ThreatQuotient

Citrix (Netscaler) WAF Connector Guide

Version 1.0.0

Monday, April 20, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Monday, April 20, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions `>= 4.30.0`

Operating System	OS Version	Python Version	Notes
RedHat/CentOs	7	2.7.12	
Ubuntu	16.04	2.7.12	This has not been tested
Windows	2012R2/10	2.7.12	This has not been tested

Introduction

Citrix (Netscaler) WAF is a custom connector that sends IP Addresses from ThreatQ to a block list in Citrix VPX. The connector uses Citrix's IP reputation functionality built into the platform.

Installation

The connector package is available in `.tar.gz` and `.whl` formats, and can be installed from the ThreatQ integrations repository.

To install the `.tar.gz` or `.whl` formats:

1. Run the following command:

```
pip install /path/to/file.extension
```

Executing the Driver

The connector package comes with a driver called `tq-conn-citrix-waf`. After installing with `pip` or `setup.py`, a script stub will appear in `/usr/bin/tq-conn-citrix-waf`.

1. Run the following command to execute the feed:

```
tq-conn-citrix-waf -c
/path/to/config/directory/ -ll
/path/to/log/directory/ -v VERBOSITY_LEVEL
```

   The driver will run once, where it will connect to the TQ instance and will install the UI component of the connector. After installation, the user will need to go into the connector UI and configure the required fields.

Configuration

ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.

To Configure the operation:

1. Click on the **Settings** icon and select **Operations Management**
2. Locate the **Citrix WAF** operation and click on **Operation Settings**.
3. Enter the following parameters for the operation:

Parameter	Details
API IP/Host-name	Hostname or IP address of the Citrix WAF API.
Username	The username for the Citrix WAF API.
Password	The password for the Citrix WAF API.
Saved Search	The name of the saved search in the ThreatQ instance. You can include multiple saved searches by separting each seach with a comma. **Example:** search1,search2
IP Block List	The name of a block list created on the Citrix VPX appliance.
Use HTTPS	Check this box if the connection to the Citrix VPX appliance is secure.

4. Click on **Save Changes** then click on the toggle switch next to the operation name to enable the operation.

Citrix VPX Configuration

Follow these steps to configure Citrix to accept the IP addresses sent via the connector, and add them to a block list on the device.

1. Log into Citrix VPX via the UI.
2. Click on the **Configuration** tab.
3. Confirm that **IP Reputation** is enabled by clicking on **Security** in the left pane menu. If there is an exclamation mark next to **Reputation**, you will need to enable it by right-clicking on the **Reputation** menu and selecting **Enable Feature** in the pop up.

   The next step is configure a block list.

4. Under the **Configuration** tab, click on **AppExpert** in the menu on the left pane menu, and select **Data Sets**.
5. If there are no block lists under **Data Sets**, create a new one by clicking on the **Add** button. Enter a name for the new block list, and make sure that the type is **ipv4**. Once this is done, click on the **Create** button
6. Navigate back to your ThreatQ instance and create a **saved search** in the Threat Library.

   Confirm that the saved search is only for IP Address type indicator objects. Citrix does not accept other indicator types and will skip over all objects that are not an IP Address.

CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis use CRON or some other jobs scheduler. The argument in the CRON script ***must*** specify the config and log locations.

To send new IPs to a block list on Citrix at a regular interval, you can configure a CRON entry to run the connector. Depending on how quickly you want updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

```
tq-conn-citrix-waf -c /path/to/config/directory/ -ll /path/to/-
log/directory/ -v VERBOSITY_LEVEL
```

Driver Command Line Options

The connector's driver has several command line arguments that will help you and your customers execute this. They are listed below. You can see these by executing `/usr/bin/tq-conn-citrix-waf --help`

```
usage: Citrix WAF connector -ll [LOGLOCATION] -c [CONFIG] -v [VERBOSITY_LEVEL]


Optional arguments:
  -h, --help            Shows this help message and exits
  -ll LOGLOCATION, --loglocation LOGLOCATION
                        Sets the logging location for the connector. The
                        location should exist and be writable by the current
                        user. A special value of 'stdout' means to log to the
                        console (this happens by default)
  -c CONFIG, --config CONFIG
                        This is the location of the configuration file for the
                        connector. This location must be readable and writable
                        by the current user. If no config file path is given, the
                        current directory will be used. This file is also
                        where some information from each run of the connector
                        may be put (last run time, private oauth, etc.)
```

```
-v {1,2,3}, --verbosity {1,2,3}
                        This is the logging verbosity level. The default is 1
                        (Warning)
```