ThreatQuotient

CrowdStrike Insight EDR CDF Guide

Version 1.0.1

September 30, 2021

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.

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 `1.0.1`
- 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.

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 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:

   Both 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`
Client ID	The CrowdStrike Falcon X Client ID used for authentication.
Client Secret	The CrowdStrike Falcon X Secret used for authentication.

CrowdStrike Insight EDR - IOC Export | Additional Parameters

PARAMETER	DESCRIPTION
Data Collection Hash	The hash for your ThreatQ Data Collection to export.
Policy Type	The Policy Type to apply to the exported indicators. Options include: • Detection (Default) • None
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.

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.

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

CrowdStrike Insight EDR - IOC Export

This feed will export indicators of compromise from a ThreatQ Data Collection to the Custom IOC list in CrowdStrike Insight EDR

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

POST Body

```
[
    {
        "type": "domain",
        "value": "leakforums.sx",
        "source": "ThreatQ",
        "policy": "detect"
    },
    {
        "type": "domain",
        "value": "hackforums.net",
        "source": "ThreatQ",
        "policy": "detect"
    }
]
```

CrowdStrike Insight EDR - Detections

This endpoint ingests aggregated detections, along with their behavioral events and related IOCs, into ThreatQ.

`GET https://{HOST}/detects/queries/detects/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": [
        "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`

POST Body


```
{
    "ids": [
        "ldt:4c3db6145a704a179a6dacd924f6e8cc:73697616107",
        "ldt:4c3db6145a704a179a6dacd924f6e8cc:73695566300",
        "ldt:4c3db6145a704a179a6dacd924f6e8cc:73694280199"
    ]
}
```


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
                }
            },
            {
                "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 -s",
                "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": "dstyres",
                "user_id": "S-1-5-21-339478916-1098358577-1090285819-1106",
                "control_graph_id": "ctg:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
                "triggering_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656469680329",
                "sha256": "4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
                "md5": "d1c27ee7ce18675974edf42d4eea25c6",
                "parent_details": {
                    "parent_sha256": "4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
                    "parent_md5": "d1c27ee7ce18675974edf42d4eea25c6",
                    "parent_cmdline": "c:\\Users\\demo\\Desktop\\Malware\\runningdiskpartmg16.exe -k",
                    "parent_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656468848626"
                },
                "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
                }
            },
            {
                "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 -s",
                "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": "demo",
                "user_id": "S-1-5-21-1282896948-3968879297-3178583196-1002",
                "control_graph_id": "ctg:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
                "triggering_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656470648952",
                "sha256": "4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
                "md5": "d1c27ee7ce18675974edf42d4eea25c6",
                "parent_details": {
                    "parent_sha256": "4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
                    "parent_md5": "d1c27ee7ce18675974edf42d4eea25c6",
                    "parent_cmdline": "c:\\Users\\demo\\Desktop\\Malware\\runningdiskpartmg16.exe -k",
                    "parent_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656468848626"
                },
                "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
                    }
                },
                {
                    "device_id": "4c3db6145a704a179a6dacd924f6e8cc",
                    "timestamp": "2021-08-31T00:20:18Z",
                    "behavior_id": "5702",
                    "filename": "igfxtrayex.exe",
                    "filepath": "\\Device\\HarddiskVolume2\\Users\\demo\\Desktop\\Malware\\igfxtrayex.exe",
                    "alleged_filetype": "exe",
                    "cmdline": "c:\\Users\\demo\\Desktop\\Malware\\igfxtrayex.exe -i",
                    "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": "e2ecec43da974db02f624ecadc94baf1d21fd1a5c4990c15863bb9929f781a0a",
                    "ioc_source": "library_load",
                    "ioc_description": "\\Device\\HarddiskVolume2\\Users\\demo\\Desktop\\Malware\\igfxtrayex.exe",
                    "user_name": "dstyres",
                    "user_id": "S-1-5-21-339478916-1098358577-1090285819-1106",
                    "control_graph_id": "ctg:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
                    "triggering_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656474610435",
                    "sha256": "e2ecec43da974db02f624ecadc94baf1d21fd1a5c4990c15863bb9929f781a0a",
                    "md5": "760c35a80d758f032d02cf4db12d3e55",
                    "parent_details": {
                        "parent_sha256": "e2ecec43da974db02f624ecadc94baf1d21fd1a5c4990c15863bb9929f781a0a",
                        "parent_md5": "760c35a80d758f032d02cf4db12d3e55",
                        "parent_cmdline": "\"c:\\Users\\demo\\Desktop\\Malware\\igfxtrayex.exe\"",
                        "parent_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656471670052"
                    },
                    "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
                }
            },
            {
                "device_id": "4c3db6145a704a179a6dacd924f6e8cc",
                "timestamp": "2021-08-31T00:20:18Z",
                "behavior_id": "5702",
                "filename": "igfxtrayex.exe",
                "filepath": "\\Device\\HarddiskVolume2\\Users\\demo\\Desktop\\Malware\\igfxtrayex.exe",
                "alleged_filetype": "exe",
                "cmdline": "\"c:\\Users\\demo\\Desktop\\Malware\\igfxtrayex.exe\"",
                "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": "e2ecec43da974db02f624ecadc94baf1d21fd1a5c4990c15863bb9929f781a0a",
                "ioc_source": "library_load",
                "ioc_description": "\\Device\\HarddiskVolume2\\Users\\demo\\Desktop\\Malware\\igfxtrayex.exe",
                "user_name": "dstyres",
                "user_id": "S-1-5-21-339478916-1098358577-1090285819-1106",
                "control_graph_id": "ctg:4c3db6145a704a179a6dacd924f6e8cc:73693643274",
                "triggering_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656471670052",
                "sha256": "e2ecec43da974db02f624ecadc94baf1d21fd1a5c4990c15863bb9929f781a0a",
                "md5": "760c35a80d758f032d02cf4db12d3e55",
                "parent_details": {
                    "parent_sha256": "4d4b17ddbcf4ce397f76cf0a2e230c9d513b23065f746a5ee2de74f447be39b9",
                    "parent_md5": "d1c27ee7ce18675974edf42d4eea25c6",
                    "parent_cmdline": "c:\\Users\\demo\\Desktop\\Malware\\runningdiskpartmg16.exe -s",
                    "parent_process_graph_id": "pid:4c3db6145a704a179a6dacd924f6e8cc:656469680329"
                },
                "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 the feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
`data.title`	Event Title	Alert	N/A	`data.additional_dates.event_date`	Chinese Group Targeting French National Cybersecurity Agency (ANSSI)	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 - ThreatQ Data Collection containing ~12k indicators

METRIC	RESULT
Run Time	3 minutes

CrowdStrike Insight EDR - IOC Export exports indicators to CrowdStrike Insight EDR and does not ingest ThreatQ.

CrowdStrike Insight EDR - Detections

METRIC	RESULT
Run Time	1 minute
Incidents	100
Incident Attributes	900
Events	230
Event Attributes	1,654
Indicators	51
Indicator Attributes	122

Change Log

- **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