ThreatQuotient

CrowdStrike Falcon Intelligence CDF User Guide

Version 3.2.7

September 05, 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

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	3.2.7
Compatible with ThreatQ Versions	>= 4.42.0
Support Tier	ThreatQ Supported

Introduction

CrowdStrike is a cybersecurity technology firm pioneering cloud-delivered next-generation endpoint protection and services. The CrowdStrike Falcon platform stops breaches by preventing, detecting, and responding to all attacks types, at every stage – even malware-free intrusions.

The CrowdStrike Falcon Intelligence integration includes three feeds:

- CrowdStrike Actors
- CrowdStrike Indicators
- CrowdStrike Reports

The integration ingests the following system objects:

- Adversaries
- Adversary Attributes
- Indicators
- Indicator Attributes
- Malware
- Reports
- Vulnerabilities

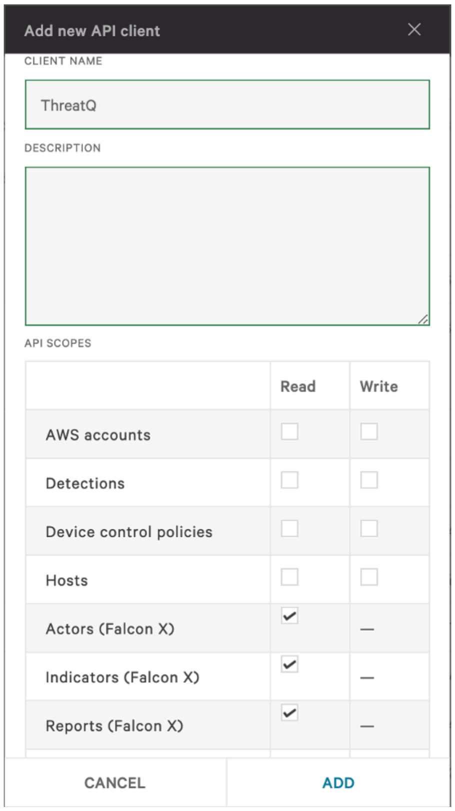
Prerequisites

The following is required for this integration.

CrowdStrike API Client Configuration

To use the CrowdStrike Falcon Intelligence Feeds, one 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 these Feeds and given the following API **Read** Scopes by clicking the **Add new API Client** button:

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



Add new API client

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.

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

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

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 **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Client ID	Required. Your CrowdStrike Client ID.
Secret	Required. Your CrowdStrike Secret key.
API Host	Select the appropriate CrowdStrike host. Options include: ◦ US-1: `api.crowdstrike.com` ◦ US-2: `api.us-2.crowdstrike.com` (Default) ◦ EU-1: `api.eu-1.crowdstrike.com` ◦ US-GOV-1: `api.laggar.gcw.crowdstrike.com`

Additional Parameter for CrowdStrike Actors

PARAMETER	DESCRIPTION
Save CVE Data as	This is a **required** multi-select field and can be configured to have the Feed ingest CVE data as CVE Indicators, Vulnerabilities, or both.

Additional Parameters for CrowdStrike Indicators

PARAMETER	DESCRIPTION
Save CVE Data as	This is a **required** multi-select field and can be configured to have the Feed ingest CVE data as CVE Indicators, Vulnerabilities, or both.
***CrowdStrike Types**	This optional parameter is a multi-select field that allows you to filter CrowdStrike's data based on indicator type. The default setting is all indicator types.
***Ingest Indirect Related Indicators**	This checkbox controls the ingestion of related indirect indicators from CrowdStrike. Unchecking this option will override any setting for **CrowdStrike Indirect Related Indicators** and all indirect indicators will be dropped. This option is disabled by default.
***CrowdStrike Indirect Related Indicator Types**	This optional parameter is a multi-select field that allows you to filter Indirect Related Indicators based on their type. The default setting is all indicator types.
***CrowdStrike Malicious Confidence Levels**	This optional parameter is a multi-select field that allows you to filter CrowdStrike's data based on CrowdStrike's malicious confidence rating for IoCs. The default setting is all confidence ratings.
***CrowdStrike Kill Chain Phases**	This optional parameter is a multi-select field that allows you to filter CrowdStrike's data based on the kill chain phase associated with IoCs.

PARAMETER	DESCRIPTION
	The default setting is all kill chains.

> * When using these filtering parameters with CrowdStrike Indicators, the specified filters will be joined together in the following manner:

- Individual options within a filtering parameter will be joined with OR statements
- Filtering parameters will be joined together with AND statements

Thus, if you were to configure CrowdStrike to filter as the following:

FILTERING PARAMETERS	VALUE
CrowdStrike Types	email_address, ip_address
CrowdStrike Malicious Confidence Level	high
CrowdStrike Kill Chain Phases	c2

CrowdStrike would only return indicators that:

- are Email or IP Addresses
- are of High Malicious Confidence and are associated with the C2 Kill Chain Phase

This filtering is ultimately sent to CrowdStrike as FQL formatted:

```
+(type: 'Target/Aerospace', type: 'Target/Agricultural')
+(malicious_confidence: 'high',)
+(kill_chains: 'c2',)
```

Due to the **AND** association between the filtering parameters, checking all the provided filter options ***will not*** result in CrowdStrike returning a full data set. In fact, a significantly smaller data set will be returned as CrowdStrike rarely supplies all filterable fields with each object. In order to pull a full, unfiltered data set from CrowdStrike, you must leave the filtering parameters unchecked.

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.

ThreatQ Mapping

CrowdStrike Actors

`GET https://{HOST}/intel/combined/actors/v1`

Sample Response:

```
{
    "meta": {
        "query_time": 0.096869734,
        "pagination": {
            "offset": 0,
            "limit": 50,
            "total": 142
        },
        "powered_by": "msa-api",
        "trace_id": "0c587865-296e-4502-a39a-10febd0a3006"
    },
    "resources": [
        {
            "id": 10006,
            "name": "HELIX KITTEN",
            "slug": "helix-kitten",
            "url": "https://falcon.crowdstrike.com/intelligence/actors/helix-
kitten/",
            "thumbnail": {
                "url": "https://cf-s.falcon.crowdstrike.com/2017/02/24181334/
HELIX-KITTEN.jpg"
            },
            "image": {
                "url": "https://cf-s.falcon.crowdstrike.com/2017/02/24181334/
HELIX-KITTEN.jpg"
            },
            "description": "HELIX KITTEN is an Iran-nexus adversary active
since...",
            "short_description": "HELIX KITTEN is an Iran-nexus adversary
active since...",
            "rich_text_description": "<p><span style=\"font-weight:
400;\">HELIX KITTEN is an Iran-nexus adversary active since...",
            "created_date": 1487960014,
            "last_modified_date": 1595568692,
            "first_activity_date": 1462060800,
            "last_activity_date": 1580860800,
            "active": false,
            "actor_type": "targeted",
            "capability": {
                "id": 246,
                "slug": "average",
                "value": "Average"
            },
            "kill_chain": {
                "actions_and_objectives": "Theft of sensitive data",
                "command_and_control": "Use of DNS for communication...",
                "delivery": "Spear Phishing (including from compromised
accounts)\r\nSocial Media",
                "exploitation":
"CVE-2017-0199\r\nCVE-2017-11882\r\nCVE-2018-15982",
                "installation": "Helminth PowerShell Tool\r\nAgentDrable
RAT\r\nEarthquakeRAT...",
                "reconnaissance": "Suspected social media engagement",
                "weaponization": "Microsoft Office Documents",
                "rich_text_actions_and_objectives": "<p>Theft of sensitive
data</p>",
                "rich_text_command_and_control": "<p><span style=\"font-weight:
400;\">Use of DNS for communication...",
                "rich_text_delivery": "<p><span style=\"font-weight:
400;\">Spear Phishing (including from...",
                "rich_text_exploitation": "<p>CVE-2017-0199</
p>\r\n<p>CVE-2017-11882</p>\r\n<p>CVE-2018-15982</p>",
                "rich_text_installation": "<p><span style=\"font-weight:
400;\">Helminth PowerShell Tool</span></p>\r\n...",
                "rich_text_reconnaissance": "<p>Suspected social media
engagement</p>",
                "rich_text_weaponization": "<p>Microsoft Office Documents</p>"
            },
            "known_as": "OilRig, Helminth, Clayslide, APT34, IRN2, COBALT
GYPSY, ITG13, CHRYSENE, HEXANE, LYCEUM",
            "motivations": [
                {
                    "id": 352,
                    "slug": "espionage",
                    "value": "Espionage"
                }
            ],
            "notify_users": false,
            "origins": [
                {
                    "id": 101,
                    "slug": "ir",
                    "value": "Iran"
                }
            ],
            "region": {
                "id": 252,
                "slug": "iran",
                "value": "Iran"
            },
            "target_countries": [
                {
                    "id": 18,
                    "slug": "az",
                    "value": "Azerbaijan"
                }
            ],
            "target_industries": [
                {
                    "id": 457,
                    "slug": "academic",
                    "value": "Academic"
                },
                ...
            ]
        },
        {
            "name": "GENIE SPIDER",
            "ecrime_kill_chain": {
                "attribution": "Unknown",
                "crimes": "\r\n\tAccessing a computer without 
authorization...",
                "customers": "CrowdStrike Intelligence assesses...",
                "marketing": "Not openly advertised",
                "services_offered": "Unknown",
                "services_used": "Unknown",
                "technical_tradecraft": "\r\n\tConducts phishing campaigns 
using links...",
                "victims": "GENIE SPIDER primarily targets companies...",
                "rich_text_attribution": "<p>Unknown</p>",
                "rich_text_crimes": "<ul>\r\n\t<li>Accessing a computer without 
authorization...",
                "rich_text_customers": "<p><span style=\"font-weight: 
400;\">CrowdStrike Intelligence assesses...",
                "rich_text_marketing": "<p>Not openly advertised</p>",
                "rich_text_monetization": "<p>Unknown</p>",
                "rich_text_services_offered": "<p>Unknown</p>",
                "rich_text_services_used": "<p>Unknown</p>",
                "rich_text_technical_tradecraft": "<ul>\r\n\t<li style=\"font-
weight: 400;\"><span style=\"font-weight: 400;\">Conducts phishing...",
                "rich_text_victims": "<p>GENIE SPIDER primarily targets..."
            }
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].name	Adversary.Name	N/A	.resources[].created_date	HELIX KITTEN	N/A
.resources[].url	Adversary.Attribute	Vendor Link	.resources[].created_date	https://falcon.crowdstrike.com/intelligence/actors/helix-kitten/	N/A
.resources[].rich_text_description	Adversary.Description	N/A	N/A	`<p><span style=\"font-weight: 400;\">HELIX KITTEN is an Iran-nexus adversary active since...`	N/A
.resources[].first_activity_date	Adversary.Attribute	First Activity At	.resources[].created_date	2016-05-01 00:00:00-00:00	Formatted from Epoch timestamp
.resources[].active	Adversary.Attribute	Active	.resources[].created_date	False	N/A
.resources[].capability.value	Adversary.Attribute	Capability	.resources[].created_date	Average	N/A
.resources[].kill_chain.actions_and_objectives	Adversary.Attribute	Kill Chain Actions and Objectives	.resources[].created_date	Theft of sensitive data	Values split on \r\n
.resources[].kill_chain.command_and_control	Adversary.Attribute	Kill Chain Command and Control	.resources[].created_date	Use of DNS for communication...	Values split on \r\n
.resources[].kill_chain.delivery	Adversary.Attribute	Kill Chain Delivery	.resources[].created_date	Spear Phishing (including from compromised accounts) \r\nSocial Media	Values split on \r\n
.resources[].kill_chain.exploitation	Adversary.Attribute \ Indicator.Value \ Vulnerability.Value	Kill Chain Exploitation \ CVE \ N/A	.resources[].created_date	CVE-2017-0199\r\nCVE-2017-11882\r\nCVE-2018-15982	Values split on \r\n. Indicator and/or Vulnerability objects are created based on user configuration. The Published At value only applies to the Adversary.Attribute
.resources[].kill_chain.installation	Adversary.Attribute	Kill Chain Installation	.resources[].created_date	Helminth PowerShell Tool\r\nAgentDrable RAT\r\nEarthquakeRAT...	Values split on \r\n
.resources[].kill_chain.reconnaissance	Adversary.Attribute	Kill Chain Reconnaissance	.resources[].created_date	Suspected social media engagement	Values split on \r\n
.resources[].kill_chain.weaponization	Adversary.Attribute	Kill Chain Weaponization	.resources[].created_date	Microsoft Office Documents	Values split on \r\n
.resources[].ecrime_kill_chain.rich_text_attribution	Adversary.Description	N/A	N/A	`<p>Unknown</p>`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_crimes	Adversary.Description	N/A	N/A	`<ul>\r\n\t<li>Accessing a computer without authorization...`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_customers	Adversary.Description	N/A	N/A	`<p><span style=\"font-weight: 400;\">CrowdStrike Intelligence assesses...`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_marketing	Adversary.Description	N/A	N/A	`<p>Not openly advertised</p>`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_monetization	Adversary.Description	N/A	N/A	`<p>Unknown</p>`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_services_offered	Adversary.Description	N/A	N/A	`<p>Unknown</p>`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_services_used	Adversary.Description	N/A	N/A	`<p>Unknown</p>`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_technical_tradecraft	Adversary.Description	N/A	N/A	`<ul>\r\n\t<li style=\"font-weight: 400;\"><span style=\"font-weight: 400;\">Conducts phishing...`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].ecrime_kill_chain.rich_text_victims	Adversary.Description	N/A	N/A	`<p>GENIE SPIDER primarily targets...`	`ecrime_kill_chain` is mutually exclusive with `kill_chain`. Concatenated on to the end of the Adversary Description.
.resources[].known_as	Adversary.Name	N/A	.resources[].created_date	OilRig, Helminth, Clayslide, APT34, IRN2, COBALT GYPSY, ITG13, CHRYSENE, HEXANE, LYCEUM	Values split on ",". A related alias Adversary with the same Attributes and Description as the primary Adversary will be created.
.resources[].motivations[].value	Adversary.Attribute	Motivation	.resources[].created_date	Espionage	If the 'value' attribute is missing from an object in the array the reference to that object is discarded

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].origins[].value	Adversary.Attribute	Origin	.resources[].created_date	Iran	If the 'value' attribute is missing from an object in the array the reference to that object is discarded
.resources[].region.value	Adversary.Attribute	Region	.resources[].created_date	Iran	N/A
.resources[].target_countries [].value	Adversary.Attribute	Target Country	.resources[].created_date	Azerbaijan	If the 'value' attribute is missing from an object in the array the reference to that object is discarded
.resources[].target_industries [].value	Adversary.Attribute	Target Industry	.resources[].created_date	Academic	If the 'value' attribute is missing from an object in the array the reference to that object is discarded

CrowdStrike Indicators

`GET https://{HOST}/intel/combined/indicators/v1`

Sample Response:

```
{
    "meta": {
        "query_time": 1.077970568,
        "pagination": {
            "offset": 0,
            "limit": 100,
            "total": 12046205
        },
        "powered_by": "msa-api",
        "trace_id": "d934e4be-5172-4365-adff-2073044236cb"
    },
    "resources": [
        {
            "id":
"hash_sha256_994bf4a94c154fb3e7566e469aadee2f157d95fc4d5b1107e2fdf631da8b4532",
            "indicator":
"994bf4a94c154fb3e7566e469aadee2f157d95fc4d5b1107e2fdf631da8b4532",
            "type": "hash_sha256",
            "deleted": false,
            "published_date": 1577708859,
            "last_updated": 1597327932,
            "reports": [
                "CSA-18538"
            ],
            "actors": [
                "FANCYBEAR"
            ],
            "malware_families": [
                "DarkComet"
            ],
            "kill_chains": [
                "CommandAndControl"
            ],
            "ip_address_types": [
                "TorProxy"
            ],
            "domain_types": [
                "ActorControlled"
            ],
            "malicious_confidence": "high",
            "_marker": "1597327932d724b22d350df2eb489d7e0c0a69ea79",
            "labels": [
                {
                    "name": "ThreatType/Downloader",
                    "created_on": 1588277899,
                    "last_valid_on": 1592567532
                },
                ...
            ],
            "relations": [
                {
                    "id": "url_https://ns8.softline.top:443/s/
ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books",
                    "indicator": "https://ns8.softline.top:443/s/
ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books",
                    "type": "url",
                    "created_date": 1592344896,
                    "last_valid_date": 1592344896
                }
            ],
            "targets": [
                "Finance"
            ],
            "threat_types": [
                "Downloader",
                "Ransomware",
                "CredentialHarvesting"
            ],
            "vulnerabilities": [
                "CVE-2020-1234"
            ]
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].indicator	Indicator.Value	See .resources[].type	.resources[].published_date	994bf4a94c154fb3e7566e469aadee2f157d95fc4d5b1107e2fdf631da8b4532	N/A
.resources[].type	Indicator.Type	See Indicator Type Mapping table below	.resources[].published_date	hash_sha256	Records with a type not found in the Indicator Type Mapping below are dropped and not ingested
.resources[].reports	Report.Value	N/A	N/A	CSA-18538	CrowdStrike only returns report code IDs like the example

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					provided. These must be referenced against a full mapping of report code IDs -> report names pulled from CrowdStrike's Reports endpoint
.resources[].actors	Adversary.Name	N/A	N/A	FANCYBEAR	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	.resources[].published_date	DarkComet	N/A
.resources[].kill_chains	Indicator.Attribute	Attack Phase	.resources[].published_date	CommandAndControl	N/A
.resources[].ip_address_types	Indicator.Attribute	IP Address Type	.resources[].published_date	TorProxy	N/A
.resources[].domain_types	Indicator.Attribute	Domain Type	.resources[].published_date	ActorControlled	N/A
.resources[].malicious_confidence	Indicator.Attribute	Confidence	.resources[].published_date	high	Value title cased
.resources[].labels	AttackPattern	N/A	.resources[].published_date	T1012 - Query Registry	N/A
.resources[].relations[].indicator	Related Indicator.Value	See .resources[].relations[].type	.resources[].relations[].created_date	https://ns8.softline.top:443/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books	Related Indicators are brought in with the Indirect status
.resources[].relations[].type	Related Indicator.Type	See Indicator Type Mapping table below	.resources[].relations[].created_date	url	N/A
.resources[].targets	Indicator.Attribute	Target Industry	.resources[].published_date	Finance	N/A
.resources[].threat_types	Indicator.Attribute	Threat Type	.resources[].published_date	Downloader	Single Camel-case values will be broken up

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					into multiple words, eg. `Credential Harvesting->Credential Harvesting`
.resources[].vulnerabilities	Related Indicator.Value \ Vulnerability.Value	CVE \ N/A	N/A	CVE-2020-1234	Indicator and/or Vulnerability objects are created based on user configuration
.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. Since attack pattern lookup is based on the MITRE ATT&CK attack pattern name and not its ID,

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					there may be multiple attack patterns in the ThreatQ system that match a single CrowdStrike `MitreATTCK` label.

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

CROWDSTRIKE INDICATOR TYPE	THREATQ INDICATOR TYPE
ip_address	IP Address
ip_address_block	CIDR Block
mutex_name	Mutex
password	Password
registry	Registry Key
service_name	Service Name
url	URL
user_agent	User-agent
username	Username
x509_serial	x509 Serial
x509_subject	x509 Subject

CrowdStrike Reports

`GET https://{HOST}/intel/combined/reports/v1`

Sample Response:

```
{
    "meta": {
        "query_time": 0.050410539,
        "pagination": {
            "offset": 0,
            "limit": 50,
            "total": 7
        },
        "powered_by": "msa-api",
        "trace_id": "420fa3f4-f5f2-48c1-a9cf-f3da4fb96fb7"
    },
    "resources": [
        {
            "id": 72478,
            "name": "Situational Awareness: Activity in Middle East",
            "slug": "situational-awareness-activity-in-middle-east",
            "type": {
                "id": 2883,
                "slug": "overwatch",
                "name": "OverWatch"
            },
            "sub_type": {
                "id": 391,
                "slug": "snort-suricata",
                "name": "Snort/Suricata"
            },
            "url": "https://falcon.crowdstrike.com/intelligence/reports/
situational-awareness-activity-in-middle-east/",
            "short_description": "                         Situational
Awareness    Â  Published on 06...",
            "description": "[vc_row][vc_column] CVE-2021-44228 [vc_page]
[vc_column_text]\r\n
05c43a9166a79bc793c1ef0707642df0f605ae9a0bf9937610015f1b3853f0f3d079cb458b9283c
12ea4dd8457d7682b96ecd6b96e6705c8a1cf499972f88900
\r\n\r\n\r\n\r\n\r\nSituational Awareness\r\n\r\n\r\n\r\nÂ
\r55a9f4f8994b1bbf2058ea38c8efb6c459000814d5f39c087002571639e6230e\n 127.0.0.1,
2fe04e524ba40505a82e03a2819429cc, 793f970c52ded1276b9264c742f19d1888cbaf73,
Published on... ",
            "rich_text_description": "<p><div class=\"vc_row wpb_row vc_row-
fluid\"><div class=\"wpb_column vc_column_container vc_col-sm-12\">...",
            "created_date": 1578332574,
            "last_modified_date": 1579880737,
            "image": {
                "url": "https://cf-s.falcon.crowdstrike.com/2016/10/04222253/
```

```
product_release_banner.png"
            },
            "thumbnail": {
                "url": "https://cf-s.falcon.crowdstrike.com/2019/07/15200051/
overwatch_thumb-1.png"
            },
            "actors": [
                {
                    "id": 82425,
                    "name": "TRACER KITTEN",
                    "slug": "tracer-kitten",
                    "url": "https://falcon.crowdstrike.com/intelligence/actors/
tracer-kitten",
                    "thumbnail": {
                        "url": "https://assets-public.falcon.crowdstrike.com/
2017/02/24181136/kitten.png"
                    }
                }
            ],
            "tags": [
                {
                    "id": 394,
                    "slug": "all-news",
                    "value": "All News"
                },
                {
                    "id": 793,
                    "slug": "intel",
                    "value": "Intel"
                },
                {
                    "id": 2852,
                    "slug": "overwatch",
                    "value": "Overwatch"
                }
            ],
            "target_industries": [
                {
                    "id": 328,
                    "slug": "technology",
                    "value": "Technology"
                }
            ],
            "target_countries": [
                {
                    "id": 1,
                    "slug": "us",
                    "value": "United States"
                }
            ],
            "motivations": [
                {
                    "id": 352,
                    "slug": "espionage",
                    "value": "Espionage"
                }
            ]
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].name	Report.Value	N/A	.resources[].created_date	Situational Awareness: Activity in Middle East	Report names are truncated at 252 characters. If truncated, the report name ends with an ellipsis.<br/>There are several known duplicate report names provided by CrowdStrike that the filter chain makes unique by appending the report's formatted `.resources[].created_date` value to the report name. See the **Known Duplicate CrowdStrike Report Names** list below.
.resources[].rich_text_description	Report.Description	N/A	N/A	`<p><div class=\"vc_row wpb_row vc_row-fluid\"><div class=\"wpb_column vc_column_container vc_col-sm-12\">...`	A link to the report (from `.resources[].url`) is prepended to the description.<br/>The HTML is modified for ideal display in the ThreatQ UI.<br/>`<img>` tags are replaced with a

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					link to the image.<br/>If the description exceeds 32,630 characters, <table>'s are removed from the report and, if the description still exceeds 32,630 characters, the HTML is truncated.
.resources[].url	Report.Attribute	Vendor Link	.resources[].created_date	https://falcon.crowdstrike.com/intelligence/reports/situational-awareness-activity-in-middle-east/	N/A
.resources[].type.name	Report.Attribute	Type	.resources[].created_date	OverWatch	N/A
.resources[].sub_type.name	Report.Attribute	Sub Type	.resources[].created_date	Snort/Suricata	N/A
.resources[].tags[].value	Report.Attribute	Tag	.resources[].created_date	Intel	If the 'value' attribute is missing from an object in the array the reference to that object is discarded
.resources[].target_industries[].value	Report.Attribute	Target Industry	.resources[].created_date	Technology	If the 'value' attribute is missing from an object in the array the reference to that object is discarded
.resources[].target_countries[].value	Report.Attribute	Target Country	.resources[].created_date	United States	If the 'value' attribute is missing from an object in the array the reference to that object is discarded
.resources[].motivations[].value	Report.Attribute	Motivation	.resources[].created_date	Espionage	If the 'value' attribute is missing from an object in the array the reference to

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					that object is discarded
.resources[].description / .resources[].rich_text_description	AttackPattern.Value	N/A	N/A	T1088 - Bypass User Account Control	If the description or rich text description contains any MITRE ATT&CK attack pattern IDs for MITRE ATT&CK Attack Patterns that already exist in the ThreatQ system, the associated attack patterns are related to the report.
.resources[].actors[].name	Adversary.Name	N/A	N/A	TRACER KITTEN	Associated adversaries that are related to the report. If the 'name' attribute is missing from an object in the array the reference to that object is discarded
.resources[].description	Related Indicator.Value	MD5	N/A	2fe04e524ba40505a82e03a2819429cc	MD5 objects are parsed out of the description and automatically ingested
.resources[].description	Related Indicator.Value	SHA-1	N/A	793f970c52ded1276b9264c742f19d1888cbaf73	SHA-1 objects are parsed out of the description and automatically ingested
.resources[].description	Related Indicator.Value	SHA-256	N/A	55a9f4f8994b1bbf2058ea38c8efb6c459000814d5f39c087002571639e6230e	SHA-256 objects are parsed out of the description and automatically ingested
.resources[].description	Related Indicator.Value	SHA-512	N/A	05c43a9166a79bc793c1ef0707642df0f605ae9a0bf9937610015f1b3853f0f3d079cb458b9283c12ea4dd8457d7682b96ecd6b96e6705c8a1cf499972f88900	SHA-512 objects are parsed out of the description and

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					automatically ingested
.resources[].description	Related Indicator.Value	IP Address	N/A	127.0.0.1	IP Address objects are parsed out of the description and automatically ingested
.resources[].description	Related Indicator.Value	CVE	N/A	CVE-2021-44228	CVE objects are parsed out of the description and automatically ingested

Known Duplicate CrowdStrike Report Names

- C2 Update
- CEF Master
- Common Event Format
- Common Event Format Master
- Netwitness
- Netwitness Master / NetWitness Master
- Snort Changelog
- Snort Update
- Yara Master
- Yara Update

Average Feed Run

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

CrowdStrike Actors (24h)

Scheduled Run with a 24 hour period

METRIC	RESULT
Run Time	1 minute
Adversaries	7
Adversary Attributes	269
Indicators	4
Vulnerabilities	4

CrowdStrike Actors (manual)

Manual Run for all CrowdStrike Actors (January 01, 1997 - September 03, 2020)

METRIC	RESULT
Run Time	5 minutes
Adversaries	500
Adversary Attributes	18,296
Indicators	114
Vulnerabilities	114

CrowdStrike Indicators (hourly)

Hourly Run

METRIC	RESULT
Run Time	5 minutes
Indicators	1,480
Indicator Attributes	7,267
Adversaries	27
Reports	398
Malware	30

CrowdStrike Reports

METRIC	RESULT
Run Time	1 minute
Reports	13
Report Attributes	129
Adversaries	7

CrowdStrike Reports (manual)

Manual Run for CrowdStrike Reports (January 01, 1997 - September 08, 2020)

METRIC	RESULT
Run Time	30 minutes
Reports	9,495
Report Attributes	78,660
Adversaries	141
Attack Patterns	248

Known Issues / Limitations

General

- Occasionally, CrowdStrike may respond with a `403 Forbidden` error even if the provided access token is still valid. CrowdStrike has attributed this to possible load balancing issues with their servers. In the event of receiving one of these errors, ThreatQ will attempt to re-authenticate on the first `403 Forbidden` received, and usually proceed without incident. If it occurs a consecutive time however, the feed run will complete with errors.

CrowdStrike Indicators

- There could be cases where indicators ingested from CrowdStrike Indicators are not related to the reports ingested by CrowdStrike Reports. This is due to CrowdStrike Reports not creating relationships between these threat objects. CrowdStrike Indicators must be ran in order to relate the objects.
- Due to the enormous size of CrowdStrike's data throughput on their Indicators endpoint, ThreatQ strongly recommends an **hourly** run frequency and applying a number of filters via UI configuration parameters to pare down the amount of data CrowdStrike returns.
- MITRE ATT&CK Attack Patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK Attack Patterns extracted from an indicator's `MitreATTCK` labels to be related to the indicator. The following feeds ingest MITRE ATT&CK Attack Patterns:
    - MITRE ATT&CK CAPEC
    - MITRE ATT&CK ICS
    - MITRE Enterprise ATT&CK
    - MITRE Mobile ATT&CK
    - MITRE PRE-ATT&CK
- Sometimes, CrowdStrike may respond with a `500 Internal Server Error` even if the provided access token is still valid and the request query is properly formed. In the event of receiving one of these errors, ThreatQ will attempt to re-authenticate on the first `500 Internal Server Error` received, and usually proceed without incident. If it occurs a consecutive time however, the feed run will complete with errors.

CrowdStrike Reports

- MITRE ATT&CK Attack Patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK Attack Patterns extracted from a report's `description` or `rich_text_description` fields to be related to the report. The following feeds ingest MITRE ATT&CK Attack Patterns:
    - MITRE ATT&CK CAPEC
    - MITRE ATT&CK ICS

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

Change Log

- **Version 3.2.7**
  - Resolved an issue where IOCs from reports were not ingested.
- **Version 3.2.6**
  - Resolved an issue where CrowdStrike reports did not contain a `sub_type` key.
- **Version 3.2.5**
  - Removed the **CrowdStrike Target Vertical Sectors** configuration filter as this option is no longer supported by the provider.
- **Version 3.2.4**
  - Fixed an error that would occur when the received JSON data contained keys that had `None` as their value.
- **Version 3.2.3**
  - Updated CrowdStrike Target Vertical Sectors configuration options for the CrowdStrike Indicators feed.
  - Removed the relationships between the related alias adversaries.
  - Updated all filter options to be enabled by default.
- **Version 3.2.2**
  - Fixed the following issues:
    - where the response from CrowdStrike contains objects in an array that is missing an expected attribute.
    - a potential issue where response from CrowdStrike contains a region object with no value attribute.
    - Added a new known Issue regarding ingested indicators are not related to the reports ingested by CrowdStrike Reports. See the CrowdStrike Indicators heading in the Known Issues/Limitations chapter for more details.
- **Version 3.2.1**
  - Fixed an issue where the response from CrowdStrike occasionally did not contain the expected attribute arrays.
  - The **Ingest Indirect Related Indicators** configuration option for the **CrowdStrike Indicators** feed is now disabled by default. See the Configuration chapter for more information on configuring the integration.
- **Version 3.1.2**
  - Added a new **API Host** configuration parameter that will allow you to select a CrowdStrike host. See step 4 in the Configuration chapter for more information.
  - Increased the API call limit for **CrowdStrike Indicators** to 10,000.
- **Version 3.1.1**
  - Added a new configuration option, **Ingest Indirect Related Indicators**, to CrowdStrike Indicators
  - Added a new configuration option, **CrowdStrike Indirect Related Indicator Types**, to CrowdStrike Indicators
- **Version 3.1.0**
  - Added the following new configuration options to CrowdStrike Indicators:
    - CrowdStrike Target Vertical Sectors

        - CrowdStrike Types
        - CrowdStrike Malicious Confidence Levels
        - CrowdStrike Kill Chain Phases
- **Version 3.0.3**
    - Fixed a bug which caused a Filter error to be raised by CrowdStrike Actors when parsing data for Solar Spider.
- **Version 3.0.2**
    - Fixed a bug which caused the Threat Type Attribute value of `DDoS` to be spaced as `D Do S`
    - Updated user fields to more accurately reflect CrowdStrike's naming conventions
    - Added CrowdStrike API Client Configuration section to documentation
- **Version 3.0.1**
    - Fixed bug in the CrowdStrike Indicators filter chain to account for CrowdStrike report codes that are not accounted for by the CrowdStrike Reports API
- **Version 3.0.0**
    - Rewritten for CrowdStrike's v3 API:
        - Added support for OAuth2 Authentication
        - Split single CrowdStrike Feed into three feeds:
            - CrowdStrike Actors
            - CrowdStrike Indicators
            - CrowdStrike Reports
- **Version 1.0.0**
    - Initial release