ThreatQuotient

Google Chronicle Detections CDF

Version 1.0.0

July 30, 2024

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	>= 6.0.1
Support Tier	ThreatQ Supported

Introduction

The Google Chronicle Detections CDF for ThreatQ enables the automatic ingestion of detections into the ThreatQ platform in the form of Events. The integration allows you to ingest all of your detections and automatically extract indicators such as IP addresses, domains, and URLs from the detection events and entities. You can also submit via specifying a list of rule IDs.

The integration provides the following feed:

- **Google Chronicle Detections** - ingests Google Chronicle Detections in the form of ThreatQ events.

The integration ingests the following system objects:

- Assets
- Events
- Indicators

Prerequisites

The following is required in order to utilize this integration:

- A **Google Chronicle Service Account (Non-Ingestion API) JSON** is required for this integration. This service account configuration should be for use with the Ingestion API. If you do not have this JSON file, contact your Google Chronicle representative to obtain one.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the file on your local machine
6. Select the individual feeds to install, when prompted and click **Install**.

   > 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 feed(s) 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
Chronicle API Region	Select which API region to connect to when communicating with Google Chronicle. Options include: ◦ USA - malachiteingestion-pa.googleapis.com ◦ Europe - europe-malachiteingestion-pa.googleapis.com ◦ London - europe-west2-malachiteingestion-pa.googleapis.com ◦ Singapore - asia-southeast1-malachiteingestion-pa.googleapis.com
Dedicated API Hostname	Optional - Enter you dedicated API region endpoint if you have one. This field will override your selection for the Chronicle API region field.
Service Account JSON	Copy and paste your Google Chronicle Service Account's JSON here. This is given to you by your Google Chronicle representative and allows access to the Non-Ingestion API (Backstory API).
Detection Rule IDs	Enter a line-separated list of Rule IDs to pull detections for. If left blank, all detections from all rules will be pulled.
Ingest Related Assets	Enable this option to ingest assets related to events.

PARAMETER	DESCRIPTION
Event Context Filter	Select the pieces of enrichment context to ingest into ThreatQ for an event. Options include: ◦ Detection Rule Labels (default) ◦ Detection Outcomes (default) ◦ Rule Name (default) ◦ Rule Type (default) ◦ Chronicle Link (default) ◦ Alert State (default) ◦ Detection Time (default) ◦ Detection Type (default) ◦ Detection ID (default)
Related IoCs Filter	Select which related IoCs should be ingested into ThreatQ. Options include: ◦ MD5 (default) ◦ SHA-1 (default) ◦ SHA256 (default) ◦ Email Address (default) ◦ FQDN (default) ◦ IP Address/ IPv6 Address ◦ MAC Address (default) ◦ Filename (default) ◦ File Path (default) ◦ Registry Key (default) ◦ URL (default)
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

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

Google Chronicle Detections

The Google Chronicle Detections feed ingests Google Chronicle Detections as ThreatQ events and will automatically extract indicators such as IP addresses, domains, and URLs from the detection events & entities.

`GET https://{REGION}/v2/detect/rules/-/detections`

Sample Parameters:

```
{
  "start_time": "2024-07-01T00:00:00Z",
  "end_time": "2024-08-01T00:00:00Z",
  "page_size": 1000
}
```

Sample Response:

```
{
  "detections": [
    {
      "collectionElements": [
        {
          "label": "e",
          "references": [
            {
              "event": {
                "about": [
                  {
                    "asset": {
                      "hostname": "host1.dummy.threatq.com",
                      "ip": [
                        "192.168.50.12"
                      ],
                      "category": "Workstation",
                      "networkDomain": "dummy.threatq.com",
                      "type": "WORKSTATION",
                      "deploymentStatus": "deployed",
                      "location": {
                        "city": "New York",
                        "countryOrRegion": "USA",
                        "name": "New York City",
                        "state": "NY"
                      },
                      "platformSoftware": {
                        "platform": "Linux"
                      },
```

```
                    "vulnerabilities": [
                      {
                        "cveId": "CVE-2004-0230"
                      }
                    ]
                  },
                  "file": {
                    "md5": "72fe869aa394ef0a62bb8324857770dd"
                  }
                }
              ],
              "src": {
                "hostname": "vetfashion.xyz",
                "user": {
                  "emailAddresses": "fashion@vet.com"
                },
                "mac": [
                  "00:b0:d0:c2:26"
                ],
                "registry": {
                  "registryKey": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\
\Windows\\CurrentVersion\\Uninstall\\Google Chrome"
                },
                "domain": {
                  "name": "vetfashion.xyz",
                  "registrar": "Fashion",
                  "nameServer": "Fashion US",
                  "firstSeenTime": "2023-07-23T11:42:00Z",
                  "contactEmail": "fashion@vet.com"
                },
                "url": "https://vetfashion.xyz/css/10/admin/index.php",
                "file": {
                  "sha1": "9a301f2a0259bdedb85e2ea4c071534776d471ab",
                  "md5": "72fe869aa394ef0a62bb8324857770bb",
                  "sha256":
"1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586cc",
                  "names": "eicar.exe",
                  "fullPath": "/root/eicar.exe",
                  "fileType": "exe",
                  "mimeType": "application/octet",
                  "capabilitiesTags": [
                    "t1",
                    "t2"
                  ]
                },
                "process": {
                  "file": {
                    "fileType": "cmd",
                    "mimeType": "application/octet",
                    "sha1": "9a301f2a0259bdedb85e2ea4c071534776d47aaa",
```

```
                      "md5": "72fe869aa394ef0a62bb8324857770dd",
                      "sha256":
"1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586b3",
                      "names": "eicar_cmd",
                      "fullPath": "/root/eicar_cmd.exe",
                      "capabilitiesTags": [
                        "t1"
                      ]
                    }
                  }
                },
                "target": {
                  "ip": [
                    "1.2.3.4",
                    "dbc3:d974:24f4:bee8:5a27:135f:31c9:b133"
                  ]
                },
                "metadata": {
                  "baseLabels": {
                    "allowScopedAccess": true,
                    "logTypes": [
                      "UDM"
                    ]
                  },
                  "collectedTimestamp": "2024-07-23T11:41:10Z",
                  "eventTimestamp": "2024-07-23T11:41:10Z",
                  "eventType": "GENERIC_EVENT",
                  "id": "AAAAAPWwZKCHDTZ+APe+vncmzmMAAAAAFAAAAAEAAAA=",
                  "ingestedTimestamp": "2024-07-23T11:41:10.756162Z",
                  "logType": "UDM",
                  "productName": "ThreatQ",
                  "vendorName": "ThreatQuotient"
                },
                "securityResult": [
                  {
                    "about": {
                      "asset": {
                        "hostname":
"dummy.hostbc69ddcd6febc4e74f4f49b699ff0f1e61ccb1a5"
                      },
                      "file": {
                        "md5": "72fe869aa394ef0a62bb8324857770dd"
                      }
                    },
                    "alertState": "NOT_ALERTING",
                    "category": [
                      "SOFTWARE_MALICIOUS"
                    ],
                    "categoryDetails": [
                      ""
```

```
                    ],
                    "confidence": "HIGH_CONFIDENCE",
                    "priority": "MEDIUM_PRIORITY",
                    "severity": "LOW",
                    "threatFeedName": "Bank",
                    "threatStatus": "ACTIVE",
                    "urlBackToProduct": "https://
crinela.sandbox.threatq.online/indicators/1400022/details"
                  }
                ]
              },
              "id": {
                "id": "NTY3YWY5ZjJjOGU4N2QwOGNlMmYwOWI3YWIxZmM4NTA="
              }
            }
          ]
        },
        {
          "label": "ioc",
          "references": [
            {
              "entity": {
                "entity": {
                  "ip": [
                    "148.72.164.179"
                  ]
                },
                "metadata": {
                  "collectedTimestamp": "2024-07-02T08:40:32Z",
                  "entityType": "IP_ADDRESS",
                  "eventMetadata": {
                    "baseLabels": {
                      "allowScopedAccess": true,
                      "logTypes": [
                        "UDM"
                      ]
                    },
                    "id": "AAAAANSfEX62Vhg/yyXXbtHoRo8AAAAABwAAAAIAAAA="
                  },
                  "interval": {
                    "endTime": "2024-07-24T00:00:00Z",
                    "startTime": "2024-07-23T11:30:05Z"
                  },
                  "productName": "ThreatQ",
                  "sourceLabels": [
                    {
                      "key": "threat_source",
                      "value": "BankInfo Security"
                    },
                    {
```

```
                    "key": "threat_source",
                    "value": "AhnLab Security Emergency Response Center"
                  }
                ],
                "sourceType": "ENTITY_CONTEXT",
                "threat": [
                  {
                    "about": {
                      "ip": [
                        "148.72.164.179"
                      ],
                      "user": {
                        "emailAddresses": "fashion2@vet.com"
                      },
                      "mac": [
                        "00:b0:d0:c2:33"
                      ],
                      "registry": {
                        "registryKey": "HKEY_LOCAL_MACHINE\\SOFTWARE\
\Microsoft\\Windows\\CurrentVersion\\Install\\Google Chrome"
                      },
                      "domain": {
                        "name": "vetfashion.abc",
                        "registrar": "ThreatQ2",
                        "nameServer": "ThreatQ2 US",
                        "firstSeenTime": "2024-07-23T11:42:00Z",
                        "contactEmail": "fashion2@vet.com"
                      },
                      "url": "https://vetfashion.abc/css/10/admin/index.php",
                      "file": {
                        "sha1": "9a301f2a0259bdedb85e2ea4c071534776d47111",
                        "md5": "72fe869aa394ef0a62bb832485777011",
                        "sha256":
"1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c958611",
                        "names": "eicar2.exe",
                        "fullPath": "/root/eicar2.exe",
                        "fileType": "exe",
                        "mimeType": "application/octet",
                        "capabilitiesTags": [
                          "a1",
                          "a2"
                        ]
                      },
                      "process": {
                        "file": {
                          "sha1": "9a301f2a0259bdedb85e2ea4c071534776d47a22",
                          "md5": "72fe869aa394ef0a62bb83248577702",
                          "sha256":
"1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c958622",
                          "names": "eicar_cmd2",
```

```
                          "fullPath": "/root/eicar_cmd2.exe"
                        }
                      }
                    },
                    "alertState": "NOT_ALERTING",
                    "category": [
                      "NETWORK_MALICIOUS"
                    ],
                    "categoryDetails": [
                      "test"
                    ],
                    "confidence": "HIGH_CONFIDENCE",
                    "priority": "MEDIUM_PRIORITY",
                    "severity": "LOW",
                    "threatFeedName": "Bank",
                    "threatStatus": "ACTIVE",
                    "threatName": "redline",
                    "urlBackToProduct": "https://threatq.online/indicators/
1400021/details"
                  }
                ],
                "vendorName": "ThreatQuotient"
              }
            },
            "id": {
              "id": "MTNjZjY3NDc2NzJiOTQ1Mzk0MTk3ZjE1OWQ2MTNmMWM="
            }
          }
        ]
      }
    ],
    "createdTime": "2024-07-23T17:58:53.063066Z",
    "detection": [
      {
        "alertState": "NOT_ALERTING",
        "description": "Match ThreatQ IOCs against incoming events",
        "detectionFields": [
          {
            "key": "ip",
            "source": "udm.about.ip",
            "value": "148.72.164.179"
          }
        ],
        "riskScore": 15,
        "ruleId": "ru_a76085f0-31a3-4601-9fed-f4bf30657c0f",
        "ruleLabels": [
          {
            "key": "author",
            "value": "ThreatQuotient"
          },
```

```
            {
              "key": "description",
              "value": "Match ThreatQ IOCs against incoming events"
            },
            {
              "key": "severity",
              "value": "HIGH"
            },
            {
              "key": "priority",
              "value": "MEDIUM_PRIORITY"
            }
          ],
          "ruleName": "threatq_ioc_match_ips",
          "ruleType": "MULTI_EVENT",
          "ruleVersion": "ru_a76085f0-31a3-4601-9fed-
f4bf30657c0f@v_1679587313_251503000",
          "urlBackToProduct": "https://nfr-thrtq.backstory.chronicle.security/
ruleDetections?ruleId=ru_a76085f0-31a3-4601-9fed-
f4bf30657c0fselectedList=RuleDetectionsViewTimelineselectedDetectionId=de_93a23
2f7-0d01-54a7-
ec7a-9db433044c5cselectedTimestamp=2024-07-23T11:42:00ZversionTimestamp=2023-03
-23T16:01:53.251503Z",
          "variables": {
            "ip": {
              "sourcePath": "udm.about.ip",
              "stringVal": "148.72.164.179",
              "type": "MATCH",
              "value": "148.72.164.179"
            }
          },
          "outcomes": [
            {
              "key": "risk_score",
              "value": "1"
            },
            {
              "key": "priority",
              "value": "MEDIUM_PRIORITY"
            },
            {
              "key": "severity",
              "value": "LOW"
            },
            {
              "key": "asset_id_count"
            }
          ]
        }
      ],
```

```
      "detectionTime": "2024-07-23T11:42:00Z",
      "id": "de_93a232f7-0d01-54a7-ec7a-9db433044c5c",
      "timeWindow": {
        "endTime": "2024-07-23T11:42:00Z",
        "startTime": "2024-07-23T11:27:00Z"
      },
      "type": "RULE_DETECTION"
    }
  ]
}
```

ThreatQuotient provides the following default mapping *based on each item with the* `.detections` *list.*

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.detection[].ruleName`	Event.Title	Detection	`.createdTime`	`threatq_ioc_match_ips`	Only the first entry in `detections[]` that has a value for `ruleName` is used.
`.detection[0].detectionFields`	Event.Title	Detection	`.createdTime`	`ip: 148.72.164.179`	Fields `.key` and `.value` are concatenated.
`.detection[0].outcomes[key='risk_score']`	Event.Title	Detection	`.createdTime`	`Risk Score: 1`	If `.key` equals 'risk_score'.
`.detection[0].ruleLabels[key='priority']`	Event.Title	Detection	`.createdTime`	`MEDIUM_PRIORITY`	If `.key` equals 'priority'.
`.detection[0].ruleLabels[key='severity']`	Event.Title	Detection	`.createdTime`	`LOW_SEVERITY`	If `.key` equals 'severity'. `_SEVERITY` appended.
`.detection[].ruleType`	Event.Title	Detection	`.createdTime`	`MULTI_EVENT`	Only the first entry in `detections[]` that has a value for `ruleType` is used.
`.detection[].alertState`	Event.Title	Detection	`.createdTime`	`NOT_ALERTING`	Only the first entry in `detections[]` that has a value for `alertState` is used.
`.detectionTime`	Event.Happened_At	Detection	N/A	`2024-07-23T11:42:00Z`	N/A
`.collectionElements`	Event.Description	Detection	N/A	N/A	Added as JSON to the description.
`.detection[].ruleLabels[].value`	Event.Attribute	`.detection[].ruleLabels[].key`	`.createdTime`	N/A	The attribute name has title case and _ is replaced by . Key `Severity` is replaced with `Rule Severity`.If enabled in configuration.
`.detection[].outcomes[].value`	Event.Attribute	`.detection[].outcomes[].key`	`.createdTime`	N/A	The attribute name has title case and _ is replaced by . Key `Risk Score` is replaced with `Rule Risk Score`. If enabled in configuration.
`.detection[].ruleName`	Event.Attribute	Rule Name	`.createdTime`	`threatq_ioc_match_ips`	If enabled in configuration.
`.detection[].urlBackToProduct`	Event.Attribute	Chronicle Link	`.createdTime`	`https://nfr-thrtq.backstory.chronicle...`	If enabled in configuration.
`.detection[].alertState`	Event.Attribute	Alert State	`.createdTime`	`NOT_ALERTING`	Updated at ingestion. If enabled in configuration.
`.detection[].ruleType`	Event.Attribute	Rule Type	`.createdTime`	`MULTI_EVENT`	If enabled in configuration.
`.type`	Event.Attribute	Detection Type	`.createdTime`	`RULE_DETECTION`	If enabled in configuration.
`.detectionTime`	Event.Attribute	Detection Time	`.createdTime`	`2024-07-23T11:42:00Z`	Updated at ingestion. If enabled in configuration.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.id`	Event.Attribute	Detection ID	`.createdTime`	`de_93a232f7-0d01-54a7-ec7a-9db433044c5c`	If enabled in configuration.
`.collectionElements[].references[].event.src / target.user.emailAddresses`	Event.Related Indicator.Value	Email Address	N/A	`fashion@vet.com`	If enabled in configuration.
`.collectionElements[].references[].event.src /target.hostname`	Event.Related Indicator.Value	FQDN	N/A	`vetfashion.xyz`	If enabled in configuration.
`.collectionElements[].references[].event.src/ target.mac`	Event.Related Indicator.Value	Mac Address	N/A	`00:b0:d0:c2:26`	If enabled in configuration.
`.collectionElements[].references[].event.src / target.process.file.md5`	Event.Related Indicator.Value	MD5	N/A	`72fe869aa394ef0a62bb8324857770dd`	If enabled in configuration.
`.collectionElements[].references[].event.src / target.process.file.sha1`	Event.Related Indicator.Value	SHA-1	N/A	`9a301f2a0259bdedb85e2ea4c071534776d47aaa`	If enabled in configuration.
`.collectionElements[].references[].event.src/ target.process.file.sha256`	Event.Related Indicator.Value	SHA-256	N/A	`1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586cc`	If enabled in configuration.
`.collectionElements[].references[].event.src/ target.process.file.names`	Event.Related Indicator.Value	Filename	N/A	`eicar_cmd`	If enabled in configuration.
`.collectionElements[].references[].event.src/ target.process.file.fullPath`	Event.Related Indicator.Value	File Path	N/A	`/root/eicar_cmd.exe`	If enabled in configuration.
`.collectionElements[].references[].event.src/ target.process.file.fileType`	Event.Related Indicator.Attribute	File Type	N/A	`cmd`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.collectionElements[].references[].event.src/target.process.file.mimeType`	Event.Related Indicator.Attribute	MIME Type	N/A	`application/octet`	N/A
`.collectionElements[].references[].event.src/target.process.file.capabilitiesTags`	Event.Related Indicator.Attribute	Capabilities Tag	N/A	`t1`	N/A
`.collectionElements[].references[].event.src/target.file.md5`	Event.Related Indicator.Value	MD5	N/A	`72fe869aa394ef0a62bb8324857770bb`	If enabled in configuration.
`.collectionElements[].references[].event.src/target.file.sha1`	Event.Related Indicator.Value	SHA-1	N/A	`9a301f2a0259bdedb85e2ea4c071534776d471ab`	If enabled in configuration.
`.collectionElements[].references[].event.src/target.file.sha256`	Event.Related Indicator.Value	SHA-256	N/A	`1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586cc`	If enabled in configuration.
`.collectionElements[].references[].event.src/target.file.names`	Event.Related Indicator.Value	Filename	N/A	`eicar`	If enabled in configuration.
`.collectionElements[].references[].event.src/target.file.fullPath`	Event.Related Indicator.Value	File Path	N/A	`/root/eicar.exe`	If enabled in configuration.
`.collectionElements[].references[].event.src/target.file.fileType`	Event.Related Indicator.Attribute	File Type	N/A	`exe`	N/A
`.collectionElements[].references[].event.src/target.file.mimeType`	Event.Related Indicator.Attribute	MIME Type	N/A	`application/octet`	N/A
`.collectionElements[].references[].event.src/target.file.capabilitiesTags`	Event.Related Indicator.Attribute	Capabilities Tag	N/A	`t1`	N/A
`.collectionElements[].references[].event.src/target.registry.registryKey`	Event.Related Indicator.Value	Registry Key	N/A	`HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft...`	If enabled in configuration.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.collectionElements[].references[].event.src/target.url`	Event.Related Indicator.Value	URL	N/A	`https://vetfashion.xyz/css/10/admin/index.php`	If enabled in configuration.
`.collectionElements[].references[].event.src/target.domain.name`	Event.Related Indicator.Value	FQDN	N/A	`vetfashion.xyz`	If enabled in configuration.
`.collectionElements[].references[].event.src/target.domain.registrar`	Event.Related Indicator.Attribute	Registrar	N/A	`Fashion`	N/A
`.collectionElements[].references[].event.src/target.domain.nameServer`	Event.Related Indicator.Attribute	Nameserver	N/A	`Fashion US`	N/A
`.collectionElements[].references[].event.src/target.domain.firstSeenTime`	Event.Related Indicator.Attribute	First Seen	N/A	`2023-07-23T11:42:00Z`	Updated at ingestion.
`.collectionElements[].references[].event.src/target.domain.contactEmail`	Event.Related Indicator.Attribute	Contact Email	N/A	`fashion@vet.com`	N/A
`.collectionElements[].references[].event.src/target.ip`	Event.Related Indicator.Value	IP Address/IPv6 Address	N/A	`1.2.3.4`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.user.emailAddresses`	Event.Related Indicator.Value	Email Address	N/A	`fashion2@vet.com`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.hostname`	Event.Related Indicator.Value	FQDN	N/A	`vetfashion.xyz`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.mac`	Event.Related Indicator.Value	Mac Address	N/A	`00:b0:d0:c2:33`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.process.file.md5`	Event.Related Indicator.Value	MD5	N/A	`72fe869aa394ef0a62bb832485777011`	If enabled in configuration.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.collectionElements[].references[].entity.metadata.threat[].about.process.file.sha1	Event.Related Indicator.Value	SHA-1	N/A	9a301f2a0259bdedb85e2ea4c071534776d47aaa	If enabled in configuration.
.collectionElements[].references[].entity.metadata.threat[].about.process.file.sha256	Event.Related Indicator.Value	SHA-256	N/A	1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586cc	If enabled in configuration.
.collectionElements[].references[].entity.metadata.threat[].about.process.file.names	Event.Related Indicator.Value	Filename	N/A	eicar_cmd2	If enabled in configuration.
.collectionElements[].references[].entity.metadata.threat[].about.process.file.fullPath	Event.Related Indicator.Value	File Path	N/A	/root/eicar_cmd2.exe	If enabled in configuration.
.collectionElements[].references[].entity.metadata.threat[].about.process.file.fileType	Event.Related Indicator.Attribute	File Type	N/A	cmd	N/A
.collectionElements[].references[].entity.metadata.threat[].about.process.file.mimeType	Event.Related Indicator.Attribute	MIME Type	N/A	application/octet	N/A
.collectionElements[].references[].entity.metadata.threat[].about.process.file.capabilitiesTags	Event.Related Indicator.Attribute	Capabilities Tag	N/A	A1	N/A
.collectionElements[].references[].entity.metadata.threat[].about.file.md5	Event.Related Indicator.Value	MD5	N/A	72fe869aa394ef0a62bb8324857770bb	If enabled in configuration.
.collectionElements[].references[].entity.metadata.threat[].about.file.sha1	Event.Related Indicator.Value	SHA-1	N/A	9a301f2a0259bdedb85e2ea4c071534776d471ab	If enabled in configuration.
.collectionElements[].references[].entity.metadata.threat[].about.file.sha256	Event.Related Indicator.Value	SHA-256	N/A	1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586cc	If enabled in configuration.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.collectionElements[].references[].entity.metadata.threat[].about.file.names`	Event.Related Indicator.Value	Filename	N/A	`eicar2`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.file.fullPath`	Event.Related Indicator.Value	File Path	N/A	`/root/eicar2.exe`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.file.fileType`	Event.Related Indicator.Attribute	File Type	N/A	`exe`	N/A
`.collectionElements[].references[].entity.metadata.threat[].about.file.mimeType`	Event.Related Indicator.Attribute	MIME Type	N/A	`application/octet`	N/A
`.collectionElements[].references[].entity.metadata.threat[].about.file.capabilitiesTags`	Event.Related Indicator.Attribute	Capabilities Tag	N/A	`a1`	N/A
`.collectionElements[].references[].entity.metadata.threat[].about.registry.registryKey`	Event.Related Indicator.Value	Registry Key	N/A	`HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft...`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.url`	Event.Related Indicator.Value	URL	N/A	`https://vetfashion.xyz/css/10/admin/index.php`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.domain.name`	Event.Related Indicator.Value	FQDN	N/A	`vetfashion.xyz`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].about.domain.registrar`	Event.Related Indicator.Attribute	Registrar	N/A	`Fashion`	N/A
`.collectionElements[].references[].entity.metadata.threat[].about.domain.nameServer`	Event.Related Indicator.Attribute	Nameserver	N/A	`Fashion US`	N/A
`.collectionElements[].references[].entity.metadata.`	Event.Related Indicator.Attribute	First Seen	N/A	`2023-07-23T11:42:00Z`	Updated at ingestion.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`threat[].about.domain.firstSeenTime`					
`.collectionElements[].references[].entity.metadata.threat[].about.domain.contactEmail`	Event.Related Indicator.Attribute	Contact Email	N/A	`fashion2@vet.com`	N/A
`.collectionElements[].references[].entity.metadata.threat[].about.ip`	Event.Related Indicator.Value	IP Address/IPv6 Address	N/A	`148.72.164.179`	If enabled in configuration.
`.collectionElements[].references[].entity.metadata.threat[].category`	Event.Related Indicator.Attribute	Category	N/A	`NETWORK_MALICIOUS`	N/A
`.collectionElements[].references[].entity.metadata.threat[].categoryDetails`	Event.Related Indicator.Attribute	Category Detail	N/A	`test`	N/A
`.collectionElements[].references[].entity.metadata.threat[].threatName`	Event.Related Indicator.Attribute	Threat Name	N/A	`redline`	N/A
`.collectionElements[].references[].entity.metadata.threat[].severity`	Event.Related Indicator.Attribute	Severity	N/A	`LOW`	Updated at ingestion
`.collectionElements[].references[].entity.metadata.threat[].confidence`	Event.Related Indicator.Attribute	Confidence	N/A	`HIGH_CONFIDENCE`	Updated at ingestion
`.collectionElements[].references[].entity.metadata.threat[].priority`	Event.Related Indicator.Attribute	Priority	N/A	`MEDIUM_PRIORITY`	Updated at ingestion
`.collectionElements[].references[].entity.metadata.threat[].urlBackToProduct`	Event.Related Indicator.Attribute	Product URL	N/A	`https://threatq.online/indicators/1400021/details`	N/A
`.collectionElements[].references[].entity.metadata.threat[].threatFeedName`	Event.Related Indicator.Attribute	Threat Feed	N/A	`Bank`	N/A
`.collectionElements[].references[].event.src/target/about/`	Event.Related Asset.Value	N/A	N/A	`host1.dummy.threatq.com`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
principal.asset.hostname					
.collectionElements[].references[].event.src/target/about/principal.asset.ip	Event.Related Asset.Value	N/A	N/A	192.168.50.12	If hostname is not present.
.collectionElements[].references[].event.src/target/about/principal.asset.category	Event.Related Asset.Attribute	Category	N/A	Workstation	N/A
.collectionElements[].references[].event.src/target/about/principal.asset.deploymentStatus	Event.Related Asset.Attribute	Deployment Status	N/A	deployed	N/A
.collectionElements[].references[].event.src/target/about/principal.asset.ip	Event.Related Asset.Attribute	IP Address	N/A	192.168.50.12	N/A
.collectionElements[].references[].event.src/target/about/principal.asset.location.city	Event.Related Asset.Attribute	City	N/A	New York	N/A
.collectionElements[].references[].event.src/target/about/principal.asset.location.countryOrRegion	Event.Related Asset.Attribute	Country	N/A	USA	N/A
.collectionElements[].references[].event.src/target/about/principal.asset.location.name	Event.Related Asset.Attribute	Location	N/A	New York City	N/A
.collectionElements[].references[].event.src/target/about/principal.asset.location.state	Event.Related Asset.Attribute	State	N/A	NY	N/A
.collectionElements[].references[].event.src/target/about/	Event.Related Asset.Attribute	Network Domain	N/A	dummy.threatq.com	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`principal.asset.networkDomain`					
`.collectionElements[].references[].event.src/target/about/principal.asset.platformSoftware`	Event.Related Asset.Attribute	Platform	N/A	`Linux`	N/A
`.collectionElements[].references[].event.src/target/about/principal.asset.type`	Event.Related Asset.Attribute	Asset Type	N/A	`WORKSTATION`	N/A
`.collectionElements[].references[].event.src/target/about/principal.asset.vulnerabilities.cveId`	Event.Related Asset.Related Indicator.Value	CVE	N/A	`CVE-2004-0230`	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.

METRIC	RESULT
Run Time	1 minute
Events	27
Event Attributes	300
Indicators	30
Indicator Attributes	250
Assets	15
Asset Attributes	20

Change Log

- **Version 1.0.0**
  - Initial release