ThreatQuotient

CrowdStrike Insight EDR CDF Guide

Version 1.0.3

April 12, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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.

Copyright © 2022 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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.

Versioning

- Current integration version `1.0.3`
- Supported on ThreatQ versions >= `4.50.0`

Introduction

The CrowdStrike Insight EDR CDF for ThreatQ is a bi-directional integration aimed to give analysts the ability to export data collections to CrowdStrike, as well as bring back detection incidents from CrowdStrike.

The integration provides the following feeds:

- **CrowdStrike Insight EDR - IOC Export** - exports indicators of compromise from a ThreatQ Data Collection to the Custom IOC list in CrowdStrike Insight EDR.
- **CrowdStrike Insight EDR - Detections** - brings in aggregated detections, along with their behavioral events and related IOCs, into ThreatQ.
- **Get Detections by IDs (supplemental)** - fetches the full details for a given set of detection IDs.
- **CrowdStrike Insight EDR - Hosts** - feeds brings in aggregated detections into ThreatQ.
- **Get Host by IDs (supplemental)** - fetches the full details for a given host IDs.

The following object types are ingested from the feeds above:

- Assets (custom object)
- Attack Patterns
- Events
- Incidents
- Indicators
  - Filename
  - File Path
  - Username
  - MD5
  - SHA-256
  - FQDN
  - Filename
  - Registry Key

See the ThreatQ Mapping chapter for more information.

Prerequisites

The CrowdStrike Insight EDR CDF requires the installation of the following custom object:

- Asset

The files associated with the custom object are included in the integration zip file downloaded from the ThreatQ Marketplace.

Custom Objects Installation

ThreatQuotient provides two methods to install the required custom objects: via script and manual installation.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the custom object zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Install the custom objects using the one of the following methods:

   Via Script

   ThreatQuotient provides a script that will copy the SVG icon and JSON definition file to the correct directories and automatically install the required custom object.

   a. Navigate to tmp directory:

   ```
   <> cd /tmp/
   ```

b. Create a new directory:

```
<> mkdir crowdstrike_insight_edr_cdf
```

c. Upload the **asset.json**, **asset.svg file**, and **install.sh** script into this new directory.

d. Navigate to the new directory, **/tmp/crowdstrike_insight_edr_cdf**, if you have not done so yet.

The directory should resemble the following:

- tmp
  - **crowdstrike_insight_edr_cdf**
    - **asset.json**
    - **install.sh**
    - **asset.svg**

e. Run the following command:

```
<> sudo bash install.sh
```

> You must be in the directory that houses the install.sh, SVG, and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

```
Installing Custom Objects - Step 1 of 5 (Entering Maintenance Mode)

Application is now in maintenance mode.
Installing Custom Objects - Step 2 of 5 (Installing the Asset Custom Object)
Installing Custom Objects - Step 3 of 5 (Configuring image for Asset Custom
Object)
Installing Custom Objects - Step 4 of 5 (Updating Permissions in ThreatQ)
Installing Custom Objects - Step 5 of 5 (Exiting Maintenance Mode)

Application is now live.
```

f. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
<> rm -rf crowdstrike_insight_edr_cdf
```

Manually

Run the following commands via the ThreatQ system's CLI:

a. Navigate to the API directory:

```
<> cd /var/www/api/
```

b. Put your ThreatQ instance into maintenance mode:

```
<> sudo php artisan down
```

c. Upload the asset.json file to the following directory:

`/var/www/api/database/seeds/data/custom_objects/`

d. Upload the SVG icon file included in to the zip to the following directory:

`/var/www/api/database/seeds/data/icons/images/custom_objects/`

e. Run the following command to install the Custom Object Definition:

```
<> sudo php artisan threatq:make-object-set --file=/var/www/
   api/database/seeds/data/custom_objects/asset.json
```

f. Run the following

```
<> sudo php artisan threatq:object-settings --code=object --
   icon=/var/www/api/database/seeds/data/icons/images/
   custom_objects/asset.svg --background-color='#03ac14'
```

g. Clear the ThreatQ object cache and update permissions:

```
<> sudo php /var/www/api/artisan cache:clear

   sudo php /var/www/api/artisan threatq:update-permissions
```

h. Take your ThreatQ instance out of maintenance mode and restart Dynamo:

```
<> sudo php artisan up

   sudo systemctl restart threatq-dynamo
```

Installation

> The CDF requires the installation of a custom object before installing the actual CDF. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

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 integration.

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   All Feeds

PARAMETER	DESCRIPTION
API Hostname	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`
CrowdStrike Client ID	The CrowdStrike Insight EDR API Client ID to authenticate.
CrowdStrike Client Secret	The CrowdStrike Insight EDR API Client Secret to authenticate.

   CrowdStrike Insight EDR - IOC Export | Additional Parameters

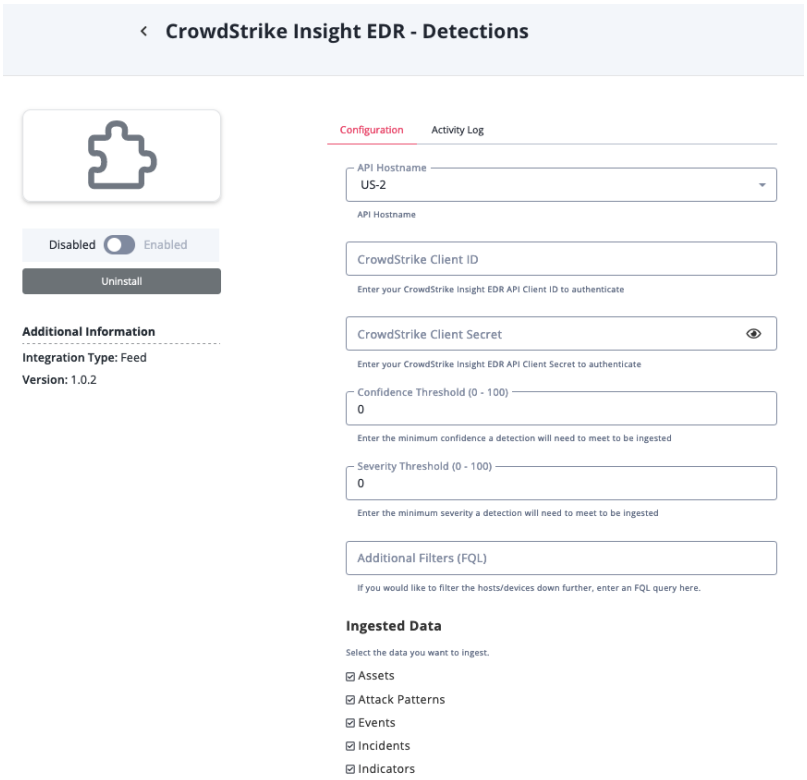
PARAMETER	DESCRIPTION
Data Collection Hash	The hash for your ThreatQ Data Collection to export.
Default Source	The source where this indicator originated. This can be used for tracking where this indicator was defined. The limit 200 characters.
Default Expiration Days	The amount of days the indicators should remain active in CrowdStrike Insight EDR. The default setting is 30 days.
Default Platforms	The platforms where the indicator originated.

CrowdStrike Insight EDR - Detections | Additional Parameters

PARAMETER	DESCRIPTION
Confidence Threshold (0-100)	The minimum confidence a detection will need to meet to be ingested. The default setting is 0.
Severity Threshold (0-100)	The minimum severity a detection will need to meet to be ingested. The default setting is 0.
Additional Filters (FQL)	Enter a FQL query in the field provided to filter the hosts/ devices down further.
Ingested Data	Select the data that will be ingested. Options include: • Assets • Attack Patterns • Events • Incidents • Indicators At least one option must be selected. All options are selected by default.

CrowdStrike Insight EDR - Hosts | Additional Parameters

PARAMETER	DESCRIPTION
Additional Filters (FQL)	Enter a FQL query in the field provided to filter the hosts/ devices down further.



5. Review the **Settings** configuration, 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

ThreatQuotient provides the following mapping for the CrowdStrike Insight EDR CDF.

CrowdStrike Insight EDR - IOC Export

CrowdStrike Insight EDR - IOC Export will export indicators of compromise from a ThreatQ Data Collection to the Custom IOC list in CrowdStrike Insight EDR.

> No data from this feed is ingested back into ThreatQ. The sole purpose is to export indicators to CrowdStrike EDR.

```
POST https://{HOST}/iocs/entities/indicators/v1
```

POST Body

```
[
    {
        "type": "domain",
        "value": "leakforums.sx",
        "expiration": "2023-04-07T10:31:59.236Z",
        "description": "Score: 0; Related Adversaries: FinFisher",
        "source": "ThreatQ",
        "platforms": ["mac", "windows", "linux", "ios", "android"],
        "applied_globally": true
    },
    {
        "type": "ipv4",
        "value": "46.182.107.112",
        "expiration": "2023-04-07T10:31:59.236Z",
        "description": "Score: 0; Related Adversaries: FinFisher",
        "source": "ThreatQ",
        "platforms": ["mac", "windows", "linux", "ios", "android"],
        "applied_globally": true
    }
]
```

CrowdStrike Insight EDR - Detections

`CrowdStrike Insight EDR - Detections` and `Get Detections by IDs (Supplemental)` feeds brings in aggregated detections, along with their behavioral events and related IOCs, into ThreatQ.

This feed retrieves the .resources[] key which is further on used in the `Get Detections by IDs (Supplemental)` supplemental feed call in order to fetch the rest of data.

```
GET https://{HOST}/detects/queries/detects/v1
```

Sample Response


```
{
    "meta": {
        "query_time": 0.016082104,
        "pagination": {
            "offset": 0,
            "limit": 100,
            "total": 3065
        },
        "powered_by": "msa-api",
        "trace_id": "e0f6d630-1558-42d9-86df-d495d9b7e535"
    },
    "resources": [
        "ldt:4c3db6145a704a179a6dacd924f6e8cc:73697616107",
        "ldt:4c3db6145a704a179a6dacd924f6e8cc:73695566300",
        "ldt:4c3db6145a704a179a6dacd924f6e8cc:73694280199"
    ],
    "errors": []
}
```

Get Detections by IDs (Supplemental)

This supplemental feed fetches the full details for a given set of detection IDs.

`POST https://{HOST}/detects/entities/summaries/GET/v1`

Sample Response


```
{
    "meta": {
        "query_time": 0.016374054,
        "powered_by": "msa-api",
        "trace_id": "08a7c526-0fcc-44c0-bf8d-368b3a661cd7"
    },
    "resources": [
        {
            "cid": "e5d4a79a091448bfb80afc724b3cf952",
            "created_timestamp": "2021-08-31T00:20:57.828992776Z",
            "detection_id": "ldt:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
            "device": {
                "device_id": "4c3db6145a704a179a6dacd924f6e8cc",
                "cid": "e5d4a79a091448bfb80afc724b3cf952",
                "agent_load_flags": "0",
                "agent_local_time": "2021-08-12T12:08:19.328Z",
                "agent_version": "6.27.14105.0",
                "bios_manufacturer": "Xen",
                "bios_version": "4.2.amazon",
                "config_id_base": "65994753",
                "config_id_build": "14105",
                "config_id_platform": "3",
                "external_ip": "54.89.138.42",
                "hostname": "WIN10DETECTION",
                "first_seen": "2021-02-09T16:06:00Z",
                "last_seen": "2021-08-31T00:08:11Z",
                "local_ip": "172.17.0.31",
                "mac_address": "02-7d-30-2b-bc-f7",
                "machine_domain": "csanfr.local",
                "major_version": "10",
                "minor_version": "0",
                "os_version": "Windows 10",
                "platform_id": "0",
                "platform_name": "Windows",
                "product_type": "1",
                "product_type_desc": "Workstation",
                "site_name": "Default-First-Site-Name",
                "status": "normal",
                "system_manufacturer": "Xen",
                "system_product_name": "HVM domU",
                "groups": [
                    "47582c7801a4431e8d81d85aae570cd4"
                ],
                "modified_timestamp": "2021-08-31T00:10:03Z",
                "instance_id": "i-084e546a6695e1412",
                "service_provider": "AWS_EC2",
                "service_provider_account_id": "390847698897"
            },
```

```
            "behaviors": [
                {
                    "device_id": "4c3db6145a704a179a6dacd924f6e8cc",
                    "timestamp": "2021-08-31T00:20:17Z",
                    "behavior_id": "5702",
                    "filename": "runningdiskpartmg16.exe",
                    "filepath": "\\Device\\HarddiskVolume2\\Users\\demo\\Desktop\\Malware\\runningdiskpartmg16.exe",
                    "alleged_filetype": "exe",
                    "cmdline": "c:\\Users\\demo\\Desktop\\Malware\\runningdiskpartmg16.exe -k",
                    "scenario": "NGAV",
                    "objective": "Falcon Detection Method",
                    "tactic": "Machine Learning",
                    "tactic_id": "CSTA0004",
                    "technique": "Sensor-based ML",
                    "technique_id": "CST0007",
                    "display_name": "",
                    "description": "This file meets the machine learning-based on-sensor AV protection's high
confidence threshold for malicious files.",
                    "severity": 70,
                    "confidence": 70,
                    "ioc_type": "hash_sha256",
                    "ioc_value": "4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
                    "ioc_source": "library_load",
                    "ioc_description": "\\Device\\HarddiskVolume2\\Users\\demo\\Desktop\\Malware\
\runningdiskpartmg16.exe",
                    "user_name": "WIN10DETECTION$",
                    "user_id": "S-1-5-18",
                    "control_graph_id": "ctg:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
                    "triggering_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656468848626",
                    "sha256": "4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
                    "md5": "d1c27ee7ce18675974edf42d4eea25c6",
                    "parent_details": {
                        "parent_sha256": "9077b1aa0afb8db329fded0e51085de1c51b22a986162f29037fca404a80d512",
                        "parent_md5": "",
                        "parent_cmdline": "C:\\Windows\\system32\\services.exe",
                        "parent_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:476751454426"
                    },
                    "pattern_disposition": 2304,
                    "pattern_disposition_details": {
                        "indicator": false,
                        "detect": false,
                        "inddet_mask": false,
                        "sensor_only": false,
                        "rooting": false,
                        "kill_process": false,
                        "kill_subprocess": false,
                        "quarantine_machine": false,
                        "quarantine_file": false,
                        "policy_disabled": true,
                        "kill_parent": false,
                        "operation_blocked": false,
                        "process_blocked": true,
                        "registry_operation_blocked": false,
                        "critical_process_disabled": false,
                        "bootup_safeguard_enabled": false,
                        "fs_operation_blocked": false,
                        "handle_operation_downgraded": false,
                        "kill_action_failed": false,
                        "blocking_unsupported_or_disabled": false,
                        "suspend_process": false,
                        "suspend_parent": false
```

```
                }
            }
        ],
        "email_sent": true,
        "first_behavior": "2021-08-31T00:20:17Z",
        "last_behavior": "2021-08-31T00:20:18Z",
        "max_confidence": 70,
        "max_severity": 70,
        "max_severity_displayname": "High",
        "show_in_ui": true,
        "status": "new",
        "hostinfo": {
            "domain": ""
        },
        "seconds_to_triaged": 0,
        "seconds_to_resolved": 0,
        "behaviors_processed": [
            "pid:4c3db6145a704a179a6dacd924f6e8cc:656471670052:5702",
            "pid:4c3db6145a704a179a6dacd924f6e8cc:656474610435:5702",
            "pid:4c3db6145a704a179a6dacd924f6e8cc:656470648952:5702",
            "pid:4c3db6145a704a179a6dacd924f6e8cc:656469680329:5702",
            "pid:4c3db6145a704a179a6dacd924f6e8cc:656468848626:5702"
        ]
    }
  ],
  "errors": []
}
```


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[].device.machine_domain + '' + .resources[].device.hostname + ' (' + data.device.local_ip + ')'	Asset. Value	N/A	.resources[]. device.first_seen	csanfr.local\WIN10 DETECTION (172.17 .0.31)	Will be ingested if the `Assets` user_field is checked.
.resources[].device.local_ip	Asset. Attribute	IP Address	.resources[]. device.first_seen	172.17.0.31	N/A
.resources[].device.hostname	Asset. Attribute	Hostname	.resources[]. device.first_seen	WIN10DETECTION	N/A
.resources[].device.external_ip	Asset. Attribute	External IP Address	.resources[]. device.first_seen	54.89.138.42	N/A
.resources[].device.device_id	Asset. Attribute	CrowdStrike Device ID	.resources[]. device.first_seen	4c3db6145a704a17 9a6dacd924f6e8cc	N/A
.resources[].device.os_version	Asset. Attribute	Operating System	.resources[]. device.first_seen	Windows 10	N/A
.resources[].device.product_type_desc	Asset. Attribute	Product Type	.resources[]. device.first_seen	Workstation	N/A
.resources[].device.site_name	Asset. Attribute	Site Name	.resources[]. device.first_seen	Default-First-Site-Name	N/A
.resources[].device.status	Asset. Attribute	Status	.resources[]. device.first_seen	normal	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].device.service_provider	Asset. Attribute	Service Provider	.resources[].device.first_seen	AWS_EC2	N/A
.resources[].device.detection_suppression_status	Asset. Attribute	Detection Suppression Status	.resources[].device.first_seen	unsuppressed	N/A
.resources[].device.service_provider	Asset. Attribute	Service Provider	.resources[].device.first_seen	AWS_EC2	N/A
.resources[].device.host_hidden_status	Asset. Attribute	Host Hidden Status	.resources[].device.first_seen	visible	N/A
.resources[].device.ou	Asset. Attribute	Organizational Unit	.resources[].device.first_seen	Domain Controllers	N/A
.resources[].device.reduced_functionality_mode	Asset. Attribute	Reduced Functionality Mode	.resources[].device.first_seen	no	N/A
.resources[].device.provision_status	Asset. Attribute	Provision Status	.resources[].device.first_seen	Provisioned	N/A
.resources[].device.zone_group	Asset. Attribute	Zone Group	.resources[].device.first_seen	us-east-1a	N/A
.resources[].behaviors[].filename	Indicator. Value	Filename	.resources[].behaviors[].timestamp	runningdiskpartmg16.exe	The status of the indicator is Indirect. Will be ingested if the `Indicators` user_field is checked.
.resources[].behaviors[].filepath	Indicator. Value	File Path	.resources[].behaviors[].timestamp	\Device\HarddiskVolume2\Users\demo\Desktop\Malware\runningdiskpartmg16.exe	The status of the indicator is Indirect. Will be ingested if the `Indicators` user_field is checked.
.resources[].behaviors[].user_name	Indicator. Value	Username	.resources[].behaviors[].timestamp	dstyres	The status of the indicator is Indirect. Will be ingested if the `Indicators` user_field is checked.
.resources[].behaviors[].md5	Indicator. Value	MD5	.resources[].behaviors[].timestamp	d1c27ee7ce18675974edf42d4eea25c6	The status of the indicator is Indirect. Will be ingested if the `Indicators` user_field is checked.
.resources[].behaviors[].sha256	Indicator. Value	SHA-256	.resources[].behaviors[].timestamp	4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9	The status of the indicator is Indirect. Will be ingested if the `Indicators` user_field is checked.
.resources[].behaviors[].alleged_filetype	Indicator. Attribute	Alleged File Type	.resources[].behaviors[].timestamp	exe	N/A
.resources[].behaviors[].confidence	Indicator. Attribute	Confidence	.resources[].behaviors[].timestamp	70	N/A
.resources[].behaviors[].severity	Indicator. Attribute	Severity	.resources[].behaviors[].timestamp	70	N/A
.resources[].behaviors[].ioc_type	Indicator. Type	N/A	.resources[].behaviors[].timestamp	SHA-256	Mapped by using the CrowdStrike Detection Type Mapping table below.
.resources[].behaviors[].ioc_value	Indicator. Value	N/A	.resources[].behaviors[].timestamp	4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9	Will be ingested if the `Indicators` user_field is checked.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].behaviors[].ioc_description	Indicator.Description	N/A	.resources[].behaviors[].timestamp	\Device\HarddiskVolume2\Users\demo\Desktop\Malware\runningdiskpartmg16.exe	N/A
.resources[].behaviors[].ioc_source	Indicator.Attribute	IOC Source	.resources[].behaviors[].timestamp	library_load	N/A
.resources[].max_severity_displayname + 'Severity Detection on' + .resources[].device.hostname + '-' + .resources[].detection_id	Incident.Value	N/A	.resources[].created_timestamp	High Severity Detection on WIN10DETECTION - ldt:4c3db6145a704a179a6dacd924f6e8cc:73693643276	Will be ingested if the `Incidents` user_field is checked.
.resources[].first_behavior	Incident.Started_at	N/A	N/A	2021-08-31T02:30:59	N/A
.resources[].last_behavior	Incident.Ended_at	N/A	N/A	2021-08-31T02:30:59	N/A
.resources[].email_sent	Incident.Attribute	Email Sent	.resources[].created_timestamp	True	N/A
.resources[].max_severity	Incident.Attribute	Max Severity	.resources[].created_timestamp	10	N/A
.resources[].max_confidence	Incident.Attribute	Max Confidence	.resources[].created_timestamp	100	N/A
.resources[].max_severity_displayname	Incident.Attribute	Severity	.resources[].created_timestamp	Medium	N/A
.resources[].detection_id	Incident.Attribute	CrowdStrike Detection ID	.resources[].created_timestamp	ldt:4c3db6145a704a179a6dacd924f6e8cc:73619780939	N/A
.resources[].status	Incident.Attribute	Status	.resources[].created_timestamp	new	N/A
.resources[].seconds_to_resolved	Incident.Attribute	Seconds to Resolved	.resources[].created_timestamp	0	N/A
.resources[].seconds_to_triaged	Incident.Attribute	Seconds to Triaged	.resources[].created_timestamp	70	N/A
.resources[].quarantined_files	Incident.Attribute	Quarantined Files	.resources[].created_timestamp	70	Number of items in .resources[].quarantined_files
.resources[].behaviors[].technique_id + ' - ' + .resources[].behaviors[].technique	Attack Pattern.Value	N/A	.resources[].behaviors[].timestamp	CST0017 - Sensor-based ML	If .resources[].behaviors[].technique_id is a known Mitre Attack, the already existing attack pattern is linked to the objects. The object will be ingested/linked if the `Attack Patterns` user_field is checked.
.resources[].behaviors[].tactic	Attack Pattern.Attribute	Tactic	.resources[].behaviors[].timestamp	Machine Learning	The attribute is added only to new attack patterns
.resources[].behaviors[].scenario + ':' + .resources	Event.Title	N/A	.resources[].behaviors[].timestamp	Ngav: This file meets the machine learning-based on-sensor AV protection's high	Will be ingested if the `Events` user_field is checked. The Event Type is `Detection`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].behaviors[].description				confidence threshold for malicious files.	
.resources[].behaviors[].description	Event. Description	N/A	.resources[].behaviors[].timestamp	This file meets the machine learning-based on-sensor AV protection's high confidence threshold for malicious files.	N/A
.resources[].behaviors[].display_name	Event. Attribute	Behavior	.resources[].behaviors[].timestamp	machine learning	N/A
.resources[].behaviors[].ioc_source	Event. Attribute	IOC Source	.resources[].behaviors[].timestamp	library_load	N/A
.resources[].behaviors[].objective	Event. Attribute	Behavior Objective	.resources[].behaviors[].timestamp	Falcon Detection Method	N/A

CrowdStrike Detection Type Mapping

The CrowdStrike Detection Type (as found in `.resources[].behaviors[].ioc_type` in the Get Detections by IDs Supplemental feed) to ThreatQ Type mapping is as follows:

CROWDSTRIKE INDICATOR TYPE	THREATQ INDICATOR TYPE
domain	FQDN
filename	Filename
hash_md5	MD5
hash_sha256	SHA-256
registry_key	Registry Key

CrowdStrike Insight EDR - Hosts

`CrowdStrike Insight EDR - Hosts` and `Get Host by IDs (Supplemental)` feeds brings in aggregated detections into ThreatQ.

This feed retrieves the .resources[] key which is further on used in the `Get Host by IDs (Supplemental)` supplemental feed call in order to fetch the details.

```
GET https://{HOST}/detects/entities/summaries/GET/v1
```


```
{
    "meta": {
        "query_time": 0.016082104,
        "pagination": {
            "offset": 0,
            "limit": 100,
            "total": 3065
        },
        "powered_by": "msa-api",
        "trace_id": "e0f6d630-1558-42d9-86df-d495d9b7e535"
    },
    "resources": [
        "0b5abb999c1544f1af71983753ff8d22",
        "3eb0e8e03d1245eaa643046f84bc51f8",
        "3fd9b8a8a7ba426a9bf3aaa2ddfc5b02"
    ],
    "errors": []
}
```

Get Host by IDs (Supplemental)

This supplemental feed fetches the full details for a given host IDs.

`POST https://{HOST}/devices/entities/devices/v1`

Sample Response


```
{
  "meta": {
    "query_time": 0.005269768,
    "powered_by": "device-api",
    "trace_id": "d04ebb63-4aab-48ec-a7bc-5495bc6f0f03"
  },
  "resources": [
    {
      "device_id": "3fd9b8a8a7ba426a9bf3aaa2ddfc5b02",
      "cid": "e5d4a79a091448bfb80afc724b3cf952",
      "agent_load_flags": "0",
      "agent_local_time": "2021-10-21T22:05:09.512Z",
      "agent_version": "6.30.14406.0",
      "bios_manufacturer": "American Megatrends Inc.",
      "bios_version": "090008 ",
      "build_number": "19042",
      "config_id_base": "65994753",
      "config_id_build": "14406",
      "config_id_platform": "3",
      "cpu_signature": "329303",
      "external_ip": "20.58.113.63",
      "mac_address": "00-22-48-00-63-1f",
      "instance_id": "3c4c3d6f-fa6d-44d3-8a29-1e7d16ce5dfd",
      "service_provider": "AZURE",
      "service_provider_account_id": "ec5c2f3b-9a85-498b-b609-e81a8e6e2cbd",
      "hostname": "SENTINEL-C-02",
      "first_seen": "2021-06-01T07:48:08Z",
      "last_seen": "2021-10-26T10:11:57Z",
      "local_ip": "172.18.0.9",
      "machine_domain": "illusive-sacumen.com",
      "major_version": "10",
      "minor_version": "0",
      "os_version": "Windows 10",
      "os_build": "19042",
      "ou": [],
      "platform_id": "0",
      "platform_name": "Windows",
      "policies": [
        {
          "policy_type": "prevention",
          "policy_id": "fcde00f4eef9466c8578f2dc587b437a",
          "applied": true,
          "settings_hash": "adc849a6",
          "assigned_date": "2021-09-02T00:14:29.894848191Z",
          "applied_date": "2021-09-02T00:16:03.578241038Z",
          "rule_groups": []
        }
      ],
```

```
"reduced_functionality_mode": "no",
"device_policies": {
  "prevention": {
    "policy_type": "prevention",
    "policy_id": "fcde00f4eef9466c8578f2dc587b437a",
    "applied": true,
    "settings_hash": "adc849a6",
    "assigned_date": "2021-09-02T00:14:29.894848191Z",
    "applied_date": "2021-09-02T00:16:03.578241038Z",
    "rule_groups": []
  },
  "sensor_update": {
    "policy_type": "sensor-update",
    "policy_id": "5b568dec090c480b808830586c134441",
    "applied": true,
    "settings_hash": "65994753|3|2|automatic;101",
    "assigned_date": "2021-10-21T22:03:38.322395302Z",
    "applied_date": "2021-10-21T22:06:51.608393214Z",
    "uninstall_protection": "ENABLED"
  },
  "device_control": {
    "policy_type": "device-control",
    "policy_id": "25d6ae9765624a0b9c1ec577836a8925",
    "applied": true,
    "assigned_date": "2021-10-21T00:51:26.169208737Z",
    "applied_date": "2021-10-21T00:56:09.944670879Z"
  },
  "global_config": {
    "policy_type": "globalconfig",
    "policy_id": "dc483372e2474e2fb5efc99a49a80fc1",
    "applied": true,
    "settings_hash": "c6c03d6",
    "assigned_date": "2021-10-21T22:06:57.220323195Z",
    "applied_date": "2021-10-21T22:08:24.58680563Z"
  },
  "remote_response": {
    "policy_type": "remote-response",
    "policy_id": "ab8edf33dd1e4a178eac44f2b4fc2c25",
    "applied": true,
    "settings_hash": "f472bd8e",
    "assigned_date": "2021-06-01T07:49:34.07955937Z",
    "applied_date": "2021-06-01T07:49:53.428657794Z"
  },
  "firewall": {
    "policy_type": "firewall",
    "policy_id": "b07aa203e1b24a1581b5403390746a36",
    "applied": true,
    "assigned_date": "2021-10-21T00:51:26.169225468Z",
    "applied_date": "2021-10-21T00:56:10.455799263Z",
    "rule_set_id": "b07aa203e1b24a1581b5403390746a36"
  }
},
"groups": [],
"group_hash": "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
"product_type": "1",
"product_type_desc": "Workstation",
"provision_status": "Provisioned",
"serial_number": "0000-0004-3449-1529-1657-8152-51",
"service_pack_major": "0",
"service_pack_minor": "0",
"pointer_size": "8",
```

```
      "site_name": "Default-First-Site-Name",
      "status": "contained",
      "system_manufacturer": "Microsoft Corporation",
      "system_product_name": "Virtual Machine",
      "tags": [],
      "modified_timestamp": "2021-10-26T10:12:02Z",
      "slow_changing_modified_timestamp": "2021-10-26T10:05:23Z",
      "meta": {
        "version": "11755"
      },
      "zone_group": "Sentinel"
    }
  ],
  "errors": []
}
```


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[].machine_domain + '' + .resources[].hostname + '(' + .resources[].local_ip + ')'	Asset.Value	N/A	.resources[].first_seen	illusive-sacumen.com\SENTINEL-C-02 (172.18.0.9)	N/A
.resources[].local_ip	Asset.Attribute	IP Address	.resources[].first_seen	172.17.0.31	N/A
.resources[].hostname	Asset.Attribute	Hostname	.resources[].first_seen	WIN10DETECTION	N/A
.resources[].external_ip	Asset.Attribute	External IP Address	.resources[].first_seen	54.89.138.42	N/A
.resources[]_id	Asset.Attribute	CrowdStrike Device ID	.resources[].first_seen	4c3db6145a704a179a6dacd924f6e8cc	N/A
.resources[].os_version	Asset.Attribute	Operating System	.resources[].first_seen	Windows 10	N/A
.resources[].product_type_desc	Asset.Attribute	Product Type	.resources[].first_seen	Workstation	N/A
.resources[].site_name	Asset.Attribute	Site Name	.resources[].first_seen	Default-First-Site-Name	N/A
.resources[].status	Asset.Attribute	Status	.resources[].first_seen	normal	N/A
.resources[].service_provider	Asset.Attribute	Service Provider	.resources[].first_seen	AWS_EC2	N/A
.resources[].detection_suppression_status	Asset.Attribute	Detection Suppression Status	.resources[].first_seen	unsuppressed	N/A
.resources[].service_provider	Asset.Attribute	Service Provider	.resources[].first_seen	AWS_EC2	N/A
.resources[].host_hidden_status	Asset.Attribute	Host Hidden Status	.resources[].first_seen	visible	N/A
.resources[].ou	Asset.Attribute	Organizational Unit	.resources[].first_seen	Domain Controllers	N/A
.resources[].reduced_functionality_mode	Asset.Attribute	Reduced Functionality Mode	.resources[].first_seen	no	N/A
.resources[].provision_status	Asset.Attribute	Provision Status	.resources[].first_seen	Provisioned	N/A
.resources[].zone_group	Asset.Attribute	Zone Group	.resources[].first_seen	us-east-1a	N/A
.resources[].tags[]	Asset.Tag	N/A	N/A	FalconGroupingTags/testtag	N/A

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 Insight EDR - IOC Export

This run is based on a ThreatQ Data Collection containing ~12k indicators

METRIC	RESULT
Run Time	3 minutes

CrowdStrike Insight EDR - Hosts

METRIC	RESULT
Run Time	1 minute
Assets	3
Asset Attributes	41

CrowdStrike Insight EDR - Detections

METRIC	RESULT
Run Time	1 minute
Assets	1
Asset Attributes	9
Attack Patterns	4
Attack Pattern Attributes	3
Events	2
Event Attributes	10
Incidents	1
Incident Attributes	9
Indicators	9
Indicator Attributes	14

Known Issues / Limitations

- As of the release of version 1.0.3, Host Groups cannot be customized. All indicators will be applied globally.

Change Log

- **Version 1.0.3**
  - Updated the **CrowdStrike Insight EDR - IOC Export** endpoint's URL and body.
  - Added **Default Platform** configuration parameter.
  - Removed the **Policy Type** configuration parameter.
- **Version 1.0.2 rev-a**
  - Updated Custom Object installation steps in the Prerequisites chapter.
- **Version 1.0.2**
  - Fixed an issue where custom object files were missing from the integration download. Updated documentation with steps to install the Asset custom object - see the Prerequisites chapter.
  - Added an Attack Pattern object from Behavior Techniques data in CrowdStrike Insight EDR - Detections Feed.
  - Removed Behavior Technique and Behavior Tactic attributes.
  - Removed the `Ingest Behavior Events` option from the **CrowdStrike Insight EDR - Detections** feed configuration.
  - Users can now select what data will be ingested in ThreatQ by selecting the appropriate option(s) in **CrowdStrike Insight EDR - Detections** feed configuration.
- **Version 1.0.1**
  - 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.
- **Version 1.0.0**
  - Initial release