ThreatQuotient

A Securonix Company

Censys Operation

Version 2.0.0

March 02, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	2.0.0
Compatible with ThreatQ Versions	>= 5.15.0
Support Tier	ThreatQ Supported

Introduction

The Censys Operation enriches ThreatQ objects with context obtained from the Censys API.

The operation provides the following actions:

- **Submit IP** - submits a selected IP Address for analysis.
- **Submit Domain** - submits a selected domain for analysis.
- **Submit Hash** - submits a selected hash for analysis.

The operation is compatible with the following indicator types:

- FQDN
- IP Address
- SHA-256

Prerequisites

The following is required to run the integration:

- A Censys Personal Access Token - this can be found on you Censys account under My Account > Personal Access Tokens.
- A Censys Organization ID - this can be found on you Censys account under My Account.

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

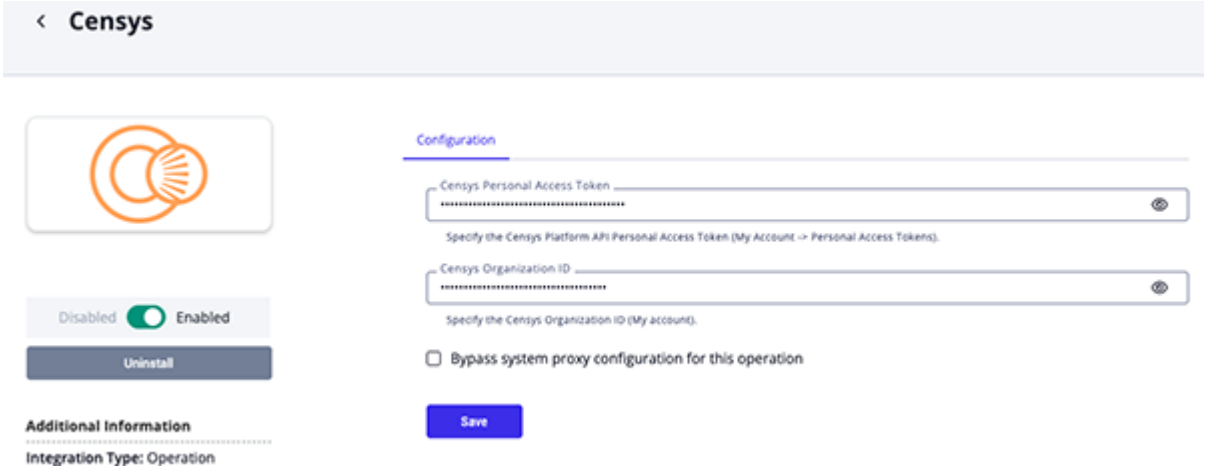
Configuration

> 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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Censys Personal Access Token	Enter your Censys Platform API Personal Access Token.
Censys Organization ID	Enter your Censys Organization ID.



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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Submit IP	Submits IP for analysis.	Indicator	IP
Submit Domain	Submits domain for analysis.	Indicator	FQDN
Submit Hash	Submits hash for analysis.	Indicator	SHA-256

Submit IP

The Submit IP action submits an ip address for analysis.

`GET https://api.platform.censys.io/v3/global/asset/host/{{ip}}`

Sample Response:


```
{
  "result": {
    "resource": {
      "ip": "1.1.1.1",
      "location": {
        "continent": "Oceania",
        "country": "Australia",
        "country_code": "AU",
        "city": "Brisbane",
        "postal_code": "9010",
        "timezone": "Australia/Brisbane",
        "province": "Queensland"
      },
      "autonomous_system": {
        "asn": 13335,
        "description": "CLOUDFLARENET - Cloudflare, Inc.",
        "bgp_prefix": "1.1.1.0/24",
        "name": "CLOUDFLARENET - Cloudflare, Inc.",
        "country_code": "US"
      },
      "operating_system": {
        "vendor": "Red Hat",
        "product": "Enterprise Linux",
        "uniform_resource_identifier": "cpe:2.3:o:redhat:enterprise_linux:7:*:*:*:*:*:*:*"
      },
      "services": [
        {
          "port": 80,
          "protocol": "HTTP",
          "transport_protocol": "tcp",
          "software": [
            {
              "vendor": "cloudflare",
              "product": "cloudflare_load_balancer",
              "cpe": "cpe:2.3:a:cloudflare:cloudflare_load_balancer:*:*:*:*:*:*:*:*"
            }
          ],
          "labels": [
            {
              "value": "WAF"
            }
          ],
          "banner_hashes": [
            "sha256:446a6087825fa73eadb045e5a2e9e2adf7df241b571228187728191d961dda1f"
          ],
          "http": {
            "response": {
              "body_hashes": [
                "sha256:446a6087825fa73eadb045e5a2e9e2adf7df241b571228187728191d961dda1f"
              ],
              "favicons": {
                "hashes": [
                  "sha256:446a6087825fa73eadb045e5a2e9e2adf7df241b571228187728191d961dda1f"
                ]
              }
```

```
          }
        },
        "jarm": {
          "fingerprint": "27d27d27d00027d00042d43d00041df04c41293ba84f6efe3a613b22f983e6"
        },
        "tls": {
          "ja3s": "d75f9129bb5d05492a65ff78e081bcb2",
          "ja4s": "t130200_1303_234ea6891581",
          "certificates": {
            "leaf_data": {
              "names": [
                "google.com"
              ]
            }
          }
        }
      }
    ],
    "dns": {
      "reverse_dns": {
        "names": [
          "one.one.one.one"
        ]
      },
      "names": [
        "one.one.one.one"
      ]
    },
    "labels": [
      "remote-access"
    ]
  }
 }
}
```


ThreatQ provides the following default mapping for this operation action:

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.resource.autonomous_system.country_code	Indicator.Attribute	Network Country Code	US	N/A
.result.resource.autonomous_system.name	Indicator.Attribute	Network	CLOUDFLARENET - Cloudflare, Inc.	N/A
.result.resource.autonomous_system.bgp_prefix	Indicator.Attribute	BGP Prefix	1.1.1.0/24	N/A
.result.resource.autonomous_system.description	Indicator.Attribute	Description	CLOUDFLARENET - Cloudflare, Inc.	N/A
.result.resource.autonomous_system.asn	Indicator.Attribute	ASN	13335	N/A
.result.resource.location.postal_code	Indicator.Attribute	Postal Code	9010	N/A
.result.resource.location.timezone	Indicator.Attribute	Timezone	Australia/Brisbane	N/A
.result.resource.location.province	Indicator.Attribute	Province	Queensland	N/A
.result.resource.location.country_code	Indicator.Attribute	Country Code	AU	N/A

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.resource.location.continent	Indicator.Attribute	Continent	Oceania	N/A
.result.resource.location.city	Indicator.Attribute	City	Brisbane	N/A
.result.resource.location.country	Indicator.Attribute	Country	Australia	N/A
.result.resource.operating_system.vendor	Indicator.Attribute	Vendor	Red Hat	N/A
.result.resource.operating_system.product	Indicator.Attribute	Product	Enterprise Linux	N/A
.result.resource.operating_system.uniform_resource_identifier	Indicator.Attribute	CPE	cpe:2.3:o:redhat:enterprise_linux:7:*:*:*:*:*:*:*	N/A
.result.resource.dns.names	Related Indicator.Value	FQDN	one.one.one.one	N/A
.result.resource.dns.reverse_dns.names	Related Indicator.Value	FQDN	one.one.one.one	N/A
.result.resource.services[].tls.certificates.leaf_data.names	Related Indicator.Value	FQDN	google.com	Values validated as FQDN. Entries that are IP literals are converted to IP Address/IPv6 Address indicators.
.result.resource.services[].labels	Indicator.Attribute	Tag	WAF	N/A
.result.resource.services[].port	Indicator.Attribute	Service Port	80	N/A
.result.resource.services[].protocol	Indicator.Attribute	Service Protocol	HTTP	N/A
.result.resource.services[].transport_protocol	Indicator.Attribute	Service Transport	tcp	N/A
.result.resource.services[].software.vendor	Indicator.Attribute	Service Vendor	cloudflare	N/A
.result.resource.services[].software.product	Indicator.Attribute	Service Product	cloudflare_load_balancer	N/A
.result.resource.services[].software.cpe	Indicator.Attribute	Service CPE	cpe:2.3:a:cloudflare:cloudflare_load_balancer:*	N/A
.result.resource.services[].banner_hashes	Related Indicator.Value	SHA-256/MD5/SHA-1/Hash ION	446a6087825fa73e...	See the Hash Logic Mapping Table
.result.resource.services[].http.response.body_hashes	Related Indicator.Value	SHA-256/MD5/SHA-1/Hash ION	446a6087825fa73e...	See the Hash Logic Mapping Table
.result.resource.services[].http.response.favicons.hashes	Related Indicator.Value	SHA-256/MD5/SHA-1/Hash ION	446a6087825fa73e...	See the Hash Logic Mapping Table

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.result.resource.services[].jarm.fingerprint`	Related Fingerprint Indicator.Value	Hash ION	`27d27d27d00027d...`	N/A
`.result.resource.services[].tls.ja3s`	Related Fingerprint Indicator.Value	Hash ION	`d75f9129bb5d05492a65ff78e081bcb2`	N/A
`.result.resource.services[].tls.ja4s`	Related Fingerprint Indicator.Value	Hash ION	`t130200_1303_234ea6891581`	N/A
`.result.resource.labels`	Indicator.Attribute	Tag	`remote-access`	N/A

Hash Logic Mapping Table

The following tables illustrates hash mapping logic from Censys to ThreatQ.

PREFIX	TARGET INDICATOR TYPE	EXAMPLE
`md5`	MD5	`49532cbc459e8e7ceb1249f5fdbab31c`
`sha1`	SHA-1	`7436e0b4b1f8c222c38069890b75fa2baf9ca620`
`sha256`	SHA-256	`9a2e3208b3b63b0f17c1e901a31bb8f1efa50fb21e5260583af2f6e9e4ef9ba8`
`phash`	Hash ION	`904e5baf3b54324b`
`tlsh`	Hash ION	`46a2623386099470ad747eafcba7750d80f8f19288c357c4e4ad0d65dd6ef0a3a5b298`

Submit Domain

The Submit Domain action submits a selected domain for analysis.

`POST https://api.platform.censys.io/v3/global/search/query`

Sample Body:

```
{
  "query": "web.hostname=google.com"
}
```

Sample Response:


```
{
  "result": {
    "hits": [
      {
        "webproperty_v1": {
          "resource": {
            "hostname": "google.com",
            "port": 443,
            "scan_time": "2026-02-25T00:08:29Z",
            "software": [
              {
                "vendor": "google",
                "product": "google_web_services",
                "cpe": "cpe:2.3:a:google:google_web_services:*:*:*:*:*:*:*:*"
              }
            ],
            "endpoints": [
              {
                "ip": "74.125.202.100",
                "banner_hash_sha256": "54f536037940b0c56b477cce7912ba1c209905a36b6be4f4f0301551407c417a"
              }
            ],
            "cert": {
              "names": [
                "google.com"
              ],
              "fingerprint_sha1": "fc294d585ee67445800c2cfe142f15e5f55219fc",
              "fingerprint_md5": "fce4197f1b3ed1409d707be058f4cf86",
              "fingerprint_sha256": "977eca18f030b2d8f5c6f872e1cf30b5ceea5dcf26ac0bbbcf1723e233e05612",
              "tbs_fingerprint_sha256": "dc4460f296f53cf272611c861a2df814edb7bbf7914b4eb52fa8296c720231fc",
              "tbs_no_ct_fingerprint_sha256": "a5c9302f1e11dc513e860f090c6c6f5eb20da295161567ae3eeaf1db9fb5a0f5",
              "spki_fingerprint_sha256": "148782892d0c4fc01005265504b2f1757893d02e12b2f0f4aaad6286195f780d",
              "parent_spki_fingerprint_sha256": "95b148afc4c249d314067527813d43973574f8e11a905040c881510026ae74f9",
              "spki_subject_fingerprint_sha256": "148782892d0c4fc01005265504b2f1757893d02e12b2f0f4aaad6286195f780d",
              "parent_spki_subject_fingerprint_sha256":
"95b148afc4c249d314067527813d43973574f8e11a905040c881510026ae74f9",
              "parsed": {
                "subject": {
                  "common_name": [
                    "*.google.com"
                  ]
                },
                "issuer_dn": "C=US, O=Google Trust Services, CN=WR2",
                "validity_period": {
                  "not_before": "2026-01-26T08:39:20Z",
                  "not_after": "2026-04-20T08:39:19Z"
                }
              }
            }
```

```
        }
      }
    }
  ]
 }
}
```

ThreatQ provides the following default mapping for this operation action:

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.hits[].webproperty_v1.resource.hostname	Related Indicator.Value	FQDN	google.com	N/A
.result.hits[].webproperty_v1.resource.endpoints.ip	Related Indicator.Value	IP Address	74.125.202.100	N/A
.result.hits[].webproperty_v1.resource.endpoints.banner_hash_sha256	Related Indicator.Value	SHA-256	54f536037940b0c56b477cce7912ba1c209905a36b6be4f4f0301551407c417a	N/A
.result.hits[].webproperty_v1.resource.cert.names	Related Indicator.Value	FQDN	google.com	N/A
.result.hits[].webproperty_v1.resource.cert.fingerprint_sha1	Related Indicator.Value	SHA-1	fc294d585ee67445800c2cfe142f15e5f55219fc	N/A
.result.hits[].webproperty_v1.resource.cert.fingerprint_md5	Related Indicator.Value	MD5	fce4197f1b3ed1409d707be058f4cf86	N/A
.result.hits[].webproperty_v1.resource.cert.fingerprint_sha256	Related Indicator.Value	SHA-256	977eca18f030b2d8f5c6f872e1cf30b5ceea5dcf26ac0bbbcf1723e233e05612	N/A
.result.hits[].webproperty_v1.resource.cert.tbs_fingerprint_sha256	Related Indicator.Value	SHA-256	dc4460f296f53cf272611c861a2df814edb7bbf7914b4eb52fa8296c720231fc	N/A
.result.hits[].webproperty_v1.resource.cert.tbs_no_ct_fingerprint_sha256	Related Indicator.Value	SHA-256	a5c9302f1e11dc513e860f090c6c6f5eb20da295161567ae3eeaf1db9fb5a0f5	N/A
.result.hits[].webproperty_v1.resource.cert.spki_fingerprint_sha256	Related Indicator.Value	SHA-256	148782892d0c4fc01005265504b2f1757893d02e12b2f0f4aaad6286195f780d	N/A
.result.hits[].webproperty_v1.resource.cert.parent_spki_fingerprint_sha256	Related Indicator.Value	SHA-256	95b148afc4c249d314067527813d43973574f8e11a905040c881510026ae74f9	N/A
.result.hits[].webproperty_v1.resource.cert.spki_subject_fingerprint_sha256	Related Indicator.Value	SHA-256	148782892d0c4fc01005265504b2f1757893d02e12b2f0f4aaad6286195f780d	N/A
.result.hits[].webproperty_v1.resource.cert.parent_spki_subject_fingerprint_sha256	Related Indicator.Value	SHA-256	95b148afc4c249d314067527813d43973574f8e11a905040c881510026ae74f9	N/A
.result.hits[].webproperty_v1.resource.cert.parsed.subject.common_name	Indicator.Attribute	Common Name	*.google.com	N/A

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.hits[].webproperty_v1.resource.cert.parsed.issuer_dn	Indicator.Attribute	Issuer Distinguished Name	C=US, O=Google Trust Services, CN=WR2	N/A
.result.hits[].webproperty_v1.resource.cert.parsed.validity_period.not_before	Indicator.Attribute	Cert Not Before	2026-01-26T08:39:20Z	N/A
.result.hits[].webproperty_v1.resource.cert.parsed.validity_period.not_after	Indicator.Attribute	Cert Not After	2026-04-20T08:39:19Z	N/A
.result.hits[].webproperty_v1.resource.port	Indicator.Attribute	Port	443	N/A
.result.hits[].webproperty_v1.resource.scan_time	Indicator.Attribute	Scan Time	2026-02-25T00:08:29Z	N/A
.result.hits[].webproperty_v1.resource.software.cpe	Indicator.Attribute	CPE	cpe:2.3:a:google:google_web_services:*:*:*:*:*:*:*:*	N/A
.result.hits[].webproperty_v1.resource.software.vendor	Indicator.Attribute	Vendor	google	N/A
.result.hits[].webproperty_v1.resource.software.product	Indicator.Attribute	Product	google_web_services	N/A

Submit Hash

The Submit Hash submits the selected hash for analysis.

`GET https://api.platform.censys.io/v3/global/asset/certificate/{{hash}}`

Sample Response:


```
{
  "result": {
    "resource": {
      "fingerprint_sha1": "d508e7f8163fb67434f84091dc7c2ca8afd5234d",
      "fingerprint_md5": "3818d99263b47ab28f7de5b293ee1418",
      "tbs_fingerprint_sha256": "4b098b6bd9459340fb0f3cfb80f0bc3283370c455d57ca20da40e7eecce341d5",
      "tbs_no_ct_fingerprint_sha256": "5c095a40e76c245323086d26d1fa428d3b443b42fb58c7dbb19b32dfe516b749",
      "spki_subject_fingerprint_sha256": "754cb1e2e2088214a5970662bb5a60aec8a2e29b94f53529aa608abee6682c60",
      "parent_spki_subject_fingerprint_sha256": "390bc358202771a65e7be7a87924d7f2a079de04feb5ffd4163fae4fbf9b11e9",
      "added_at": "2022-12-31T12:37:55Z",
      "validated_at": "2022-12-31T12:37:55Z",
      "ever_seen_in_scan": true,
      "parse_status": "success",
      "parsed": {
        "issuer_dn": "C=US, O=Let's Encrypt, CN=R3",
        "validity_period": {
          "not_before": "2022-12-31T11:37:55Z",
          "not_after": "2023-03-31T11:37:54Z"
        },
        "serial_number": "311703586789118042424998420179537559397550",
        "signature": {
          "self_signed": null,
          "signature_algorithm": {
            "name": "SHA256-RSA",
            "oid": "1.2.840.113549.1.1.11"
          },
          "value": "95347a7bd89da6a6bd9adcc509669d933b5e2a29..."
        },
        "extensions": {
          "subject_alt_name": {
            "dns_names": [
              "kgcontracting.co",
              "www.kgcontracting.co"
            ]
          },
          "key_usage": {
            "key_encipherment": true,
            "digital_signature": true
          },
          "extended_key_usage": {
            "server_auth": true,
            "client_auth": true
          },
          "authority_info_access": {
            "ocsp_urls": [
              "http://r3.o.lencr.org"
            ],
            "issuer_urls": [
              "http://r3.i.lencr.org/"
            ]
          }
        },
        "subject": {
          "common_name": [
            "www.kgcontracting.co"
```

```
        ]
      },
      "subject_key_info": {
        "key_algorithm": {
          "name": "RSA"
        },
        "rsa": {
          "length": 2048,
          "modulus": "c0b3b7d595e250fcbc54c6f9e81113c12da29fe3..."
        }
      }
    },
    "validation": {
      "apple": {
        "had_trusted_path": true
      },
      "microsoft": {
        "had_trusted_path": true
      },
      "nss": {
        "had_trusted_path": true
      },
      "chrome": {
        "had_trusted_path": true
      }
    },
    "ct": {
      "entries": {
        "google_argon_2023": {
          "index": 2161615293,
          "added_to_ct_at": "2026-02-16T01:40:24Z"
        },
        "google_xenon_2023": {
          "index": 1991771848,
          "added_to_ct_at": "2026-02-16T01:43:07Z"
        }
      }
    }
  }
 }
}
```


ThreatQ provides the following default mapping for this operation action:

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
`.result.resource.added_at`	`Indicator.Attribute`	`Added At`	`2022-12-31T12:37:55Z`	`N/A`
`.result.resource.validated_at`	`Indicator.Attribute`	`Validated At`	`2022-12-31T12:37:55Z`	`N/A`
`.result.resource.ever_seen_in_scan`	`Indicator.Attribute`	`Ever Seen In Scan`	`true`	`N/A`
`.result.resource.parse_status`	`Indicator.Attribute`	`Parse Status`	`success`	`N/A`
`.result.resource.parsed.issuer_dn`	`Indicator.Attribute`	`Issuer Distinguished Name`	`C=US, O=Let's Encrypt, CN=R3`	`N/A`
`.result.resource.parsed.validity_period.not_before`	`Indicator.Attribute`	`Cert Not Before`	`2022-12-31T11:37:55Z`	`N/A`

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.resource.parsed.validity_period.not_after	Indicator.Attribute	Cert Not After	2023-03-31T11:37:54Z	N/A
.result.resource.parsed.serial_number	Indicator.Attribute	Serial Number	311703586789118042424998420179537559397550	N/A
.result.resource.parsed.signature.self_signed	Indicator.Attribute	Self Signed	null	N/A
.result.resource.parsed.signature.signature_algorithm.name	Indicator.Attribute	Signature Algorithm Name	SHA256-RSA	N/A
.result.resource.parsed.signature.signature_algorithm.oid	Indicator.Attribute	Signature Algorithm OID	1.2.840.113549.1.1.11	N/A
.result.resource.parsed.signature.value	Indicator.Attribute	Signature	95347a7bd89da6a6bd9adcc509669d933b5e2a29...	N/A
.result.resource.parsed.extensions.subject_alt_name.dns_names	Indicator.Attribute	DNS Names	kgcontracting.co	N/A
.result.resource.validation.apple.had_trusted_path	Indicator.Attribute	Browser Trust Apple	true	N/A
.result.resource.validation.microsoft.had_trusted_path	Indicator.Attribute	Browser Trust Microsoft	true	N/A
.result.resource.validation.nss.had_trusted_path	Indicator.Attribute	Browser Trust Mozilla NSS	true	N/A
.result.resource.validation.chrome.had_trusted_path	Indicator.Attribute	Browser Trust Chrome	true	N/A
.result.resource.parsed.subject.common_name	Indicator.Attribute	Common Name	www.kgcontracting.co	N/A
.result.resource.parsed.subject_key_info.key_algorithm.name	Indicator.Attribute	Key Type	RSA	N/A
.result.resource.parsed.subject_key_info.rsa.length	Indicator.Attribute	Key Length	2048	N/A
.result.resource.parsed.subject_key_info.rsa.modulus	Indicator.Attribute	Modulus	c0b3b7d595e250fcbc54c6f9e81113c12da29fe3...	N/A
.result.resource.parsed.extensions.key_usage.key_encipherment	Indicator.Attribute	Key Encipherment	true	N/A
.result.resource.parsed.extensions.key_usage.digital_signature	Indicator.Attribute	Digital Signature	true	N/A
.result.resource.parsed.extensions.extended_key_usage.server_auth	Indicator.Attribute	Server Auth	true	N/A
.result.resource.parsed.extensions.extended_key_usage.client_auth	Indicator.Attribute	Client Auth	true	N/A
.result.resource.parsed.extensions.authority_info_access.ocsp_urls	Indicator.Attribute	AIA Paths OCSP	http://r3.o.lencr.org	N/A
.result.resource.parsed.extensions.authority_info_access.issuer_urls	Indicator.Attribute	AIA Paths Issuer	http://r3.i.lencr.org/	N/A
.result.resource.ct.entries.google_argon_2023.index	Indicator.Attribute	Certificate Transparency Argon	2161615293	N/A

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.resource.ct.entries.google_argon_2023.added_to_ct_at	Indicator.Attribute	Certificate Transparency Argon Date	2026-02-16T01:40:24Z	N/A
.result.resource.ct.entries.google_xenon_2023.index	Indicator.Attribute	Certificate Transparency Xenon	1991771848	N/A
.result.resource.ct.entries.google_xenon_2023.added_to_ct_at	Indicator.Attribute	Certificate Transparency Xenon Date	2026-02-16T01:43:07Z	N/A
.result.resource.fingerprint_sha1	Related Indicator.Value	SHA-1	d508e7f8163fb67434f84091dc7c2ca8afd5234d	N/A
.result.resource.fingerprint_md5	Related Indicator.Value	MD5	3818d99263b47ab28f7de5b293ee1418	N/A
.result.resource.tbs_fingerprint_sha256	Related Indicator.Value	SHA-256	4b098b6bd9459340fb0f3cfb80f0bc3283370c455d57ca20da40e7eecce341d5	N/A
.result.resource.tbs_no_ct_fingerprint_sha256	Related Indicator.Value	SHA-256	5c095a40e76c245323086d26d1fa428d3b443b42fb58c7dbb19b32dfe516b749	N/A
.result.resource.spki_subject_fingerprint_sha256	Related Indicator.Value	SHA-256	754cb1e2e2088214a5970662bb5a60aec8a2e29b94f53529aa608abee6682c60	N/A
.result.resource.parent_spki_subject_fingerprint_sha256	Related Indicator.Value	SHA-256	390bc358202771a65e7be7a87924d7f2a079de04feb5ffd4163fae4fbf9b11e9	N/A

Change Log

- **Version 2.0.0**
  - Updated the integration to leverage the Censys v3 API endpoints and incorporated additional attributes based on the revised API response structure.
  - Added the following new configuration parameters for authentication:
    - **Censys Personal Access Token**
    - **Censys Organization ID**
  - Removed the following authentication-related configuration parameters:
    - **API Key**
    - **API Secret**
- **Version 1.2.0**
  - Service labels are now mapped to Tag attributes. Banner data is preserved, and banner, body, and favicon hashes are normalized and ingested as related indicators, ensuring these fields are consistently captured.
  - DNS and FQDN coverage has been enhanced. Both forward (`dns.names`) and reverse DNS records are now ingested as related FQDN indicators, ensuring all hostnames associated with an IP address—including those previously omitted—are returned.
  - A new fingerprint section has been introduced to surface service JARM fingerprints and TLS JA3S/JA4S values, which are ingested as Hash ION indicators with the corresponding fingerprint type.
  - The minimum supported ThreatQ version has been updated to 5.15.0.
- **Version 1.1.0**
  - Updated the API version and endpoints utilized by the operation.
    - Updated the ingested data samples and mapping tables.
- **Version 1.0.0**
  - Initial release