ThreatQuotient for Auto Focus Application

April 3, 2018

Version 1.0

11400 Commerce Park Dr
Suite 200,
Reston, VA
20191, USA
https://www.threatq.com/
Support: support@threatq.com
Sales: sales@threatq.com

ThreatQuotient Confidential. All printed copies and/or duplicate soft copies are to be considered uncontrolled and the latest original version should be referred to for the latest version.

Contents

ThreatQuotient Confidential. All printed copies and/or duplicate soft copies are to be considered uncontrolled and the latest original version should be referred to for the latest version.

List of Figures and Tables

About This ThreatQuotient for AutoFocus Application

Author ThreatQuotient Professional Services

History

Table 1: Document History Information

Version No.	Issue Date	Status	Reason for Change
0.1	21 Mar 2018	Initial Draft	Initial draft
0.2	23 Mar 2018	First Draft	ThreatQuotient internal review
1.0	3 Apr 2018	Release	Document Release

Review

Table 2: Document Revision Information

Reviewer’s Details	Version No.	Date
Zach Shames	0.1	21 Mar 2018
Les Adams	0.2	23 Mar 2018
Leon Brown	1.0	3 Apr 2018

Document Conventions

📝 Alerts readers to take note. Notes contain suggestions or references to material not covered in the document.

⚠ Alerts readers to be careful. In this situation, you may do something that could result in equipment damage or loss of data.

⏰ Alerts the reader that they could save time by performing the action described in the paragraph.

ℹ Alerts the reader that the information could help them solve a problem. The information might not be troubleshooting or even an action.

1 Introduction

1.1 Application Function

The ThreatQuotient for Auto Focus Application is a unidirectional connector that pulls information from AutoFocus and uploads it into the ThreatQ instance. It pulls samples from AutoFocus, and creates events based off of them within ThreatQ. In addition, it will pull any related indicators, tags, regions, and signatures that it finds using AutoFocus' API.

Depending on the number of updated/new samples to download, the upload can take quite some time. (>1 hour).

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Auto Focus Application. This document is not specifically intended to form a site reference guide.
It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and AutoFocus Engineers.
2. ThreatQuotient Professional Services Project Team & Engineers.

1.4 Scope

This document covers the implementation of the ThreatQuotient for Auto Focus Application only.

Table 3: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Auto Focus Application	2.0.0	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for Auto Focus Application into the managed estate:

- All ThreatQuotient equipment is online and in service.
- Infrastructure/transmission at all sites and between sites is in place to support the network traffic.
- All required firewall ports have been opened.
- All equipment is powered from permanent power supplies.
- A clock source of sufficient accuracy is connected to the network and the network and devices are using it as the primary clock source.

2 Implementation Overview

This document explains how to install the ThreatQuotient for Auto Focus Application.

2.1 Prerequisites

Throughout this implementation document, there will be referrals to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time, time zone and date, and using a clock source available to all.

For Example:

Figure 1: Time Zone Change Example

```
sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

2.2 Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required.

All engineers are reminded that all data belonging and pertaining to the business is strictly confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

3 Auto Focus Application Installation

3.1 Setting up the Integration

Ensure the file `tqAutoFocus-2.0.1-py2-none-any.whl` has been added to the ThreatQ instance, or the Threat Q instance has internet connectivity.

1. Install the .whl file using the following command.

Figure 2: Installing .whl File (Inc Example Output)

```
[root@localhost]# sudo pip install -i
https://<USERNAME>:<PASSWORD>@extensions.threatq.com/threatq/integrations
tqAutoFocus
You are using pip version 7.1.0, however version 9.0.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Collecting tqAutoFocus
  Downloading
https://extensions.threatq.com/threatq/integrations/+f/f53/98cc19aad550b/tqAutoFocu
s-2.0.0-py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): threatqsdk>1.6 in
/usr/lib/python2.7/site-packages (from tqAutoFocus)
Requirement already satisfied (use --upgrade to upgrade): threatqcc>=1.3.0 in
/usr/lib/python2.7/site-packages (from tqAutoFocus)
Requirement already satisfied (use --upgrade to upgrade): requests in
/usr/lib/python2.7/site-packages (from tqAutoFocus)
Requirement already satisfied (use --upgrade to upgrade): jinja2==2.8 in
/usr/lib/python2.7/site-packages (from threatqcc>=1.3.0->tqAutoFocus)
Requirement already satisfied (use --upgrade to upgrade): MarkupSafe in
/usr/lib64/python2.7/site-packages (from jinja2==2.8->threatqcc>=1.3.0-
>tqAutoFocus)
Installing collected packages: tqAutoFocus
Successfully installed tqAutoFocus-2.0.0
[root@localhost]#
```

Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir` command. See example below:

Figure 3: Creating Integration directories Example

```
$>cd /opt/
$>mkdir integrations
$>mkdir autoFocus
$>cd integrations
$>mkdir config
$>mkdir logs
$>mkdir files
```

A driver which will be called `tq-auto-focus` or `tqAutoFocus` is installed.

2. Issue the commands shown in **Figure 4: Running the Integration** to initialize the integration.
   - **ThreatQ Host**: ThreatQ Hostname or IP Address
   - **Connector Name:** Request Tracker – Auto Filled
   - **Client ID**:

The Client ID can be found within the ThreatQ instance, under **Settings → Oauth Management**.

- **E-Mail Address**: ThreatQ account associated with the RTIR integration.
- **Password**: ThreatQ account passwordassociated with the RTIR integration.
- **Status**: Active

Figure 4: Running the Integration

```
[root@localhost]# tq-auto-focus -c /path/to/config/directory/ -ll
/path/to/log/directory/ -v3
ThreatQ Host: xxx.xxx.xxx.xxx
Client ID: xxxxxxxxxxxxxxxxxxxxxxxxxx
E-Mail Address: email@domain.com
Password:
Status: Active
Connector configured.  Set information in UI. 20xx-xx-xx 00:00:00 - Intelligence
Mailbox CRITICAL: Connector has been created, please use UI for final configuration
```

The driver will run once, where it will connect to the TQ instance and install the UI component of the connector.

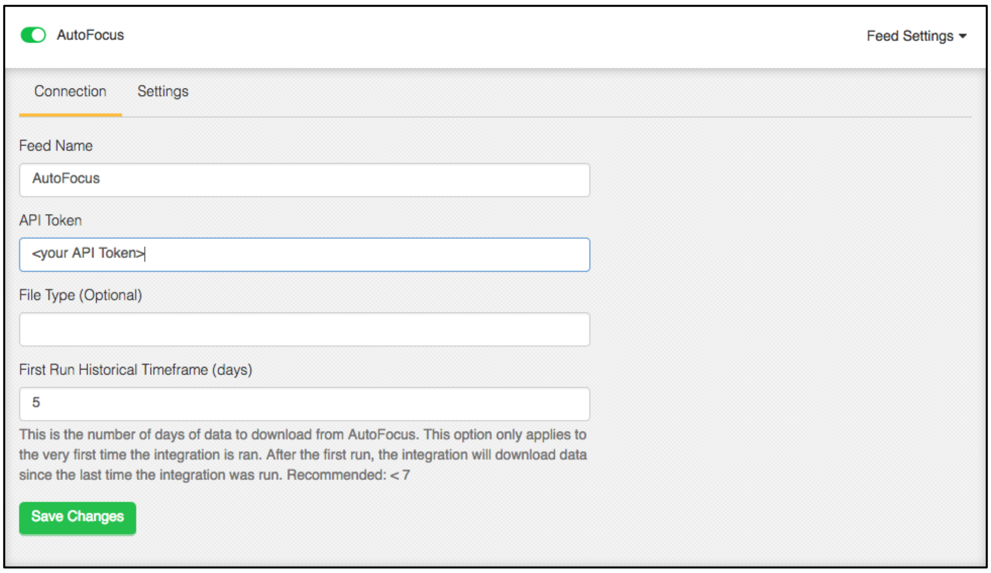
3.2 Configuring the connector

To edit the configuration, go to the **Incoming Feeds** page within ThreatQ, click the **ThreatQ Labs** tab, then expand the Feed Settings for the **AutoFocus** section.

3. The following information will need to be entered as described below.
   - **API Token**: This is the API Token associated to your Palo Alto AutoFocus Account.
   - **File Type**: (optional) The types of file to be downloaded. If you want to download all (except Android APKs), leave this blank.
   - **First Run Historical Timeframe (days)**: This is the number of days of data to download from AutoFocus.

   This option only applies to the *first time* the integration is run.
   After the first time the integration is run, the integration will download data from the last time the integration was previously run. It is recommended that this setting is less than *7 days*, or it may take longer than 1 hour.

Figure 5: ThreatQ UI Configuration



Feed Name: AutoFocus

API Token: <your API Token>

File Type (Optional):

First Run Historical Timeframe (days): 5

This is the number of days of data to download from AutoFocus. This option only applies to the very first time the integration is ran. After the first run, the integration will download data since the last time the integration was run. Recommended: < 7

Downloading and running the application can take longer than *60 Minutes*.

Figure 6: Running Of The Integration (Example Output)

```
$> tq-auto-focus -c /opt/integrations/autoFocus/config/ -ll
/opt/integrations/autoFocus/logs/ -v3
0000-00-00 00:00:00 - tqAutoFocus DEBUG: Private Connection Established
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Fetching samples since XXXX-XX-XX
00:00:00
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Hits found so far: XX (0%)
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Query still in progress. Waiting 10
seconds.
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Hits found so far: 13 (96%)
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] 13 hits found. Parsing.
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Creating Event for sample: - (1/xxx)
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Found 1 related artifacts. Parsing.
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Creating Event for sample: - (xxx/xxx)
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Found 1 related artifacts. Parsing.
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Bulk Loading XX indicators.
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Bulk Loading entries 0 - XXX
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Delaying 3 seconds...
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Completed. 44 indicators imported.
0000-00-00 00:00:00 - tqAutoFocus INFO: [::] Completed execution of the AutoFocus
Connector in XXX seconds.
0000-00-00 00:00:00 - tqAutoFocus INFO: [+] Completed. xxxx indicators imported.
```

```
0000-00-00 00:00:00 - tqAutoFocus INFO: [::] Completed execution of the AutoFocus
Connector in xxxxx seconds.
$>
```

3.3 CRON

To run this script on a reoccurring basis, use CRON or some other system schedule. The argument in the cron script ***must*** specify the config and log locations.

This can be run multiple times a day and should not be run more often than once per hour.

3.3.1 Setting Up the CRONJOB

1. Login via a CLI terminal session to your ThreatQ host.
2. Input the commands below.

Figure 7: Command Line Crontab Command

```
$> crontab -e
```

This will enable the editing of the crontab, using vi.

Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

1. Input the commands below – this example shows every **4 Hours**.

Figure 8: Command Line Crontab Auto Focus Command

```
0 */4 * * * $> sudo tq-auto-focus -c /path/to/config/directory/ -ll
/path/to/log/directory/ -v3
```

To run this script on a reoccurring basis use CRON or some other on system schedule. Here is shown CRON.

The argument in the cron script ***must*** specify the config and log locations.

This can be run multiple times a day and should **not** be run more often than once per hour.

For further reference, see the ThreatQ Help Center.

Appendix A: Supplementary Information.

Uninstalling the Connector

```
sudo pip uninstall tq-auto-focus
```

Driver command line options

The tq-auto-focus 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-auto-focus  --help.`

```
usage: tq-auto-focus Connector [-h] [-ll LOGLOCATION][-c CONFIG] [-v VERBOSITY]
```

```
tq-auto-focus
```

optional arguments:

```
  -h, --help
```

Shows the help message and exit

```
  -ll LOGLOCATION, --loglocation LOGLOCATION
```

This sets the logging location for this 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 have read and write permissions for the current user. If no config file is given, the current directory will be used. This file is also where some information from each run of the connector may be put (e.g. 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).

```
  -o, --org-only
```

Adding this flag will tell the integration to only download private samples (from your organization). This will *not* download public samples.

```
 -n, --name CONNECTOR_NAME
```

This allows you to set a custom name for the integration. Doing so will enable you to install/run multiple instances of this integration.

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ThreatQuotient and the ThreatQuotient Logo are trademarks of ThreatQuotient, Inc. and/or its affiliates in the U.S. and other countries.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

©2018 ThreatQuotient Systems, Inc. All rights reserved.