# ThreatQuotient

## Blueliv CTI CDF User Guide

**Version 1.0.0**

October 18, 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

# 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** | 1.0.0 |
| **Compatible with ThreatQ Versions** | >= 4.25.0 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Blueliv Intelligence integration for ThreatQ allows a user to ingest Blueliv's cyber threat intelligence from their v1 API Supported CTI feeds:

- **Bot IPs** - allows the user to pull back CTI about IPs that are related to botnets, that Blueliv tracks. This includes IP Addresses and URLs.
- **Crimeservers** - allows the user to pull back CTI about crimeservers that Blueliv tracks. This includes URLs, IPs, and ASNs.
- **Attacking IPs** - allows the user to pull back CTI about IPs that are currently "attaacking" that Blueliv tracks. This includes only IP Addresses.
- **Malware** - allows the user to pull back CTI about malware hashes that Blueliv tracks. This includes MD5s, SHA-1s, and SHA-256s.

Blueliv provides automated, real-time threat intelligence data, ultimately streamlining the delivery of valuable data into ThreatQ for analysis and correlation with network events.

Pairing Blueliv's confidence level with ThreatQ's Scoring System helps analysts reduce the noise and identify relevant events more quickly.

- Blueliv's attack feed provides targeted information, making it easier to find, mitigate and contain the attack.
- Importing IP and FQDN indicators associated with botnets and crime servers.
- Ingesting hashes and attributes indicating the type, family, architecture and confidence of the malware.
- Creating relationships between related IPs, hashes and FQDNs.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Malware
  - Malware Attributes

# 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 **Labs** 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:

   **All Feeds**

| PARAMETER | DESCRIPTION |
|---|---|
| **API Key** | Your Blueliv API Key (v1) for authentication. |

   **Blueliv Crimeservers**

| PARAMETER | DESCRIPTION |
|---|---|
| **Endpoint** | The Blueliv API endpoint determines the time range for fetched threat intelligence.<br>Options include:<br>◦ Last (Rate Limit: 2 Requests / 15m)<br>◦ Online (Rate Limit: 2 Requests / 1h) (Default)<br>◦ Recent (Rate Limit: 2 Requests / 24h) |

   **Blueliv Malware Hashes**

| PARAMETER | DESCRIPTION |
|---|---|
| **Confidence Filter** | The Confidence Levels to be ingested.<br>Options include:<br>◦ High (default) |

| | |
|---|---|
| | ◦ Medium (default)<br>◦ Low |
| **Endpoint** | The Blueliv API endpoint determines the time range for fetched threat intelligence.<br>Options include:<br>◦ Last (Rate Limit: 2 Requests / 15m)<br>◦ Online (Rate Limit: 2 Requests / 1h) (Default)<br>◦ Recent (Rate Limit: 2 Requests / 24h) |

**Blueliv Attacking IPs**

| PARAMETER | DESCRIPTION |
|---|---|
| **Attack Type Filter** | The Attack Types to be ingested<br>Options include:<br>◦ Brute Force (Default)<br>◦ Random SYN Attack (Default)<br>◦ Targeted Service Scan (Default)<br>◦ Login Attempt<br>◦ Service Scan<br>◦ Port Scan |
| **Endpoint** | The Blueliv API endpoint determines the time range for fetched threat intelligence.<br>Options include:<br>◦ Last (Rate Limit: 2 Requests / 15m)<br>◦ Online (Rate Limit: 2 Requests / 1h) (Default) |

**Blueliv Bot IPs**

| PARAMETER | DESCRIPTION |
|---|---|
| **Endpoint** | The Blueliv API endpoint determines the time range for fetched threat intelligence.<br>Options include:<br>◦ Last (Rate Limit: 2 Requests / 10m)<br>◦ Recent (Rate Limit: 2 Requests / 1h)<br>◦ POS Last (Rate Limit: 2 Requests / 10m)<br>◦ POS Recent (Rate Limit: 2 Requests / 1h)<br>◦ Full Last (Rate Limit: 2 Requests / 10m) |

- Full Recent (Rate Limit: 2 Requests / 1h) (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

## All Feeds

The following mapping applies to all feeds (where `Object` represents the object ingested by each feed, regardless of type).

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .{endpoint_name}.country | Object.Attribute | Country Code | .createdAt or .firstSeenAt | US | N/A |
| .{endpoint_name}.countryName | Object.Attribute | Country | .createdAt or .firstSeenAt | United States | N/A |
| .{endpoint_name}.city | Object.Attribute | City | .createdAt or .firstSeenAt | New York City | N/A |
| .{endpoint_name}.latitude | Object.Attribute | Latitude | .createdAt or .firstSeenAt | 37.751 | N/A |
| .{endpoint_name}.longitude | Object.Attribute | Longitude | .createdAt or .firstSeenAt | -97.822 | N/A |

## Blueliv Crimeservers

The Blueliv Crimeservers feed allows the user to pull back CTI about crimeservers that Blueliv tracks. This includes URLs, IPs, and ASNs.

`GET https://api.blueliv.com/v1/crimeserver/<frequency>`

**Sample Response:**

```
{
    "crimeServers": [
        {
            "_id":
"4e3e47ffcfdf26540790c5011f0e6c97b67d0521ea518dc4e7ae518298f3545b",
            "url": "https://atendimentoonlinecliente.live/home.php",
            "type": "PHISHING",
            "subType": "UNCLASSIFIED",
            "status": "ONLINE",
            "domain": "atendimentoonlinecliente.live",
            "host": "atendimentoonlinecliente.live",
            "updatedAt": "2020-05-07T12:45:00+0000",
            "firstSeenAt": "2020-04-23T00:34:40+0000",
            "lastSeenAt": "2020-05-07T12:35:02+0000",
            "confidence": 1
        },
        {
            "_id":
"ada6a4216c480190eddbbd92c1df42dcca40aae7d913411845091eeeac5dc2ae",
```

```
            "url": "http://afterworld.net/index.php",
            "type": "C_AND_C",
            "subType": "BAYROB",
            "country": "US",
            "countryName": "United States",
            "status": "ONLINE",
            "statusCode": 200,
            "domain": "afterworld.net",
            "host": "afterworld.net",
            "latitude": 37.751,
            "longitude": -97.822,
            "ip": "69.172.201.153",
            "updatedAt": "2020-05-07T12:49:51+0000",
            "asnId": 19324,
            "asnDesc": "DOSARREST, US",
            "firstSeenAt": "2017-08-18T21:29:20+0000",
            "lastSeenAt": "2020-05-07T12:49:50+0000",
            "confidence": 4
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .crimeServers[].url | Indicator.Value | URL | .crimeServers[].firstSeenAt | https://atendimentoonlinecliente.live/home.php | N/A |
| .crimeServers[].ip | Indicator.Value | IP Address | .crimeServers[].firstSeenAt | 11.22.33.44 | N/A |
| .crimeServers[].asnId | Indicator.Value | ASN | .crimeServers[].firstSeenAt | 19324 | N/A |
| .crimeServers[].subType | Malware.Value | N/A | .crimeServers[].firstSeenAt | PONY | 'UNCLASSIFIED' is ignored |
| .crimeServers[].type | Indicator.Attribute | Type | .crimeServers[].firstSeenAt | PHISHING | Title-cased |
| .crimeServers[].status | Indicator.Attribute | Status | .crimeServers[].firstSeenAt | ONLINE | Title-cased |
| .crimeServers[].statusCode | Indicator.Attribute | Status Code | .crimeServers[].firstSeenAt | 200 | N/A |
| .crimeServers[].confidence | Indicator.Attribute | Confidence | .crimeServers[].firstSeenAt | 0 | |

# Blueliv Malware Hashes

The Blueliv Malware Hashes feed allows the user to pull back CTI about malware hashes that Blueliv tracks. This includes MD5s, SHA-1s, and SHA-256s.

`GET https://api.blueliv.com/v1/malware/<frequency>`

**Sample Response:**

```
{
    "malwares": [
        {
            "filename":
"bcd3dd873b1211fc243ad6754838dcef8041012d39fe755dd2612f21165699c0",
            "contentType": "application/x-dosexec",
            "md5": "ccfd75bbe6d1dc9dcd09c01f4b4e91dd",
            "sha1": "4e9d5154d0ada0ec892fe36a75243f73935f25ff",
            "sha256":
"bcd3dd873b1211fc243ad6754838dcef8041012d39fe755dd2612f21165699c0",
            "analyzedAt": "2020-05-07T12:00:04+0000",
            "firstSeenAt": "2020-05-07T11:17:31+0000",
            "fileType": "PE32 executable (GUI) Intel 80386, for MS Windows, UPX
compressed",
            "fileSize": 54429,
            "malwareType": "SYTRO",
            "confidence": "HIGH",
            "architecture": "WIN32",
            "signatures": [
                {
                    "description": "The signatures of the analysis have reached
INFORMATIVE severity level. This level holds uncommon non-malicious actions,
and behavioral information of the analyzed sample",
                    "name": "Signature severity - Informative",
                    "severity": 1
                },
                {
                    "description": "The analyzed sample creates Windows
executable files on the filesystem",
                    "name": "Creates Window executable",
                    "severity": 2
                },
                {
                    "description": "The analyzed sample creates a slightly
modified copy of itself",
                    "name": "Detected Polymorphism",
                    "severity": 3
                },
                {
                    "description": "File has been identified by at least 40
AntiVirus engines on VirusTotal as malicious. The reliability of the data
regarding this signature comes from the retrieved values from third party
applications or functionalities based on their criteria",
                    "name": "VirusTotal matches",
                    "severity": 6
                },
                {
                    "description": "The signatures of the analysis have reached
MALICIOUS severity level. This level holds malicious actions and common malware
behavior like process injection, process inspection, anti-analysis techniques,
stealth and persistence mechanisms, and so on",
```

```
                    "name": "Signature severity - Malicious",
                    "severity": 3
                }
            ]
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .malwares[].md5 | Indicator.Value | MD5 | .malwares[].firstSeenAt | 1f6d1b5a948bf563cbe45a236c47422b | N/A |
| .malwares[].sha1 | Indicator.Value | SHA-1 | .malwares[].firstSeenAt | 3D852B2CA270617FA53BFB48589A2DA8ED940F4B | N/A |
| .malwares[].sha256 | Indicator.Value | SHA-256 | .malwares[].firstSeenAt | 66335C38D58473F0269C96D5FD6E16C57EE7DE4F35B71B7BFD8ED12DE9C97D01 | N/A |
| .malwares[].signatures[].name | Signature.Title | Indirect | .malwares[].firstSeenAt | Detected Polymorphism | N/A |
| .malwares[].signatures[].description | Signature.Value | Indirect | .malwares[].firstSeenAt | The analyzed sample creates a slightly modified copy of itself | N/A |
| .malwares[].malwareType | Malware.Value | N/A | .malwares[].firstSeenAt | SYTRO | Title-cased; 'UNCLASSIFIED' is ignored |
| .malwares[].signatures[].severity | Signature.Attribute | Severity | .malwares[].firstSeenAt | 4 | 1-10 |
| .malwares[].contentType | Indicator.Attribute, Malware.Attribute | Content Type | .malwares[].firstSeenAt | application/x-dosexec | N/A |
| .malwares[].confidence | Indicator.Attribute, Malware.Attribute | Confidence | .malwares[].firstSeenAt | HIGH | Title-cased |
| .malwares[].architecture | Indicator.Attribute, Malware.Attribute | Architecture | .malwares[].firstSeenAt | WIN32 | Title-cased |
| .malwares[].malwareFamily | Indicator.Attribute, Malware.Attribute | Malware Family | .malwares[].firstSeenAt | POS | N/A |
| .malwares[].fileSize | Indicator.Attribute, Malware.Attribute | File Size | .malwares[].firstSeenAt | N/A | N/A |
| .malwares[].analyzedAt | Indicator.Attribute, Malware.Attribute | Analyzed At | .malwares[].firstSeenAt | N/A | N/A |

# Blueliv Attacking IPs

The Blueliv Attaclomg IPs feed allows the user to pull back CTI about IPs that are currently "attacking" that Blueliv tracks. This includes only IP Addresses.

`GET https://api.blueliv.com/v1/attack/<frequency>`

**Sample Response:**


```
{
    "attacks": [
      {
        "_id": "5ed790c9a3f96154f24a532b",
        "attackType": "BRUTE_FORCE",
        "firstEvent": "2020-06-03T11:38:02+0000",
        "lastEvent": "2020-06-03T12:22:24+0000",
        "numEvents": 12,
        "source": {
          "ip": "5.188.87.51",
          "country": "IE",
          "countryName": "Ireland",
          "city": "Ballingeary",
          "port": [
            56964,
            36742,
            55112,
            61868,
            40684,
            43596,
            55566,
            49206,
            34838,
            63800,
            63450,
            50812
          ],
          "latitude": 51.85,
          "longitude": -9.2333
        },
        "destination": {
          "ip": "xxx.xxx.141.155",
          "country": "GB",
          "countryName": "United Kingdom",
          "city": "London",
          "port": [
            22
          ],
          "serviceName": [
            "ssh"
          ],
          "latitude": 51.5128,
          "longitude": -0.0638
        },
        "createdAt": "2020-06-03T12:00:01+0000",
        "updatedAt": "2020-06-03T12:30:00+0000",
        "confidence": 0
      },
      {
```

```
        "_id": "5ed790c9a3f96154f24a532a",
        "attackType": "LOGIN_ATTEMPT",
        "firstEvent": "2020-06-03T11:50:17+0000",
        "lastEvent": "2020-06-03T11:50:17+0000",
        "numEvents": 1,
        "source": {
          "ip": "88.214.26.97",
          "country": "DE",
          "countryName": "Germany",
          "port": [
            53946
          ],
          "latitude": 51.2993,
          "longitude": 9.491
        },
        "destination": {
          "ip": "xxx.xxx.113.72",
          "country": "SG",
          "countryName": "Singapore",
          "city": "Singapore",
          "port": [
            22
          ],
          "serviceName": [
            "ssh"
          ],
          "latitude": 1.3001,
          "longitude": 103.7864
        },
        "createdAt": "2020-06-03T12:00:01+0000",
        "updatedAt": "2020-06-03T12:00:01+0000",
        "confidence": 0
      }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .attacks[].source.ip | Indicator.Value | IP Address | .attacks[].createdAt | 51.36.64.40 | N/A |
| .attacks[].confidence | Indicator.Attribute | Confidence | .attacks[].createdAt | 0 | N/A |
| .attacks[].destination.serviceName | Indicator.Attribute | Target Service | .attacks[].createdAt | smbd | N/A |
| .attacks[].attackType | Indicator.Attribute | Attack Type | .attacks[].createdAt | BRUTE_FORCE | Formatted by replacing underscores and title-casing |

# Blueliv Bot IPs

The Blueliv Bot IPs feed allows the user to pull back CTI about IPs that are related to botnets, that Blueliv tracks. This includes IP Addresses and URLs.

```
GET https://api.blueliv.com/v1/ip/<frequency>
```

**Sample Response:**


```
{
    "ips": [
        {
            "confidence": 0,
            "botnetFamily": [
                "Credential Grabber"
            ],
            "ip": "51.36.64.40",
            "country": "SA",
            "countryName": "Saudi Arabia",
            "latitude": 21.5168,
            "longitude": 39.2192,
            "seenAt": "2017-09-26T05:57:19+0000",
            "destinationPort": 443,
            "botnetType": "PONY",
            "operatingSystem": "Windows 7",
            "botId":
"b7ae4cfb58c159149a297865312748e6688c3f7e59d9aa8fd3d8ba44ba8f01d4",
            "city": "Jeddah",
            "portalUrl": "https://login.live.com/login.srf",
            "portalDomain": "live.com",
            "createdAt": "2020-05-07T12:50:20+0000"
        },
        {
            "confidence": 0,
            "botnetFamily": [
                "Trojan Banker"
            ],
            "ip": "59.115.110.121",
            "country": "TW",
            "countryName": "Taiwan",
            "latitude": 25.0478,
            "longitude": 121.5318,
            "seenAt": "2017-09-26T05:57:51+0000",
            "botnetUrl": "http://poluxradio.com/wp-content/plugins/akismet/
gate.php",
            "botnetIp": "108.59.11.19",
            "botnetType": "ZEUS",
            "userAgent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0; GTB7.5)",
            "city": "Taipei",
            "createdAt": "2020-05-07T12:54:04+0000"
```

```
            }
        ]
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .ips[].botnetIp | Indicator.Value | IP Address | .ips[].createdAt | 59.115.110.121 | N/A |
| .ips[].botnetUrl | Indicator.Value | URL | .ips[].createdAt | http://poluxradio.com/wp-content/plugins/akismet/gate.php | N/A |
| .ips[].ip | Indicator.Value | IP Address | .ips[].createdAt | 108.59.11.19 | N/A |
| .ips[].botnetType | Malware.Value | N/A | .ips[].createdAt | ZEUS | 'unknown' is ignored |
| .ips[].confidence | Indicator.Attribute | Confidence | .ips[].createdAt | 0 | N/A |
| .ips[].botnetFamily[] | Indicator.Attribute, Malware.Attribute | Malware Family | .ips[].createdAt | Trojan Banker | N/A |
| .ips[].operatingSystem | Indicator.Attribute, Malware.Attribute | Bot Operating System | .ips[].createdAt | Windows 7 | 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.

## Blueliv Crimeservers

| METRIC | RESULT |
|---|---|
| **Run Time** | 10 minutes |
| **Indicators** | 8,000 |
| **Indicator Attributes** | 61,000 |
| **Malware** | 80 |

## Blueliv Malware Hashes

| METRIC | RESULT |
|---|---|
| **Run Time** | 4 minutes |
| **Indicators** | 4,400 |
| **Indicator Attributes** | 26,000 |
| **Malware** | 100 |

## Blueliv Attacking IPs

| METRIC | RESULT |
|---|---|
| **Run Time** | < 1 minute |
| **Indicators** | 110 |
| **Indicator Attributes** | 760 |

## Blueliv Bot IPs

| METRIC | RESULT |
|---|---|
| **Run Time** | < 1 minute |
| **Indicators** | 75 |
| **Indicator Attributes** | 110 |
| **Malware** | 8 |
| **Malware Attributes** | 7 |

# Known Issues / Limitations

- For feeds with an endpoint with a rate limit of less than 1 request/hour, choosing that endpoint while doing hourly runs may cause feed runs to fail due to the provider's rate limiting policy.

# Change Log

- **Version 1.0.0**
  - Initial release