ThreatQuotient

Cisco Threat Grid Guide

Version 1.0.1

Monday, November 9, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

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

Contents

Versioning

- Current integration version: 1.0.1
- Supported on ThreatQ versions: 4.34.0 or greater

Introduction

Cisco Threat Grid is a sandbox which allows the detonation of samples to generate analysis reports. The Cisco Threat Grid CDF for ThreatQ enables a user to ingest their organization's sample analysis reports from Threat Grid. These samples can be filtered down by their threat score, so you are able to ingest only the detonations that your organization deems important to track.

Installation

Perform the following steps to install the integration:

Note: *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

Note: *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 Commercial category for integrations. You will still need to configure and then enable the feed.

Configuration

Note: *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.*

To configure the feed:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** tab (optional).
3. Click on the integration to open its details page.
4. Under the Connection tab, enter the following configuration parameters:

Parameter	Description
Threat Grid Host	Enter your Threat Grid host. **Default**: panacea.threatgrid.com
API Key	Enter your Cisco threat Grid API key for authentication.
Threat Score Criteria	Select the threat scores you would like to ingest: • Critical (default) • High (default) • Medium • Low
IOC Severity Threshold	Enter a threshold severity for ingested IOCs **Default**: 50
Ingest Samples	Enabling this will import the malware samples into ThreatQ. ***Note:*** *You must enable downloading sample content via the API in your Threat Grid Account Profile* **Default**: False
Ingest Behavioral Indicators as	Select the object type you would like behavioral indicators stored in

Parameter	Description
	• TTP (default) • Attack Pattern

5. Click on **Save**.
6. Click on the toggle switch to the left of the integration name to enable it.

ThreatQ Mapping

Cisco Threat Grid

This feed ingests analyses as Report Objects within ThreatQ. Any metadata surrounding the reports will be included, as well as related IOCs, related TTPs, and their relevant attribution.

```
GET https://panacea.threatgrid.com/api/v2/search/submissions
```


```
{
  "api_version": 2,
  "id": 6654269,
  "data": {
    "index": 0,
    "total": 5,
    "took": 486,
    "timed_out": false,
    "items_per_page": 10,
    "current_item_count": 5,
    "items": [
      {
        "score": 1000000,
        "matches": {},
        "item": {
          "properties": {
            "metadata": null
          },
          "tags": [],
          "vm_runtime": 300,
          "md5": "2128689698b9a7e496b20bac4ddd42b1",
          "private": false,
          "organization_id": 12882,
          "state": "succ",
          "login": "strivers",
          "sha1": "4d6f2012d5521f240f10b53c769d250d02cd5697",
          "sample": "898bf464b34b3806d9f817004fc31533",
          "filename": "9S659EHDCSI72649DS.doc",
          "analysis": {
            "metadata": {
              "sandcastle_env": {
                "controlsubject": "win7-x64-intel-2020.06.17",
                "vm": "win7-x64",
                "vm_id": "898bf464b34b3806d9f817004fc31533",
                "sample_executed": 1597133073,
                "analysis_end": "2020-08-11T08:10:10Z",
                "analysis_features": [],
                "analysis_start": "2020-08-11T08:03:45Z",
                "display_name": "Windows 7 64-bit",
                "run_time": 300,
                "sandcastle": "3.5.62.17003.0a6e3cc14-1",
                "current_os": "7601.18798.amd64fre.win7sp1_gdr.150316-1654"
              },
              "submitted_file": {
```

```
                "magic": "Composite Document File V2 Document, Little Endian,
Os: Windows, Version 6.1, ...",
                "sha1": "4d6f2012d5521f240f10b53c769d250d02cd5697",
                "filename": "9S659EHDCSI72649DS.doc",
                "sha256":
"10281a188a26dbb10562bdc6f5467abad4b0e7fe73672b48a11fdd55819f81f3",
                "type": "doc",
                "md5": "2128689698b9a7e496b20bac4ddd42b1"
              },
              "general_details": {
                "report_created": "2020-08-11T08:10:17Z",
                "sandbox_version": "pilot-d",
                "sandbox_id": "mtv-work-028"
              },
              "malware_desc": [
                {
                  "sha1": "4d6f2012d5521f240f10b53c769d250d02cd5697",
                  "magic": "Composite Document File V2 Document, Little
Endian, Os: Windows, Version 6.1 ...",
                  "filename": "9S659EHDCSI72649DS.doc",
                  "size": 80896,
                  "sha256":
"10281a188a26dbb10562bdc6f5467abad4b0e7fe73672b48a11fdd55819f81f3",
                  "type": "doc",
                  "md5": "2128689698b9a7e496b20bac4ddd42b1"
                }
              ],
              "analyzed_file": {
                "magic": "Composite Document File V2 Document, Little Endian,
Os: Windows, Version 6.1 ...",
                "sha1": "4d6f2012d5521f240f10b53c769d250d02cd5697",
                "filename": "9S659EHDCSI72649DS.doc",
                "sha256":
"10281a188a26dbb10562bdc6f5467abad4b0e7fe73672b48a11fdd55819f81f3",
                "type": "doc",
                "md5": "2128689698b9a7e496b20bac4ddd42b1"
              }
            },
            "behaviors": [
              {
                "name": "antivirus-flagged-artifact",
                "threat": 72,
                "title": "Artifact Flagged by Antivirus"
              },
              ...
            ],
            "threat_score": 100
          },
          "status": "job_done",
          "submitted_at": "2020-08-11T08:03:44Z",
          "sha256":
"10281a188a26dbb10562bdc6f5467abad4b0e7fe73672b48a11fdd55819f81f3"
        }
      }
    ]
  }
}
```

We do not use any fields from the above API response within ThreatQ. We use a supplemental feed to fetch the full analysis results. That JSON data is parsed for metadata, IOCs, TTPs, etc.

Get Analysis (Supplemental)

This supplemental feed will fetch the full analysis report JSON from Threat Grid's API

```
GET
https://panacea.threatgrid.com/api/v2/samples/{id}/analysis.json
```


```
{
    "version": 4,
    "versions": {
      "version": "4.0",
      "network": {
        "version": "2.0"
      },
      "file": {
        "version": "2.0",
        "html": "0.0",
        "ini": "0.0",
        "js": "0.0",
        "lnk": "2.0",
        "pdf": "0.0",
        "pe": "0.0",
        "rtf": "0.0",
        "txt": "0.0"
      },
      "yara": "1.0",
      "reversing_labs": "1.0",
      "virustotal": "1.0",
      "cognitive": "1.0",
      "heuristic_model": "0.0.20190722T000000Z"
    },
    "metadata": {
      "general_details": {
        "report_created": 1583750398,
        "sandbox_version": "pilot-d",
        "sandbox_id": "mtv-work-087"
      },
      "sandcastle_env": {
        "vm_id": "43a5ae8937855851ee142092d4cd6642",
        "current_os": "7601.18798.amd64fre.win7sp1_gdr.150316-1654",
        "analysis_start": 1583750035,
        "analysis_end": 1583750394,
        "run_time": 300,
        "sample_executed": 1583750081,
        "sandcastle": "3.5.51.16706.30e43d500-1",
        "vm": "win7-x64",
        "controlsubject": "win7-x64-intel-2020.02.03",
        "display_name": "Windows 7 64-bit",
        "analysis_features": []
      },
```

```
      "malware_desc": [
        {
          "filename": "woodguilt.com%2F87229782.png.url",
          "size": 49,
          "md5": "a28a6b6e8924ec4173241a8eff8bf8d3",
          "sha1": "45d2abc7ff3693bb8a0d93fffc36561be28cccb3",
          "sha256":
"48c02c817adef30b675938044d65862e920c494ec13e60567f2c7aca3d7cc07b",
          "magic": "MS Windows 95 Internet shortcut text
(URL=<woodguilt.com/87229782.png>), ASCII text",
          "type": "url"
        }
      ]
    },
    "warnings": [],
    "iocs": [
      {
        "category": [
          "domain"
        ],
        "hits": 1,
        "description": "This indicator indicates that a DNS query was
performed to an unregistered domain name...",
        "title": "DNS Query Returned Non-Existent Domain",
        "data": [
          {
            "Query_Type": "A",
            "Query_ID": 20750,
            "Query_Data": "woodguilt.com",
            "Answer_Code": "NXDOMAIN",
            "Network_Stream": 7
          }
        ],
        "tags": [
          "communication"
        ],
        "truncated": false,
        "confidence": 75,
        "mitre-tactics": [],
        "heuristic_coefficient": -1.88155557784,
        "orbital-queries": [],
        "mitre-techniques": [],
        "ioc": "dns-query-nxdomain",
        "severity": 25
      },
      {
        "category": [
          "network-information"
        ],
        "hits": 1,
        "description": "A name resolution query using the NetBIOS API was
made. NetBIOS is used to facilitate computers...",
        "title": "NetBIOS Name Resolution Query",
        "data": [
          {
            "Domain": "WOODGUILT.COM"
          }
```

```
        ],
        "tags": [
          "netbios"
        ],
        "truncated": false,
        "confidence": 60,
        "mitre-tactics": [],
        "heuristic_coefficient": 1.42572787641,
        "orbital-queries": [],
        "mitre-techniques": [],
        "ioc": "netbios-query",
        "severity": 60
      }
    ],
    "threat": {
      "heuristic_score": 0,
      "threat_score": 36,
      "bucket": "doc",
      "heuristic_raw_score": -5.0775348811833245
    },
    "dynamic": {
      "processes": {
        "11": {
          "registry_keys_read": [],
          "pid": 428,
          "kpid": "0xfffffa80027f37a0",
          "files_deleted": [],
          "files_created": [
            "\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Protect\\S-
1-5-21-2580483871-590521980-3826313501-500\\b0cc0ca3-d62b-440a-b6c1-
e54b3ecf60a2"
          ],
          "file_transactions": [],
          "sockets": [],
          "files_checked": [],
          "sockets_traffic": [],
          "errors": [],
          "monitored": true,
          "registry_keys_deleted": [],
          "ppid": null,
          "mutants_opened": [],
          "memory": [
            {
              "protect": [
                "PAGE_READWRITE"
              ],
              "process": "0xfffffa80027f37a0",
              "allocation_type": [
                "MEM_COMMIT"
              ],
              "entry": [
                {
                  "size": "0x44",
                  "base_address": "0x0"
                },
                ...
              ],
```

```
              "zero_bits": 0,
              "process_handle": "0x3f4"
            },
            ...
          ],
          "new": false,
          "registry_keys_opened": [
            {
              "access": [
                "ENUMERATE_SUB_KEYS",
                "NOTIFY",
                "QUERY_VALUE",
                "READ_CONTROL"
              ],
              "options": [
                "REG_OPTION_NON_VOLATILE"
              ],
              "name":
"REGISTRY\\MACHINE\\SYSTEM\\CONTROLSET001\\CONTROL\\SECURITYPROVIDERS\\SCHANN
EL"
            },
            ...
          ],
          "parent": "",
          "startup_info": {
            "upid": 428,
            "shell_info": "C:\\Windows\\system32\\lsass.exe",
            "current_directory": "C:\\Windows\\system32\\",
            "command_line": "C:\\Windows\\system32\\lsass.exe",
            "uthread": 0,
            "desktop_info": "",
            "tid": "0xfffffa80027b7b50",
            "image_pathname": "C:\\Windows\\system32\\lsass.exe",
            "dll_path":
"C:\\Windows\\system32;C:\\Windows\\system32;C:\\Windows\\system;C:\\Windows;
.;C:\\Windows\\system32;...",
            "runtime_data": "",
            "window_title": "C:\\Windows\\system32\\lsass.exe",
            "incomplete": false
          },
          "process_name": "lsass.exe",
          "registry_keys_modified": [
            {
              "value_name": "LanguageList",
              "data_type": "MULTI_SZ",
              "data": "en-US\u0000en\u0000\u0000",
              "name": "REGISTRY\\USER\\.DEFAULT\\SOFTWARE\\CLASSES\\LOCAL
SETTINGS\\MUICACHE\\3E\\52C64B7E"
            },
            ...
          ],
          "threads": [
            {
              "return": 0,
              "thread": "0x00000000",
              "process": "0x00000000",
              "create_suspended": "0x1",
```

```
              "client_id": 8397322214375721288,
              "process_handle": "0x80000238"
            },
            ...
          ],
          "mutants_created": [],
          "analyzed_because": "Process activity after target sample
started.",
          "files_modified": [
            "\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Protect\\S-
1-5-21-2580483871-590521980-3826313501-500\\Preferred",
            "\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Protect\\S-
1-5-21-2580483871-590521980-3826313501-500\\b0cc0ca3-d62b-440a-b6c1-
e54b3ecf60a2"
          ],
          "atoms_added": [],
          "children": [],
          "registry_keys_created": [],
          "files_read": [
            "\\Users\\Administrator\\AppData\\Roaming\\Microsoft\\Protect\\S-
1-5-21-2580483871-590521980-3826313501-500\\Preferred"
          ],
          "time": "Mon, 09 Mar 2020 10:34:42 UTC"
        },
        ...
      },
      "extracted_keys": [
        {
          "pattern": "openssl",
          "key":
"AAAAAAAAAABSU0RTt6U4JJaqwk+5GKG0zGzxwAEAAABITmV0Q2ZnLnBkYgAAAAAA",
          "offset": 508270176
        },
        ...
      ]
    },
    "disk": {
      "mbr": {
        "hashes": {
          "orig": {
            "md5": "9e9e7db0e9aae4e1c0368a303657893e",
            "sha1": "3ef2fda0124bc0011632e128da23341f3ef369f5",
            "sha256":
"03b44beb83adb31d85667b4cd806cb28a96cef9f3bc815b2ba7c8c68021607b8"
          },
          "curr": {
            "md5": "9e9e7db0e9aae4e1c0368a303657893e",
            "sha1": "3ef2fda0124bc0011632e128da23341f3ef369f5",
            "sha256":
"03b44beb83adb31d85667b4cd806cb28a96cef9f3bc815b2ba7c8c68021607b8"
          }
        },
        "contents": {
          "orig":
"3\u00c0\u008e\u00d0\u00bc\u0000|\u008e\u00c0\u008e\u00d8\u00be\u0000|\u00bf\
u0000\u0006\u00b9\u0000...",
```

```
          "curr":
"3\u00c0\u008e\u00d0\u00bc\u0000|\u008e\u00c0\u008e\u00d8\u00be\u0000|\u00bf\
u0000\u0006\u00b9\u0000..."
        },
        "changed": false
      },
      "partition_tables": {
        "orig": [
          {
            "start": 1048576,
            "type": 7,
            "size": 104857600
          },
          ...
        ],
        "curr": [
          {
            "start": 1048576,
            "type": 7,
            "size": 104857600
          },
          ...
        ],
        "changed": false,
        "changes": {}
      }
    },
    "network": {
      "1": {
        "bytes": 664,
        "bytes_missed": 0,
        "bytes_orig": 0,
        "bytes_orig_payload": 0,
        "bytes_payload": 608,
        "bytes_resp": 664,
        "bytes_resp_payload": 608,
        "conn_state": "SHR",
        "decoded": [
          {
            "client_ip": "192.168.1.41",
            "client_mac": "00:50:a5:4a:ec:7b",
            "dns_servers": [
              "192.168.1.1"
            ],
            "lease_time": 1200,
            "netmask": "255.255.255.0",
            "routers": [
              "192.168.1.1"
            ],
            "server_ip": "192.168.1.1",
            "type": "DHCP_ACK"
          }
        ],
        "dst": "192.168.1.1",
        "dst_port": 67,
        "duration": 0.004355,
        "history": "^d",
```

```
        "packets": 2,
        "packets_orig": 0,
        "packets_resp": 2,
        "protocol": "DHCP",
        "service": "dhcp",
        "session": 1,
        "src": "192.168.1.41",
        "src_port": 68,
        "transport": "UDP",
        "ts_begin": 1583750059.184499,
        "ts_end": 1583750059.188854,
        "uid": "CnmnL8FPcbmixXLv1"
      },
      ...
    },
    "annotations": {
      "network": {
        "204.79.197.200": {
          "country": "US",
          "ts": "2020-03-09T10:39:51Z",
          "reverse_dns": [
            "a-0001.a-msedge.net"
          ],
          "country_name": "United States",
          "org": "Microsoft Corporation",
          "asn": 8068
        },
        ...
      }
    },
    "artifacts": {
      "24": {
        "antivirus": {
          "reversing_labs": {
            "status": "UNKNOWN",
            "scanner_count": 0,
            "scanner_match": 0,
            "threat_name": "",
            "query_hash": {
              "sha256":
"7e9422f3ff99cd583d23daac980b4bbfa9f9da7db7daf5d0698312f9998e71e5"
            },
            "first_seen": "0001-01-01T00:00:00Z",
            "threat_level": 0,
            "trust_factor": 0,
            "last_seen": "0001-01-01T00:00:00Z"
          }
        },
        "created-time": 0,
        "created_by": [],
        "entropy": 3.3735620533361894,
        "executed_from": [],
        "magic-type": "data",
        "md5": "41f805506d2635ed832726196191973c",
        "mime-type": "application/octet-stream; charset=binary",
        "modified_by": [],
        "origin": "extracted",
```

```
        "path": "/\u0005kjjaqfajn2c0uzgv1l4qy5nfwe",
        "read_by": [],
        "relation": {
          "process": null,
          "extracted_from": [
            "5"
          ],
          "contains": null,
          "network": null
        },
        "sha1": "1c8f8f62a7f60281a882d65cc7602afdf9190e98",
        "sha256":
"7e9422f3ff99cd583d23daac980b4bbfa9f9da7db7daf5d0698312f9998e71e5",
        "size": 168,
        "type": "",
        "whitelist": []
      },
      ...
    },
    "status": {
      "origin": "sandcastle",
      "ran": true,
      "vm": "win7-x64",
      "playbook": "default",
      "id": "43a5ae8937855851ee142092d4cd6642",
      "analysis_submitted_at": 1583750033,
      "state": "proc",
      "ven": "phl-ven",
      "sha256":
"48c02c817adef30b675938044d65862e920c494ec13e60567f2c7aca3d7cc07b",
      "status": "Updating analysis status.",
      "running_on": "mtv-work-087",
      "analysis_started_at": 1583750035,
      "md5": "a28a6b6e8924ec4173241a8eff8bf8d3",
      "vm_runtime": 300,
      "sha1": "45d2abc7ff3693bb8a0d93fffc36561be28cccb3",
      "sample_started_at": 1583750081,
      "queue": "NA",
      "original_filename": "woodguilt.com%2F87229782.png.url"
    },
    "domains": {
      "woodguilt.com": {
        "status": "indeterminate",
        "content_categories": [],
        "security_categories": []
      },
      ...
    }
  }
```

The following table shows the mapping for the analysis results:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
data.status.original_filename	Value	Report	Limited to 50 chars	data.status.analysis_started_at	N/A	N/A
data.metadata.malware_desc[].filename	Title	Attachment	Limited to 50 chars	data.status.analysis_started_at	N/A	N/A
data.status.id	Attribute	Threat Grid Link	Formatted into URL	data.status.analysis_started_at	N/A	N/A
data.status.vm	Attribute	Threat Grid VM	N/A	data.status.analysis_started_at	N/A	N/A
data.status.playbook	Attribute	Threat Grid Playbook	N/A	data.status.analysis_started_at	N/A	N/A
data.threat.heuristic_score	Attribute	Heuristic Score	N/A	data.status.analysis_started_at	N/A	N/A
data.threat.threat_score	Attribute	Threat Score	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.malware_desc[].filename	Indicator Value	Filename	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.malware_desc[].magic	Indicator Value	URL	Value is split so we can get the actual URL	data.status.analysis_started_at	N/A	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
data.metadata.malware_desc[].md5	Indicator Value	MD5	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.malware_desc[].sha1	Indicator Value	sha1	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.malware_desc[].sha256	Indicator Value	SHA-256	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].title	Value	TTP / Attack Pattern	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].description	Description	TTP / Attack Pattern	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[]	Value	Indicator	N/A	data.status.analysis_started_at	N/A	Mapped using the iocs[].data[] entries below
data.metadata.iocs[].mitre-tactics[]	Value	TTP	Mapped: {MITRE ID} - {Value}	data.status.analysis_started_at	N/A	If no mapping found, just title case
data.metadata.iocs[].mitre-techniques[]	Attribute	Technique	Title-cased	data.status.analysis_started_at	N/A	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
data.metadata.iocs[].data[].Path	Indicator Value	File Path	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[].Domain	Indicator Value	FQDN	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[].URL	Indicator Value	URL	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[].IP	Indicator Value	IP Address	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[].SHA256	Indicator Value	SHA-256	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[].Process_Name	Indicator Value	Filename	N/A	data.status.analysis_started_at	N/A	Status: Indirect
data.metadata.iocs[].data[].Original_Filename	Indicator Value	Filename	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[].Antivirus_Result	Attribute	Antivirus Detection	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].data[].Security	Attribute	Security Category	N/A	data.status.analysis_started_at	N/A	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
data.metadata.iocs[].data[].Category	Attribute	Content Category	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].Category	Attribute	Category	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].ioc	Attribute	Indicator	N/A	data.status.analysis_started_at	N/A	A programmatic name for the TTP
data.metadata.iocs[].severity	Attribute	Severity	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].tags	Attribute	Tag	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.iocs[].suspected-sample-categories	Attribute	Suspected Sample Category	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.domains.{domain}	Value	Indicator	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.domains.{domain}.content_categories	Attribute	Content Category	N/A	data.status.analysis_started_at	N/A	N/A
data.metadata.domains.{domain}.security_categories	Attribute	Security Category	N/A	data.status.analysis_started_at	N/A	N/A

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples	Notes
data.metadata.domains.{domain}.status	Attribute	Status	N/A	data.status.analysis_started_at	N/A	N/A

Average Run Time

Note: *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
Indicators	47
Indicator Attributes	77
Report	4
Report Attributes	23
TTPs	48
TTP Attributes	280

Change Log

Version	Details
1.0.1	Fixed filter error during ingestion
1.0.0	Initial Release