ThreatQuotient

ESET CDF Guide

Version 1.0.0

April 18, 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	>= 4.45.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/eset-cdf

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** - ingests all the data that ESET has about the Botnet network.
- **ESET Domain** - ingests all the domains that ESET considers malicious.
- **ESET Malicious Files** - ingests all the information from ESET about malicious executable files.
- **ESET URL** - ingests all the URL addresses that ESET considers malicious.

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

   > 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.

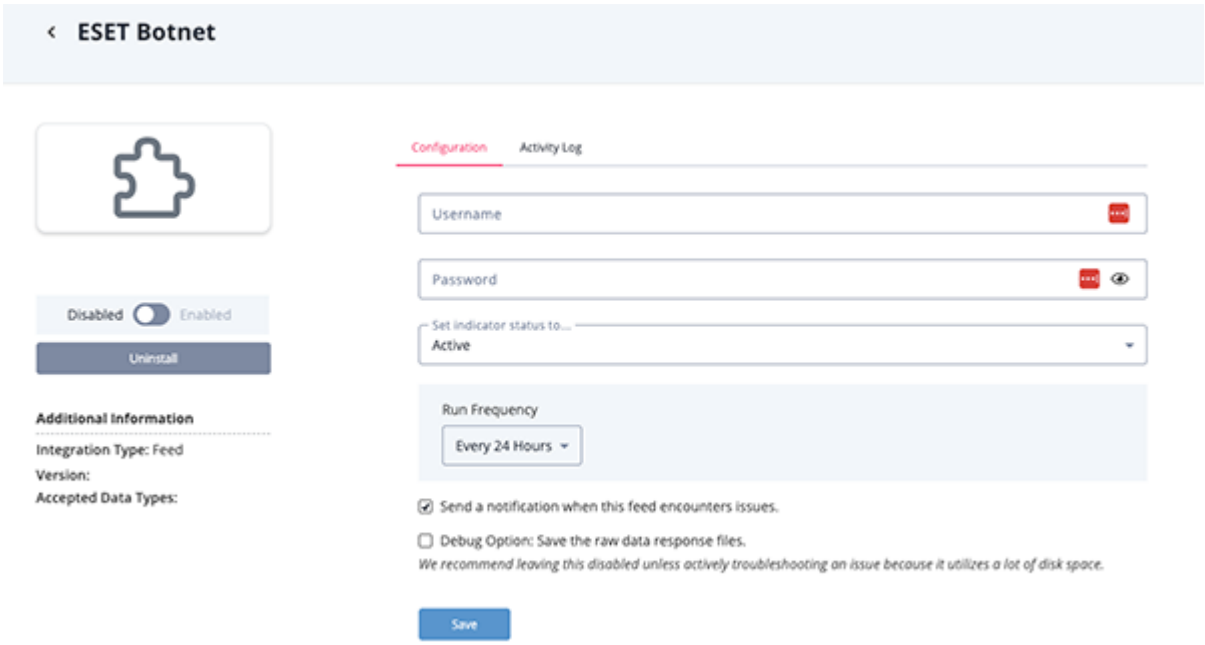
To configure the integration:

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
Username	Your ESET Threat Intelligence username.
Password	Your ESET Threat Intelligence password.



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

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

Sample Response:

```
[
  {
    "type": "bundle",
    "id": "bundle--641d5f27-7ef0-4054-a600-f69057ab3806",
    "spec_version": "2.0",
    "objects": [
      {
        "type": "indicator",
        "id": "indicator--b8402472-9596-48d3-830d-a7d949ee94f6",
        "created": "2023-04-03T23:00:08.000Z",
        "modified": "2023-04-03T23:00:08.000Z",
        "name": "Malware variant",
        "description": "Each of these file hashes indicates that a variant of Win32/Smokeloader.H trojan is
present.",
        "pattern": "[file:hashes.'SHA-256'='5ff522ebf07f1690a47e48acd18b0943767b0f7d260364da4f94b93317a31730'] OR
[file:hashes.'SHA-1'='37f4f5bdc93a84bda083534ae955d392360fe1c3'] OR
[file:hashes.'MD5'='4152c7b57926b5bedcfec17767773b01']",
        "valid_from": "2023-04-03T23:00:08Z",
        "valid_until": "2023-04-05T23:00:08Z",
        "labels": [
          "malicious-activity"
```

```
      ]
    },
    {
      "type": "malware",
      "id": "malware--a2a6cd60-2a56-49a6-bae9-88e5c64f1b00",
      "created": "2023-04-03T23:00:08.000Z",
      "modified": "2023-04-03T23:00:08.000Z",
      "name": "Win32/Smokeloader.H trojan",
      "labels": [
        "trojan"
      ]
    },
    {
      "type": "relationship",
      "id": "relationship--56e9bb28-2206-4138-96ca-741d9baf0865",
      "created": "2023-04-03T21:00:20.021Z",
      "modified": "2023-04-03T21:00:20.021Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--b8402472-9596-48d3-830d-a7d949ee94f6",
      "target_ref": "malware--a2a6cd60-2a56-49a6-bae9-88e5c64f1b00"
    }
  ]
 }
]
```


The response was truncated due to its large content.

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

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

Sample Response:


```
[
  {
    "type": "bundle",
    "id": "bundle--3fe2712c-b84b-4ce3-bca6-39b059cf6624",
    "spec_version": "2.0",
    "objects": [
      {
        "type": "indicator",
        "id": "indicator--a7607110-56e3-4085-8e20-42a29412c783",
        "created": "2023-04-03T23:01:27.000Z",
        "modified": "2023-04-03T23:01:27.000Z",
        "name": "BlockedObject",
        "description": "Host actively distributes high-severity threat in the form of executable code.",
        "pattern": "[domain-name:value='tagavara.medipno.ee']",
        "valid_from": "2023-04-03T23:01:27Z",
        "valid_until": "2023-04-05T23:01:27Z",
        "labels": [
          "benign"
        ]
      },
      {
        "type": "observed-data",
        "id": "observed-data--9053c68d-5731-4e20-a68c-aa2c569b1078",
        "created": "2023-04-03T23:01:27.000Z",
        "modified": "2023-04-03T23:01:27.000Z",
        "first_observed": "2022-02-05T23:00:00Z",
        "last_observed": "2023-04-03T20:06:52Z",
        "number_observed": 27,
        "objects": {
          "0": {
            "type": "domain-name",
```

```
          "value": "tagavara.medipno.ee"
        }
      }
    },
    {
      "type": "relationship",
      "id": "relationship--0e5c2302-80d8-4cb9-b056-1a533708086a",
      "created": "2023-04-03T21:03:10.217Z",
      "modified": "2023-04-03T21:03:10.217Z",
      "relationship_type": "based-on",
      "source_ref": "indicator--a7607110-56e3-4085-8e20-42a29412c783",
      "target_ref": "observed-data--9053c68d-5731-4e20-a68c-aa2c569b1078"
    }
  ]
 }
]
```


The response was truncated due to its large content.

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

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

Sample Response:


```
[
  {
    "type": "bundle",
    "id": "bundle--788cb4ee-10ca-4001-bf13-0ae66e9dad25",
    "spec_version": "2.0",
    "objects":[
       {
        "type": "indicator",
        "id": "indicator--25abe44f-b442-41e5-bc58-f24827bee0dc",
        "created": "2023-04-03T23:10:25.000Z",
        "modified": "2023-04-03T23:10:25.000Z",
        "name": "Malware variant",
        "description": "Each of these file hashes indicates that a variant of HTML/Phishing.Microsoft.MO trojan is
present.",
        "pattern": "[file:hashes.'SHA-256'='4b65eaabd5c3ff60022395193b42522cb87de570ffe0783772623f3d758cf920'] OR
[file:hashes.'SHA-1'='021c93e227780a67e353aa2b8f3042e88cdfb64f'] OR
[file:hashes.'MD5'='3bc468899d6a9b7e72b7fa74a3656f6a']",
        "valid_from": "2023-04-03T23:10:25Z",
        "valid_until": "2023-04-05T23:10:25Z",
        "labels": [
          "malicious-activity"
        ]
      },
      {
        "type": "malware",
        "id": "malware--ddd8f67f-689a-438e-b379-07db3a2dfdec",
        "created": "2023-04-03T23:10:25.000Z",
        "modified": "2023-04-03T23:10:25.000Z",
        "name": "HTML/Phishing.Microsoft.MO trojan",
        "labels": [
          "trojan"
```

```
      ]
    },
    {
      "type": "relationship",
      "id": "relationship--13c92b9d-00be-4dd9-a6c3-c291e45497c7",
      "created": "2023-04-03T21:13:02.749Z",
      "modified": "2023-04-03T21:13:02.749Z",
      "relationship_type": "indicates",
      "source_ref": "indicator--25abe44f-b442-41e5-bc58-f24827bee0dc",
      "target_ref": "malware--ddd8f67f-689a-438e-b379-07db3a2dfdec"
    }
  ]
 }
]
```


The response was truncated due to its large content.

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

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

Sample Response:


```
[
  {
    "type": "bundle",
    "id": "bundle--be49ffff-9713-42b9-ae3d-64f26d23b459",
    "objects": [
      {
        "type": "indicator",
        "id": "indicator--cbbeeb43-dd54-41b6-8259-db62a61272c4",
        "created": "2023-04-03T23:05:07.000Z",
        "modified": "2023-04-03T23:05:07.000Z",
        "name": "BlockedObject",
        "description": "Host actively distributes high-severity threat in the form of executable code.",
        "pattern": "[url:value='http://www.fazendariogrande.pr.gov.br/transparencia/licitacoes']",
        "valid_from": "2023-04-03T23:05:07Z",
        "valid_until": "2023-04-05T23:05:07Z",
        "labels": [
          "benign"
        ]
      },
      {
        "type": "identity",
        "id": "identity--40aa094b-29e2-4801-bd22-5f61a1adaba0",
        "created": "2023-04-03T21:05:22.521Z",
        "modified": "2023-04-03T21:05:22.521Z",
        "name": "customer",
        "identity_class": "individual",
        "contact_information": "BR"
      },
```

```
    {
      "type": "relationship",
      "id": "relationship--bc0b9c4a-c768-4d2c-a1c0-09a82a75e783",
      "created": "2023-04-03T21:05:22.521Z",
      "modified": "2023-04-03T21:05:22.521Z",
      "relationship_type": "related-to",
      "source_ref": "identity--40aa094b-29e2-4801-bd22-5f61a1adaba0",
      "target_ref": "indicator--cbbeeb43-dd54-41b6-8259-db62a61272c4"
    }
  ]
 }
]
```


The response was truncated due to its large content.

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

Change Log

- **Version 1.0.0**
  - Initial release