ThreatQuotient

Censys Operation User Guide

Version 1.1.0

August 29, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Installation **7**
Configuration **8**
Actions **9**
submit_ip 10
submit_domain 13
submit_hash 17
Change Log **30**

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	1.1.0
Compatible with ThreatQ Versions	>= 4.34.0
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

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
API Key	Private or public Censys API key.
Username	Username associated to the API Key.

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://search.censys.io/api/v2/hosts/{{}}`

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": "323230202876734654506420332e302e32290d0a",
                "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"
        ]
    }
}
```


ThreatQ provides the following default mapping for this operation action:

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.autonomous_system.country_code	Indicator.Attribute	Network Country Code	GB	N/A
.result.autonomous_system.name	Indicator.Attribute	Network	AS-NUXTCLOUD	N/A
.result.autonomous_system.bgp_prefix	Indicator.Attribute	BGP Prefix	194.28.226.0/24	N/A
.result.autonomous_system.description	Indicator.Attribute	Description	AS-NUXTCLOUD	N/A
.result.autonomous_system.asn	Indicator.Attribute	ASN	201671	N/A
.result.location.postal_code	Indicator.Attribute	Postal Code	60313	N/A
.result.location.timezone	Indicator.Attribute	Timezone	Europe/Berlin	N/A
.result.location.province	Indicator.Attribute	Province	Hesse	N/A
.result.location.country_code	Indicator.Attribute	Country Code	DE	N/A
.result.location.continent	Indicator.Attribute	Continent	Europe	N/A
.result.location.city	Indicator.Attribute	City	Frankfurt am Main	N/A
.result.location.country	Indicator.Attribute	Country	Germany	N/A
.result.dns.reverse_dns.names	Related Indicator.Value	FQDN	google.com	N/A
.result.operating_system.vendor	Indicator.Attribute	Vendor	Red Hat	N/A
.result.operating_system.product	Indicator.Attribute	Product	Enterprise Linux	N/A
.result.operating_system.uniform_resource_identifier	Indicator.Attribute	CPE	`cpe:2.3:o:redhat:enterprise_linux:7:*:*:*:*:*:*:*`	N/A
.result.labels	Indicator.Attribute	Tag	email	N/A

submit_domain

The submit_domain action submits a selected domain for analysis.

`GET https://search.censys.io/api/v2/hosts/search?q={{domain}}`

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
                },
                "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"
                    },
                    {
                        "service_name": "DNS",
                        "port": 53,
                        "transport_protocol": "UDP",
                        "extended_service_name": "DNS"
                    },
                    {
                        "port": 80,
                        "transport_protocol": "TCP",
                        "extended_service_name": "HTTP",
                        "service_name": "HTTP"
                    },
                    {
                        "extended_service_name": "POP3",
                        "port": 110,
                        "transport_protocol": "TCP",
                        "service_name": "POP3"
                    },
                    {
                        "transport_protocol": "TCP",
                        "extended_service_name": "IMAP",
                        "service_name": "IMAP",
                        "port": 143
                    },
                    {
                        "certificate":
"0da9ea92b7a8f30a79e3c59effda579a9a016455c7e24f6db46419a0b117b6c8",
                        "transport_protocol": "TCP",
                        "extended_service_name": "SMTP-STARTTLS",
                        "service_name": "SMTP",
                        "port": 587
                    },
```

```
                    {
                        "extended_service_name": "UNKNOWN",
                        "service_name": "UNKNOWN",
                        "transport_protocol": "TCP",
                        "port": 8243
                    },
                    {
                        "transport_protocol": "TCP",
                        "extended_service_name": "HTTP",
                        "port": 9189,
                        "service_name": "HTTP"
                    }
                ],
                "dns": {
                    "reverse_dns": {
                        "names": [
                            "google.com"
                        ]
                    }
                }
            }
        ]
    }
}
```


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[].autonomous_system.country_code	Indicator.Attribute	Network Country Code	RU	N/A
.result.hits[].autonomous_system.name	Indicator.Attribute	Network	SPACENET-AS Internet Service Provider	N/A
.result.hits[].autonomous_system.bgp_prefix	Indicator.Attribute	BGP Prefix	62.173.128.0/19	N/A
.result.hits[].autonomous_system.description	Indicator.Attribute	Description	SPACENET-AS Internet Service Provider	N/A
.result.hits[].autonomous_system.asn	Indicator.Attribute	ASN	34300	N/A
.result.hits[].location.postal_code	Indicator.Attribute	Postal Code	101000	N/A
.result.hits[].location.timezone	Indicator.Attribute	Timezone	Europe/Moscow	N/A
.result.hits[].location.province	Indicator.Attribute	Province	Moscow	N/A
.result.hits[].location.country_code	Indicator.Attribute	Country Code	RU	N/A
.result.hits[].location.continent	Indicator.Attribute	Continent	Europe	N/A
.result.hits[].location.city	Indicator.Attribute	City	Moscow	N/A
.result.hits[].location.country	Indicator.Attribute	Country	Russia	N/A
.result.hits[].ip	Related Indicator.Value	IP Address/ IPv6 Address	62.173.142.225	N/A
.result.hits[].operating_system.source	Indicator.Attribute	Source	OSI_TRANSPORT_LAYER	N/A

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.hits[].operating_system.product	Indicator.Attribute	Product	linux	N/A
.result.hits[].operating_system.cpe	Indicator.Attribute	CPE	`cpe:2.3:o:*:linux:*:*:*:*:*:*:*:*`	N/A

submit_hash

The submit_hash submits the selected hash for analysis.

`GET https://search.censys.io/api/v2/certificates/{{hash}}`

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"
        ]
    }
}
```

ThreatQ provides the following default mapping for this operation action:

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.fingerprint_sha1	Related Indicator.Value	SHA-1	d508e7f8163fb67434f84091dc7c2ca8afd5234d	N/A
.result.fingerprint_md5	Related Indicator.Value	MD5	3818d99263b47ab28f7de5b293ee1418	N/A
.result.tbs_fingerprint_sha256	Related Indicator.Value	SHA-256	4b098b6bd9459340fb0f3cfb80f0bc3283370c455d57ca20da40e7eecce341d5	N/A
.result.tbs_no_ct_fingerprint_sha256	Related Indicator.Value	SHA-256	5c095a40e76c245323086d26d1fa428d3b443b42fb58c7dbb19b32dfe516b749	N/A
.result.spki_fingerprint_sha256	Related Indicator.Value	SHA-256	cc9b074ebf41b484a56923d5585594967bda7a7f8b5be187ef0e7ae1ec90003c	N/A
.result.parent_spki_fingerprint_sha256	Related Indicator.Value	SHA-256	390bc358202771a65e7be7a87924d7f2a079de04feb5ffd4163fae4fbf9b11e9	N/A
.result.parsed.issuer_dn	Indicator.Attribute	Issuer Distinguished Name	C=US, O=Let's Encrypt, CN=R3	N/A
.result.parsed.serial_number	Indicator.Attribute	Serial Number	311703586789118042424998420179537559397550	N/A
.result.parsed.signature.self_signed	Indicator.Attribute	Self Signed	False	N/A
.result.parsed.signature.valid	Indicator.Attribute	Valid Signature	True	N/A
.result.parsed.signature.signature_algorithm.name	Indicator.Attribute	Signature Algorithm Name	SHA256-RSA	N/A
.result.parsed.signature.signature_algorithm.oid	Indicator.Attribute	Signature Algorithm OID	1.2.840.113549.1.1.11	N/A

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.parsed.signature.value	Indicator.Attribute	Signature	95347a7bd89da6a6bd9adcc50 9669d933b5e2a29b414317d72 b02c583bfadbf616f5b6977824e e80484fe4ae0c38dbb1013d896 b5a9db12fdc62296fbefbba84ed 089a6e62c148cc9d1e60bfd9cf6e 7d1c8f5e0f315872618a6805e5bf 48432ce2d0aac07d4ab845a7f68c 1a61c3dd37c0e40c26b386b1f37f f2fc50e6eacdc305ecd13da1c43bb 1209cb13c5a6387cffb57fad81d01 496b3c6499817ed1cf1a0ef809b6b 408035b5de72423c6c7f84c3a9e95 13c89fa8fc49bf6f90746561ebd1b4 ea22e7557d3e505b5ecd289dbb8ce 71c4d3acc2e67a27bbb12dd242c8f a512d19dc8b7bd6b88bcc6a6484bb 39c894f7b756630a10525a9ab33590 30aa2ad	N/A
.result.parsed.extensions.subject_alt_name.dns_names	Indicator.Attribute	DNS Names	kgcontracting.co	N/A
.result.validation.apple.had_trusted_path	Indicator.Attribute	Browser Trust Apple	True	N/A
.result.validation.microsoft.had_trusted_path	Indicator.Attribute	Browser Trust Microsoft	True	N/A
.result.validation.nss.had_trusted_path	Indicator.Attribute	Browser Trust Mozilla NSS	True	N/A
.result.validation.chrome.had_trusted_path	Indicator.Attribute	Browser Trust Chrome	True	N/A
.result.labels	Indicator.Attribute	Tag	leaf	N/A
.result.parsed.subject.common_name	Indicator.Attribute	Common Name	www.kgcontracting.co	N/A
.result.parsed.subject_key_info.key_algorithm.name	Indicator.Attribute	Key Type	RSA	N/A
.result.parsed.subject_key_info.rsa.length	Indicator.Attribute	Key Length	2048	N/A
.result.parsed.subject_key_info.rsa.modulus	Indicator.Attribute	Modulus	c0b3b7d595e250fcbc54c6f9e81113c 12da29fe35350a02b8ab769a5e43f07 df7ac8ff72c482b3e838d64e97cb3fa1 5e415acbcfe6758a4e7ac401b4a5294e cca6ad1b583ec2136a408524eeadca5 5ba4a8af490cb9c764efbdecbe59a4ca1 60905e5972548018f55194e7ac94b215 3d97bd5f055d58ad3abe0d1daa3b3c9 7fed490f1bb58fc5c819618891d05c32 d68aeaabada321736e417f0fa58d7093 d352c1800191645d1b820f5f7c93301a b7ca78393e953b82719741b735a67ce6 a63faec0ac9d2d917f03b9fc0a0ab8012f 4763c50118663af897294e85ba6e11c5c a0fd749645c2a58ddf14ad62717b40b5e 7b620d256be28789e1ebd62e8046acd	N/A
.result.parsed.extensions.key_usage.key_encipherment	Indicator.Attribute	Key Encipherment	True	N/A

PROVIDER DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.result.parsed.extensions.key_usage.digital_signature	Indicator.Attribute	Digital Signature	True	N/A
.result.parsed.extensions.extended_key_usage.server_auth	Indicator.Attribute	Server Auth	True	N/A
.result.parsed.extensions.extended_key_usage.client_auth	Indicator.Attribute	Client Auth	True	N/A
.result.parsed.extensions.basic_constraints.is_ca	Indicator.Attribute	Constraints	False	N/A
.result.parsed.extensions.authority_info_access.ocsp_urls	Indicator.Attribute	AIA Paths OCSP	http://r3.i.lencr.org/	N/A
.result.parsed.extensions.authority_info_access.issuer_urls	Indicator.Attribute	AIA Paths Issuer	http://r3.o.lencr.org	N/A
.result.ct.entries.google_argon_2023.index	Indicator.Attribute	Certificate Transparency Argon	521618614	N/A
.result.ct.entries.google_argon_2023.added_to_ct_at	Indicator.Attribute	Certificate Transparency Argon Date	2022-12-31T12:37:55.858Z	N/A
.result.ct.entries.google_xenon_2023.index	Indicator.Attribute	Certificate Transparency Xenon	593655844	N/A
.result.ct.entries.google_xenon_2023.added_to_ct_at	Indicator.Attribute	Certificate Transparency Xenon Date	2022-12-31T12:37:55.906Z	N/A

Change Log

- **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