ThreatQuotient

Silent Push CDF

Version 1.0.0

December 10, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.10.0
Support Tier	ThreatQ Supported

Introduction

The Silent Push CDF integration ingests FQDNs and related IP Addresses from the Silent Push provider.

The integration provides the following feed:

- **Silent Push Domains -** ingests FQNs and their associated IP Addresses from Silent Push.

The integration ingests indicator type system objects.

Prerequisites

You will need a Silent Push API Key to use the integration.

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 yaml file.
3. Navigate to the integrations management page on 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 on your local machine
6. Select the individual feeds to install, when prompted and 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 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).

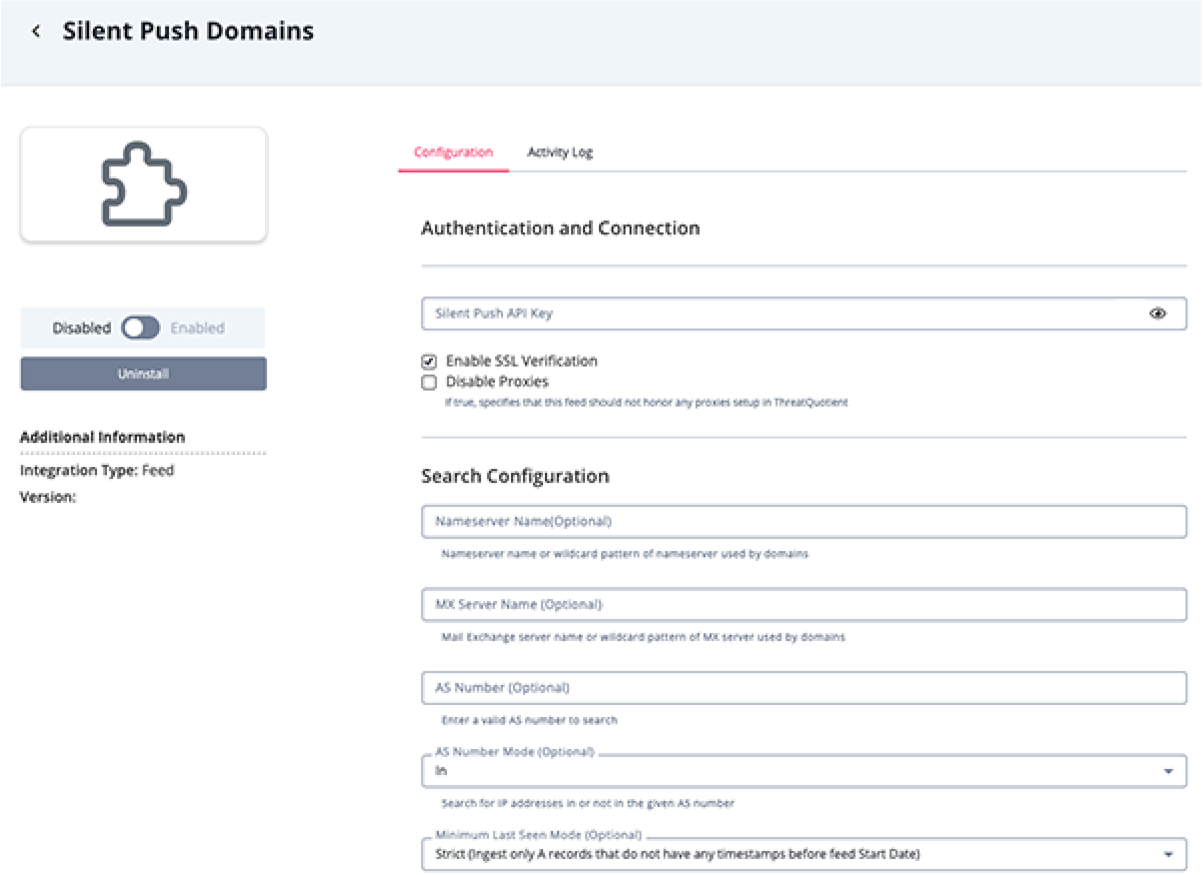
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

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

PARAMETER	DESCRIPTION
Silent Push API Key	Enter your Silent Push API Key used to connect to Silent Push.
Enable SSL Verification	Enable this parameter for the feed to validate the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Nameserver Name	Optional - Enter the Nameserver name or wildcard pattern of nameserver used by domains.
MX Server Name	Optional - Enter the Mail Exchange server name or wildcard pattern of MX server used by domains.
AS Number	Optional - Enter a valid AS number to search.
AS Number Mode	Optional - Search for IP addresses in or not in the given AS number. Options are: ◦ In ◦ Not In

PARAMETER	DESCRIPTION
Minimum Last Seen Mode	Optional - Search for IP address seen or not before feed Start Date. Options are: ◦ Any (Ingest A records that have at least one timestamp after feed Start Date) ◦ Strict (Ingest only A records that do not have any timestamps before feed Start Date)
Maximum Last Seen Mode	Optional - Search for IP address seen or not before feed End Date. Options are: ◦ Any (Ingest A records that have at least one timestamp after feed End Date) ◦ Strict (Ingest only A records that do not have any timestamps before feed End Date)
Registrar	Optional - Enter the name or partial name of registrar used to register domains. Wildcards are not allowed, the given string is used in partial match. This is a slow search option
Certificates Issuer	Optional - Enter the SSL certificate issuer to ingest domains from. If this parameter is used, only domains from the supplied issuer will be ingested. The use of wildcards is allowed. Use the `+` symbol to represent spaces.
ASN Diversity	Optional - Enter the ASN Diversity (integer). This is an exact match.
Minimum ASN Diversity	Optional - Enter the minimum ASN Diversity limit (integer).
Maximum ASN Diversity	Optional - Enter the maximum ASN Diversity limit (integer).
IP Diversity All	Optional - IP Diversity All (integer). This is an exact match.
Minimum IP Diversity All	Optional - Enter the Minimum IP Diversity All limit (integer).

PARAMETER	DESCRIPTION
Maximum IP Diversity All	Optional - Enter the maximum IP Diversity All limit (integer).
IP Diversity Groups	Optional - Enter the IP Diversity Groups (integer). This is an exact match.
Minimum IP Diversity Groups	Optional - Enter the Minimum IP Diversity Groups limit (integer).
Maximum IP Diversity Groups	Optional - Enter the Maximum IP Diversity Groups limit (integer).
Max Pages	Enter the maximum number of pages to return. Each page contains 100 indicators. ⚠ Silent Push without any search criteria can return a large number of results.
FQDN Context	Select which pieces of context to bring in with each FQDN. Options include: ◦ ASN Diversity ◦ IP Diversity ◦ IP Diversity Groups
Fetch Related IP Addresses	Enable this parameter to ingest IP addresses associated with each FQDN.
IP Context	Select which pieces of context to bring in with each related IP Address. Options include: ◦ ASN ◦ AS Name ◦ Last Seen



‹ Silent Push Domains

Disabled Enabled

Additional Information

Integration Type: Feed

Version:

Authentication and Connection

Silent Push API Key

☑ Enable SSL Verification

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Search Configuration

Nameserver Name(Optional)

Nameserver name or wildcard pattern of nameserver used by domains

MX Server Name (Optional)

Mail Exchange server name or wildcard pattern of MX server used by domains

AS Number (Optional)

Enter a valid AS number to search

AS Number Mode (Optional): In

Search for IP addresses in or not in the given AS number

Minimum Last Seen Mode (Optional): Strict (Ingest only A records that do not have any timestamps before feed Start Date)

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

Silent Push Domains

The Silient Push Domains feed ingests FQDN and their associated IP Addresses from Silent Push.

`GET https://api.silentpush.com/api/v1/merge-api/explore/domain/search`

Sample Request Parameters:

```
{
  "with_metadata": "1",
  "timeline": "1",
  "prefer": "result",
  "max_wait": "25",
  "last_seen_min": "2024-12-01",
  "last_seen_max": "2024-12-03",
  "last_seen_min_mode": "strict",
  "last_seen_max_mode": "strict",
  "ip_diversity_all_min": "5"
}
```

Sample Response:

```
{
  "status_code": 200,
  "error": null,
  "response": {
    "metadata": {
      "job_id": "e274b7e9-bf7e-4037-8236-377a180f885a",
      "query_name": "padns/search/ipdiversity",
      "results_returned": 100,
      "results_total_at_least": 104,
      "timestamp": 1733402483,
      "with_metadata": 1
    },
    "records": [
      {
        "asn_diversity": 18,
        "host": "0-168.com.a.bdydns.com",
        "ip_diversity_all": 38,
        "ip_diversity_groups": 8,
        "timeline": [
          {
            "asn": 38283,
            "asname": "CHINANET-SCIDC-AS-AP CHINANET SiChuan Telecom Internet
Data",
            "first_seen": "2022-08-25 20:23:44",
            "ip": "182.140.225.35",
            "last_seen": "2024-11-29 03:08:16"
          },
          {
            "asn": 4134,
            "asname": "CHINANET-BACKBONE No.31,Jin-rong Street, CN",
            "first_seen": "2024-07-01 04:29:52",
            "ip": "121.14.156.35",
            "last_seen": "2024-12-01 14:07:01"
          }
        ]
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

> This mapping is based on each item within the `.response.records` from the HTTP response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.host`	Indicator	FQDN	N/A	`0-168.com.a.bdydns.com`	N/A
`.asn_diversity`	Indicator.Attribute	ASN Diversity	N/A	`18`	Updatable
`.ip_diversity_all`	Indicator.Attribute	IP Diversity	N/A	`38`	Updatable
`.ip_diversity_groups`	Indicator.Attribute	IP Diversity Groups	N/A	`8`	Updatable
`.timeline.ip`	Related Indicator	IP Address	`.timeline.first_seen`	`182.140.225.35`	N/A
`.timeline.asname`	Related Indicator Attribute	AS Name	`.timeline.first_seen`	`CHINANET-SCID-AS-AP CHINANET...`	N/A
`.timeline.asn`	Related Indicator Attribute	ASN	`.timeline.first_seen`	`38283`	N/A
`.timeline.last_seen`	Related Indicator Attribute	Last Seen	`.timeline.first_seen`	`2024-11-29 03:08:16`	Updatable

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	2 minutes
Indicators	206
Indicator Attributes	424

Known Issues / Limitations

- API usage is limited to your Silent Push API rate limit. Users should be aware of their limit and adjust the Max Pages configuration parameter accordingly. A request will be made for each page.

> ⚠ ThreatQuotient highly recommends using the search configuration parameters to ingest your selected data as Silent Push returns large amounts of data.

Change Log

- **Version 1.0.0**
    - Initial release