ThreatQuotient

ESET CDF

Version 2.0.0

May 28, 2025

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	2.0.0
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The ESET CDF for ThreatQ enables analysts to automatically ingest ESET feeds that contain information about: Botnet network, malicious domains, files and URLs.

The integration provides the following feeds:

- **ESET Botnet -** based on ESET's proprietary, automated botnet tracking system, this feed features two types of sub-feeds: C&C and targets. The data provided includes items such as detection, hash, last alive, files downloaded, IP addresses, protocols, targets, and other information. IoCs (Indicators of Compromise) include MD5, SHA-1, SHA-256, C&Cs (URLs).
- **ESET Domain -** blocks malicious domains to prevent users from visiting the sites and, therefore, stay protected against infections and data breaches. Such domains are usually part of phishing campaigns, malware distribution, or a larger cyber attack. The feed covers the domain name, the data associated with it, and respective malicious activity. The feed also provides information on the level of confidence in the form of an assessment of which domain to block.
- **ESET Malicious Files -** provides real-time information on the currently prevalent malware samples as well as their characteristics and IoCs (Indicators of Compromise). It features the assessment of shared hashes of malicious executable files and associated data.
- **ESET URL -**
- provides information about current and prevalent malicious URLs and associated data. The feed is created from all URL sources every five minutes, deduplication happens every 24 hours, and the filtering in this case is stricter to ensure no sensitive information is being shared. Therefore, it is based on sharing URLs without parameters.
- **ESET PUA Adware Files -** provides real-time information on the currently prevalent PUA (Potentially Unwanted Application) samples that contain adware or have another unclear objective.
- **ESET PUA Dual-Use App Files -** provides real-time information on the currently prevalent PUA dual-use applications. Dual-use apps, such as RMM or other multi-purpose tools, are legitimate (possibly commercial) software that attackers might misuse.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Malware
  - Malware Attributes
- Signatures
  - Signature Attributes
- Identities
  - Identity Attributes
- Events
  - Event Attributes

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
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(s).

Configuration

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

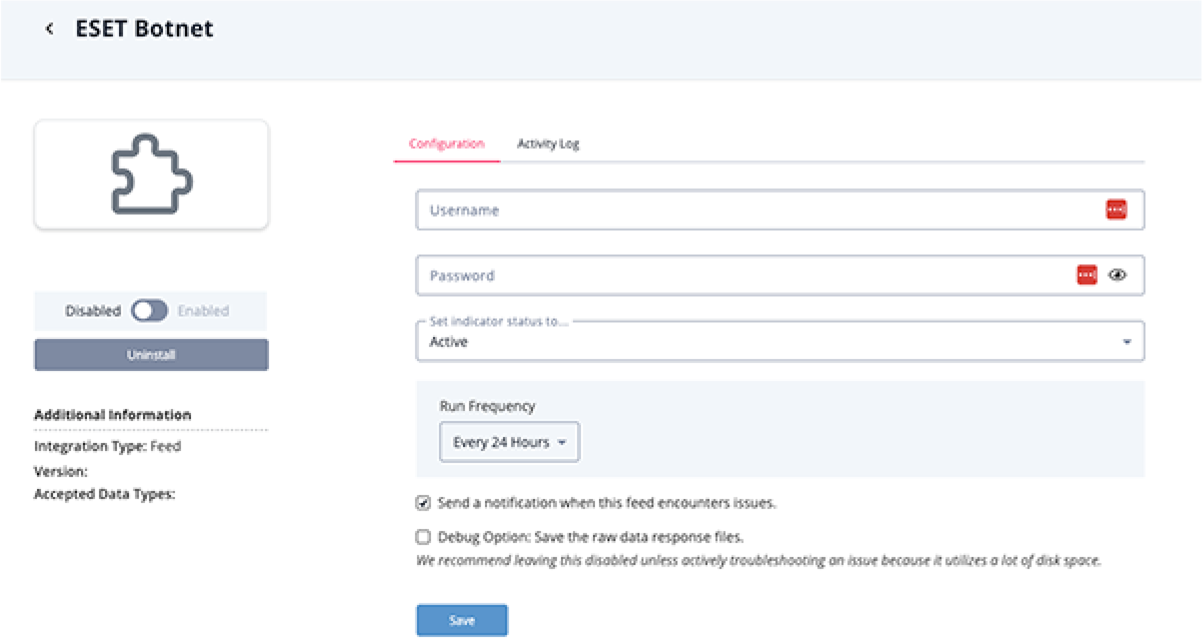
To configure the integration:

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
Username	Your ESET Threat Intelligence username.
Password	Your ESET Threat Intelligence password.
Enable SSL Certificate Verification	When enabled, the feed will validate the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	When enabled, feed will not honor proxies set in the ThreatQ UI.


ESET Botnet
Configuration
Activity Log
Username
Password
Set indicator status to...
Active
Run Frequency
Every 24 Hours
Disabled
Enabled
Uninstall
Additional Information
Integration Type: Feed
Version:
Accepted Data Types:
☑ Send a notification when this feed encounters issues.
☐ Debug Option: Save the raw data response files.
We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.
Save

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

All feeds access the same endpoint, https://eti.eset.com/taxiiservice, each requesting the content of a specific collection.

ESET Botnet

The ESET Botnet feed connects to the `ei.botnet (stix2)` collection. The feed ingests data about the Botnet network, and it also retrieves information about Command and Control (CnC) servers. The feed returns a list of STIX bundles, each of them containing:

- Indicators
- Malware
- Signatures
- Identities
- Events
- The relationships between the returned objects

`GET https://taxii.eset.com/taxii2/643f4eb5-f8b7-46a3-a606-6d61d5ce223a/collections/0abb06690b0b47e49cd7794396b76b20/objects?added_after=2025-05-19T00:00:00.000000Z`

> The JSON data returned is a list of qualified STIX bundles that are passed into ThreatQ's STIX Parser.

Sample Response:

```
{
  "objects": [
    {
      "id": "indicator--21817511-8742-449d-89f8-2008260120f3",
      "type": "indicator",
      "spec_version": "2.1",
      "created_by_ref": "identity--55f6ea5e-51ac-4344-bc8c-4170950d210f",
      "created": "2025-05-18T20:06:31.000Z",
      "modified": "2025-05-18T20:06:31.000Z",
      "name": "Malware variant",
      "description": "Each of these file hashes indicates that a variant of a
variant of MSIL/Kryptik.ANRN trojan is present.",
      "pattern": "[file:hashes.'SHA-256' =
'2675f542d19822f027a4d3cfd38e8dc1946f2bb714531140f158de05b8cae40d'] OR
[file:hashes.'SHA-1' = '0069ed4853c0e1fe4c106c7b1063a41ceed6161b'] OR
[file:hashes.'MD5' = 'ec8847e14d45376c1e82431e0cc66d06']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "valid_from": "2025-05-18T20:06:31Z",
      "valid_until": "2025-05-20T20:06:31Z",
      "labels": ["malicious-activity"],
      "confidence": 85,
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ]
    },
    {
      "id": "relationship--01bf9c75-57b4-412e-b9b9-2eadd0607aaf",
      "type": "relationship",
      "spec_version": "2.1",
      "created": "2025-05-18T20:06:31.000Z",
      "modified": "2025-05-18T20:06:31.000Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--21817511-8742-449d-89f8-2008260120f3",
      "target_ref": "malware--bbae912b-a2cc-47b3-9c92-7a7b7c05fca8"
    }
  ]
}
```

> The response was truncated due to its large content. The mapping for this feed is handled by the native ThreatQ STIX 2 parser. The value of the attributes `Modified At`, `Confidence`, `Valid From`, `Valid Until`, `Last Seen` is updated at ingestion.

ESET Domain

The ESET Domain feed connects to the `ei.domains v2 (stix2)` collection. The feed ingests domains that are considered malicious. The feed returns a list of STIX bundles, each of them containing:

- Indicators
- Malware
- Signatures
- Identities
- Events
- The relationships between the returned objects

```
GET https://taxii.eset.com/taxii2/643f4eb5-f8b7-46a3-a606-6d61d5ce223a/
collections/a34aa0a4f9de419582a883863503f9c4/objects?
added_after=2025-05-19T00:00:00.000000Z
```

> The JSON data returned is a list of qualified STIX bundles that are passed into ThreatQ's STIX Parser.

Sample Response:

```
{
  "objects": [
    {
      "id": "indicator--21f664ef-d515-4b5b-82a5-ef1d233387a6",
      "type": "indicator",
      "spec_version": "2.1",
      "created_by_ref": "identity--55f6ea5e-51ac-4344-bc8c-4170950d210f",
      "created": "2025-05-19T17:36:20.000Z",
      "modified": "2025-05-19T17:36:20.000Z",
      "name": "Unwanted",
      "description": "Host is known source of active fraudulent content.",
      "pattern": "[domain-name:value = 'simplyumedia.com']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "valid_from": "2025-05-19T17:36:20Z",
      "valid_until": "2025-05-21T17:36:20Z",
      "labels": ["unwanted-activity"],
      "confidence": 50,
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ]
    },
    {
      "id": "sighting--e3c356af-23fe-4bba-ac1e-4ea6483b5320",
      "type": "sighting",
      "spec_version": "2.1",
      "created": "2025-05-19T17:36:20.000Z",
      "modified": "2025-05-19T17:36:20.000Z",
      "sighting_of_ref": "indicator--21f664ef-d515-4b5b-82a5-ef1d233387a6",
      "where_sighted_refs": ["location--6975048e-da66-4dc3-ad4e-36588085df91"]
    },
    {
      "id": "ipv4-addr--68fbfe33-bc13-47b9-ac36-b1c644a641eb",
      "type": "ipv4-addr",
      "spec_version": "2.1",
      "value": "77.111.246.40",
      "modified": "2025-05-19T17:36:20.000Z",
      "created": "2025-05-19T17:36:20.000Z"
    }
  ]
}
```

The response was truncated due to its large content. The mapping for this feed is handled by the native ThreatQ STIX 2 parser. The value of the attributes `Modified At`, `Confidence`, `Valid From`, `Valid Until`, `Last Seen` is updated at ingestion.

ESET Malicious Files

The ESET Malicious Files feed connects to the `ei.malicious files v2 (stix2)` collection. It ingest data about executable files that are considered malicious. The feed returns a list of STIX bundles, each of them containing:

- Indicators
- Malware
- Signatures
- Identities
- Events
- The relationships between the returned objects

```
GET https://taxii.eset.com/taxii2/643f4eb5-f8b7-46a3-a606-6d61d5ce223a/
collections/ee6a153ed77e4ec3ab21e76cc2074b9f/objects?
added_after=2025-05-19T00:00:00.000000Z
```

> The JSON data returned is a list of qualified STIX bundles that are passed into ThreatQ's STIX Parser.

Sample Response:

```
{
  "objects": [
    {
      "id": "indicator--ae88887c-2535-4160-a375-bbc17612627e",
      "type": "indicator",
      "spec_version": "2.1",
      "created_by_ref": "identity--55f6ea5e-51ac-4344-bc8c-4170950d210f",
      "created": "2025-05-19T17:13:26.000Z",
      "modified": "2025-05-19T17:13:26.000Z",
      "name": "Malware variant",
      "description": "Each of these file hashes indicates that a variant of
HTML/Phishing.Agent.GTH trojan is present.",
      "pattern": "[file:hashes.'SHA-256' =
'a7837b46d380ea4da505304b33008c30dbad2d5bcb9ccb7b2108b3c23f318942'] OR
[file:hashes.'SHA-1' = '062e90a1a71962a2fb5b8fa72031a26307adc5be'] OR
[file:hashes.'MD5' = '7188bcc1c65d4aaa0b392f3764547ab9']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "valid_from": "2025-05-19T17:13:26Z",
      "valid_until": "2025-05-21T17:13:26Z",
      "labels": ["malicious-activity"],
      "confidence": 85,
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ]
    },
    {
      "id": "relationship--0facb46a-394c-4393-8709-588e13f71a70",
      "type": "relationship",
      "spec_version": "2.1",
      "created": "2025-05-19T17:13:26.000Z",
      "modified": "2025-05-19T17:13:26.000Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--ae88887c-2535-4160-a375-bbc17612627e",
      "target_ref": "malware--f243d5cf-5643-4c89-9ed1-2ddfe293e346"
    }
  ]
}
```

The response was truncated due to its large content. The mapping for this feed is handled by the native ThreatQ STIX 2 parser. The value of the attributes `Modified At`, `Confidence`, `Valid From`, `Valid Until`, `Last Seen` is updated at ingestion.

ESET URL

The ESET URL feed connects to the `ei.urls (stix2)` collection. It ingests addresses that are considered malicious. THis feed is different from the ESET Domain feed based on the filter options ESET has it place. For example, there are objects blocked on the URL level only and not at the domain level. in this case the ESET Domain feed will not return the objects. The feed returns a list of STIX bundles, each of them containing:

- Indicators
- Malware
- Signatures
- Identities
- Events
- The relationships between the returned objects

```
GET https://taxii.eset.com/taxii2/643f4eb5-f8b7-46a3-a606-6d61d5ce223a/
collections/1d3208c143be49da8130f5a66fd3a0fa/objects?
added_after=2025-05-19T00:00:00.000000Z
```

> The JSON data returned is a list of qualified STIX bundles that are passed into ThreatQ's STIX Parser.

Sample Response:

```
{
  "objects": [
    {
      "id": "indicator--51c49522-3968-4b19-bcc3-9f61ea33e519",
      "type": "indicator",
      "spec_version": "2.1",
      "created_by_ref": "identity--55f6ea5e-51ac-4344-bc8c-4170950d210f",
      "created": "2025-05-19T17:35:23.000Z",
      "modified": "2025-05-19T17:35:23.000Z",
      "name": "BlockedObject",
      "description": "Host actively distributes high-severity threat in the
form of executable code.",
      "pattern": "[url:value = 'https://bsc.macomp.co.il/netfiles/
104012e89E80D70C65F42EB8DC303A8D7117A1C.pdf']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "valid_from": "2025-05-19T17:35:23Z",
      "valid_until": "2025-05-21T17:35:23Z",
      "labels": ["benign"],
      "confidence": 85,
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ]
    },
    {
      "id": "sighting--ebceba56-729a-4851-8188-1757aa73028c",
      "type": "sighting",
      "spec_version": "2.1",
      "created": "2025-05-19T17:35:23.000Z",
      "modified": "2025-05-19T17:35:23.000Z",
      "sighting_of_ref": "indicator--51c49522-3968-4b19-bcc3-9f61ea33e519",
      "where_sighted_refs": ["location--bce13320-c8fd-4329-b431-539446ec67df"]
    },
    {
      "id": "relationship--0f877f7d-2120-4ae9-ac79-b89506377f55",
      "type": "relationship",
      "spec_version": "2.1",
      "created": "2025-05-19T17:35:23.000Z",
      "modified": "2025-05-19T17:35:23.000Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--51c49522-3968-4b19-bcc3-9f61ea33e519",
      "target_ref": "malware--6b3fea19-50c4-46ab-8e77-d58739599e26"
    }
  ]
}
```

The response was truncated due to its large content. The mapping for this feed is handled by the native ThreatQ STIX 2 parser. The value of the attributes `Modified At`, `Confidence`, `Valid From`, `Valid Until`, `Last Seen` is updated at ingestion.

ESET PUA Adware Files

The ESET PUA Adware Files feed connects to the `puaadware stix 2.1` collection. It ingests PUA (Potentially Unwanted Application) samples from the ESET Portal as the following objects below which contain adware or have another unclear objective. The feed returns a list of STIX bundles, each of them containing:

- Indicators
- Malware
- Signatures
- Identities
- The relationships between the returned objects

```
GET https://taxii.eset.com/taxii2/643f4eb5-f8b7-46a3-a606-6d61d5ce223a/
collections/d1bfc81202fc4c6599326771ec2da41d/objects?
added_after=2025-05-19T00:00:00.000000Z
```

> The JSON data returned is a list of qualified STIX bundles that are passed into ThreatQ's STIX Parser.

Sample Response:

```
{
  "objects": [
    {
      "id": "indicator--313a3c03-d717-491f-83fa-e5b727eaaa83",
      "type": "indicator",
      "spec_version": "2.1",
      "created_by_ref": "identity--55f6ea5e-51ac-4344-bc8c-4170950d210f",
      "created": "2025-05-19T19:50:58.000Z",
      "modified": "2025-05-19T19:50:58.000Z",
      "name": "Malware variant",
      "description": "Each of these file hashes indicates that a variant of a
variant of Win32/Toolbar.AVG.B potentially unwanted application is present.",
      "pattern": "[file:hashes.'SHA-256' =
'4215b6e375fe739773a8575cd1ab568cc18954d657650e7d73be1e023d28029e'] OR
[file:hashes.'SHA-1' = '18ea49910e4e0812c5fcc4fbdc49c202c6164c93'] OR
[file:hashes.'MD5' = '543a68d0df53f69a991381a7b7ecc874']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "valid_from": "2025-05-19T19:50:58Z",
      "valid_until": "2025-05-21T19:50:58Z",
      "labels": ["malicious-activity"],
      "confidence": 85,
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ]
    },
    {
      "id": "relationship--1c42d2c6-d574-4174-9a03-e6fabe78e595",
      "type": "relationship",
      "spec_version": "2.1",
      "created": "2025-05-19T19:50:58.000Z",
      "modified": "2025-05-19T19:50:58.000Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--313a3c03-d717-491f-83fa-e5b727eaaa83",
      "target_ref": "malware--e70845a5-a720-479d-882a-72b2481b1070"
    }
  ]
}
```

> The response was truncated due to its large content. The mapping for this feed is handled by the native ThreatQ STIX 2 parser. The value of the attributes `Modified At`, `Confidence`, `Valid From`, `Valid Until`, `Last Seen` is updated at ingestion.

ESET PUA Dual-Use App Files

The ESET PUA Dual-Use App Files feed connects to the `puadualapps stix 2.1` collection. It ingests PUA (Potentially Unwanted Application) dual-use applications from the ESET Portal as the following objects below which contain have another unclear objectives. The feed returns a list of STIX bundles, each of them containing:

- Indicators
- Malware
- Signatures
- Identities
- The relationships between the returned objects

`GET https://taxii.eset.com/taxii2/643f4eb5-f8b7-46a3-a606-6d61d5ce223a/collections/970a7d0039ac4668addf058cd9feb953/objects?added_after=2025-05-19T00:00:00.000000Z`

> The JSON data returned is a list of qualified STIX bundles that are passed into ThreatQ's STIX Parser.

Sample Response:

```
{
  "more": true,
  "objects": [
    {
      "id": "indicator--59f5219e-4de1-4aa6-8f56-13d2b0a722ee",
      "type": "indicator",
      "spec_version": "2.1",
      "created_by_ref": "identity--55f6ea5e-51ac-4344-bc8c-4170950d210f",
      "created": "2025-05-19T20:05:50.000Z",
      "modified": "2025-05-19T20:05:50.000Z",
      "name": "Malware variant",
      "description": "Each of these file hashes indicates that a variant of
Python/CoinMiner.B potentially unsafe application is present.",
      "pattern": "[file:hashes.'SHA-256' =
'3dc41d3f46c61de16e556265d95a3a9945e31d73eff7f1d47d823f096dbc9a00'] OR
[file:hashes.'SHA-1' = '8628f7002498a14678e32406aa63b8233b791d08'] OR
[file:hashes.'MD5' = '1aa523e6886c463415b056eb0b724c8d']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "valid_from": "2025-05-19T20:05:50Z",
      "valid_until": "2025-05-21T20:05:50Z",
      "labels": ["malicious-activity"],
      "confidence": 85,
      "object_marking_refs": [
        "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
      ]
    },
    {
      "id": "malware--1b89ebce-486e-4334-a22d-a6bb686015ae",
      "type": "malware",
      "spec_version": "2.1",
      "created": "2025-05-19T20:05:50.000Z",
      "modified": "2025-05-19T20:05:50.000Z",
      "name": "Python/CoinMiner.B potentially unsafe application",
      "malware_types": ["trojan"],
      "is_family": false,
      "labels": ["trojan"],
      "confidence": 85
    }
  ]
}
```

The response was truncated due to its large content. The mapping for this feed is handled by the native ThreatQ STIX 2 parser. The value of the attributes `Modified At`, `Confidence`, `Valid From`, `Valid Until`, `Last Seen` is updated at ingestion.

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.

ESET Botnet

METRIC	RESULT
Run Time	1 hour 52 minutes
Identities	372
Identity Attributes	4,572
Indicators	3,566
Indicator Attributes	75,499
Malware	37
Malware Attributes	1,693
Signatures	883
Signatures Attributes	29,266

ESET Domain

METRIC	RESULT
Run Time	2 hours 10 minutes
Identities	1
Identity Attributes	385
Indicators	28,588
Indicator Attributes	130,279
Malware	218
Malware Attributes	1,098
Signatures	21,788
Signatures Attributes	87,152

ESET Malicious Files

METRIC	RESULT
Run Time	2 hours 33 minutes
Indicators	46,681
Indicator Attributes	294,292
Malware	829

METRIC	RESULT
Malware Attributes	4,823
Signatures	11,192
Signatures Attributes	44,777

ESET URL

METRIC	RESULT
Run Time	1 hour 2 minutes
Events	726
Event Attributes	15,435
Identities	1
Identity Attributes	225
Indicators	10,231
Indicator Attributes	52,048
Malware	215
Malware Attributes	1,063
Signatures	8,345
Signatures Attributes	33,380

ESET PUA Adware Files

METRIC	RESULT
Run Time	4 minutes 12 seconds
Identities	1
Identity Attributes	2
Indicators	2,069
Indicator Attributes	14,389
Malware	147
Malware Attributes	441
Signatures	433
Signatures Attributes	2165

ESET PUA Dual-Use App Files

METRIC	RESULT
Run Time	6 minutes 24 seconds
Identities	1
Identity Attributes	2
Indicators	4,254

METRIC	RESULT
Indicator Attributes	29,759
Malware	168
Malware Attributes	504
Signatures	903
Signatures Attributes	4,515

Known Issues / Limitations

- The data feeds' retention is two weeks. Data older than 14 days is not available for retrieval.

Change Log

- **Version 2.0.0**
  - Updated the feeds to use new available endpoints.
  - Added two new feeds:
    - ESET PUA Adware Files
    - ESET PUA Dual-Use App Files
  - Updated the minimum ThreatQ version to 5.12.0.
  - Added a new known issue / limitation to the guide - the data feeds' retention is two weeks. Data older than 14 days is not available for retrieval.
- **Version 1.0.0**
  - Initial release