ThreatQuotient

CrowdStrike Spotlight CDF User Guide

Version 1.0.0

August 28, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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

Contents

Warning and Disclaimer

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

Support

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

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

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

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

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

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.10.0
Support Tier	ThreatQ Supported

Introduction

CrowdStrike is a cybersecurity technology firm pioneering cloud-delivered next-generation endpoint protection and services. The CrowdStrike Spotlight feed ingests detailed information about the vulnerabilities in your environment. Falcon tracks vulnerabilities by industry-standard frameworks like Common Vulnerabilities and Exposures (CVE) and provides information about specific vulnerabilities on your hosts using the Falcon sensor.

The integration provides the following feeds:

- **CrowdStrike Spotlight** - queries CrowdStrike to get a list of vulnerability IDs.
- **CrowdStrike Spotlight Fetch All Data (supplemental)** - queries CrowdStrike to get all vulnerability IDs.
- **CrowdStrike Spotlight Vulnerabilities (supplemental)** - retrieves detailed info about a vulnerability.
- **CrowdStrike Spotlight Remediations (supplemental)** - retrieves detailed remediation info for a vulnerability.
- **CrowdStrike Spotlight Evaluation Logic (supplemental)** - retrieves the evaluation logic used to assess the vulnerability.

The integration ingests the following system objects:

- Assets
- Events
- Indicators
- Vulnerabilities

Prerequisites

You must create a properly scoped API Client within CrowdStrike's Falcon platform in order to use the CrowdStrike feeds.

API Clients can be created and configured via the **API Clients and Keys** page under **Support**.

An API Client must be created for the feeds utilized by the CDF and be given the following API **Read** Scopes by clicking the **Add new API Client** button for **Spotlight Vulnerabilities**.

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

Installation

Perform the following steps to install the integration:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

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

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

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

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

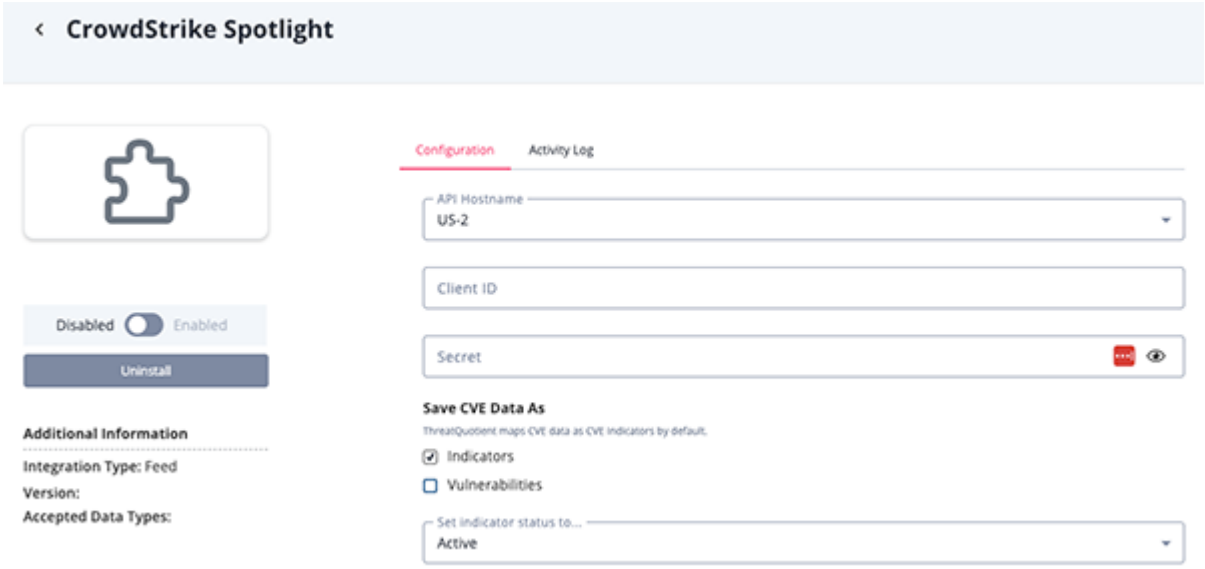
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
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	Your CrowdStrike Client ID.
Secret	Your CrowdStrike Secret Key.
Save CVE Data as	Select where to ingest CVE data as Indicators, Vulnerabilities, or both. The default selection is Indicators.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

CrowdStrike Spotlight

The CrowdStrike Spotlight feed queries CrowdStrike to get a list of vulnerability IDs. When triggered manually, it retrieves all the IDs of vulnerabilities that were created in the range specified at run time. For scheduled runs it retrieves the vulnerabilities updated in the interval set in the scheduler.

`GET https://{HOST}/spotlight/queries/vulnerabilities/v1`

Manual Run API Request Parameters:

```
  {
  "filter":
"created_timestamp:>'2023-08-08T00:00:00Z'%2Bcreated_timestamp:<'2023-08-22T00:
00:00Z'%2Bstatus:!'expired'",
  "limit": 100,
  "sort": "created_timestamp|asc"
}
```

Scheduled Run API Request Parameters

```
  {
  "filter":
"updated_timestamp:>'2023-08-08T00:00:00Z'%2Bupdated_timestamp:<'2023-08-22T00:
00:00Z'%2Bstatus:!'expired'",
  "limit": 100,
  "sort": "updated_timestamp|asc"
}
```

Sample Response:

```
{
  "meta": {
    "query_time": 0.311881787,
    "pagination": {
      "limit": 100,
      "total": 5,
      "after": ""
    },
    "powered_by": "spapi",
    "trace_id": "84a4ad6c-bb1d-4ec1-abdc-47c28ef8c834"
  },
  "resources": [
    "53b17dad0cac483db16ba4b836d6ebcb_b0e6f2c8054930be9d421bd08aad4fc9",
    "53b17dad0cac483db16ba4b836d6ebcb_a9960a82169636738e94245e5f5615f5",
    "53b17dad0cac483db16ba4b836d6ebcb_95ded80fcbc931bdad9a3b1228546636",
    "53b17dad0cac483db16ba4b836d6ebcb_045de5f0f80438dabe0b79bac155d95a",
    "53b17dad0cac483db16ba4b836d6ebcb_299b13de0658352f96b726a559feda54"
```

```
  ]
}
```

CrowdStrike Spotlight Fetch All Data (Supplemental)

The CrowdStrike Spotlight Fetch All Data supplemental feed queries CrowdStrike to all the vulnerability IDs that are inside the time interval of the feed run. This feed uses the same endpoint and parameters as `CrowdStrike Spotlight`. The purpose of this feed is to fetch all the IDs before processing them. This was required because Crowdstrike resets search cursors before the processing is done, and asking for next vulnerability IDs returns an error.

`GET https://{HOST}/spotlight/queries/vulnerabilities/v1`

Manual Run API Request Parameters:

```
  {
  "filter":
"created_timestamp:>'2023-08-08T00:00:00Z'%2Bcreated_timestamp:<'2023-08-22T00:
00:00Z'%2Bstatus:!'expired'",
  "limit": 100,
  "sort": "created_timestamp|asc"
}
```

Scheduled Run API Request Parameters

```
  {
  "filter":
"updated_timestamp:>'2023-08-08T00:00:00Z'%2Bupdated_timestamp:<'2023-08-22T00:
00:00Z'%2Bstatus:!'expired'",
  "limit": 100,
  "sort": "updated_timestamp|asc"
}
```

Sample Response:

```
{
  "meta": {
    "query_time": 0.311881787,
    "pagination": {
      "limit": 100,
      "total": 5,
      "after": ""
    },
    "powered_by": "spapi",
    "trace_id": "84a4ad6c-bb1d-4ec1-abdc-47c28ef8c834"
  },
  "resources": [
    "53b17dad0cac483db16ba4b836d6ebcb_b0e6f2c8054930be9d421bd08aad4fc9",
    "53b17dad0cac483db16ba4b836d6ebcb_a9960a82169636738e94245e5f5615f5",
    "53b17dad0cac483db16ba4b836d6ebcb_95ded80fcbc931bdad9a3b1228546636",
    "53b17dad0cac483db16ba4b836d6ebcb_045de5f0f80438dabe0b79bac155d95a",
    "53b17dad0cac483db16ba4b836d6ebcb_299b13de0658352f96b726a559feda54"
  ]
}
```

CrowdStrike Spotlight Vulnerabilities (Supplemental)

The CrowdStrike Spotlight Vulnerabilities supplemental feed retrieves detailed information about a vulnerability.

```
GET https://{HOST}/spotlight/entities/vulnerabilities/v2?ids={VULN_ID}
```

Sample Response:


```
{
  "meta": {
    "query_time": 0.003822716,
    "powered_by": "spapi",
    "trace_id": "9de15cd2-2842-4d62-afe1-c0d605c97e40"
  },
  "resources": [
    {
      "id":
"53b17dad0cac483db16ba4b836d6ebcb_fd763d4d790032e186e965add846b4a1",
      "cid": "ace79a13936f4ec8ad4de36606814bfc",
      "aid": "53b17dad0cac483db16ba4b836d6ebcb",
      "vulnerability_id": "CVE-2023-0929",
      "data_providers": [
        {
          "provider": "Falcon sensor"
        }
      ],
      "created_timestamp": "2023-05-03T20:26:40Z",
      "updated_timestamp": "2023-06-23T03:29:38Z",
      "status": "expired",
      "apps": [
        {
          "product_name_version": "Chrome",
          "sub_status": "open",
          "remediation": {
            "ids": [
              "5f7d9fc628f13a94b45c9372f60a43d0"
            ]
          },
          "evaluation_logic": {
            "id": "9439f9166e823384a1447c912509b46a"
          }
        }
      ],
      "suppression_info": {
        "is_suppressed": false
      },
      "app": {
        "product_name_version": "Chrome"
      },
```

```
      "cve": {
        "id": "CVE-2023-0929",
        "base_score": 8.8,
        "severity": "HIGH",
        "exploit_status": 0,
        "exprt_rating": "LOW",
        "remediation_level": "O",
        "cisa_info": {
          "is_cisa_kev": false
        },
        "spotlight_published_date": "2023-02-24T12:12:00Z",
        "description": "Use after free in Vulkan in Google Chrome prior to
110.0.5481.177 allowed a remote attacker to potentially exploit heap corruption
via a crafted HTML page. (Chromium security severity: High)\n",
        "published_date": "2023-02-22T00:00:00Z",
        "vendor_advisory": [
          "https://chromereleases.googleblog.com/2023/02/stable-channel-
desktop-update_22.html",
          "https://chromereleases.googleblog.com/2023/02/stable-channel-
desktop-update_22.html"
        ],
        "references": [
          "https://crbug.com/1399742",
          "https://security-tracker.debian.org/tracker/CVE-2023-0929"
        ],
        "exploitability_score": 2.8,
        "impact_score": 5.9,
        "vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H"
      },
      "host_info": {
        "hostname": "WINDOWS-NEW",
        "local_ip": "172.16.114.109",
        "machine_domain": "",
        "os_version": "Windows Server 2012 R2",
        "ou": "",
        "site_name": "",
        "system_manufacturer": "RDO",
        "tags": [],
        "platform": "Windows",
        "os_build": "9600",
        "product_type_desc": "Server",
        "asset_criticality": "Unassigned",
        "internet_exposure": "Unknown",
        "managed_by": "Falcon sensor"
      },
      "remediation": {}
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].vulnerability_id	Vulnerability/ Indicator Value	N/A / CVE	.resources[].cve.published_date	CVE-2023-0929	Depends on user config `Save CVE Data as`
.resources[].cve.description	Vulnerability/ Indicator Description	N/A	N/A	Use after free in Vulkan in Google Chrome prior...	N/A
.resources[].data_providers[].provider	Vulnerability/ Indicator Attribute	Provider	.resources[].cve.published_date	Falcon sensor	N/A
.resources[].updated_timestamp	Vulnerability/ Indicator Attribute	Last updated	.resources[].cve.published_date	2023-06-23T03:29:38Z	If the attribute already exists, the value will be updated
.resources[].apps[].product_name_version	Vulnerability/ Indicator Attribute	Product	.resources[].cve.published_date	Chrome	N/A
.resources[].cve.base_score	Vulnerability/ Indicator Attribute	CVSS Score	.resources[].cve.published_date	8.8	If the attribute already exists, the value will be updated
.resources[].cve.severity	Vulnerability/ Indicator Attribute	Severity	.resources[].cve.published_date	HIGH	If the attribute already exists, the value will be updated
.resources[].cve.exploit_status	Vulnerability/ Indicator Attribute	Exploit Status	.resources[].cve.published_date	0	If the attribute already exists, the value will be updated
.resources[].cve.exprt_rating	Vulnerability/ Indicator Attribute	ExPRT rating	.resources[].cve.published_date	LOW	If the attribute already exists, the value will be updated
.resources[].cve.vendor_advisory	Vulnerability/ Indicator Attribute	Vendor Advisory	.resources[].cve.published_date	https://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	N/A
.resources[].cve.exploitability_score	Vulnerability/ Indicator Attribute	Exploitability	.resources[].cve.published_date	2.8	If the attribute already exists, the value will be updated
.resources[].cve.impact_score	Vulnerability/ Indicator Attribute	CVSS Impact Score	.resources[].cve.published_date	5.9	If the attribute already exists, the value will be updated
.resources[].cve.vector	Vulnerability/ Indicator Attribute	CVSS Vector	.resources[].cve.published_date	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].cve.references	Vulnerability/ Indicator Attribute	Reference URL	.resources[].cve. published_date	https://crbug.com/1399742	N/A
.resources[].host_info.local_ip	Related Asset Value	N/A	N/A	172.16.114.109	N/A
.resources[].host_info.hostname	Related Asset Attribute	Hostname	N/A	WINDOWS-NEW	N/A
.resources[].host_info.os_version	Related Asset Attribute	Operating System	N/A	Windows Server 2012 R2	N/A
.resources[].host_info.product_ type_desc	Related Asset Attribute	Product Type	N/A	Server	N/A
.resources[].host_info.internet_ exposure	Related Asset Attribute	Internet Exposure	N/A	Unknown	N/A

CrowdStrike Spotlight Remediations (Supplemental)

The CrowdStrike Spotlight Remediations supplemental feed receives a remediation ID `.resources[].apps.remediation.ids[]` from `CrowdStrike Spotlight Vulnerabilities` feed and retrieves remediation info for a vulnerability.

```
GET https://{HOST}/spotlight/entities/remediations/v2?ids={REMEDIATION_ID}
```

Sample Response:

```
{
  "meta": {
    "query_time": 0.000200098,
    "powered_by": "spapi",
    "trace_id": "e1b604df-4dd8-4e69-965f-024416fb4708"
  },
  "resources": [
    {
      "id": "5f7d9fc628f13a94b45c9372f60a43d0",
      "reference": "KB5029247",
      "title": "Update Microsoft Windows Server 2019",
      "action": "Install patch for Microsoft Windows Server 2019 17763
(Server): Security Update KB5029247",
      "link": "https://catalog.update.microsoft.com/v7/site/Search.aspx?
q=KB5029247",
      "vendor_url": ""
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].action	Vulnerability/ Indicator Attribute	Remediation	.resources[].cve.published_date	Install patch for Microsoft Windows Server 2019 17763 (Server): Security Update KB5029247	N/A
.resources[].link	Vulnerability/ Indicator Attribute	Remediation Link	.resources[].cve.published_date	https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB5029247	N/A

CrowdStrike Spotlight Evaluation Logic (Supplemental)

The CrowdStrike Spotlight Evaluation Logic supplemental feed receives an evaluation logic ID `.resources[].apps.evaluation_logic.id` from `CrowdStrike Spotlight Vulnerabilities` feed and retrieves information about the tests performed to assess the vulnerability. For each performed test the feed creates and Event.

`GET https://{HOST}/spotlight/entities/evaluation-logic/v1?ids={EVALUATION_LOGIC_ID}`

Truncated Sample Response:


```
{
  "meta": {
    "query_time": 0.079994233,
    "powered_by": "spapi",
    "trace_id": "c9e9c660-f1fc-43ba-9805-98282303915b"
  },
  "resources": [
    {
      "id": "9439f9166e823384a1447c912509b46a",
      "cid": "ace79a13936f4ec8ad4de36606814bfc",
      "aid": "53b17dad0cac483db16ba4b836d6ebcb",
      "data_provider": "Falcon sensor",
      "created_timestamp": "2023-05-03T20:26:41Z",
      "updated_timestamp": "2023-08-22T03:22:19Z",
      "logic": [
        {
          "id": 8626434154966133174,
          "title": "Google Chrome is installed",
          "type": "inventory",
          "description": "",
          "negate": false,
          "existence_check": "at_least_one_exists",
          "comparison_check": "at least one",
          "determined_by_comparison": true,
          "comparisons": {
            "state_operator": "AND",
            "state_comparisons": [
              {
                "entity_operator": "AND",
                "entity_comparisons": [
                  {
                    "actual_value_field": "value",
                    "expected_value": "^Google Chrome.*$",
                    "operation": "pattern match",
                    "value_datatype": "string"
                  }
                ]
              }
```

```
            ]
          },
          "items": [
            {
              "comparison_result": "true",
              "hive": "HKEY_LOCAL_MACHINE",
              "item_type": "registry_item",
              "key": "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\
\Google Chrome",
              "name": "DisplayName",
              "type": "reg_sz",
              "value": [
                "Google Chrome"
              ],
              "windows_view": "32_bit"
            },
            {
              "comparison_result": "true",
              "filename": "Ntoskrnl.exe",
              "filepath": "C:\\windows\\System32\\Ntoskrnl.exe",
              "item_type": "file_item",
              "product_name": "MicrosoftÂ® WindowsÂ® Operating System",
              "product_version": "6.3.9600.18589",
              "version": "6.3.9600.18589",
              "windows_view": "64_bit"
            }
          ]
        }
      ],
      "host_info": {
        "entities_matched": [
          {
            "asset_id": "53b17dad0cac483db16ba4b836d6ebcb"
          }
        ]
      }
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].logic[].title	Related Event Title	N/A	.resources[].created_timestamp	CrowdStrike Spotlight Evaluation Logic: Google Chrome is installed	Prepended with `CrowdStrike Spotlight`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`Evaluation Logic:`
.resources[].description	Related Event Description	N/A	N/A	N/A	Concatenated with other values
.resources[].logic[].negate	Related Event Description	N/A	N/A	Is the threshold for passing the test negated: False	Concatenated with other values
.resources[].logic[].comparison_check	Related Event Description	N/A	N/A	Number of state comparison checks required to validate the vulnerability: at least one	Concatenated with other values if `.resources[].logic[].determined_by_comparison` is true
.resources[].logic[].existence_check	Related Event Description	N/A	N/A	Testing parameters that must match with items found on the host to validate the vulnerability: at_least_one_exists	Concatenated with other values if `.resources[].logic[].determined_by_comparison` is false
.resources[].logic[].comparisons.entity_comparisons[].operation	Related Event Description	N/A	N/A	Operation: pattern match	Concatenated with other values
.resources[].logic[].comparisons.entity_comparisons[].value_datatype	Related Event Description	N/A	N/A	Expected value: ^Google Chrome.*$	Concatenated with other values
.resources[].logic[].comparisons.entity_comparisons[].expected_value	Related Event Description	N/A	N/A	Data type: string	Concatenated with other values
.resources[].logic[].type	Related Event Attribute	Type	.resources[].created_timestamp	inventory	N/A
.resources[].logic[].items[].key	Related Indicator Value	Registry Key	.resources[].created_timestamp	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome	if `.resources[].logic.items[].item_type` is `registry_item`. Prepended with `.resources[].logic.items[].hive`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.resources[].logic[].items[].name	Related Indicator Attribute	Name	.resources[].created_timestamp	DisplayName	if `.resources[].logic.items[].item_type` is `registry_item`
.resources[].logic[].items[].type	Related Indicator Attribute	Type	.resources[].created_timestamp	reg_sz	if `.resources[].logic.items[].item_type` is `registry_item`
.resources[].logic[].items[].value	Related Indicator Attribute	Registry Value	.resources[].created_timestamp	Google Chrome	if `.resources[].logic.items[].item_type` is `registry_item`
.resources[].logic[].items[].filepath	Related Indicator Value	File Path	.resources[].created_timestamp	C:\windows\System32\Ntoskrnl.exe	if `.resources[].logic.items[].item_type` is `file_item`
.resources[].logic[].items[].product_name	Related Indicator Attribute	Product Name	.resources[].created_timestamp	MicrosoftÂ® WindowsÂ® Operating System	if `.resources[].logic.items[].item_type` is `file_item`
.resources[].logic[].items[].product_version	Related Indicator Attribute	Product Version	.resources[].created_timestamp	6.3.9600.18589	if `.resources[].logic.items[].item_type` is `file_item`
.resources[].logic[].items[].windows_view	Related Indicator Attribute	Windows View	.resources[].created_timestamp	64_bit	if `.resources[].logic.items[].item_type` is `file_item`

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.

METRIC	RESULT
Run Time	1 min
Assets	1
Asset Attributes	4
Events	19
Event Attributes	19
Indicators	7
Indicator Attributes	21
Vulnerabilities	12
Vulnerability Attributes	168

Change Log

- **Version 1.0.0**
  - Initial release