ThreatQuotient

Slashnext CDF User Guide

Version 1.0.1

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	1.0.1
Compatible with ThreatQ Versions	>= 4.17.1
Support Tier	ThreatQ Supported

Introduction

The SlashNext for ThreatQ integration allows a user to ingest active zero-hour phishing IOCs from the following three feeds published by SlashNext Intel:

- SlashNext Intel - Phishing IPs
- SlashNext Intel - Phishing FQDNs
- SlashNext Intel - Phishing Wildcard URLs

The integration ingests the following system objects:

- Indicators
    - Indicator 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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
SlashNext Threat Intel API Key	The system uses this API key to authenticate with SlashNext Cloud. If you don’t have a valid API key, you can reach out to support@slashnext.com.

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

SlashNext Intel - Phishing IPs

`GET https://intel.slashnext.cloud/api/feed/ips`

Sample Response:

```
[
    {
        "hostip": "52.160.67.152/32",
        "threat_name": "Fake Login Page",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 16:09:12 UTC",
        "last_seen": "08-04-2020 16:09:12 UTC"
    },
    {
        "hostip": "111.90.144.15/32",
        "threat_name": "Fake Login Page",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 14:38:47 UTC",
        "last_seen": "08-04-2020 14:38:47 UTC"
    },
    {
        "hostip": "191.232.191.232/32",
        "threat_name": "Fake Login Page",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 14:28:14 UTC",
        "last_seen": "08-04-2020 14:28:14 UTC"
    }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.[].hostip	Indicator.Value	IP Address	N/A	191.232.191.232	The netmask is dropped from the value.
.[].threat_name	Indicator.Attribute	Threat Name	N/A	Fake Login Page	
.[].threat_type	Indicator.Attribute	Threat Type	N/A	Phishing & Social Engineering	
.[].first_seen	Indicator.Attribute	First Seen	N/A	08-04-2020 16:09:12 UTC	
.[].last_seen	Indicator.Attribute	Last Seen	N/A	08-04-2020 16:09:12 UTC	

SlashNext Intel - Phishing FQDNs

```
GET https://intel.slashnext.cloud/api/feed/domains
```

Sample Response:

```
[
    {
        "domain": "adventury.club",
        "threat_name": "Rogue Software",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 16:57:45 UTC",
        "last_seen": "08-04-2020 16:57:45 UTC"
    },
    {
        "domain": "39.vaterlines.com",
        "threat_name": "Rogue Software",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 16:57:29 UTC",
        "last_seen": "08-04-2020 16:57:29 UTC"
    },
    {
        "domain": "vir.xooinc.com",
        "threat_name": "Fake Login Page",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 16:57:28 UTC",
        "last_seen": "08-04-2020 16:57:28 UTC"
    }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].domain	Indicator.Value	FQDN	N/A	gbett.addresspuma.icu	
.[].threat_name	Indicator.Attribute	Threat Name	N/A	Rogue Software	
.[].threat_type	Indicator.Attribute	Threat Type	N/A	Phishing & Social Engineering	
.[].first_seen	Indicator.Attribute	First Seen	N/A	08-04-2020 16:56:29 UTC	
.[].last_seen	Indicator.Attribute	Last Seen	N/A	08-04-2020 16:56:29 UTC	

SlashNext Intel - Phishing Wildcard URLs

`GET https://intel.slashnext.cloud/api/feed/wildcardurls`

Sample Response:

```
[
    {
        "wildcardurl": "www.wwwc568.vip/*",
        "threat_name": "Fake Login Page",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 17:06:59 UTC",
        "last_seen": "08-04-2020 17:06:59 UTC"
    },
    {
        "wildcardurl": "fluride.com/*",
        "threat_name": "Fake Login Page",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 17:06:54 UTC",
        "last_seen": "08-04-2020 17:06:54 UTC"
    },
    {
        "wildcardurl": "find.masters-media.net/*",
        "threat_name": "Internet Scam",
        "threat_type": "Phishing & Social Engineering",
        "first_seen": "08-04-2020 17:06:48 UTC",
        "last_seen": "08-04-2020 17:06:48 UTC"
    }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.[].wildcardurl	Indicator.Value	URL	N/A	secure-access-65d42fn8rocb7219.videogate.xyz/*	
.[].threat_name	Indicator.Attribute	Threat Name	N/A	Fake Login Page	
.[].threat_type	Indicator.Attribute	Threat Type	N/A	Phishing & Social Engineering	
.[].first_seen	Indicator.Attribute	First Seen	N/A	08-04-2020 17:06:34 UTC	
.[].last_seen	Indicator.Attribute	Last Seen	N/A	08-04-2020 17:06:34 UTC	

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.

SlashNext Intel - Phishing IPs

METRIC	RESULT
Run Time	2 minutes
Indicators	385
Indicator Attributes	1,540

SlashNext Intel - Phishing FQDNs

METRIC	RESULT
Run Time	4 minutes
Indicators	1,800
Indicator Attributes	7,200

SlashNext Intel - Phishing Wildcard URLs

METRIC	RESULT
Run Time	3 minutes

METRIC	RESULT
Indicators	1,800
Indicator Attributes	7,200

Known Issues / Limitations

- Due to the dynamic nature of the SlashNext Intel feeds, SlashNext recommends setting the feed run frequency to `Every Hour`.

Change Log

- **Version 1.0.1**
  - Update yaml with `namespace` field
  - Refactor yaml according to CDF Best Practices guidelines
- **Version 1.0.0**
  - Initial release