ThreatQuotient

ThreatQuotient for Resilient Custom Threat Service

Version 1.0.0

May 29, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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: Friday, May 29, 2019

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for Resilient Custom Threat Service integration implements Resilient's Custom Threat Service API, enabling automatic artifact lookups in ThreatQ.

1.2 Preface

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

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ Security/Engineers
2. ThreatQuotient Professional Services Project Team & Engineers

1.4 Scope

This document covers the implementation of the ThreatQuotient for Resilient Custom Threat Service only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for Resilient Custom Threat Service	1.0.0	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for Resilient Custom Threat Service into the managed estate:

- All ThreatQuotient equipment is online and in service.
- All required firewall ports have been opened.

2 Implementation Overview

This document will show how to install the ThreatQuotient for Resilient Custom Threat Service .

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.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option. For example, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

To change the time zone to UTC, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

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 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 Resilient Custom Threat Service Installation

3.1 Installation Steps

The following steps outline the installation of the ThreatQuotient for Resilient Custom Threat Service application.

1. SSH into the Resilient Server or a Resilient Integration Server.
2. Ensure Python 3.2+ is installed.
    a. If Python 3.2+ isn't installed, then please follow the link below to install it: https://phoenixnap.com/kb/how-to-install-python-3-centos-7
3. Below is an overview of the guide:

Figure 3: Set-Up of a Python3 Environment

```
# Make sure everything is updated
?> sudo yum update

# Install SCL so we can install multiple versions of the same software
?> sudo yum install centos-release-scl

# Install python 3.6
?> sudo yum install rh-python36

# Enable the python 3.6 SCL environment
?> scl enable rh-python36 bash

# Verify your python version. It should be 3.6 or higher
?> python --version
```

4. Transfer the Custom Threat Service for ThreatQ (.whl) onto your Resilient Server (or Resilient Integration Server).
    a. Build using python **setup.py bdist_wheel**.
5. Install the .whl file.
    a. Ensure that the python 3.6 SCL environment activated.

```
pip install rc_cts_threatq-<version>-py3-none-any.whl
```

6. If a resilient configuration file has not been created, this will need to be done before continuing. If you already have a configuration file, run the update command.
    a. The default config location is **~/.resilient/app.config**

```
# Create the config
resilient-circuits config -c

# Update the config
resilient-circuits config -u
```

    b. The default config location is **`~/.resilient/app.config**
7. Edit the `app.config` file and append the configuration found in `rc_cts_threatq/data/app.config.cts-threatq`
8. Fill out the required fields in the configuration.
        i. Resilient information
        ii. ThreatQ authentication information
    b. Save the file.
9. Run resilient-circuits to execute the custom threat service.

```
resilient-circuits run
```

3.1.1 Adding the Custom Threat Service

1. SSH into your Resilient Server as resadmin.
2. Add the custom threat service using resutil.

```
resutil threatserviceedit -name "ThreatQ" -resturl "http://<CTS
Server|127.0.0.1:>:<PORT>/cts/threatq_cts"
```

3. Once it is added, you will want to test it using resutil.

```
resutil threatservicetest -name "ThreatQ" -v
```

4. Check to make sure everything is working.
    a. Make sure you get a success message on the Resilient Server as well (threatservicetest).
    b. If you get a failure, but the configuration is correct, a proxy might be interfering with the connection. To ignore the proxy settings, use the "-ignoreProxy" flag when using "threatserviceedit".

3.1.2 Advanced Installation/Usage

If the following is required, ThreatQuotient recommends that you refer to the following document for further instructions: IBM's Integration Server Guide:
https://github.com/ibmresilient/resilient-reference/blob/master/developer_guides/Integration%20Server%20Guide.pdf

- Automatically run Integrations on startup (or restart)
- Offline Installation
- Updating the configuration file

Appendix A: Proxy Support

If a proxy is enabled, and you are having issues getting resutil or resilient to connect to the ThreatQ Custom Threat Service, you can disable the proxy via a CLI flag.

Below is an example:

```
resutil threatserviceedit -name "ThreatQ" -resturl "http://<CTS
Server|127.0.0.1>/cts/threatq_cts" -ignoreProxy true
```

Appendix B: Using HTTPS (Self-Signed Certificate)

If an integration server is being used, and a requirement is to use HTTPS with the Custom Threat Service, you will need to create your own self-sign certificate, and then apply it using Nginx or Apache.

Setting Up Nginx

1. Install Nginx, if you have not already:

```
# Install
?> sudo yum install nginx
# Enable the server for boot
?> sudo systemctl enable nginx
# Start Nginx
?> sudo systemctl start nginx
```

2. Edit /etc/nginx/nginx.conf and add/replace the "server" with the following:

```
server {
        listen       443 ssl http2;
        listen       [::]:443 ssl http2;
        server_name  <SERVER IP OR HOST>;

        ssl_certificate       <CERTIFICATE PATH>;
        ssl_certificate_key   <CERTIFICATE KEY PATH>;

        # Load configuration files for the default server block.
        include /etc/nginx/default.d/*.conf;

        location / {
            proxy_pass http://localhost:9000;
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection 'upgrade';
            proxy_set_header Host $host;
            proxy_cache_bypass $http_upgrade;
        }
    }
```

   a. Replace <SERVER IP OR HOST> with the IP or hostname of the integration server.
   b. Replace <CERTIFICATE PATH> with the path to the .crt file generated in "Generating a Self-Signed Certificate".
   c. Replace <CERTIFICATE KEY PATH> with the path to the .key file generated in "Generating a Self-Signed Certificate".

3. Allow HTTPS through your firewall.

```
?> sudo firewall-cmd --permanent --add-port=443/tcp
?> sudo firewall-cmd --reload
```

4. Restart Nginx.

```
sudo systemctl restart nginx
```

Please contact IBM Support for Apache instructions.

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING 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 TERMS AND CONDITIONS WHEN PURCHASED. 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.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

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.