ThreatQuotient

EternalLiberty CDF

Version 1.0.0

July 08, 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 3
Support 4
Integration Details 5
Introduction 6
Installation 7
Configuration 8
ThreatQ Mapping 9
EternalLiberty 9
Average Feed Run 12
Change Log 13

Warning and Disclaimer

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

Support

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

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

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

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

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

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.25.0
Support Tier	ThreatQ Supported

Introduction

The EternalLiberty CDF enables users to automatically ingest threat actor details from the EternalLiberty GitHub repository. This allows you to stay up-to-date on advisories, bulletins, and analyses' from the Abnormal Security team.

The integration provides the following feed:

- **EternalLiberty** - pulls threat actor data from the EternalLiberty Repo and ingests them into ThreatQ as Adversary objects.

The integration ingests Adversary object types and 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 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 **OSINT** 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. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

EternalLiberty

The EternalLiberty feed periodically pulls threat actor data from the EternalLiberty Repo and ingests them into ThreatQ as Adversary objects.

`GET https://raw.githubusercontent.com/StrangerealIntel/EternalLiberty/main/EternalLiberty.json`

Sample Response:


```
{
    "name":  "EternalLiberty",
    "author":  [
                   "Arkbird_SOLG",
                   "BushidoToken",
                   "Faisalusuf"
               ],
    "version":  "1.2",
    "data":  [
                  {
                      "official_name":  "FIN1",
                      "confidence":  "High",
                      "type":  "Organized Crime",
                      "country":  "Russia",
                      "alias":  [
                                    {
                                        "entity":  "Mandiant/FireEye",
                                        "name":  "FIN1"
                                    }
                                ]
                  },
                  {
                      "official_name":  "FIN4",
                      "confidence":  "High",
                      "type":  "Organized Crime",
                      "country":  "Romania",
                      "alias":  [
                                    {
                                        "entity":  "Mandiant/FireEye",
                                        "name":  "FIN4"
                                    },
                                    {
                                        "entity":  "CrowdStrike",
                                        "name":  "Wolf Spider"
                                    },
                                    {
```

```
                                    "entity":  "MITRE",
                                    "name":  "G0085"
                                }
                            ]
                },
                {
                    "official_name":  "FIN5",
                    "confidence":  "High",
                    "type":  "Organized Crime",
                    "country":  "Unknown",
                    "alias":  [
                                {
                                    "entity":  "Mandiant/FireEye",
                                    "name":  "FIN5"
                                },
                                {
                                    "entity":  "MITRE",
                                    "name":  "G0053"
                                }
                            ]
                },
...
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data[].official_name	Adversary.Name	Adversary	Uses the Created At date	FIN4	N/A
data[].confidence	Adversary.Attribute	Confidence	N/A	High	Updatable
data[].type	Adversary.Attribute	Type	N/A	Organized Crime	N/A
data[].country	Adversary.Attribute	Country	N/A	Romania	N/A
data[].alias.name	Related Adversary.Name	Adversary	N/A	Wolf Spider	List of related alias names
data[].alias.entity	Related Adversary.Attribute	Source	N/A	CrowdStrike	Intel source per alias

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	8 minutes
Adversaries	2,024
Adversary Attributes	3,943

Change Log

- **Version 1.0.0**
  - Initial release