ThreatQuotient

Project Honey Pot CDF User Guide

Version 1.0.0

November 27, 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

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.

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The Project Honey Pot CDF enables analysts to automatically ingest IP Addresses related to spammers, harvesters, attackers, and more into ThreatQ.

Project Honey Pot is a distributed system for identifying spammers and the spambots they use to scrape addresses from your website. Project Honey Pot tracks IPs that are known to be used by spammers, harvesters, and other malicious actors. These IPs are then used to generate a blacklist that can be used to block malicious traffic.

The integration provides the following feed:

- **Project Honey Pot -** pulls IPs from the Project Honey Pot RSS feed based on the specified `ip_type.`

The integration ingests IP Address type indicators.

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.

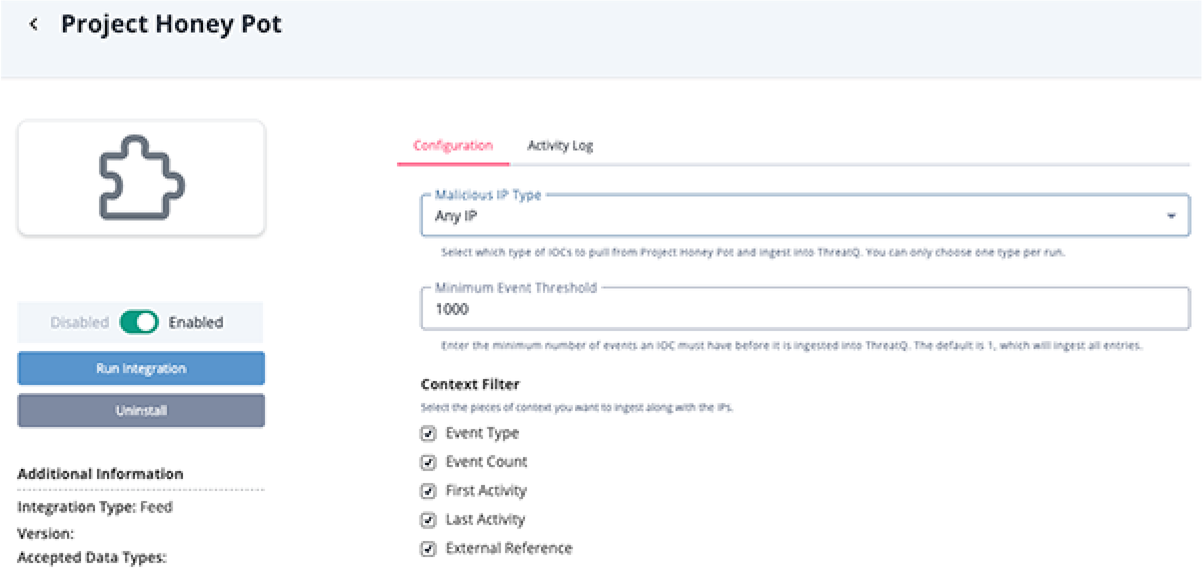
To configure the integration:

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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Malicious IP Type	Select which type of IOCs to pull from Project Honey Pot and ingest into ThreatQ. Options include: ◦ All IPs (default) ◦ Harvesters ◦ Spam Servers ◦ Bad Web Hosts ◦ Comment Spammers ◦ Dictionary Attackers ◦ Rule Breakers ◦ Search Engines You can only choose one type per run.
Minimum Event Threshold	Enter the minimum number of events an IOC must have before it is ingested into ThreatQ. The default is 1, which will ingest all entries.
Context Filter	Select the pieces of context you want to ingest along with the IPs. Options include: ◦ Event Type (default) ◦ Event Count ◦ First Activity ◦ Last Activity ◦ External Reference



Project Honey Pot

Disabled ● Enabled

Malicious IP Type: Any IP

Select which type of IOCs to pull from Project Honey Pot and ingest into ThreatQ. You can only choose one type per run.

Minimum Event Threshold: 1000

Enter the minimum number of events an IOC must have before it is ingested into ThreatQ. The default is 1, which will ingest all entries.

Context Filter

Select the pieces of context you want to ingest along with the IPs.

- ☑ Event Type
- ☑ Event Count
- ☑ First Activity
- ☑ Last Activity
- ☑ External Reference

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

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

Project Honey Pot

The Project Honey Pot feed periodically pulls IPs from the Project Honey Pot RSS feed based on the specified `ip_type`.

`GET https://www.projecthoneypot.org/list_of_ips.php?rss=1&t={{ip_type}}`

Sample Response:

```
<rss version="2.0">
        <channel>
                <title>Search Engine IPs | By Last Crawl | Project Honey Pot</
title>
                <link><![CDATA[ http://www.projecthoneypot.org/
list_of_ips.php&t=se ]]></link>
                <description />
                <copyright>Copyright 2023 Unspam Technologies, Inc</copyright>
                <language>en-us</language>
                <lastBuildDate>July 16 2023 10:00:21 PM</lastBuildDate>
                <image>
                        <url>http://www.projecthoneypot.org/images/
small_phpot_logo.jpg</url>
                        <title>Project Honey Pot | Distribute Spammer Tracking
System</title>
                        <link>http://www.projecthoneypot.org</link>
                </image>
                <item>
                        <title>66.249.66.6 | Se</title>
                        <link>http://www.projecthoneypot.org/ip_66.249.66.6</
link>
                        <description>Event: Crawl | Total: 2,207 | First:
2017-01-07 | Last: 2023-07-16</description>
                        <pubDate>July 16 2023 10:00:21 PM</pubDate>
                </item>
        </channel>
</rss>
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Indicator.Value	IP Address	`.pubDate`	`66.249.66.6`	N/A
`.link`	Indicator.Attribute	External Reference	`.pubDate`	`http://www.projecthoneypot.org/ip_66.249.66.6`	N/A
`.description`	Indicator.Attribute	Event Type	`.pubDate`	`Crawl`	First section of field
`.description`	Indicator.Attribute	Event Count	`.pubDate`	`2207`	Second section of field. Updates at ingestion time.
`.description`	Indicator.Attribute	First Activity	`.pubDate`	`2017-01-07`	Third section of field
`.description`	Indicator.Attribute	Last Activity	`.pubDate`	`2023-07-16`	Fourth section of field. Updates at ingestion time.

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	32
Indicator Attributes	160

Known Issues / Limitations

- The Project Honey Pot feed only pulls back a maximum of 50 results per run.
- Country Codes will not be available through this feed.

Change Log

- **Version 1.0.0**
  - Initial release