ThreatQuotient

Censys Action

Version 1.0.0

February 18, 2025

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	>= 6.5.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Censys Action integration enriches ThreatQ indicators with context obtained from the Censys API that can be used to proactively protect an organization against advanced threat actors.

The integration provides the following action:

- **Censys Enrichment** - ingests data about indicators of compromise related to network activity.

The action is compatible with and returns the 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 indicator objects.
- A Censys Search API App ID.
- A Censys API Secret.

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:

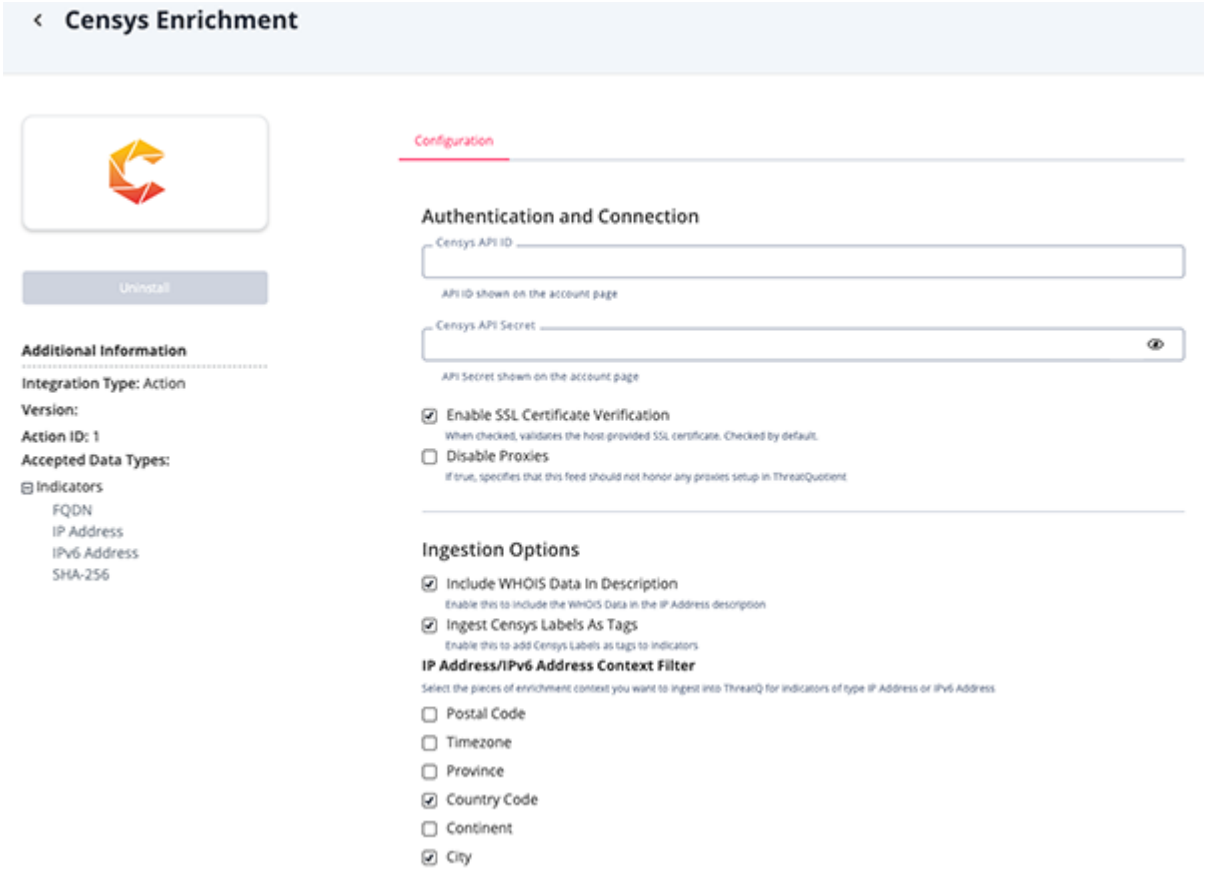
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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
Censys API ID	Your Censys API ID.
Censys API Secret	Your Census API Secret.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Include WHOIS Data In Description	Enable this to include the WHOIS Data in the IP Address description.
Ingest Censys Labels As Tags	Enable this to add Censys Labels as tags to indicators.

PARAMETER	DESCRIPTION
IP Address/IPv6 Address Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for IP Address or IPv6 Address type indicators. Options include: ◦ Postal Code ◦ Timezone ◦ Province ◦ Country Code (default) ◦ Continent ◦ City (default) ◦ Country ◦ Network Country Code ◦ AS Name (default) ◦ BGP Prefix ◦ Description ◦ ASN (default) ◦ Vendor ◦ Product ◦ CPE ◦ Source
Certificates Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for SHA-256 type indicators. Options include: ◦ Issuer Distinguished Name (default) ◦ Serial Number (default) ◦ Self Signed ◦ Valid Signature ◦ Signature Algorithm Name ◦ Signature Algorithm OID ◦ Signature ◦ DNS Name (default) ◦ Browser Trust Apple ◦ Browser Trust Microsoft ◦ Browser Trust Mozilla NSS ◦ Browser Trust Chrome ◦ Common Name ◦ Key Type (default) ◦ Key Length ◦ Modulus ◦ Key Encipherment ◦ Digital Signature ◦ Server Auth ◦ Client Auth ◦ Is Certificate Authority ◦ AIA Paths OCSP ◦ AIA Paths Issuer ◦ Certificate Transparency Argon ◦ Certificate Transparency Argon Date ◦ Certificate Transparency Xenon ◦ Certificate Transparency Xenon Date ◦ Valid Until ◦ Valid From
Certificates Relationship Filter	Select which relationship context to ingest into ThreatQ for SHA-256 type indicators. Options include:

PARAMETER	DESCRIPTION
	◦ Fingerprint SHA-1 (default) ◦ Fingerprint MD5 (default) ◦ TBS Fingerprint SHA-256 ◦ TBS No CT Fingerprint SHA-256 ◦ SPKI Fingerprint SHA-256 ◦ Parent SPKI Fingerprint SHA-256
Objects per run	Maximum number of objects to process per-run.



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
Censys Enrichment	Enriches indicators with Censys data	Indicator	FQDN, IP Address, IPv6 Address, SHA-256

Censys Enrichment

This integration queries indicators contained in a threat-library collection against Censys Search API. The API Mapping depends on the indicator type.

IP Address, IPv6 Address

`GET https://search.censys.io/api/v2/hosts/194.28.226.169`

Sample Response:


```
{
  "code": 200,
  "status": "OK",
  "result": {
    "ip": "194.28.226.169",
    "services": [
      {
        "_decoded": "ftp",
        "_encoding": {
          "banner": "DISPLAY_UTF8",
          "banner_hex": "DISPLAY_HEX"
        },
        "banner": "220 (vsFTPd 3.0.2)\r\n",
        "banner_hashes": [

"sha256:be807b6c864510e24fcd790176022670a059784cdb11dbad8edca428037bcabb"
        ],
        "banner_hex": "32323020287673465450642033 2e302e32290d0a",
        "discovery_method": "IPV4_WALK_FULL_PRIORITY_1",
        "extended_service_name": "FTP",
        "ftp": {
          "_encoding": {
            "banner": "DISPLAY_UTF8",
            "auth_tls_response": "DISPLAY_UTF8",
            "auth_ssl_response": "DISPLAY_UTF8"
          },
          "banner": "220 (vsFTPd 3.0.2)\r\n",
          "auth_tls_response": "530 Please login with USER and PASS.\r\n",
          "auth_ssl_response": "530 Please login with USER and PASS.\r\n",
          "status_code": 220,
          "status_meaning": "Service ready for new user.",
          "implicit_tls": false
        },
        "labels": [
          "file-sharing"
        ],
        "observed_at": "2023-08-21T02:24:56.795849172Z",
        "perspective_id": "PERSPECTIVE_TATA",
```

```
        "port": 21,
        "service_name": "FTP",
        "software": [
          {
            "uniform_resource_identifier":
"cpe:2.3:a:vsftpd_project:vsftpd:3.0.2:*:*:*:*:*:*:*",
            "part": "a",
            "vendor": "vsFTPd Project",
            "product": "vsFTPd",
            "version": "3.0.2",
            "other": {
              "family": "vsFTPd"
            },
            "source": "OSI_APPLICATION_LAYER"
          }
        ],
        "source_ip": "167.94.138.36",
        "transport_fingerprint": {
          "raw": "28960,64,true,MSTNW,1408,false,false"
        },
        "transport_protocol": "TCP",
        "truncated": false
      }
    ],
    "location": {
      "continent": "Europe",
      "country": "Germany",
      "country_code": "DE",
      "city": "Frankfurt am Main",
      "postal_code": "60313",
      "timezone": "Europe/Berlin",
      "province": "Hesse",
      "coordinates": {
        "latitude": 50.1153,
        "longitude": 8.6823
      }
    },
    "location_updated_at": "2023-08-20T00:09:53.056505Z",
    "autonomous_system": {
      "asn": 201671,
      "description": "AS-NUXTCLOUD",
      "bgp_prefix": "194.28.226.0/24",
      "name": "AS-NUXTCLOUD",
      "country_code": "GB"
    },
    "autonomous_system_updated_at": "2023-08-20T00:09:53.056626Z",
    "operating_system": {
      "uniform_resource_identifier":
"cpe:2.3:o:redhat:enterprise_linux:7:*:*:*:*:*:*:*",
      "part": "o",
```

```
      "vendor": "Red Hat",
      "product": "Enterprise Linux",
      "version": "7",
      "other": {
        "family": "Linux"
      }
    },
    "dns": {
      "reverse_dns": {
        "names": [
          "google.com"
        ],
        "resolved_at": "2023-08-19T11:46:51.655505631Z"
      }
    },
    "last_updated_at": "2023-08-22T03:44:55.321Z",
    "labels": [
      "remote-access",
      "email",
      "file-sharing"
    ],
    "whois": {
      "network": {
        "allocation_type": "ALLOCATION",
        "cidrs": [
          "148.72.164.0/22",
          "148.72.168.0/21",
          "148.72.176.0/23"
        ],
        "created": "2015-10-26T00:00:00Z",
        "handle": "VIG-97",
        "name": "velia.net",
        "updated": "2024-10-21T00:00:00Z"
      },
      "organization": {
        "abuse_contacts": [
          {
            "email": "net-arin@velia.net",
            "handle": "HOSTM2182-ARIN",
            "name": "hostmaster"
          }
        ],
        "admin_contacts": [
          {
            "email": "net-arin@velia.net",
            "handle": "HOSTM2182-ARIN",
            "name": "hostmaster"
          }
        ],
        "city": "Hanau",
```

```
        "country": "DE",
        "handle": "VIG-97",
        "name": "velia.net",
        "postal_code": "63452",
        "street": "Hessen-Homburg-Platz 1",
        "tech_contacts": [
          {
            "email": "net-arin@velia.net",
            "handle": "HOSTM2182-ARIN",
            "name": "hostmaster"
          }
        ]
      }
    }
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.result.autonomous_system.country_code	Indicator.Attribute	Network Country Code	N/A	GB	User-configurable
.result.autonomous_system.name	Indicator.Attribute	AS Name	N/A	AS-NUXTCLOUD	User-configurable
.result.autonomous_system.bgp_prefix	Indicator.Attribute	BGP Prefix	N/A	194.28.226.0/24	User-configurable
.result.autonomous_system.description	Indicator.Attribute	Description	N/A	AS-NUXTCLOUD	User-configurable
.result.autonomous_system.asn	Indicator.Attribute	ASN	N/A	201671	User-configurable
.result.location.postal_code	Indicator.Attribute	Postal Code	N/A	60313	User-configurable
.result.location.timezone	Indicator.Attribute	Timezone	N/A	Europe/Berlin	User-configurable
.result.location.province	Indicator.Attribute	Province	N/A	Hesse	User-configurable
.result.location.country_code	Indicator.Attribute	Country Code	N/A	DE	User-configurable
.result.location.continent	Indicator.Attribute	Continent	N/A	Europe	User-configurable
.result.location.city	Indicator.Attribute	City	N/A	Frankfurt am Main	User-configurable
.result.location.country	Indicator.Attribute	Country	N/A	Germany	User-configurable
.result.dns.reverse_dns.names	Related Indicator.Value	FQDN	N/A	google.com	N/A
.result.operating_system.vendor	Indicator.Attribute	Vendor	N/A	Red Hat	User-configurable
.result.operating_system.product	Indicator.Attribute	Product	N/A	Enterprise Linux	User-configurable
.result.operating_system.uniform_resource_identifier	Indicator.Attribute	CPE	N/A	`cpe:2.3:o:redhat:enterprise_linux:7:*:*:*:*:*:*:*`	User-configurable
.result.labels	Indicator.Tag	N/A	N/A	email	User-configurable
.result.whois.network.name	Indicator.Description	N/A	N/A	velia.net	Concatenated with the other values.
.result.whois.network.created	Indicator.Description	N/A	N/A	2015-10-26T00:00:00Z	Concatenated with the other values.
.result.whois.network.updated	Indicator.Description	N/A	N/A	2024-10-21T00:00:00Z	Concatenated with the other values.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.result.whois.network.organization.abuse_contacts[].email	Indicator.Description	N/A	N/A	net-arin@velia.net	Concatenated with the other values.
.result.whois.network.organization.admin_contacts[].email	Indicator.Description	N/A	N/A	net-arin@velia.net	Concatenated with the other values.
.result.whois.network.organization.tech_contacts[].email	Indicator.Description	N/A	N/A	net-arin@velia.net	Concatenated with the other values.
.result.whois.network.organization.city	Indicator.Description	N/A	N/A	Hanau	Concatenated with the other values.
.result.whois.network.organization.country	Indicator.Description	N/A	N/A	DE	Concatenated with the other values.
.result.whois.network.organization.name	Indicator.Description	N/A	N/A	velia.net	Concatenated with the other values.
.result.whois.network.organization.postal_code	Indicator.Description	N/A	N/A	63452	Concatenated with the other values.
.result.whois.network.organization.state	Indicator.Description	N/A	N/A	N/A	Concatenated with the other values.
.result.whois.network.organization.street	Indicator.Description	N/A	N/A	Hessen-Homburg-Platz 1	Concatenated with the other values.

FQDN

`GET https://search.censys.io/api/v2/hosts/search?q=google.com`

Sample Response:


```
{
  "code": 200,
  "status": "OK",
  "result": {
    "query": "google.com",
    "total": 1055920,
    "duration": 629,
    "hits": [
      {
        "autonomous_system": {
          "country_code": "RU",
          "name": "SPACENET-AS Internet Service Provider",
          "description": "SPACENET-AS Internet Service Provider",
          "bgp_prefix": "62.173.128.0/19",
          "asn": 34300
        },
        "labels": [
          "remote-access",
          "email",
          "file-sharing"
        ],
        "last_updated_at": "2023-08-21T05:32:23.796Z",
        "location": {
          "postal_code": "101000",
          "timezone": "Europe/Moscow",
          "province": "Moscow",
          "country_code": "RU",
          "continent": "Europe",
          "city": "Moscow",
          "coordinates": {
            "latitude": 55.75222,
            "longitude": 37.61556
          },
          "country": "Russia"
        },
        "ip": "62.173.142.225",
        "operating_system": {
          "component_uniform_resource_identifiers": [],
          "source": "OSI_TRANSPORT_LAYER",
          "other": [],
          "part": "o",
          "product": "linux",
          "cpe": "cpe:2.3:o:*:linux:*:*:*:*:*:*:*:*"
        },
```

```
        "services": [
          {
            "service_name": "FTP",
            "transport_protocol": "TCP",
            "port": 21,
            "extended_service_name": "FTP"
          },
          {
            "transport_protocol": "TCP",
            "port": 22,
            "extended_service_name": "SSH",
            "service_name": "SSH"
          },
          {
            "certificate":
"26e97467fb89414a31953aa89f207f602b5d1acfdd939236b87b977b05029097",
            "port": 25,
            "extended_service_name": "SMTP-STARTTLS",
            "transport_protocol": "TCP",
            "service_name": "SMTP"
          }
        ],
        "dns": {
          "reverse_dns": {
            "names": [
              "host-102.45.92.175.tedata.net"
            ]
          }
        }
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.result.hits[].autonomous_system.country_code	Related Indicator.Attribute	Network Country Code	N/A	RU	User-configurable
.result.hits[].autonomous_system.name	Related Indicator.Attribute	AS Name	N/A	SPACENET-AS Internet Service Provider	User-configurable
.result.hits[].autonomous_system.bgp_prefix	Related Indicator.Attribute	BGP Prefix	N/A	62.173.128.0/19	User-configurable
.result.hits[].autonomous_system.description	Related Indicator.Attribute	Description	N/A	SPACENET-AS Internet Service Provider	User-configurable
.result.hits[].autonomous_system.asn	Related Indicator.Attribute	ASN	N/A	34300	User-configurable
.result.hits[].location.postal_code	Related Indicator.Attribute	Postal Code	N/A	101000	User-configurable
.result.hits[].location.timezone	Related Indicator.Attribute	Timezone	N/A	Europe/Moscow	User-configurable
.result.hits[].location.province	Related Indicator.Attribute	Province	N/A	Moscow	User-configurable
.result.hits[].location.country_code	Related Indicator.Attribute	Country Code	N/A	RU	User-configurable
.result.hits[].location.continent	Related Indicator.Attribute	Continent	N/A	Europe	User-configurable
.result.hits[].location.city	Related Indicator.Attribute	City	N/A	Moscow	User-configurable
.result.hits[].location.country	Related Indicator.Attribute	Country	N/A	Russia	User-configurable
.result.hits[].ip	Related Indicator.Value	IP Address/ IPv6 Address	N/A	62.173.142.225	N/A
.result.hits[].operating_system.source	Related Indicator.Attribute	Source	N/A	OSI_TRANSPORT_LAYER	User-configurable
.result.hits[].operating_system.product	Related Indicator.Attribute	Product	N/A	linux	User-configurable
.result.hits[].operating_system.vendor	Related Indicator.Attribute	Vendor	N/A	N/A	User-configurable
.result.hits[].operating_system.cpe	Related Indicator.Attribute	CPE	N/A	`cpe:2.3:o:*:linux:*:*:*:*:*:*:*:*`	User-configurable
.result.hits[].labels	Related Indicator.Tag	N/A	N/A	email	User-configurable
.result.hits[].dns.reverse_dns.names	Related Indicator.Value	FQDN	N/A	host-102.45.92.175.tedata.net	N/A

SHA-256

`GET https://search.censys.io/api/v2/certificates/9b00121b4e85d50667ded1a8aa39855771bdb67ceca6f18726b49374b41f0041`

Sample Response:


```
{
    "code": 200,
    "status": "OK",
    "result": {
        "_encoding": {
            "fingerprint_sha256": "DISPLAY_HEX",
            "fingerprint_sha1": "DISPLAY_HEX",
            "fingerprint_md5": "DISPLAY_HEX",
            "tbs_fingerprint_sha256": "DISPLAY_HEX",
            "tbs_no_ct_fingerprint_sha256": "DISPLAY_HEX",
            "spki_fingerprint_sha256": "DISPLAY_HEX",
            "parent_spki_fingerprint_sha256": "DISPLAY_HEX",
            "raw": "DISPLAY_BASE64",
            "spki_subject_fingerprint_sha256": "DISPLAY_HEX",
            "parent_spki_subject_fingerprint_sha256": "DISPLAY_HEX"
        },
        "fingerprint_sha256":
"9b00121b4e85d50667ded1a8aa39855771bdb67ceca6f18726b49374b41f0041",
        "fingerprint_sha1": "d508e7f8163fb67434f84091dc7c2ca8afd5234d",
        "fingerprint_md5": "3818d99263b47ab28f7de5b293ee1418",
        "tbs_fingerprint_sha256":
"4b098b6bd9459340fb0f3cfb80f0bc3283370c455d57ca20da40e7eecce341d5",
        "tbs_no_ct_fingerprint_sha256":
"5c095a40e76c245323086d26d1fa428d3b443b42fb58c7dbb19b32dfe516b749",
        "spki_fingerprint_sha256":
"cc9b074ebf41b484a56923d5585594967bda7a7f8b5be187ef0e7ae1ec90003c",
        "parent_spki_fingerprint_sha256":
"390bc358202771a65e7be7a87924d7f2a079de04feb5ffd4163fae4fbf9b11e9",
        "parsed": {
            "version": 3,
            "serial_number": "311703586789118042424998420179537559397550",
            "issuer_dn": "C=US, O=Let's Encrypt, CN=R3",
            "issuer": {
                "common_name": [
                    "R3"
                ],
                "country": [
                    "US"
                ],
                "organization": [
                    "Let's Encrypt"
                ]
            },
```

```
            "subject_dn": "CN=www.kgcontracting.co",
            "subject": {
                "common_name": [
                    "www.kgcontracting.co"
                ]
            },
            "subject_key_info": {
                "key_algorithm": {
                    "name": "RSA",
                    "oid": "1.2.840.113549.1.1.1"
                },
                "rsa": {
                    "exponent": 65537,
                    "_encoding": {
                        "modulus": "DISPLAY_HEX"
                    },
                    "modulus":
"c0b3b7d595e250fcbc54c6f9e81113c12da29fe35350a02b8ab769a5e43f07df7ac8ff72c482b3
e838d64e97cb3fa15e415acbcfe6758a4e7ac401b4a5294ecca6ad1b583ec2136a408524eeadca5
5ba4a8af490cb9c764efbdecbe59a4ca160905e5972548018f55194e7ac94b2153d97bd5f055d58
ad3abe0d1daa3b3c97fed490f1bb58fc5c819618891d05c32d68aeaabada321736e417f0fa58d70
93d352c1800191645d1b820f5f7c93301ab7ca78393e953b82719741b735a67ce6a63faec0ac9d2
d917f03b9fc0a0ab8012f4763c50118663af897294e85ba6e11c5ca0fd749645c2a58ddf14ad627
17b40b5e7b620d256be28789e1ebd62e8046acd",
                    "length": 2048
                },
                "_encoding": {
                    "fingerprint_sha256": "DISPLAY_HEX"
                },
                "fingerprint_sha256":
"754cb1e2e2088214a5970662bb5a60aec8a2e29b94f53529aa608abee6682c60",
                "_key": "rsa"
            },
            "validity_period": {
                "not_before": "2022-12-31T11:37:55Z",
                "not_after": "2023-03-31T11:37:54Z",
                "length_seconds": 7775999
            },
            "signature": {
                "signature_algorithm": {
                    "name": "SHA256-RSA",
                    "oid": "1.2.840.113549.1.1.11"
                },
                "_encoding": {
                    "value": "DISPLAY_HEX"
                },
                "value":
"95347a7bd89da6a6bd9adcc509669d933b5e2a29b414317d72b02c583bfadbf616f5b6977824ee
80484fe4ae0c38dbb1013d896b5a9db12fdc62296fbefbba84ed089a6e62c148cc9d1e60bfd9cf6
e7d1c8f5e0f315872618a6805e5bf48432ce2d0aac07d4ab845a7f68c1a61c3dd37c0e40c26b386
```

```
b1f37ff2fc50e6eacdc305ecd13da1c43bb1209cb13c5a6387cffb57fad81d01496b3c6499817ed
1cf1a0ef809b6b408035b5de72423c6c7f84c3a9e9513c89fa8fc49bf6f90746561ebd1b4ea22e7
557d3e505b5ecd289dbb8ce71c4d3acc2e67a27bbb12dd242c8fa512d19dc8b7bd6b88bcc6a6484
bb39c894f7b756630a10525a9ab3359030aa2ad",
                "valid": true,
                "self_signed": false
            },
            "extensions": {
                "key_usage": {
                    "digital_signature": true,
                    "key_encipherment": true,
                    "value": 5,
                    "content_commitment": false,
                    "data_encipherment": false,
                    "key_agreement": false,
                    "certificate_sign": false,
                    "crl_sign": false,
                    "encipher_only": false,
                    "decipher_only": false
                },
                "basic_constraints": {
                    "is_ca": false
                },
                "subject_alt_name": {
                    "dns_names": [
                        "kgcontracting.co",
                        "www.kgcontracting.co"
                    ]
                },
                "_encoding": {
                    "authority_key_id": "DISPLAY_HEX",
                    "subject_key_id": "DISPLAY_HEX"
                },
                "authority_key_id": "142eb317b75856cbae500940e61faf9d8b14c2c6",
                "subject_key_id": "a6a1b9ac9d0886b3b58f5faba9f42f741d9ef29d",
                "extended_key_usage": {
                    "server_auth": true,
                    "client_auth": true,
                    "apple_code_signing": false,
                    "apple_code_signing_development": false,
                    "apple_software_update_signing": false,
                    "apple_code_signing_third_party": false,
                    "apple_resource_signing": false,
                    "apple_ichat_signing": false,
                    "apple_ichat_encryption": false,
                    "apple_system_identity": false,
                    "apple_crypto_env": false,
                    "apple_crypto_production_env": false,
                    "apple_crypto_maintenance_env": false,
                    "apple_crypto_test_env": false,
                    "apple_crypto_development_env": false,
```

```
                "apple_crypto_qos": false,
                "apple_crypto_tier0_qos": false,
                "apple_crypto_tier1_qos": false,
                "apple_crypto_tier2_qos": false,
                "apple_crypto_tier3_qos": false,
                "microsoft_cert_trust_list_signing": false,
                "microsoft_qualified_subordinate": false,
                "microsoft_key_recovery_3": false,
                "microsoft_document_signing": false,
                "microsoft_lifetime_signing": false,
                "microsoft_mobile_device_software": false,
                "microsoft_smart_display": false,
                "microsoft_csp_signature": false,
                "microsoft_timestamp_signing": false,
                "microsoft_server_gated_crypto": false,
                "microsoft_sgc_serialized": false,
                "microsoft_encrypted_file_system": false,
                "microsoft_efs_recovery": false,
                "microsoft_whql_crypto": false,
                "microsoft_nt5_crypto": false,
                "microsoft_oem_whql_crypto": false,
                "microsoft_embedded_nt_crypto": false,
                "microsoft_root_list_signer": false,
                "microsoft_drm": false,
                "microsoft_drm_individualization": false,
                "microsoft_licenses": false,
                "microsoft_license_server": false,
                "microsoft_enrollment_agent": false,
                "microsoft_smartcard_logon": false,
                "microsoft_ca_exchange": false,
                "microsoft_key_recovery_21": false,
                "microsoft_system_health": false,
                "microsoft_system_health_loophole": false,
                "microsoft_kernel_mode_code_signing": false,
                "dvcs": false,
                "sbgp_cert_aa_service_auth": false,
                "eap_over_ppp": false,
                "eap_over_lan": false,
                "code_signing": false,
                "email_protection": false,
                "ipsec_end_system": false,
                "ipsec_tunnel": false,
                "ipsec_user": false,
                "time_stamping": false,
                "ocsp_signing": false,
                "ipsec_intermediate_system_usage": false,
                "netscape_server_gated_crypto": false,
                "any": false
            },
            "certificate_policies": [
```

```
                    {
                        "id": "2.23.140.1.2.1"
                    },
                    {
                        "id": "1.3.6.1.4.1.44947.1.1.1",
                        "cps": [
                            "http://cps.letsencrypt.org"
                        ]
                    }
                ],
                "authority_info_access": {
                    "ocsp_urls": [
                        "http://r3.o.lencr.org"
                    ],
                    "issuer_urls": [
                        "http://r3.i.lencr.org/"
                    ]
                },
                "signed_certificate_timestamps": [
                    {
                        "_encoding": {
                            "log_id": "DISPLAY_HEX"
                        },
                        "log_id":
"b73efb24df9c4dba75f239c5ba58f46c5dfc42cf7a9f35c49e1d098125edb499",
                        "timestamp": "2022-12-31T12:37:55Z",
                        "signature": {
                            "hash_algorithm": "SHA256",
                            "signature_algorithm": "ECDSA",
                            "_encoding": {
                                "signature": "DISPLAY_HEX"
                            },
                            "signature":
"304402203e73c9d1e7f17087b077237c715039e1d5f36cd75635df44017767227354dd7d022017
cfb6779130c48b496851d5aeb970c3b43e0fa1f31d6bc03f3338d7b8716947"
                        },
                        "version": 0
                    },
                    {
                        "_encoding": {
                            "log_id": "DISPLAY_HEX"
                        },
                        "log_id":
"e83ed0da3ef5063532e75728bc896bc903d3cbd1116beceb69e1777d6d06bd6e",
                        "timestamp": "2022-12-31T12:37:55Z",
                        "signature": {
                            "hash_algorithm": "SHA256",
                            "signature_algorithm": "ECDSA",
                            "_encoding": {
                                "signature": "DISPLAY_HEX"
```

```
                            },
                            "signature":
"30450221009c728da43c9bf4700b6d73c3b3155b5473d629d5b8f06c7335894ce61fbf3af00220
2e677d64f8e7368e39769ba45812fa3d0a2e3cce761d8e898276392d592b5475"
                        },
                        "version": 0
                    }
                ],
                "ct_poison": false
            },
            "serial_number_hex": "039403b7283199171fd9c1af1c8210f5a4ae",
            "redacted": false
        },
        "names": [
            "kgcontracting.co",
            "www.kgcontracting.co"
        ],
        "validation_level": "DV",
        "validation": {
            "nss": {
                "ever_valid": true,
                "had_trusted_path": true,
                "chains": [
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
                        "sha256fp": [

"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    },
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
                        "sha256fp": [

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    }
                ],
                "_encoding": {
                    "parents": "DISPLAY_HEX"
                },
                "parents": [
```

```
"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd"
                ],
                "type": "LEAF",
                "is_valid": false,
                "has_trusted_path": false,
                "in_revocation_set": false
            },
            "microsoft": {
                "ever_valid": true,
                "had_trusted_path": true,
                "chains": [
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
                        "sha256fp": [

"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    },
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
                        "sha256fp": [

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    }
                ],
                "_encoding": {
                    "parents": "DISPLAY_HEX"
                },
                "parents": [

"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd"
                ],
                "type": "LEAF",
                "is_valid": false,
                "has_trusted_path": false,
                "in_revocation_set": false
```

```
            },
            "apple": {
                "ever_valid": true,
                "had_trusted_path": true,
                "chains": [
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
                        "sha256fp": [

"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    },
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
                        "sha256fp": [

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    }
                ],
                "_encoding": {
                    "parents": "DISPLAY_HEX"
                },
                "parents": [

"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd"
                ],
                "type": "LEAF",
                "is_valid": false,
                "has_trusted_path": false,
                "in_revocation_set": false
            },
            "chrome": {
                "ever_valid": true,
                "had_trusted_path": true,
                "chains": [
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
```

```
                        "sha256fp": [

"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    },
                    {
                        "_encoding": {
                            "sha256fp": "DISPLAY_HEX"
                        },
                        "sha256fp": [

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd",

"96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6"
                        ]
                    }
                ],
                "_encoding": {
                    "parents": "DISPLAY_HEX"
                },
                "parents": [

"0ac730f6b3a98bab6aa97c9c4c71b34dd5599f4933630e6d24a26751bd12ebac",

"67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd"
                ],
                "type": "LEAF",
                "is_valid": false,
                "has_trusted_path": false,
                "in_revocation_set": false
            }
        },
        "ct": {
            "entries": {
                "google_xenon_2023": {
                    "index": 593655844,
                    "added_to_ct_at": "2022-12-31T12:37:55.906Z",
                    "ct_to_censys_at": "2023-06-21T10:02:57.281327695Z"
                },
                "google_argon_2023": {
                    "index": 521618614,
                    "added_to_ct_at": "2022-12-31T12:37:55.858Z",
                    "ct_to_censys_at": "2023-05-04T22:00:22.709312248Z"
                }
            }
        },
        "ever_seen_in_scan": true,
        "raw":
```

```
"MIIFPzCCBCegAwIBAgISA5QDtygxmRcf2cGvHIIQ9aSuMA0GCSqGSIb3DQEBCwUAMDIxCzAJBgNVBA
YTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQDEwJSMzAeFw0yMjEyMzExMTM3NTVaF
w0yMzAzMzExMTM3NTRaMB8xHTAbBgNVBAMTFHd3dy5rZ2NvbnRyYWN0aW5nLmNvMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwLO31ZXiUPy8VMb56BETwS2in+NTUKArirdppeQ/
B996yP9yxIKz6DjWTpfLP6FeQVrLz+Z1ik56xAG0pSlOzKatG1g+whNqQIUk7q3KVbpKivSQy5x2Tvv
ey+WaTKFgkF5ZclSAGPVRlOeslLIVPZe9XwVdWK06vg0dqjs8l/
7UkPG7WPxcgZYYiR0Fwy1orqq62jIXNuQX8PpY1wk9NSwYABkWRdG4IPX3yTMBq3yng5PpU7gnGXQbc
1pnzmpj+uwKydLZF/A7n8Cgq4AS9HY8UBGGY6+JcpToW6bhHFyg/
XSWRcKljd8UrWJxe0C157Yg0la+KHieHr1i6ARqzQIDAQABo4ICYDCCAlwwDgYDVR0PAQH/
BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQ
WBBSmobmsnQiGs7WPX6up9C90HZ7ynTAfBgNVHSMEGDAWgBQULrMXt1hWy65QCUDmH6+dixTCxjBVBg
grBgEFBQcBAQRJMEcwIQYIKwYBBQUHMAGGFWh0dHA6Ly9yMy5vLmxlbmNyLm9yZzAiBggrBgEFBQcwA
oYWaHR0cDovL3IzLmkubGVuY3Iub3JnLzAxBgNVHREEKjAoghBrZ2NvbnRyYWN0aW5nLmNvghR3d3cu
a2djb250cmFjdGluZy5jbzBMBgNVHSAERTBDMAgGBmeBDAECATA3BgsrBgEEAYLfEwEBATAoMCYGCCs
GAQUFBwIBFhpodHRwOi8vY3BzLmxldHNlbmNyeXB0Lm9yZzCCAQMGCisGAQQB1nkCBAIEgfQEgfEA7w
B1ALc++yTfnE26dfI5xbpY9Gxd/
ELPep81xJ4dCYEl7bSZAAABhWgwUWYAAAQDAEYwRAIgPnPJ0efxcIewdyN8cVA54dXzbNdWNd9EAXdn
InNU3X0CIBfPtneRMMSLSWhR1a65cMO0Pg+h8x1rwD8zONe4cWlHAHYA6D7Q2j71BjUy51covIlryQP
Ty9ERa+zraeF3fW0GvW4AAAGFaDBTWAAABAMARzBFAiEAnHKNpDyb9HALbXPDsxVbVHPWKdW48GxzNY
lM5h+/
OvACIC5nfWT45zaOOXabpFgS+j0KLjzOdh2OiYJ2OS1ZK1R1MA0GCSqGSIb3DQEBCwUAA4IBAQCVNHp
72J2mpr2a3MUJZp2TO14qKbQUMX1ysCxYO/rb9hb1tpd4JO6ASE/krgw427EBPYlrWp2xL9xiKW++
+7qE7QiabmLBSMydHmC/
2c9ufRyPXg8xWHJhimgF5b9IQyzi0KrAfUq4Raf2jBphw903wOQMJrOGsfN/
8vxQ5urNwwXs0T2hxDuxIJyxPFpjh8/7V/
rYHQFJazxkmYF+0c8aDvgJtrQIA1td5yQjxsf4TDqelRPIn6j8Sb9vkHRlYevRtOoi51V9PlBbXs0on
buM5xxNOswuZ6J7uxLdJCyPpRLRnci3vWuIvMamSEuznIlPe3VmMKEFJamrM1kDCqKt",
        "added_at": "2023-01-06T12:46:27Z",
        "modified_at": "2023-06-21T10:02:57Z",
        "validated_at": "2023-06-10T05:12:10Z",
        "parse_status": "CERTIFICATE_PARSE_STATUS_SUCCESS",
        "zlint": {
            "version": 3,
            "timestamp": "2023-06-13T05:04:17Z",
            "notices_present": true,
            "failed_lints": [
                "n_subject_common_name_included"
            ],
            "warnings_present": false,
            "errors_present": false,
            "fatals_present": false
        },
        "spki_subject_fingerprint_sha256":
"cc9b074ebf41b484a56923d5585594967bda7a7f8b5be187ef0e7ae1ec90003c",
        "parent_spki_subject_fingerprint_sha256":
"390bc358202771a65e7be7a87924d7f2a079de04feb5ffd4163fae4fbf9b11e9",
        "precert": false,
        "revoked": false,
        "labels": [
            "leaf",
            "ct",
```

```
            "ever-trusted",
            "untrusted",
            "dv",
            "was-trusted",
            "expired",
            "google-ct"
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.result.fingerprint_sha1	Related Indicator.Value	SHA-1	.added_at	d508e7f8163fb67434f84091dc7c2ca8afd5234d	User-configurable
.result.fingerprint_md5	Related Indicator.Value	MD5	.added_at	3818d99263b47ab28f7de5b293ee1418	User-configurable
.result.tbs_fingerprint_sha256	Related Indicator.Value	SHA-256	.added_at	4b098b6bd9459340fb0f3cfb80f0bc3283370c455d57ca20da40e7eecce341d5	User-configurable
.result.tbs_no_ct_fingerprint_sha256	Related Indicator.Value	SHA-256	.added_at	5c095a40e76c245323086d26d1fa428d3b443b42fb58c7dbb19b32dfe516b749	User-configurable
.result.spki_fingerprint_sha256	Related Indicator.Value	SHA-256	.added_at	cc9b074ebf41b484a56923d5585594967bda7a7f8b5be187ef0e7ae1ec90003c	User-configurable
.result.parent_spki_fingerprint_sha256	Related Indicator.Value	SHA-256	.added_at	390bc358202771a65e7be7a87924d7f2a079de04feb5ffd4163fae4fbf9b11e9	User-configurable
.result.parsed.issuer_dn	Indicator.Attribute	Issuer Distinguished Name	.added_at	C=US, O=Let's Encrypt, CN=R3	User-configurable
.result.parsed.serial_number	Indicator.Attribute	Serial Number	.added_at	311703586789118042424998420179537559397550	User-configurable
.result.parsed.signature.self_signed	Indicator.Attribute	Self Signed	.added_at	False	User-configurable. Updatable
.result.parsed.signature.valid	Indicator.Attribute	Valid Signature	.added_at	True	User-configurable. Updatable
.result.parsed.signature.signature_algorithm.name	Indicator.Attribute	Signature Algorithm Name	.added_at	SHA256-RSA	User-configurable
.result.parsed.signature.signature_algorithm.oid	Indicator.Attribute	Signature Algorithm OID	.added_at	1.2.840.113549.1.1.11	User-configurable
.result.parsed.signature.value	Indicator.Attribute	Signature	.added_at	95347a7bd89da6a6bd9adcc509669d933b5e2a29b414317d72b02c583bfad...	User-configurable
.result.parsed.extensions.subject_alt_name.dns_names	Indicator.Attribute	DNS Name	.added_at	kgcontracting.co	User-configurable
.result.validation.apple.had_trusted_path	Indicator.Attribute	Browser Trust Apple	.added_at	True	User-configurable. Updatable
.result.validation.microsoft.had_trusted_path	Indicator.Attribute	Browser Trust Microsoft	.added_at	True	User-configurable. Updatable
.result.validation.nss.had_trusted_path	Indicator.Attribute	Browser Trust Mozilla NSS	.added_at	True	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.result.validation.chrome.had_trusted_path	Indicator.Attribute	Browser Trust Chrome	.added_at	True	User-configurable. Updatable
.result.labels	Indicator.Tag	N/A	N/A	leaf	User-configurable
.result.parsed.subject.common_name	Indicator.Attribute	Common Name	.added_at	www.kgcontracting.co	User-configurable
.result.parsed.subject_key_info.key_algorithm.name	Indicator.Attribute	Key Type	.added_at	RSA	User-configurable
.result.parsed.subject_key_info.rsa.length	Indicator.Attribute	Key Length	.added_at	2048	User-configurable
.result.parsed.subject_key_info.rsa.modulus	Indicator.Attribute	Modulus	.added_at	c0b3b7d595e250fcbc54c6f9e81113c12da29fe35350a02b8ab769a5e43f07d...	User-configurable
.result.parsed.extensions.key_usage.key_encipherment	Indicator.Attribute	Key Encipherment	.added_at	True	User-configurable. Updatable
.result.parsed.extensions.key_usage.digital_signature	Indicator.Attribute	Digital Signature	.added_at	True	User-configurable. Updatable
.result.parsed.extensions.extended_key_usage.server_auth	Indicator.Attribute	Server Auth	.added_at	True	User-configurable. Updatable
.result.parsed.extensions.extended_key_usage.client_auth	Indicator.Attribute	Client Auth	.added_at	True	User-configurable. Updatable
.result.parsed.extensions.basic_constraints.is_ca	Indicator.Attribute	Is Certificate Authority	.added_at	False	User-configurable. Updatable
.result.parsed.extensions.authority_info_access.ocsp_urls	Indicator.Attribute	AIA Paths OCSP	.added_at	http://r3.i.lencr.org/	User-configurable
.result.parsed.extensions.authority_info_access.issuer_urls	Indicator.Attribute	AIA Paths Issuer	.added_at	http://r3.o.lencr.org	User-configurable
.result.ct.entries.google_argon_2023.index	Indicator.Attribute	Certificate Transparency Argon	.added_at	521618614	User-configurable
.result.ct.entries.google_argon_2023.added_to_ct_at	Indicator.Attribute	Certificate Transparency Argon Date	.added_at	2022-12-31T12:37:55.858Z	User-configurable
.result.ct.entries.google_xenon_2023.index	Indicator.Attribute	Certificate Transparency Xenon	.added_at	593655844	User-configurable
.result.ct.entries.google_xenon_2023.added_to_ct_at	Indicator.Attribute	Certificate Transparency Xenon Date	.added_at	2022-12-31T12:37:55.906Z	User-configurable
.result.parsed.validity_period.not_before	Indicator.Attribute	Valid From	.added_at	2022-12-31T11:37:55Z	User-configurable. Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.result.parsed.validity_period.not_after	Indicator.Attribute	Valid Until	.added_at	2023-03-31T11:37:54Z	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	3 minutes
Indicators	200
Indicator Attributes	5,000

Change Log

- **Version 1.0.0**
  - Initial release