ThreatQuotient

Area 1 CDF User Guide

Version 1.0.0

October 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	>= 4.11.0
Support Tier	ThreatQ Supported

Introduction

Area 1 provides anti-phishing services and intelligence data based in their research for customers. The Area 1 CDF ingests this intelligence data into your ThreatQ instance.

The integration provides the following feed:

- **Area 1** - consumes indicators from the Area 1 security vendor from their `/indicators` endpoint.

The integration ingests adversaries and indicators (FQDN, IP Address, MD5, SHA-1, SHA-256). The integration also provides the following supporting context:

- Category
- Classification Disposition
- Confidence
- Delivery Vector
- Last Seen
- Malware Family
- Threat Name
- Threat Type

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 **Labs** 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
Feed Name	The name of the feed that will be displayed in the ThreatQ UI.
Username	Your Area 1 account username for the HTTPS basic authentication.
Password	Your Area 1 account password for the HTTPS basic authentication.

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

Area 1

The Area1 feed consumes indicators from the Area1 security vendor from their `/indicators` endpoint. The feed consumption happens over https using basic authentication.

Sample Response:


```
{
    "data": [
        {
            "threat_name": "Area 1 Identified Malicious",
            "first_seen": 1539088006512,
            "last_seen": 1539088006512,
            "item_type": "url",
            "item_name": "elitebeauty.co.ke\/wp-includes\/widgetss\/",
            "threat_categories": [
                {
                    "classification_disposition": [
                        "Unclassified"
                    ],
                    "delivery_vector": [
                        "Phishing"
                    ],
                    "threat_type": [
                        "Actor Infrastructure"
                    ],
                    "category": [
                        "Universal"
                    ]
                }
            ]
        },
        {
            "tag_histories": [
                {
                    "intervals": [
                        {
                            "start": 1435384584000,
                            "end": "current"
                        }
                    ],
                    "category": "Actor",
                    "value": "PUB5"
                },
                {
                    "intervals": [
```

```
                        {
                            "start": 1435384584000,
                            "end": "current"
                        }
                    ],
                    "category": "Indicator Category",
                    "value": "Targeted"
                },
                {
                    "intervals": [
                        {
                            "start": 1435384584000,
                            "end": "current"
                        }
                    ],
                    "category": "Malware",
                    "value": "ZxShell"
                }
            ],
            "threat_name": "Area 1 Identified Malicious",
            "first_seen": 1441142508566,
            "last_seen": 1441142508566,
            "item_type": "filehash",
            "item_name":
"032f43180589c60443063f86ac42486d614c8efd1ee4660200d34466ff3fd806",
            "threat_categories": [
                {
                    "actor": [
                        "PUB5"
                    ],
                    "classification_disposition": [
                        "Unclassified"
                    ],
                    "malware": [
                        "ZxShell"
                    ],
                    "threat_type": [
                        "Actor Tool"
                    ],
                    "category": [
                        "Targeted"
                    ]
                }
            ]
        },
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
item_value	Indicator	IP Address		first_seen		item_type == 'address'
item_value	Indicator	FQDN		first_seen		item_type == 'domain'
item_value	Indicator	URL	Remove url encoding	first_seen		item_type == 'url'
item_value	Indicator	SHA-256		first_seen		item_type == 'filehash' && len(item_value) == 64
item_value	Indicator	SHA-1		first_seen		item_type == 'filehash' && len(item_value) == 40
item_value	Indicator	MD5		first_seen		item_type == 'filehash' && len(item_value) == 32
last_seen	Attribute	Last Seen		first_seen	1539063959074	
threat_name	Attribute	Threat Name		first_seen	Google Credential Harvester	
threat_categories[].actor[]	Adversary	Name		first_seen	CN41	
threat_categories[].category[]	Attribute	Category		first_seen	[Targeted, Universal]	
threat_categories[].classification_disposition[]	Attribute	Classification Disposition		first_seen	Unclassifed	
threat_categories[].delivery_vector[]	Attribute	Delivery Vector		first_seen	Phishing	
threat_categories[].malware[]	Attribute	Malware Family		first_seen	RIG_Exploit_kit	
threat_categories[].threat_type[]	Attribute	Threat Type		first_seen	Actor Infrastructure	
overall_confidence	Attribute	Confidence		first_seen	60	
tag_histories[].category + " - " +tag_histories[].value	Indicator	Tag	Split CamelCase, - to Spaces	first_seen	Escalation Reason - Promotion Multi Source Collision	

Known Issues / Limitations

- The `Tag` field on indicators is not created for this feed.

Change Log

- **Version 1.0.0**
  - Initial release