ThreatQuotient

Infoblox Threat Intelligence Data Exchange (TIDE) CDF Guide

Version 1.1.0

November 15, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

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@theatq.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.

Versioning

- Current integration version: `1.1.0`
- Supported on ThreatQ versions >= `4.31.0`

Introduction

The Infoblox Threat Intelligence Data Exchange (TIDE) CDF allows ThreatQ to ingest several dozen threat intelligence feeds from Infoblox (i.e. SURBL, Exploit Kits, EECN, DHS AIS NCCIC, TOR, DoT/DoH, etc.), as well as numerous, optional 3rd party threat indicator feeds such as those from Farsight Security, CrowdStrike, FireEye, and Proofpoint.

Additional opensource, public or private feeds can also be integrated through the Infoblox TIDE feature to further enhance ThreatQ capabilities.

The integration ingests Indicator system object types and offers the following feeds:

- **Infoblox TIDE** - allows a user to ingest lookalike FQDN indicators from the Infoblox TIDE database. The TIDE profile name parameter specifies which organization submitted the data.

  Common profiles include:
  - FarsightSecurity
  - IID
  - iSIGHTPARTNERS
  - SURBL
  - CrowdStrike
  - ThreatTrackSecurity
  - EmergingThreats
  - AISCOMM
- **Infoblox TIDE Lookalike Domains** - allows a user to ingest FQDNs that have similar spelling as popular FQDNs. The target domains parameter specifies the domain(s) to search for and return data on the lookalike domains.

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   Configuration Options - Both Feeds

PARAMETER	DESCRIPTION
API Host	The Infoblox TIDE Hostname.
API Key	The Infoblox TIDE API key.
Profile Name	The TIDE profile name parameter specifies which organization submitted the data. Some common profiles are - FarsightSecurity, IID, iSIGHTPARTNERS, SURBL, CrowdStrike, ThreatTrackSecurity, EmergingThreats, and AISCOMM.

   Additional Configuration Options - Infoblox TIDE

PARAMETER	DESCRIPTION
Property Name	The TIDE property name parameter specifies which organization submitted the data. Some common properties are MalwareC2_Generic, Phishing_Generic, Phishing_COVID19, and

	MalwareDownload_Generic. Multiple Property names should be entered in a comma-delimited format.
Class Name	The TIDE Class name parameter specifies which organization submitted the data. Some common properties are APT, Bot, MalwareC2, MalwareDownload, Proxy, Phishing, Sinkhole, and InternetInfrastructure. Multiple class names should be entered in a comma-delimited format.
Threat Score Rating	Select the threat score rating of indicators. Options include: • All • Low • Medium • High • Critical
Risk Score Rating	Select the risk score rating of indicators. Options include • All • Low • Medium • High • Critical
Configence Score Rating	Select the confidence score rating of indicators. Options include: • All • Unconfirmed • Low • Moderate • High • Confirmed

Additional Configuration Option - Infoblox TIDE Lookalike Domains

PARAMETER	DESCRIPTION
Target Domains	The TIDE target domains parameter specifies the domain(s) to search for and return data on the lookalike domains. Multiple Domain names should be entered in a comma-delimited format.

5. Review the **Settings** configuration, 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

Infoblox TIDE

`GET https://csp.infoblox.com/tide/api/data/threats`

JSON response sample:


```
{
  "threat": [
    {
      "id": "308090d4-8214-11ea-bbf0-b972d6a69c9d",
      "type": "HOST",
      "host": "facebookforamericans.com",
      "domain": "facebookforamericans.com",
      "tld": "com",
      "profile": "IID",
      "property": "Policy_LookalikeDomains",
      "class": "Policy",
      "threat_level": 0,
      "target": "facebook.com",
      "detected": "2020-04-19T01:33:50.553Z",
      "received": "2020-04-19T08:03:01.240Z",
      "imported": "2020-04-19T08:03:01.240Z",
      "expiration": "2020-05-03T01:33:50.553Z",
      "dga": false,
      "risk_score": 0,
      "confidence_score": 7.8,
      "risk_score_rating": "None",
      "confidence_score_rating": "High",
      "risk_score_vector": "RSIS:1.0/TSS:L/TLD:N/CVSS:N/EX:L/MOD:N/AVL:N/T:L/DT:M",
      "confidence_score_vector": "COSIS:1.0/SR:H/POP:N/TLD:N/CP:T",
      "batch_id": "30778fa7-8214-11ea-bbf0-b972d6a69c9d",
      "extended": {
        "reason": "partial_match",
        "cyberint_guid": "06b2eb681dd18bf42ad24bf729ac915d"
      }
    },
    {
      "id": "358ed058-8214-11ea-bbf0-b972d6a69c9d",
      "type": "HOST",
      "host": "facebookyourway.com",
      "domain": "facebookyourway.com",
      "tld": "com",
      "profile": "IID",
      "property": "Policy_LookalikeDomains",
      "class": "Policy",
      "threat_level": 0,
      "target": "facebook.com",
      "detected": "2020-04-19T01:33:50.553Z",
      "received": "2020-04-19T08:03:09.723Z",
      "imported": "2020-04-19T08:03:09.723Z",
      "expiration": "2020-05-03T01:33:50.553Z",
```

```
      "dga": false,
      "batch_id": "35861d5b-8214-11ea-bbf0-b972d6a69c9d",
      "extended": {
        "cyberint_guid": "d319490cb8f6777332fe9abe768a08d3",
        "reason": "partial_match"
      }
    },
    {
      "id": "358e3403-8214-11ea-bbf0-b972d6a69c9d",
      "type": "HOST",
      "host": "samsunggalaxytabstoreandmarket.paypal-hrsystem.com",
      "domain": "paypal-hrsystem.com",
      "tld": "com",
      "profile": "IID",
      "property": "Policy_LookalikeDomains",
      "class": "Policy",
      "threat_level": 0,
      "target": "samsung.com",
      "detected": "2020-04-19T00:31:11.955Z",
      "received": "2020-04-19T08:03:09.723Z",
      "imported": "2020-04-19T08:03:09.723Z",
      "expiration": "2020-05-03T00:31:11.955Z",
      "dga": false,
      "confidence_score": 7.8,
      "confidence_score_rating": "High",
      "confidence_score_vector": "COSIS:1.0/SR:H/POP:N/TLD:N/CP:T",
      "batch_id": "35861d5b-8214-11ea-bbf0-b972d6a69c9d",
      "extended": {
        "cyberint_guid": "49ad585f092055f61ab1ca9f03def01f",
        "reason": "partial_match"
      }
    }
  ],
  "record_count": 3
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.threat[].host	Indicator.Value	FQDN	.threat[].imported	facebookforamericans.com	N/A
.threat[].target	Indicator.Attribute	Target	.threat[].imported	facebook.com	N/A
.threat[].confidence_score	Indicator.Attribute	Confidence Score	.threat[].imported	7.8	N/A
.threat[].confidence_score_rating	Indicator.Attribute	Confidence Score Rating	.threat[].imported	High	N/A
.threat[].risk_score	Indicator.Attribute	Risk Score	.threat[].imported	0	N/A
.threat[].risk_score_rating	Indicator.Attribute	Risk Score Rating	.threat[].imported	None	N/A
.threat[].threat_score	Indicator.Attribute	Threat Score	.threat[].imported	3.5	N/A
.threat[].threat_score_rating	Indicator.Attribute	Threat Score Rating	.threat[].imported	Low	N/A
.threat[].threat_level	Indicator.Attribute	Threat Level	.threat[].imported	0	N/A
.threat[].class	Indicator.Attribute	Class	.threat[].imported	Policy	N/A
.threat[].property	Indicator.Attribute	Property	.threat[].imported	Policy_LookalikeDomains	N/A
.threat[].profile	Indicator.Attribute	Profile	.threat[].imported	IID	N/A
.threat[].tld	Indicator.Attribute	TLD	.threat[].imported	pl	N/A
.threat[].detected	Indicator.Attribute	Detected At	.threat[].imported	2020-06-08 08:27:50-00:00	N/A
.threat[].received	Indicator.Attribute	Received At	.threat[].imported	2020-06-09 11:07:24-00:00	N/A
.threat[].imported	Indicator.Attribute	Imported At	.threat[].imported	2020-06-09 11:12:26-00:00	N/A
.threat[].expiration	Indicator.Attribute	Expiration Date	.threat[].imported	2020-06-09 08:10:33-00:00	N/A
.threat[].dga	Indicator.Attribute	Domain Generation Algorithm	.threat[].imported	false	N/A
.threat[].extended.reason	Indicator.Attribute	Extended Reason	.threat[].imported	exact_match	N/A

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.

With Target Domains: google.com

METRIC	RESULT
Run Time	5 minutes
Indicators	1,164
Indicator Attributes	17,564

With Target Domains: google.com,bing.com

METRIC	RESULT
Run Time	6 minutes
Indicators	1,241
Indicator Attributes	18,862

With Target Domains: google.com,bing.com,yahoo.com

METRIC	RESULT
Run Time	10 minutes
Indicators	3,062
Indicator Attributes	46,436

Known Issues/Limitations

Occasionally during a feed run, the connector is unable to connect to the Infoblox server, resulting in the feed run completing without ingesting any indicators.

Change Log

- **Version 1.1.0**
  - Added new threat feed: Infoblox TIDE
  - Added additional parameters for new threat feed.
- **Version 1.0.0**
  - Document rebuilt to reflect product naming update
  - Initial Release (06/16/2020)