ThreatQuotient

CrowdStrike Falcon Intelligence Guide

Version 3.0.1

Monday, September 28, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Monday, September 28, 2020

Contents

Versioning

- Current integration version: `3.0.1`
- Supported on ThreatQ versions >= `4.42.0`

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

Installation

Perform the following steps to install the feeds:

> The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.

2. Locate and download the **CrowdStrike Falcon Intelligence** integration file.

3. Navigate to your ThreatQ instance.

4. Click on the **Settings** icon and select **Incoming feeds**.

5. Click on the **Add New Feed** button.

6. Upload the feed file using one of the following methods:

   - Drag and drop the file into the dialog box

   - Select **Click to Browse** to locate the feed 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.

The feeds will be added to the **Commercial** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.

2. Locate the feeds under the **Commercial** tab.

3. Click on the **Feed Settings** link for each feed.

4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
API ID	The CrowdStrike API ID. > This field is required.
API Key	The CrowdStrike API Key. > This field is required.

Additionally, the **CrowdStrike Actors** and **CrowdStrike Indicators** feeds also include the following configuration parameter:

Parameter	Description
Save CVE Data as	This multi-select field can be configured to have this Feed ingest CVE data as CVE Indicators, Vulnerabilities, or both. > This field is required.

5. Click on **Save Changes**.

6. Click on the toggle switch to the left of each feed name to enable the feeds.

ThreatQ Mapping

CrowdStrike Actors

```
GET https://api.crowdstrike.com/intel/combined/actors/v1
```

JSON response sample:

```
{
    "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\nEarth-
quakeRAT...",
            "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 Power-
Shell 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 author-
ization...",
                "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..."
        },
        ...
    },
    ...
  ]
}
```

ThreatQ 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	False	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
			[].created_ date		
.resources[].cap-ability.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 com-munication...	Values split on \r\n
.resources[].kill_ chain.delivery	Adversary.Attribute	Kill Chain Delivery	.resources [].created_ date	Spear Phishing (including from compromised account-s)\r\nSocial Media	Values split on \r\n
.resources[].kill_ chain.exploitation	Adversary.Attribute \ Indicator.Value \ Vul-	Kill Chain Exploitation \	.resources [].created_	CVE-2017-0199\r\nCVE-2017-11882\r\nCVE-2018-15982	Values split on \r\n. Indicator and/or Vul-

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
	nerability.Value	CVE \ N/A	date		nerability 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\nA-gentDrable RAT\r\nEarth-quakeRAT...	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_	Adversary.Description	N/A	N/A	`<p>Unknown</p>`	`ecrime_kill_`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
attribution					`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 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`	`ecrime_kill_ chain` is mutually exclusive with `kill_ chain`. Concatenated

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
				`assesses...`	on to the end of the Adversary Description.
.resources[].ecrime_ kill_chain.rich_text_ marketing	Adversary.Description	N/A	N/A	`<p>Not openly advert-ised</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.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attrib-ute Key	Published Date	Examples	Notes
.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 Descrip-tion.
.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 Descrip-tion.
.resources[].ecrime_ kill_chain.rich_text_ technical_tradecraft	Adversary.Description	N/A	N/A	`<ul>\r\n\t<li style- e=\"font-weight: 400;\"><span style-`	`ecrime_kill_ chain` is mutually exclusive with `kill_`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
				`=\"font-weight: 400;\">Conducts phishing...`	`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

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					be created.
.resources[].motivations[].value	Adversary.Attribute	Motivation	.resources[].created_date	Espionage	N/A
.resources[].origins[].value	Adversary.Attribute	Origin	.resources[].created_date	Iran	N/A
.resources[].region.value	Adversary.Attribute	Region	.resources[].created_date	Iran	N/A
.resources[].target_countries[].value	Adversary.Attribute	Target Country	.resources[].created_date	Azerbaijan	N/A
.resources[].target_industries[].value	Adversary.Attribute	Target Industry	.resources[].created_date	Academic	N/A

CrowdStrike Indicators

`GET https://api.crowdstrike.com/intel/combined/indicators/v1`

JSON response sample:

```
{
    "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"

        ]

    },

    ...

  ]
}
```

ThreatQ 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	994bf4a94c154fb3e7566e469 aadee2f157d95fc4d5b1107e2 fdf631da8b4532	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 provided. These must be referenced against a full mapping of report code IDs -> report names pulled from CrowdStrike's Reports endpoint

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.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 [].pub-lished_ date	DarkComet	N/A
.resources [].kill_chains	Indicator.Attribute	Attack Phase	.resources [].pub-lished_ date	CommandAndControl	N/A
.resources [].ip_ address_ types	Indicator.Attribute	IP Address Type	.resources [].pub-lished_ date	TorProxy	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.resources [].domain_ types	Indicator.Attribute	Domain Type	.resources [].pub- lished_ date	ActorControlled	N/A
.resources [].malicious_ confidence	Indicator.Attribute	Con- fidence	.resources [].pub- lished_ date	high	Value title cased
.resources [].labels	TODO!	TODO!	.resources [].pub- lished_ date	TODO!	TODO!
.resources [].relations [].indicator	Related Indic- ator.Value	See .re- sources [].re-	.resources [].relations [].created_	https://n- s8.softline.top:443/s/ref=nb_ sb_noss_1/167-3294888-	Related Indicators are brought in with the Indirect status

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
		lations [].type	date	0262949/field-keywords=books	
.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 [].pub-lished_ date	Finance	N/A
.resources [].threat_ types	Indicator.Attribute	Threat Type	.resources [].pub-lished_ date	Downloader	Single Camel-case values will be broken up into multiple words, eg. `Cre-dentialHarvesting`->`Credential Harvesting`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.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	Attack-Pattern.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, there may be multiple attack pat-

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					terns 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

CrowdStrike Indicator Type	ThreatQ Indicator Type
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
registry	Registry Key
service_name	Service Name
url	URL
user_agent	User-agent
username	Username
x509_serial	x509 Serial

CrowdStrike Indicator Type	ThreatQ Indicator Type
x509_subject	x509 Subject

CrowdStrike Reports

```
GET https://api.crowdstrike.com/intel/combined/reports/v1
```

JSON response sample:

```
{
    "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      Published
on 06...",
        "description": "[vc_row][vc_column][vc_page][vc_column_tex-
t]\r\n\r\n\r\n\r\n\r\n\r\nSituational Awareness\r\n\r\n\r\n\r\n \r\nPublished on...",
        "rich_text_description": "<p><div class=\"vc_row wpb_row vc_row-fluid\"><div class-
s=\"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-pub-
lic.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"
            }
        ]
    },
    ...
    ]
}
```

ThreatQ 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. 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- s=\"wpb_column vc_`	A link to the report (from `.resources [].url`) is prepended to the description. The HTML is modified for ideal display in the ThreatQ UI. `<img>`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
				`column_container vc_ col-sm-12\">...`	tags are replaced with a link to the image. 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.-	Report.Attribute	Sub Type	.resources [].created_	Snort/Suricata	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
name			date		
.resources [].tags[].value	Report.Attribute	Tag	.resources [].created_ date	Intel	N/A
.resources [].target_ industries [].value	Report.Attribute	Target Industry	.resources [].created_ date	Technology	N/A
.resources [].target_ countries [].value	Report.Attribute	Target Country	.resources [].created_ date	United States	N/A
.resources [].motivations [].value	Report.Attribute	Motivation	.resources [].created_ date	Espionage	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.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.

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 Runs

> 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 - 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 Run (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

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 Run (January 01, 1997 - September 08, 2020):

Metric	Result
Run Time	30 minutes
Reports	9495
Report Attributes	78660
Adversaries	141
Attack Patterns	248

Known Issues/Limitations

General

- Sometimes, 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 reauthenticate 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

- Due to the enormous size of CrowdStrike's data throughput on their Indicators end-point, ThreatQ strongly recommends an **hourly** run frequency.

- 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 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 reau-thenticate on the first `500 Internal Server Error` received, and usually pro-

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

Change Log

- **Version 3.0.1**

    - Fixed a 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