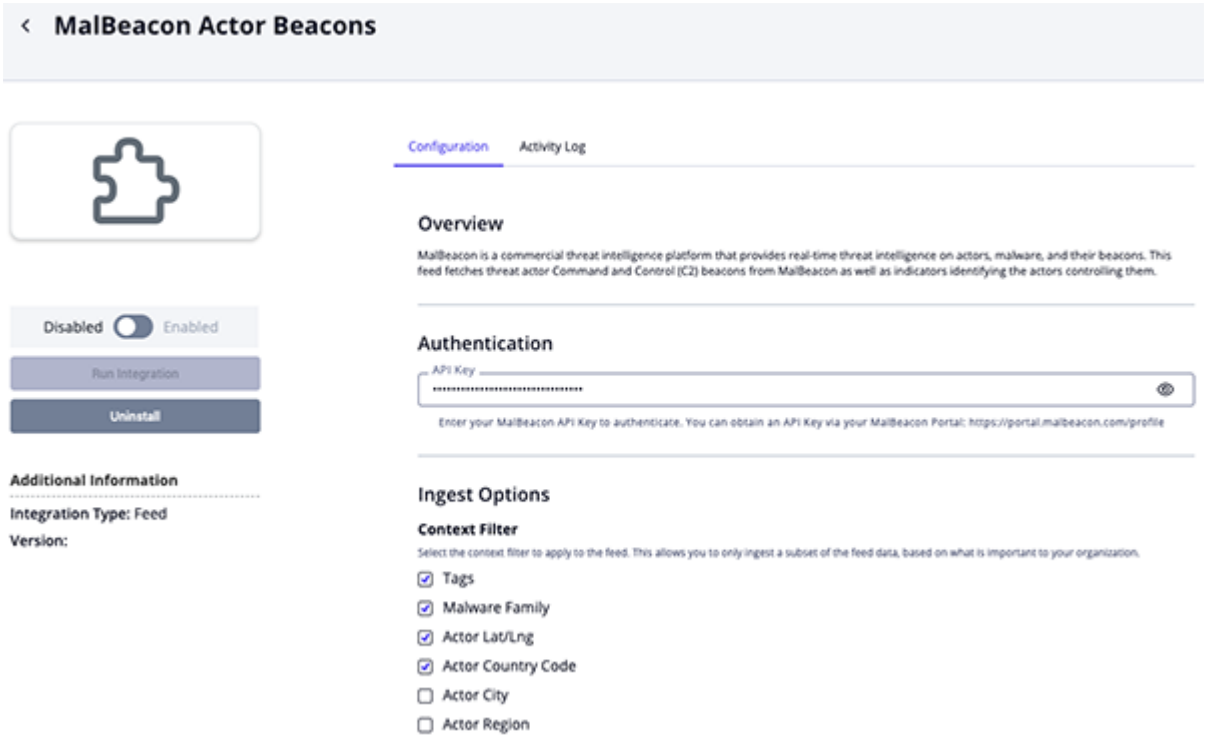
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

MalBeacon Actor Beacons

PARAMETER	DESCRIPTION
API Key	Enter your MalBeacon API Key.
Context Filter	Select the context filter to apply to the feed to ingest only the subset of data that is most relevant to your organization. Options include: ◦ Tags *(default)* ◦ Malware Family *(default)* ◦ Actor Lat/Lng ◦ Actor Country Code *(default)* ◦ Actor City ◦ Actor Region ◦ Actor AS Organization ◦ C2 Lat/Lng ◦ C2 Country Code *(default)* ◦ C2 City ◦ C2 Region ◦ C2 AS Organization
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.

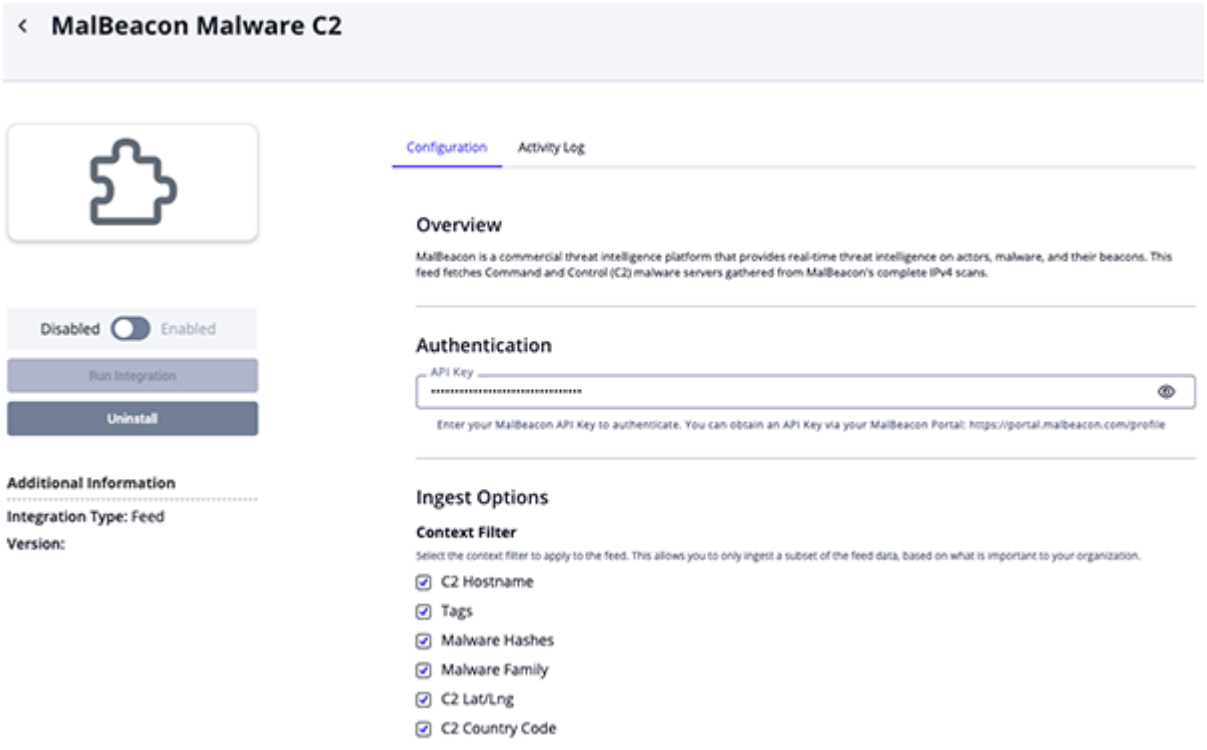
PARAMETER	DESCRIPTION
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



MalBeacon Malware C2

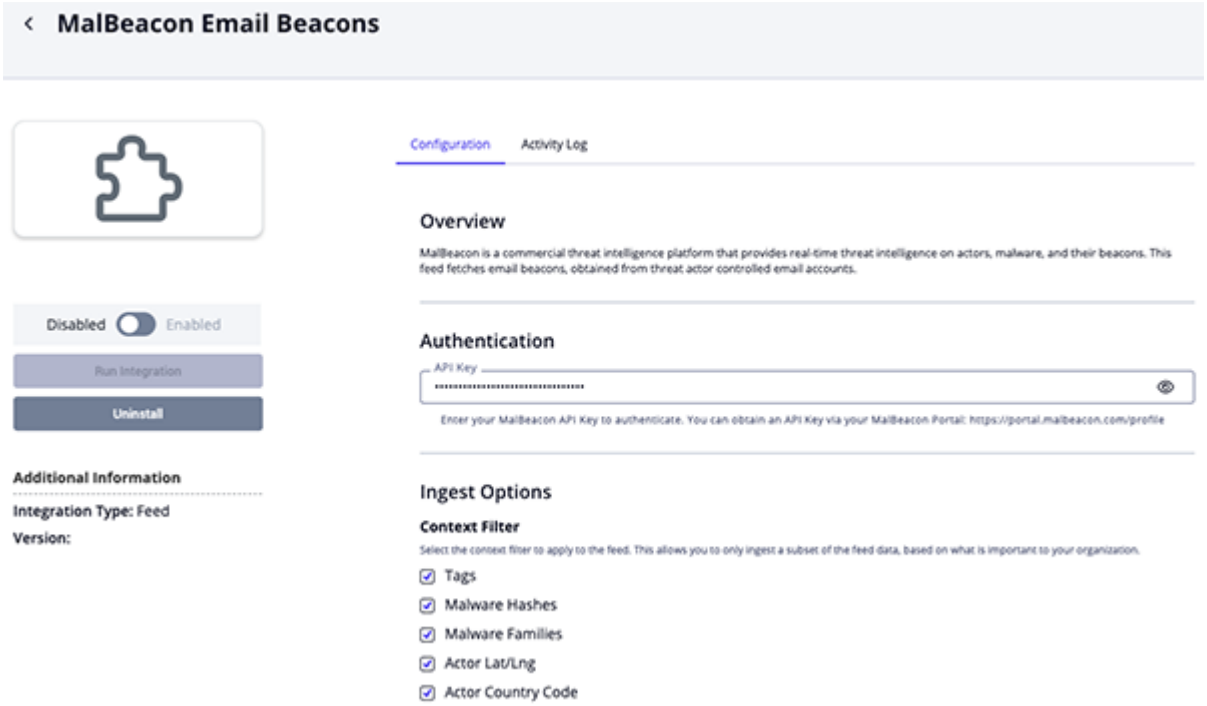
PARAMETER	DESCRIPTION
API Key	Enter your MalBeacon API Key.
Context Filter	Select the context filter to apply to the feed to ingest only the subset of data that is most relevant to your organization. Options include: ◦ Tags *(default)* ◦ C2 Hostname *(default)* ◦ Malware Hashes *(default)* ◦ C2 Country Code *(default)* ◦ C2 City ◦ C2 Region ◦ C2 AS Organization

PARAMETER	DESCRIPTION
	◦ Malware Family *(default)* ◦ C2 Lat/Lng ◦ C2 Port
C2 Hostname Status	Select the status to apply to hostnames that are associated with the C2 IPs. Options include: ◦ Active ◦ Review ◦ Indirect *(default)*
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



MalBeacon Email Beacons

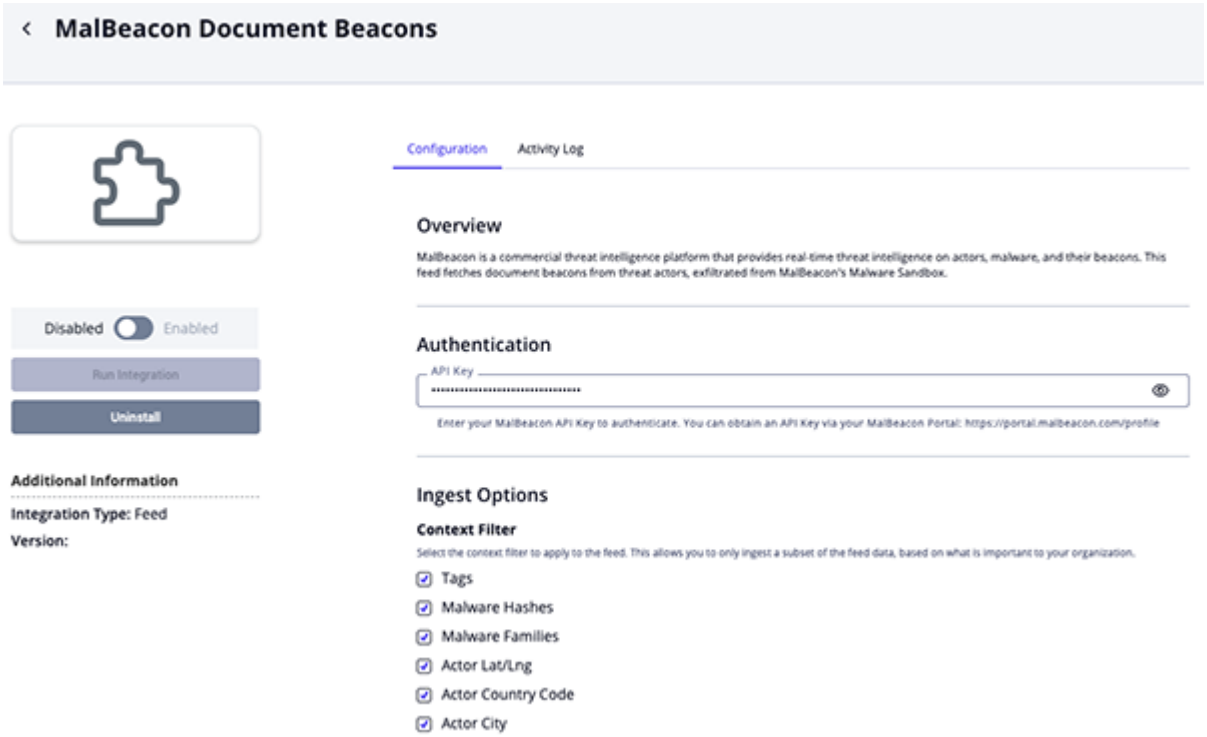
PARAMETER	DESCRIPTION
API Key	Enter your MalBeacon API Key.
Context Filter	Select the context filter to apply to the feed to ingest only the subset of data that is most relevant to your organization. Options include: ◦ Tags *(default)* ◦ Malware Hashes *(default)* ◦ Malware Family *(default)* ◦ Actor Lat/Lng ◦ Actor Country Code *(default)* ◦ Actor City ◦ Actor Region ◦ Actor AS Organization ◦ Actor Hostname ◦ Email Domain (Attribute)
Actor Hostname Status	Select the status to apply to hostnames that are associated with the actors. Options include: ◦ Active ◦ Review ◦ Indirect *(default)*
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



MalBeacon Document Beacons

PARAMETER	DESCRIPTION
API Key	Enter your MalBeacon API Key.
Context Filter	Select the context filter to apply to the feed to ingest only the subset of data that is most relevant to your organization. Options include: ◦ Tags *(default)* ◦ Malware Hashes *(default)* ◦ Malware Family *(default)* ◦ Actor Lat/Lng ◦ Actor Country Code *(default)* ◦ Actor City ◦ Actor Region ◦ Actor AS Organization ◦ Actor Hostname ◦ Actor Source Port
Actor Hostname Status	Select the status to apply to hostnames that are associated with the actors. Options include: ◦ Active ◦ Review ◦ Indirect *(default)*

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



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

MalBeacon Actor Beacons

The MalBeacon Actor Beacons feed retrieves IPs and hostnames tied to Threat Actors and their C2 infrastructure.

`GET https://api.malbeacon.com/v1/c2/feed/json`

Sample Response:


```
[
    {
        "actorloc": "50.8837,4.4730",
        "actorcountrycode": "BE",
        "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36",
        "c2domainresolved": "185.70.186.153",
        "c2region": "North Holland",
        "tags": "NA",
        "c2domain": "185.70.186.153",
        "actorcity": "Zaventem",
        "actorip": "37.120.143.202",
        "c2countrycode": "NL",
        "c2hostname": "NA",
        "actorasnorg": "AS9009 M247 Europe SRL",
        "tstamp": "2024-04-27 14:46:32",
        "c2": "http://185.70.186.153/",
        "cookie_id": "NA",
        "c2loc": "52.3740,4.8897",
        "c2asnorg": "AS57043 HOSTKEY B.V.",
        "actorhostname": "NA",
        "c2city": "Amsterdam",
        "actorregion": "Flanders",
        "actortimezone": "Europe/Brussels",
        "c2timezone": "Europe/Amsterdam"
    },
    {
        "actorloc": "50.1155,8.6842",
        "actorcountrycode": "DE",
        "useragent": "Mozilla/5.0 (X11; Linux x86_64; rv:125.0) Gecko/20100101
Firefox/125.0",
        "c2domainresolved": "128.199.113.162",
        "c2region": "Singapore",
        "tags": "NA",
        "c2domain": "128.199.113.162",
        "actorcity": "Frankfurt am Main",
        "actorip": "178.218.144.64",
```

```
        "c2countrycode": "SG",
        "c2hostname": "NA",
        "actorasnorg": "AS212508 Lowhosting services of Davide Gennari",
        "tstamp": "2024-04-27 14:15:31",
        "c2": "http://128.199.113.162/",
        "cookie_id": "6s8pl82qujvbt7ifdapgshb1m0",
        "c2loc": "1.3215,103.6957",
        "c2asnorg": "AS14061 DigitalOcean, LLC",
        "actorhostname": "178.218.144.64.lowhosting.org",
        "c2city": "Singapore",
        "actorregion": "Hesse",
        "actortimezone": "Europe/Berlin",
        "c2timezone": "Asia/Singapore"
    }
]
```

ThreatQuotient provides the following default mapping for this feed based on each item within the API response's array:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.actorip`	Indicator.Value	`IP Address`	`.tstamp`	N/A	N/A
`.actorhostname`	Indicator.Value	`FQDN`	`.tstamp`	N/A	N/A
`.c2domain`	Indicator.Value	`FQDN`	`.tstamp`	N/A	N/A
`.c2hostname`	Indicator.Value	`FQDN`	`.tstamp`	N/A	N/A
`.url`	Indicator.Value	`URL`	`.tstamp`	N/A	N/A
`.c2domainresolved`	Indicator.Value	`IP Address`	`.tstamp`	N/A	N/A
`.tags`	Malware.Value	N/A	`.tstamp`	`lokibot`	User-Configurable. Extracted from tags with the `family:` prefix
`.tags`	Tag.Name	N/A	`.tstamp`	`malware:infostealer`	User-Configurable. Parsed from comma-separated list of tags
`.c2asnorg`	Indicator.Attribute	AS Organization	`.tstamp`	`AS9009 M247 Europe SRL`	User-Configurable. Applied to C2 indicators
`.c2region`	Indicator.Attribute	Region	`.tstamp`	`Singapore`	User-Configurable. Applied to C2 indicators
`.c2city`	Indicator.Attribute	City	`.tstamp`	`Amsterdam`	User-Configurable. Applied to C2 indicators
`.c2countrycode`	Indicator.Attribute	Country Code	`.tstamp`	`NL`	User-Configurable. Applied to C2 indicators
`.c2loc`	Indicator.Attribute	Longitude	`.tstamp`	`52.3740`	User-Configurable. Applied to C2 indicators; Parsed from comma-separated coordinates
`.c2loc`	Indicator.Attribute	Latitude	`.tstamp`	`4.8897`	User-Configurable. Applied to C2 indicators; Parsed from comma-separated coordinates
`.actorasnorg`	Indicator.Attribute	AS Organization	`.tstamp`	`AS9009 M247 Europe SRL`	User-Configurable. Applied to Actor indicators

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.actorregion`	Indicator.Attribute	Region	`.tstamp`	`Singapore`	User-Configurable. Applied to Actor indicators
`.actorcity`	Indicator.Attribute	City	`.tstamp`	`Frankfurt am Main`	User-Configurable. Applied to Actor indicators
`.actorcountrycode`	Indicator.Attribute	Country Code	`.tstamp`	`DE`	User-Configurable. Applied to Actor indicators
`.actorloc`	Indicator.Attribute	Longitude	`.tstamp`	`52.3740`	User-Configurable. Applied to Actor indicators; Parsed from comma-separated coordinates
`.actorloc`	Indicator.Attribute	Latitude	`.tstamp`	`4.8897`	User-Configurable. Applied to Actor indicators; Parsed from comma-separated coordinates
N/A	Tag.Name	N/A	N/A	`actor`	Applied to Actor indicators
N/A	Tag.Name	N/A	N/A	`c2`	Applied to C2 indicators

MalBeacon Malware C2

The MalBeacon Malware C2 feed ingests IPs and hostnames gathered from complete IPv4 scans for malware C2 and other malicious threats.

`GET https://api.malbeacon.com/v1/onlyscans/feed/json`

Sample Response:


```
[
    {
        "c2_ip": "98.142.95.254",
        "c2_family": "metasploit",
        "c2_timezone": "America/Chicago",
        "c2_loc": "41.1544,-96.0422",
        "tags": "malware:metasploit",
        "c2_asnorg": "AS17378 TierPoint, LLC",
        "c2_countrycode": "US",
        "malhashes": "NA",
        "c2_port": "3790",
        "c2_city": "Papillion",
        "c2_hostname": "NA",
        "c2_region": "Nebraska"
    },
    {
        "c2_ip": "95.216.201.166",
        "c2_family": "metasploit",
        "c2_timezone": "Europe/Helsinki",
        "c2_loc": "60.1695,24.9354",
        "tags": "malware:metasploit",
        "c2_asnorg": "AS24940 Hetzner Online GmbH",
        "c2_countrycode": "FI",
        "malhashes": "NA",
        "c2_port": "3790",
        "c2_city": "Helsinki",
        "c2_hostname": "static.166.201.216.95.clients.your-server.de",
        "c2_region": "Uusimaa"
    },
    {
        "c2_ip": "94.23.43.228",
        "c2_family": "metasploit",
        "c2_timezone": "Europe/Paris",
        "c2_loc": "50.6330,3.0586",
        "tags": "malware:metasploit",
        "c2_asnorg": "AS16276 OVH SAS",
        "c2_countrycode": "FR",
        "malhashes": "NA",
        "c2_port": "3790",
        "c2_city": "Lille",
        "c2_hostname": "pedagogyk.decanet.fr",
```

```
        "c2_region": "Hauts-de-France"
    }
]
```

ThreatQuotient provides the following default mapping for this feed based on each item within the API response's array:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.c2_ip`	Indicator.Value	`IP Address`	N/A	N/A	N/A
`.c2_hostname`	Indicator.Value	`FQDN`	N/A	N/A	User-Configurable.
`.tags`	Malware.Value	N/A	N/A	`lokibot`	User-Configurable. Extracted from tags with the `family:` prefix
`.tags`	Tag.Name	N/A	N/A	`malware:infostealer`	User-Configurable. Parsed from comma-separated list of tags
`.c2_asnorg`	Indicator.Attribute	AS Organization	N/A	`AS9009 M247 Europe SRL`	User-Configurable. Applied to C2 indicators
`.c2_region`	Indicator.Attribute	Region	N/A	`Singapore`	User-Configurable. Applied to C2 indicators
`.c2_city`	Indicator.Attribute	City	N/A	`Amsterdam`	User-Configurable. Applied to C2 indicators
`.c2_countrycode`	Indicator.Attribute	Country Code	N/A	`NL`	User-Configurable. Applied to C2 indicators
`.c2_port`	Indicator.Attribute	Port	N/A	`50050`	User-Configurable. Applied to C2 indicators
`.c2_loc`	Indicator.Attribute	Longitude	N/A	`52.3740`	User-Configurable. Applied to C2 indicators; Parsed from comma-separated coordinates
`.c2_loc`	Indicator.Attribute	Latitude	N/A	`4.8897`	User-Configurable. Applied to C2 indicators; Parsed from comma-separated coordinates
N/A	Tag.Name	N/A	N/A	`c2`	Applied to C2 indicators
`.c2_family`	Malware.Value	N/A	N/A	`metasploit`	User-Configurable. N/A
`.malhashes`	Indicator.Value	MD5, SHA-1, or SHA-256	N/A	N/A	User-Configurable. Parsed from comma-separated list of hashes

MalBeacon Email Beacons

The MalBeacon Email Beacons feed ingests emails, IPs and hostnames gathered from threat actor controlled email accounts.

`GET https://api.malbeacon.com/v1/email/feed/json`

Sample Response:


```
[
    {
        "emaildomasnorg": "NA",
        "refcity": "NA",
        "emaildomcity": "NA",
        "emaildomresolved": "lookup failed",
        "actorip": "105.113.9.240",
        "actortimezone": "Africa/Lagos",
        "tags": "malware:infostealer,family:agenttesla",
        "useragent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36",
        "emaildomregion": "NA",
        "refhostname": "NA",
        "refasnorg": "NA",
        "malhashes":
"1ade01f01abf865c52e375857cccf0b8edadc83569c006bcd3a23c2bb452228c",
        "tstamp": "2024-06-10 10:16:05",
        "cookie_id": "2fi2a32ij78h5umckihg2ftug2",
        "emailaddress": "thanhoa@alite-lightlng.com",
        "referrer": "NA",
        "refdomain": "NA",
        "emaildomtimezone": "NA",
        "emaildomhostname": "NA",
        "refdomainresolved": null,
        "emaildomcountrycode": "NA",
        "emaildomloc": "NA",
        "actorloc": "4.7774,7.0134",
        "actorasnorg": "AS36873 Airtel Networks Limited",
        "refcountrycode": "NA",
        "actorregion": "Rivers State",
        "refregion": "NA",
        "actorcity": "Port Harcourt",
        "refloc": "NA",
        "actorcountrycode": "NG",
        "actorhostname": "NA",
        "reftimezone": "NA",
        "emaildomain": "alite-lightlng.com"
    },
    {
        "emaildomasnorg": "NA",
        "refcity": "NA",
```

```
        "emaildomcity": "NA",
        "emaildomresolved": "5.255.255.50",
        "actorip": "37.9.102.244",
        "actortimezone": "Europe/Moscow",
        "tags": "malware:infostealer,family:agenttesla",
        "useragent": "Mozilla/5.0 (compatible; YandexImageResizer/2.0; +http://
yandex.com/bots)",
        "emaildomregion": "NA",
        "refhostname": "NA",
        "refasnorg": "NA",
        "malhashes":
"5c3476257a9d920def565bb2414209467cc7b60dddeeb4d8d9bef3a0a9aae0c7",
        "tstamp": "2024-06-10 09:21:10",
        "cookie_id": "NA",
        "emailaddress": "morrishome1@yandex.com",
        "referrer": "NA",
        "refdomain": "NA",
        "emaildomtimezone": "NA",
        "emaildomhostname": "NA",
        "refdomainresolved": null,
        "emaildomcountrycode": "NA",
        "emaildomloc": "NA",
        "actorloc": "55.7522,37.6156",
        "actorasnorg": "AS13238 YANDEX LLC",
        "refcountrycode": "NA",
        "actorregion": "Moscow",
        "refregion": "NA",
        "actorcity": "Moscow",
        "refloc": "NA",
        "actorcountrycode": "RU",
        "actorhostname": "proxy-mds52sas.avatars.yandex.net",
        "reftimezone": "NA",
        "emaildomain": "yandex.com"
    }
]
```


ThreatQuotient provides the following default mapping for this feed based on each item within the API response's array:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.email`	Indicator.Value	`Email Address`	`.tstamp`	N/A	N/A
`.actorip`	Indicator.Value	`IP Address`	`.tstamp`	N/A	N/A
`.actorhostname`	Indicator.Value	`FQDN`	`.tstamp`	N/A	User-Configurable.
`.tags`	Malware.Value	N/A	`.tstamp`	`lokibot`	User-Configurable. Extracted from tags with the `family:` prefix
`.tags`	Tag.Name	N/A	`.tstamp`	`malware:infostealer`	User-Configurable. Parsed from comma-separated list of tags

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.actorasnorg`	Indicator.Attribute	AS Organization	`.tstamp`	`AS9009 M247 Europe SRL`	User-Configurable. Applied to Actor indicators
`.actorregion`	Indicator.Attribute	Region	`.tstamp`	`Singapore`	User-Configurable. Applied to Actor indicators
`.actorcity`	Indicator.Attribute	City	`.tstamp`	`Frankfurt am Main`	User-Configurable. Applied to Actor indicators
`.actorcountrycode`	Indicator.Attribute	Country Code	`.tstamp`	`DE`	User-Configurable. Applied to Actor indicators
`.actorloc`	Indicator.Attribute	Longitude	`.tstamp`	`52.3740`	User-Configurable. Applied to Actor indicators; Parsed from comma-separated coordinates
`.actorloc`	Indicator.Attribute	Latitude	`.tstamp`	`4.8897`	User-Configurable. Applied to Actor indicators; Parsed from comma-separated coordinates
N/A	Tag.Name	N/A	N/A	`actor`	Applied to Actor indicators
`emaildomain`	Indicator.Attribute	Email Domain	`.tstamp`	`c2`	User-Configurable. N/A
`.malhashes`	Indicator.Value	MD5, SHA-1, or SHA-256	N/A	N/A	User-Configurable. Parsed from comma-separated list of hashes

MalBeacon Document Beacons

The MalBeacon Document Beacons feed ingests IPs and hostnames gathered from threat actor document beacons, exfiltrated from MalBeacon's Malware Sandbox.

```
GET https://api.malbeacon.com/v1/document/feed/json
```

Sample Response:


```
[
    {
        "actorcity": "Zhukovka",
        "actorregion": "Bryansk Oblast",
        "referrer": "NA",
        "actorip": "93.171.181.161",
        "refregion": "NA",
        "actortimezone": "Europe/Moscow",
        "refhostname": "NA",
        "actorhostname": "NA",
        "actorsourceport": "51177",
        "cookie_id": "NA",
        "refcountrycode": "NA",
        "tags": "sandbox_exfiltrated_document",
        "reftimezone": "NA",
        "malhashes": "NA",
        "actorasnorg": "AS48949 Media-TV Ltd.",
        "refdomainresolved": null,
        "actorloc": "53.5338,33.7308",
        "refasnorg": "NA",
        "useragent": "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; ms-office;
MSOffice 14) ; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; ",
        "refcity": "NA",
        "refloc": "NA",
        "tstamp": "2024-06-11 11:31:16",
        "actorcountrycode": "RU",
        "refdomain": "NA"
    }
]
```


ThreatQuotient provides the following default mapping for this feed based on each item within the API response's array:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.actorip`	Indicator.Value	`IP Address`	`.tstamp`	N/A	N/A
`.actorhostname`	Indicator.Value	`FQDN`	`.tstamp`	N/A	User-Configurable.
`.tags`	Malware.Value	N/A	`.tstamp`	`lokibot`	User-Configurable. Extracted from tags with the `family:` prefix

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.tags`	Tag.Name	N/A	`.tstamp`	`malware:infostealer`	User-Configurable. Parsed from comma-separated list of tags
`.actorasnorg`	Indicator.Attribute	AS Organization	`.tstamp`	`AS9009 M247 Europe SRL`	User-Configurable. Applied to Actor indicators
`.actorregion`	Indicator.Attribute	Region	`.tstamp`	`Singapore`	User-Configurable. Applied to Actor indicators
`.actorcity`	Indicator.Attribute	City	`.tstamp`	`Frankfurt am Main`	User-Configurable. Applied to Actor indicators
`.actorcountrycode`	Indicator.Attribute	Country Code	`.tstamp`	`DE`	User-Configurable. Applied to Actor indicators
`.actorloc`	Indicator.Attribute	Longitude	`.tstamp`	`52.3740`	User-Configurable. Applied to Actor indicators; Parsed from comma-separated coordinates
`.actorloc`	Indicator.Attribute	Latitude	`.tstamp`	`4.8897`	User-Configurable. Applied to Actor indicators; Parsed from comma-separated coordinates
N/A	Tag.Name	N/A	N/A	`actor`	Applied to Actor indicators
`.actorsourceport`	Indicator.Attribute	Source Port	`.tstamp`	`8000`	User-Configurable. Applied to Actor indicators
`.malhashes`	Indicator.Value	MD5, SHA-1, or SHA-256	N/A	N/A	User-Configurable. Parsed from comma-separated list of hashes

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.

MalBeacon Actor Beacons

Run Time	1 minute
Indicators	34
Indicator Attributes	198
Malware	1

MalBeacon Malware C2

Run Time	1 minute
Indicators	1,327
Indicator Attributes	7,971
Malware	20

MalBeacon Email Beacons

Run Time	1 minute
Indicators	11
Indicator Attributes	56
Malware	1

MalBeacon Document Beacons

Run Time	1 minute
Indicators	1
Indicator Attributes	5

Known Issues / Limitations

- `c2` and `actor` tags are ingested by default even if tag ingestion is disabled in user configuration.

Change Log

- **Version 1.0.0**
  - Initial release