

ThreatQuotient



BotScout CDF User Guide

Version 1.0.0

December 17, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping..... 9

 BotScout Banned Bots 9

Average Feed Run..... 11

Change Log 12

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.

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	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The BotScout CDF for ThreatQ enables the automatic ingestion of IPs & Emails from BotScout into ThreatQ as Indicators.

BotScout helps prevent automated web scripts, known as "bots", from registering on forums, polluting databases, spreading spam, and abusing forms on web sites. BotScout does this by tracking the names, IPs, and email addresses that bots use and logging them as unique signatures for future reference.

The integration provides the following feed:

- **BotScout Banned Bots** - ingests the latest IPs and Emails for bots caught by BotScout.

The integration ingests indicators and indicator 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 **OSINT** 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 parameter under the **Configuration** tab:

PARAMETER

DESCRIPTION

Ingested IOCs

Select the type of IOCs to ingest. Options include:

- Bot IP Addresses (default)
- Bot IPv6 Addresses (default)
- Bot Emails

< BotScout Banned Bots



Disabled ☐ Enabled ☒

Uninstall

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Configuration Activity Log

Ingested IOCs

Select which IOC types to ingest into ThreatQ

- ☒ Bot IP Addresses
- ☒ Bot IPv6 Addresses
- ☐ Bot Emails

Set indicator status to...

Review

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

BotScout Banned Bots

The BotScout Banned Bots feed ingests the latest IPs and emails detected by BotScout.

GET https://botscout.com/last_caught_cache.htm

Sample Response:



This link returns HTML data that is parsed by the feed.

```
<table
  border="1"
  bgcolor="#aeaeae"
  id="XmostRecent"
  cellspacing="1"
  cellpadding="2"
  align="center"
  width="760"
>
  <thead>
    <tr>
      <th class="fpRecent">Bot Name</th>
      <th class="fpRecent">Bot Email</th>
      <th class="fpRecent" width="100">Bot IP</th>
      <td class="fpRecent">From</td>
    </tr>
  </thead>
  <tbody>
    <tr style="font-size:10px;" bgcolor="#f1f1f1">
      <td>2001:1460:2:0:121:8:00:17</td>
      <td>2001:1460:2:0:121:8:00:17</td>
      <td><a href="/ipcheck.htm?ip=120.40.130.70">120.40.130.70</a></td>
      <td align="center" valign="absmiddle">
        <a href="/countrycheck.htm?cc=cn"
          ></a>
        </td>
      </tr>
    <tr style="font-size:10px;" bgcolor="#cdcdcd">
```

```

<td>novikov.denis.1978.23.7</td>
<td>novikov.denis.1978.23.7@mail.ru</td>
<td><a href="/ipcheck.htm?ip=172.71.246.82">172.71.246.82</a></td>
<td align="center" valign="absmiddle">
  <a href="/countrycheck.htm?cc=xx"
    ></a>
</td>
</tr>
<tr style="font-size:10px;" bgcolor="#f1f1f1"></tr>
</tbody>
</table>

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
Bot Email	Indicator.Value	Email Address	N/A	novikov.denis.1978.23.7[@ mail.ru	N/A
Bot IP	Indicator.Value	IP Address, IPv6 Address	N/A	172.71.246.82	N/A
From	Indicator.Attribute	Country Code	N/A	CN	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.

METRIC	RESULT
Run Time	1 minute
Indicators	178
Indicator Attributes	170

Change Log

- Version 1.0.0
 - Initial release