ThreatQuotient

CrowdStrike Falcon Intelligence Operation

Version 1.0.0

March 16, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

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

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

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

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

Introduction

The CrowdStrike Falcon Intelligence operation queries the CrowdStrike Falcon Intelligence API to retrieve further information about submitted indicators.

The operation provides the following action:

- **Query -** queries the CrowdStrike Falcon Intelligence API for further information on the submitted indicator.

The operation is compatible with indicator type system objects.

Prerequisites

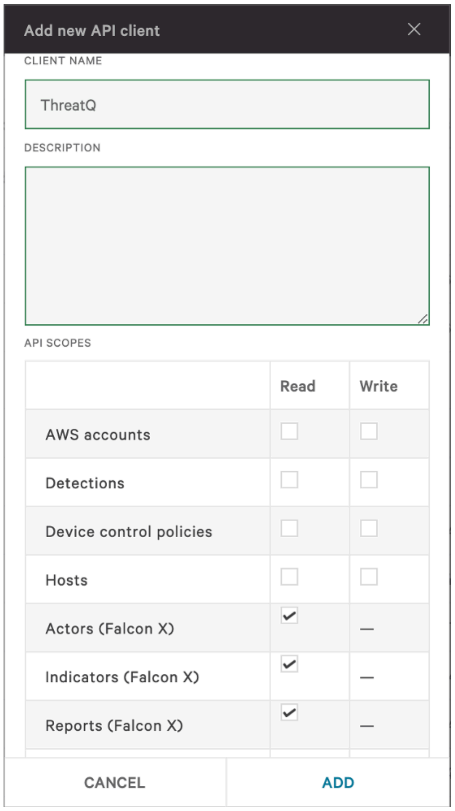
The following is required in order to run the operation:

- CrowdStrike Client ID and Client Secret
- Properly scoped CrowdStrike API Client
- MITRE ATT&CK Feeds (optional)

CrowdStrike API Client

To use the CrowdStrike Falcon Intelligence resources, you must create a properly scoped API Client within CrowdStrike's Falcon platform. API Clients can be created and configured via the **API Clients and Keys** page under **Support**. An API Client must be created for this operation and given the following API **Read** Scopes by clicking the **Add new API Client** button:

- Actors (Falcon X)
- Indicators (Falcon X)



CLIENT NAME

ThreatQ

DESCRIPTION

API SCOPES

	Read	Write
AWS accounts	□	□
Detections	□	□
Device control policies	□	□
Hosts	□	□
Actors (Falcon X)	☑	—
Indicators (Falcon X)	☑	—
Reports (Falcon X)	☑	—

> It is typically a good idea to give the API Client an identifiable name in case of future editing.

MITRE ATT&CK Feeds

To automatically ingest Attack Patterns, please make sure you have installed and run the following feeds successfully before using this operation:

- MITRE Enterprise ATT&CK
- MITRE Mobile ATT&CK
- MITRE PRE-ATT&CK

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

> 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 Hostname	The API host to communicate with CrowdStrike.
CrowdStrike Client ID	The CrowdStrike Client ID used to authenticate.
CrowdStrike Client Secret	The CrowdStrike Client Secret used to authenticate.

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 action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Queries Crowdstrike Falcon Intelligence API for an indicator	Indicator	All

Query

The Query action queries Crowdstrike Falcon Intelligence API for an indicator.

`POST https://{host}/intel/combined/indicators/v1`

Sample Request Body:

```
{
  "filter": "indicator:
'cb0fa82c79b7eed6ba356991c4c89161403162ef56d4e76c528bca857b08cb7a'",
  "sort": "last_updated|desc",
  "limit": 1
}
```

Sample Response:

```
{
  "meta": {
    "query_time": 0.053664582,
    "pagination": {
      "offset": 0,
      "limit": 1,
      "total": 1
    },
    "powered_by": "msa-api",
    "trace_id": "e6e8a29a-dacd-4aca-bb69-24e8251dd843"
  },
  "resources": [
    {
      "id":
"hash_sha256_cb0fa82c79b7eed6ba356991c4c89161403162ef56d4e76c528bca857b08cb7a",
      "indicator":
"cb0fa82c79b7eed6ba356991c4c89161403162ef56d4e76c528bca857b08cb7a",
      "type": "hash_sha256",
      "deleted": false,
      "published_date": 1708907561,
      "last_updated": 1709724487,
      "reports": [
        "CSA-18538"
      ],
      "actors": [
        "FANCYBEAR"
      ],
      "malware_families": [
        "ContiRansomware"
      ],
      "kill_chains": [
        "ActionOnObjectives"
      ],
      "ip_address_types": [
        "TorProxy"
      ],
      "domain_types": [
        "ActorControlled"
      ],
      "malicious_confidence": "high",
      "_marker": "1709724487150f1363aeae1c25de63a7a8b2814fb9",
      "labels": [
        {
          "name": "MitreATTCK/Impact/QueryRegistry",
          "created_on": 1708907563,
          "last_valid_on": 1708907563
        },
        {
          "name": "ThreatType/Criminal",
          "created_on": 1595592139,
          "last_valid_on": 1693409035
        }
      ],
      "relations": [
        {
          "id": "hash_sha1_d17c1a5550fab6ce451df922781fe8534dcd9167",
          "indicator": "d17c1a5550fab6ce451df922781fe8534dcd9167",
          "type": "hash_sha1",
          "created_date": 1708907561,
          "last_valid_date": 1708907561
        }
      ],
      "targets": [
        "Finance"
      ],
      "threat_types": [
        "Criminal",
        "Ransomware"
      ],
      "vulnerabilities": [
        "CVE-2020-1234"
      ]
    }
  ],
  "errors": []
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].actors	Adversary.Name	N/A	N/A	FANCY BEAR	Actor names are split into two words in order to overlap with records from the CrowdStrike Actors Feed on ingestion
.resources[].malware_families	Malware.Value	N/A	N/A	ContiRansomware	N/A
.resources[].kill_chains	Indicator.Attribute	Kill Chain Phase	N/A	CommandAndControl	N/A
.resources[].ip_address_types	Indicator.Attribute	IP Address Type	N/A	TorProxy	N/A
.resources[].domain_types	Indicator.Attribute	Domain Type	N/A	ActorControlled	N/A
.resources[].malicious_confidence	Indicator.Attribute	Confidence	N/A	High	Value title cased
.resources[].labels[].name	AttackPattern.Value	N/A	N/A	T1012 - Query Registry	If an Indicator has any `MitreATTCK` labels (e.g. `MitreATTCK/Discovery/QueryRegistry`) and if the attack pattern name in the label (e.g. `QueryRegistry`) matches the attack pattern name of MITRE ATT&CK Attack Patterns that already exist in the ThreatQ system (e.g. `T1012 - Query Registry`), the associated attack patterns are related to the Indicator
.resources[].relations[].indicator	Related Indicator.Value	See .resources[].relations[].type	N/A	`d17c1a5550fab6ce451df922781fe8534dcd9167`	N/A
.resources[].relations[].type	Related Indicator.Type	See Indicator Type Mapping table below	N/A	SHA-1	N/A
.resources[].targets	Indicator.Attribute	Target Industry	N/A	Finance	N/A
.resources[].threat_types	Indicator.Attribute	Threat Type	N/A	Criminal	Single Camel-case values will be broken up into multiple words, eg. `CredentialHarvesting->Credential Harvesting`
.resources[].vulnerabilities	Related Indicator.Value	CVE	N/A	CVE-2020-1234	N/A

Run Parameters

The following parameters are available when selecting to run the Action against an object:

PARAMETER	DESCRIPTION
Create an attribute from related malware:	Show related malware as the attribute `Related Malware` in the operation result.
Create an attribute from related adversaries:	Show related adversaries as the attribute `Related Adversary` in the operation result.
Create relationships for related malware during operation run:	Create relationships for related malware during operation run
Create relationships for related adversaries during operation run:	Create relationships for related adversaries during operation run
Create relationships for related attack patterns during operation run:	Create relationships for related attack patterns during operation run

Indicator Type Mapping

The following tables provides CrowdStrike to ThreatQ Indicator type mapping.

CROWDSTRIKE INDICATOR TYPE	THREATQ INDICATOR TYPE
binary_string	Binary String
domain	FQDN
email_address	Email Address
email_subject	Email Subject
file_mapping	File Mapping
file_name	Filename
file_path	File Path
hash_ion	Hash ION
hash_md5	MD5
hash_sha1	SHA-1
hash_sha256	SHA-256
ip_address	IP Address
ip_address_block	CIDR Block
mutex_name	Mutex
password	Password

CROWDSTRIKE INDICATOR TYPE	THREATQ INDICATOR TYPE
registry	Registry Key
service_name	Service Name
url	URL
user_agent	User-agent
username	Username
x509_serial	x509 Serial
x509_subject	x509 Subject

Change Log

- **Version 1.0.0**
  - Initial release