ThreatQuotient

Silent Push Action

Version 1.0.0

November 12, 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	>= 5.20.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Silent Push action for ThreatQ enables analysts to use Silent Push's APIs for enrichment. Analysts are able to enrich IOCs from their Threat Library with context from the Silent Push API including, but not limited to, the function and risk level of a domain, IPv4, or IPv6.

The integration provides the following action:

- **Silent Push Enrichment** - fetches information from Silent Push.

The action is compatible with the following indicator types:

- FQDN
- IP Address
- IPv6 Address

The action returns enriched indicator objects.

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
  - FQDN
  - IP Address
  - IPv6 Address

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

    > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

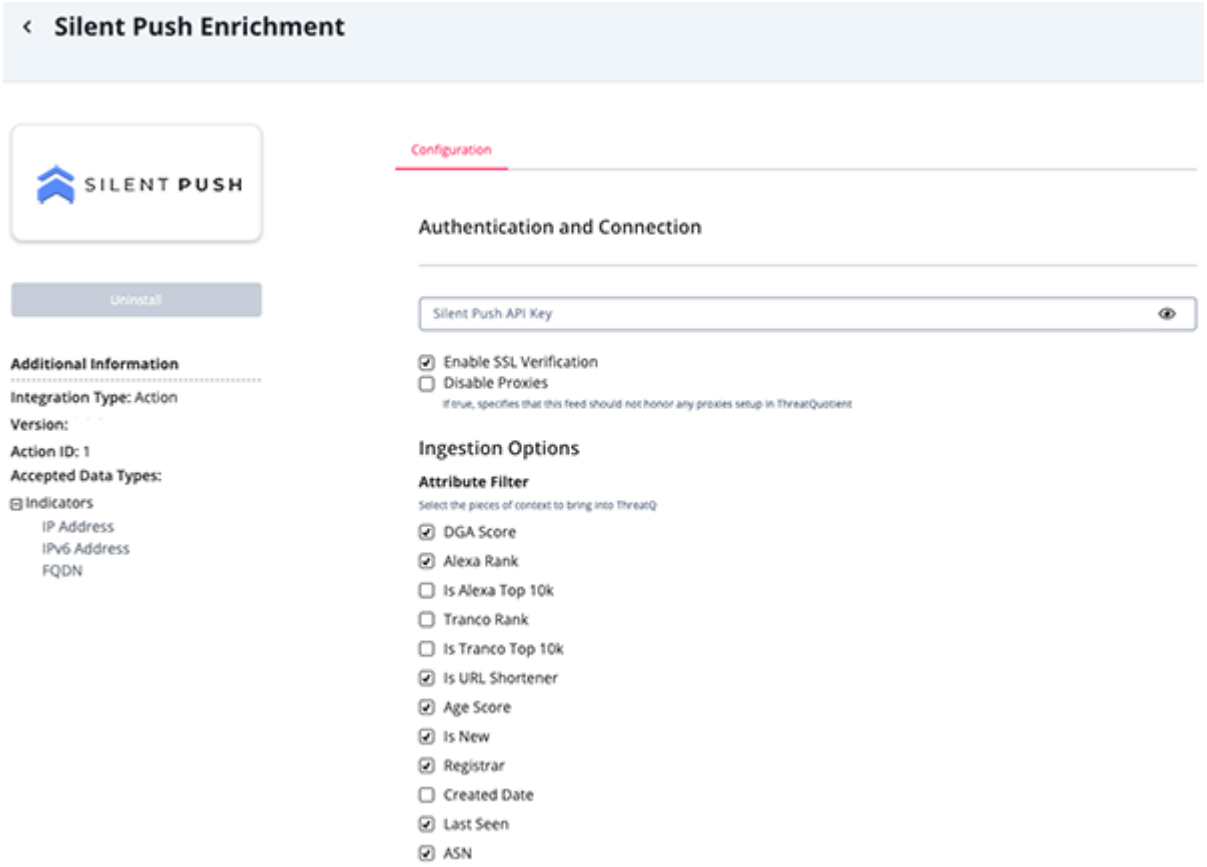
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Silent Push API Key	Enter the API Key to connect to Silent Push API.
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Attribute Filter	Select the pieces of context to bring into ThreatQ. Options include: ◦ DGA Score ◦ Alexa Rank ◦ Is Alexa Top 10k ◦ Tranco Rank ◦ Is Tranco Top 10k ◦ Is URL Shortener ◦ Age Score ◦ Is New ◦ Registrar ◦ IP Diversity ◦ Listing Score ◦ Listing Span ◦ Threat Feed ◦ NS Reputation Score ◦ Domain Density ◦ Listed Domains ◦ Entropy Score

PARAMETER	DESCRIPTION
	◦ Created Date ◦ Last Seen ◦ ASN ◦ ASN Diversity ◦ AS Name ◦ ASN Rank Score ◦ ASN Takedown Reputation Score ◦ ASN Reputation Score ◦ Entropy ◦ Density ◦ SP Risk Score ◦ Certificate Issuer ◦ Is Expired ◦ Reputation Score ◦ Country Code ◦ Country ◦ Is DSL Dynamic
Domain Related Objects Filter	Select the related objects to ingest into ThreatQ for FQDNs. Options include: ◦ x509 Serial ◦ IP Address ◦ Name Server
IP Address Related Objects Filter	Select the related objects to ingest into ThreatQ for IP Addresses. Options include: ◦ x509 Serial ◦ Subnet
IPv6 Address Related Objects Filter	Select the related objects to ingest into ThreatQ for IPv6 Addresses. Currently, the only option is **x509 Serial**.
Objects Per Run	The number of objects to process per run of the workflow.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Silent Push Enrichment	Queries data regarding IoCs against Silent Push.	Indicator	IP Address, IPv6 Address, FQDN

Silent Push Enrichment

The Silent Push Enrichment action queries indicators against Silent Push and enriches them with the returned data.

FQDN Enrichment

```
POST https://app.silentpush.com/api/v1/merge-api/explore/bulk/summary/domain
```

Request Parameters:

```
{
  "explain": 1,
  "scan_data": 1
}
```

Request Body:

```
{
  "domains": [
    "facebook.com"
  ]
}
```

Sample Response:

```
{
  "error": null,
  "response": [
    {
      "domain_string_frequency_probability": {
        "avg_probability": 5.221,
        "dga_probability_score": 0,
        "domain": "facebook.com",
        "domain_string_freq_probabilities": [
          6.336,
          4.106
        ],
        "query": "facebook.com"
      },
      "domain_urls": {
        "results_summary": {
          "actors": {
            "unknown": 12
          },
          "alexa_rank": 2,
          "alexa_top10k": true,
          "alexa_top10k_score": 100,
          "dynamic_domain_score": 0,
          "is_dynamic_domain": false,
```

```
        "is_url_shortener": false,
        "match_type": "same_domain",
        "results": 12,
        "tranco_rank": 3,
        "tranco_top10k": true,
        "tranco_top10k_score": 100,
        "url_shortener_score": 0,
        "verdicts": {
          "phishing": 11,
          "unknown": 1
        }
      }
    },
    "domaininfo": {
      "age_score": 0,
      "domain": "facebook.com",
      "info": "Domain registered before 20170101",
      "is_new": false,
      "is_new_score": 0,
      "last_seen": 20241106,
      "query": "facebook.com",
      "registrar": "RegistrarSafe, LLC",
      "whois_age": 10083,
      "whois_created_date": "1997-03-29 05:00:00",
      "zone": "com"
    },
    "host_flags": [
      {
        "domain": "facebook.com",
        "host_has_expired_certificate": false,
        "host_has_open_directory": false,
        "host_has_open_s3_bucket": false
      }
    ],
    "ip_diversity": {
      "asn_diversity": "1",
      "asns": [
        32934
      ],
      "host": "facebook.com",
      "ip_diversity_all": "16",
      "ip_diversity_groups": "16"
    },
    "is_private_suffix": false,
    "listing_score": 25,
    "listing_score_explain": {
      "listed_recent_ago": 113,
      "listed_first_ago": 357,
      "listed_recent": 20240716,
      "listed_first": 20231115,
```

```
      "listed_span": 245,
      "listings_all": 245,
      "listings_last_7": 0,
      "listings_last_30": 0,
      "listings_last_90": 0,
      "listings_last_180": 67,
      "listings_last_365": 245
    },
    "listing_score_feeds_explain": [
      {
        "feed_short_name": "assortedthreatsdomains",
        "listed_recent_ago": 113,
        "listed_first_ago": 357,
        "listed_recent": 20240716,
        "listed_first": 20231115,
        "listed_span": 245,
        "listings_all": 245,
        "listings_last_7": 0,
        "listings_last_30": 0,
        "listings_last_90": 0,
        "listings_last_180": 67,
        "listings_last_365": 245
      }
    ],
    "ns_reputation": {
      "is_expired": false,
      "is_parked": false,
      "is_sinkholed": false,
      "ns_reputation_max": 8,
      "ns_reputation_score": 8,
      "ns_srv_reputation": [
        {
          "domain": "facebook.com",
          "ns_server": "a.ns.facebook.com",
          "ns_server_domain_density": 4562,
          "ns_server_domains_listed": 2,
          "ns_server_reputation": 8
        },
        {
          "domain": "facebook.com",
          "ns_server": "b.ns.facebook.com",
          "ns_server_domain_density": 4562,
          "ns_server_domains_listed": 2,
          "ns_server_reputation": 8
        },
        {
          "domain": "facebook.com",
          "ns_server": "c.ns.facebook.com",
          "ns_server_domain_density": 4562,
          "ns_server_domains_listed": 2,
```

```
          "ns_server_reputation": 8
        },
        {
          "domain": "facebook.com",
          "ns_server": "d.ns.facebook.com",
          "ns_server_domain_density": 4562,
          "ns_server_domains_listed": 2,
          "ns_server_reputation": 8
        }
      ]
    },
    "nschanges": {
      "results_summary": {
        "changes_0_7_days": 0,
        "changes_30_90_days": 0,
        "changes_7_30_days": 0,
        "changes_last_30_days": 0,
        "changes_last_7_days": 0,
        "changes_last_90_days": 0,
        "domain": "facebook.com",
        "has_change_circular": false,
        "has_change_expire_from": false,
        "has_change_expire_to": false,
        "has_change_ns_in_domain_from": true,
        "has_change_ns_in_domain_to": true,
        "has_change_ns_srv_domain_density_low_from": false,
        "has_change_ns_srv_domain_density_low_to": false,
        "has_change_parked_from": false,
        "has_change_parked_to": false,
        "has_change_sinkhole_from": false,
        "has_change_sinkhole_to": false,
        "last_change": 20200116,
        "last_change_circular_to": false,
        "last_change_days_ago": 1756,
        "last_change_expire_from": false,
        "last_change_expire_to": false,
        "last_change_ns_in_domain_from": true,
        "last_change_ns_in_domain_to": true,
        "last_change_ns_srv_domain_density_low_from": false,
        "last_change_ns_srv_domain_density_low_to": false,
        "last_change_parked_from": false,
        "last_change_parked_to": false,
        "last_change_sinkhole_from": false,
        "last_change_sinkhole_to": false,
        "ns_entropy": 1,
        "ns_entropy_score": 1,
        "num_changes_all": 1,
        "query": "facebook.com"
      }
    },
```

```
    "private_suffix_info": {},
    "scan_data": {
      "certificates": [
        {
          "domain": "facebook.com",
          "domains": [
            "*.facebook.com",
            "*.facebook.net",
            "*.fbcdn.net",
            "*.fbsbx.com",
            "*.m.facebook.com",
            "*.messenger.com",
            "*.xx.fbcdn.net",
            "*.xy.fbcdn.net",
            "*.xz.fbcdn.net",
            "facebook.com",
            "messenger.com"
          ],
          "fingerprint_sha1": "da8270146f4b6bd925fde5fd22327db46b6fb8a9",
          "hostname": "www.facebook.com",
          "ip": "31.13.66.35",
          "is_expired": false,
          "issuer_common_name": "DigiCert SHA2 High Assurance Server CA",
          "issuer_organization": "DigiCert Inc",
          "not_after": "2024-11-13 23:59:59",
          "not_before": "2024-08-15 00:00:00",
          "scan_date": "2024-11-06 08:33:57",
          "serial_number": "107859008574815897819802270060605892 92"
        }
      ],
      "favicon": [
        {
          "favicon2_md5": "",
          "favicon2_mmh3": "",
          "favicon2_path": "",
          "favicon_md5": "3e764f0f737767b30a692fab1de3ce49",
          "favicon_mmh3": -560962771,
          "hostname": "www.facebook.com",
          "ip": "31.13.66.35",
          "scan_date": "2024-11-06 08:33:57"
        }
      ],
      "headers": [
        {
          "headers": {
            "cache-control": "private, no-cache, no-store, must-revalidate",
            "connection": "keep-alive",
            "content-encoding": "zstd",
            "content-length": "854",
            "content-type": "text/html; charset=\"utf-8\"",
```

```
              "expires": "Sat, 01 Jan 2000 00:00:00 GMT",
              "server": ""
            },
            "hostname": "www.facebook.com",
            "ip": "31.13.66.35",
            "response": 400,
            "scan_date": "2024-11-06 08:33:57"
          }
        ],
        "html": [
          {
            "hostname": "www.facebook.com",
            "html_body_murmur3": -1874931165,
            "html_body_ssdeep": "24:hzIZ0/
m0jyj1spszZivaO01Gr4nBQB6FAicrMwmTy1w4RR5hUg5MLv:+Zh0Oosi6vUuA4Aw4AgOL",
            "html_title": "Error",
            "ip": "31.13.66.35",
            "scan_date": "2024-11-06 08:33:57"
          }
        ],
        "jarm": [
          {
            "hostname": "www.facebook.com",
            "ip": "31.13.66.35",
            "jarm_hash":
"27d27d27d0000001dc41d43d00041d1c5ac8aa552261ba8fd1aa9757c06fa5",
            "scan_date": "2024-11-06 08:33:57"
          }
        ]
      },
      "sp_risk_score": 8,
      "sp_risk_score_explain": {
        "sp_risk_score_decider": "ns_reputation_score"
      }
    }
  ],
  "status_code": 200
}
```

ThreatQuotient provides the following default mapping for this action:

> Mappings are based on each of the items within the `.response[]` JSON path.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.domaininfo.domain`	Indicator.Value	FQDN	.domaininfo.whois_created_date	facebook.com	N/A
`.domain_string_frequency_probability.dga_probability_score`	Indicator.Attribute	DGA Score	.domaininfo.whois_created_date	0	User-configurable. Updatable
`.domain_urls.results_summary.alexa_rank`	Indicator.Attribute	Alexa Rank	.domaininfo.whois_created_date	2	User-configurable. Updatable
`.domain_urls.results_summary.alexa_top10k`	Indicator.Attribute	Is Alexa Top 10k	.domaininfo.whois_created_date	True	User-configurable. Updatable.
`.domain_urls.results_summary.tranco_rank`	Indicator.Attribute	Tranco Rank	.domaininfo.whois_created_date	3	User-configurable. Updatable
`.domain_urls.results_summary.tranco_top10k`	Indicator.Attribute	Is Tranco Top 10k	.domaininfo.whois_created_date	True	User-configurable. Updatable.
`.domain_urls.results_summary.is_url_shortener`	Indicator.Attribute	Is URL Shortener	.domaininfo.whois_created_date	False	User-configurable. Updatable.
`.domaininfo.age_score`	Indicator.Attribute	Age Score	.domaininfo.whois_created_date	0	User-configurable. Updatable
`.domaininfo.is_new`	Indicator.Attribute	Is New	.domaininfo.whois_created_date	False	User-configurable. Updatable
`.domaininfo.registrar`	Indicator.Attribute	Registrar	.domaininfo.whois_created_date	RegistrarSafe, LLC	User-configurable
`.domaininfo.whois_created_date`	Indicator.Attribute	Created Date	.domaininfo.whois_created_date	1997-03-29 05:00:00	User-configurable
`.domaininfo.last_seen`	Indicator.Attribute	Last Seen	.domaininfo.whois_created_date	2024-11-06 00:00:00	User-configurable. Updatable. Converted to timestamp.
`.ip_diversity.asns[]`	Indicator.Attribute	ASN	.domaininfo.whois_created_date	32934	User-configurable
`.ip_diversity.asn_diversity`	Indicator.Attribute	ASN Diversity	.domaininfo.whois_created_date	1	User-configurable. Updatable
`.ip_diversity.ip_diversity_all`	Indicator.Attribute	IP Diversity	.domaininfo.whois_created_date	16	User-configurable. Updatable
`.listing_score`	Indicator.Attribute	Listing Score	.domaininfo.whois_created_date	0	User-configurable. Updatable
`.listing_score_explain.listed_span`	Indicator.Attribute	Listing Span	.domaininfo.whois_created_date	245	User-configurable. Updatable
`.listing_score_feeds_explain[].feed_short_name`	Indicator.Attribute	Threat Feed	.domaininfo.whois_created_date	assortedthreatsdomains	User-configurable.
`.ns_reputation.ns_reputation_score`	Indicator.Attribute	NS Reputation Score	.domaininfo.whois_created_date	8	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.ns_reputation.ns_srv_reputation[].ns_server`	Related Indicator.Value	FQDN	N/A	a.ns.facebook.com	User-configurable.
`.ns_reputation.ns_srv_reputation[].ns_server_domain_density`	Related Indicator.Attribute	Domain Density	N/A	4562	User-configurable. Updatable
`.ns_reputation.ns_srv_reputation[].ns_server_domains_listed`	Related Indicator.Attribute	Listed Domains	N/A	2	User-configurable. Updatable
`.ns_reputation.ns_srv_reputation[].ns_server_reputation`	Related Indicator.Attribute	NS Reputation Score	N/A	8	User-configurable. Updatable
`.nschanges.results_summary.ns_entropy_score`	Indicator.Attribute	Entropy Score	.domaininfo.whois_created_date	1	User-configurable. Updatable
`.nschanges.results_summary.ns_entropy`	Indicator.Attribute	Entropy	.domaininfo.whois_created_date	1	User-configurable. Updatable
`.sp_risk_score`	Indicator.Attribute	SP Risk Score	.domaininfo.whois_created_date	8	User-configurable. Updatable
`.scan_data.certificates[].serial_number`	Related Indicator.Value	x509 Serial	N/A	1078590085748158978198022700606058929 2	User-configurable.
`.scan_data.certificates[].domains`	Related Indicator.Description	N/A	N/A	N/A	N/A
`.scan_data.certificates[].issuer_organization`	Related Indicator.Attribute	Certificate Issuer	N/A	DigiCert Inc	User-configurable.
`.scan_data.certificates[].is_expired`	Related Indicator.Attribute	Is Expired	N/A	False	User-configurable. Updatable
`.scan_data.certificates[].ip`	Related Indicator.Value	IP Address	N/A	31.13.66.35	User-configurable.

IP Address Enrichment

`POST https://app.silentpush.com/api/v1/merge-api/explore/bulk/summary/ipv4`

Request Parameters:

```
{
  "explain": 1,
  "scan_data": 1
}
```

Request Body:

```
{
  "ips": [
    "194.67.71.191"
  ]
}
```

Sample Response:


```
{
  "status_code": 200,
  "error": null,
  "response": [
    {
      "ip": "194.67.71.191",
      "asn": 197695,
      "asname": "AS-REG, RU",
      "asn_allocation_date": 20110328,
      "asn_allocation_age": 4972,
      "asn_rank": 0,
      "asn_rank_score": 0,
      "asn_reputation": 9,
      "asn_reputation_score": 9,
      "asn_reputation_explain": {
        "ips_in_asn": 110592,
        "ips_num_listed": 1,
        "ips_num_active": 50294
      },
      "malscore": 0,
      "asn_takedown_reputation": 0,
      "asn_takedown_reputation_explain": {},
      "asn_takedown_reputation_score": 0,
      "date": 20241106,
      "subnet": "194.67.71.0/24",
      "subnet_allocation_date": 19940712,
      "subnet_allocation_age": 11075,
      "subnet_reputation": 0,
      "subnet_reputation_explain": {},
      "subnet_reputation_score": 0,
      "ip_reputation": 74,
```

```
    "ip_reputation_explain": {
      "ip_density": 3722,
      "names_num_listed": 462
    },
    "ip_reputation_score": 74,
    "ip_location": {
      "country_code": "RU",
      "country_name": "Russia",
      "country_is_in_european_union": false,
      "continent_code": "EU",
      "continent_name": "Europe"
    },
    "ip_is_dsl_dynamic": false,
    "ip_is_dsl_dynamic_score": 0,
    "ip_ptr": "",
    "benign_info": {
      "known_benign": false,
      "actor": "",
      "tags": []
    },
    "sinkhole_info": {
      "known_sinkhole_ip": false,
      "tags": []
    },
    "ip_is_tor_exit_node": false,
    "ip_is_ipfs_node": false,
    "ip_has_open_directory": false,
    "ip_has_expired_certificate": false,
    "density": 3570,
    "listing_score": 100,
    "listing_score_explain": {
      "listed_recent_ago": 0,
      "listed_first_ago": 147,
      "listed_recent": 20241106,
      "listed_first": 20240612,
      "listed_span": 148,
      "listings_all": 146,
      "listings_last_7": 7,
      "listings_last_30": 30,
      "listings_last_90": 88,
      "listings_last_180": 146,
      "listings_last_365": 146
    },
    "listing_score_feeds_explain": [
      {
        "feed_short_name": "bulletproofhostingipranges",
        "listed_recent_ago": 0,
        "listed_first_ago": 147,
        "listed_recent": 20241106,
        "listed_first": 20240612,
```

```
        "listed_span": 148,
        "listings_all": 146,
        "listings_last_7": 7,
        "listings_last_30": 30,
        "listings_last_90": 88,
        "listings_last_180": 146,
        "listings_last_365": 146
      }
    ],
    "sp_risk_score": 74,
    "sp_risk_score_explain": {
      "sp_risk_score_decider": "ip_reputation"
    },
    "scan_data": {
      "certificates": [
        {
          "fingerprint_sha1": "",
          "scan_date": "2024-11-06 12:12:49",
          "ip": "194.67.71.191",
          "hostname": "",
          "domain": "",
          "domains": [],
          "issuer_common_name": "",
          "issuer_organization": "",
          "not_before": "",
          "not_after": "",
          "is_expired": false,
          "serial_number": ""
        }
      ],
      "jarm": [
        {
          "jarm_hash": "",
          "scan_date": "2024-11-06 12:12:49",
          "ip": "194.67.71.191",
          "hostname": ""
        }
      ],
      "favicon": [
        {
          "scan_date": "2024-11-06 12:12:49",
          "ip": "194.67.71.191",
          "hostname": "",
          "favicon_md5": "c79cecb75624b00f9e69b603e79bb4bd",
          "favicon_mmh3": 1281472986,
          "favicon2_md5": "",
          "favicon2_mmh3": "",
          "favicon2_path": ""
        }
      ],
```

```
        "headers": [
          {
            "scan_date": "2024-11-06 12:12:49",
            "ip": "194.67.71.191",
            "hostname": "",
            "response": 200,
            "headers": {
              "server": "nginx",
              "content-type": "text/html",
              "content-encoding": "gzip",
              "connection": "keep-alive"
            }
          }
        ],
        "html": [
          {
            "scan_date": "2024-11-06 12:12:49",
            "ip": "194.67.71.191",
            "hostname": "",
            "html_title": "Срок регистрации домена 194.67.71.191 истёк",
            "html_body_ssdeep":
"192:pQPM+A4oV0bGaQD9MBvFopCPEsACQavf+xypnKHerCy+mnPTR9+6:N+Toeaydopm2Cd+4rrdn7
D",
            "html_body_murmur3": -1435763211
          }
        ]
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action:

> Mappings are based on each of the items within the `.response[]` JSON path.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.ip`	Indicator.Value	IP Address	.asn_allocation_date	194.67.71.191	N/A
`.asn`	Indicator.Attribute	ASN	.asn_allocation_date	197695	User-configurable
`.asname`	Indicator.Attribute	AS Name	.asn_allocation_date	AS-REG, RU	User-configurable
`.asn_rank_score`	Indicator.Attribute	ASN Rank Score	.asn_allocation_date	0	User-configurable. Updatable
`.asn_reputation_score`	Indicator.Attribute	ASN Reputation Score	.asn_allocation_date	9	User-configurable. Updatable
`.asn_takedown_reputation_score`	Indicator.Attribute	ASN Takedown Reputation Score	.asn_allocation_date	0	User-configurable. Updatable
`.subnet`	Related Indicator.Value	CIDR Block	.subnet_allocation_date	194.67.71.0/24	User-configurable
`.subnet_reputation_score`	Related Indicator.Attribute	Reputation Score	.subnet_allocation_date	0	User-configurable. Updatable
`.ip_reputation_score`	Indicator.Attribute	Reputation Score	.asn_allocation_date	74	User-configurable. Updatable
`.ip_location.country_code`	Indicator.Attribute	Country Code	.asn_allocation_date	RU	User-configurable.
`.ip_location.country_name`	Indicator.Attribute	Country	.asn_allocation_date	Russia	User-configurable.
`.ip_is_dsl_dynamic`	Indicator.Attribute	Is DSL Dynamic	.asn_allocation_date	False	User-configurable. Updatable
`.listing_score`	Indicator.Attribute	Listing Score	.asn_allocation_date	100	User-configurable. Updatable
`.listing_score_explain.listed_span`	Indicator.Attribute	Listing Span	.asn_allocation_date	148	User-configurable. Updatable
`.listing_score_feeds_explain[].feed_short_name`	Indicator.Attribute	Threat Feed	.asn_allocation_date	bulletproofhostingipranges	User-configurable.
`.density`	Indicator.Attribute	Density	.asn_allocation_date	3570	User-configurable. Updatable
`.sp_risk_score`	Indicator.Attribute	SP Risk Score	.asn_allocation_date	74	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.scan_data.certificates[].serial_number`	Related Indicator.Value	x509 Serial	N/A	N/A	User-configurable.
`.scan_data.certificates[].domains`	Related Indicator.Description	N/A	N/A	N/A	N/A
`.scan_data.certificates[].issuer_organization`	Related Indicator.Attribute	Certificate Issuer	N/A	N/A	User-configurable.
`.scan_data.certificates[].is_expired`	Related Indicator.Attribute	Is Expired	N/A	False	User-configurable. Updatable

IPv6 Address Enrichment

`POST https://app.silentpush.com/api/v1/merge-api/explore/bulk/ip2asn/ipv6`

Request Parameters:

```
{
  "explain": 1,
  "scan_data": 1
}
```

Request Body:

```
{
  "ips": [
    "2a02:4780:37:b262:f807:71a8:e3ee:9b64"
  ]
}
```

Sample Response:


```
{
  "status_code": 200,
  "error": null,
  "response": {
    "ip2asn": [
      {
        "asn": 47583,
        "asn_allocation_age": 4967,
        "asn_allocation_date": 20110404,
        "asn_rank": 0,
        "asn_rank_score": 0,
        "asn_reputation": 100,
        "asn_reputation_explain": {
          "ips_in_asn": 415232,
          "ips_num_active": 0,
          "ips_num_listed": 3
        },
        "asn_reputation_score": 100,
        "asn_takedown_reputation": 0,
        "asn_takedown_reputation_explain": {},
        "asn_takedown_reputation_score": 0,
        "asname": "AS-HOSTINGER, CY",
        "date": 20241108,
        "density": 0,
        "ip": "2a02:4780:37:b262:f807:71a8:e3ee:9b64",
        "ip_is_ipfs_node": false,
        "sp_risk_score": 100,
        "sp_risk_score_explain": {
          "sp_risk_score_decider": "asn_reputation"
        },
        "subnet": "2a02:4780:37::/48",
```

```
        "scan_data": []
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.ip`	Indicator.Value	IPv6 Address	.asn_allocation_date	2a02:4780:37:b262:f807:71a8:e3ee:9b64	N/A
`.asn`	Indicator.Attribute	ASN	.asn_allocation_date	47583	User-configurable
`.asname`	Indicator.Attribute	AS Name	.asn_allocation_date	AS-HOSTINGER, CY	User-configurable
`.asn_rank_score`	Indicator.Attribute	ASN Rank Score	.asn_allocation_date	0	User-configurable. Updatable
`.asn_reputation_score`	Indicator.Attribute	ASN Reputation Score	.asn_allocation_date	100	User-configurable. Updatable
`.asn_takedown_reputation_score`	Indicator.Attribute	ASN Takedown Reputation Score	.asn_allocation_date	0	User-configurable. Updatable
`.density`	Indicator.Attribute	Density	.asn_allocation_date	0	User-configurable. Updatable
`.sp_risk_score`	Indicator.Attribute	SP Risk Score	.asn_allocation_date	100	User-configurable. Updatable
`.scan_data.certificates[].serial_number`	Related Indicator.Value	x509 Serial	N/A	N/A	User-configurable.
`.scan_data.certificates[].domains`	Related Indicator.Description	N/A	N/A	N/A	N/A
`.scan_data.certificates[].issuer_organization`	Related Indicator.Attribute	Certificate Issuer	N/A	N/A	User-configurable.
`.scan_data.certificates[].is_expired`	Related Indicator.Attribute	Is Expired	N/A	N/A	User-configurable. Updatable

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	2 minutes
Indicators	600
Indicator Attributes	4,800

Use Case Example

1. A Threat Analyst identifies a collection of indicators they would like to enrich with Silent Push data.
2. The Threat Analyst adds the Silent Push Enrichment Action to a Workflow.
3. The Threat Analyst configures the action with the desired parameters, and enables the Workflow.
4. The Workflow executes all Actions in the graph, including Silent Push Enrichment.
5. The action ingests all the attributes found for the input values.

Known Issues / Limitations

- API usage is limited to your Silent Push API rate limit. Be conscious of that limit, and adjust the Objects Per Run configurations accordingly. For each 100 indicators a maximum of 3 API requests are made.

Change Log

- **Version 1.0.0**
  - Initial release