Your company logo 

**Your Company – Resilient Custom Threat Service Integration Guide**

**V1.0**

*COPYRIGHT PAGE*

Table of Contents

[1. About this template 5](#_Toc1555191)

[2. Introduction 5](#_Toc1555192)

[3. Prerequisites 5](#_Toc1555193)

[4. Register the Threat Service 6](#_Toc1555194)

[5. Customer Support and Feedback 6](#_Toc1555195)

# About this template

***Use this template to create a User Guide for your Custom Threat Service (CTS).***

***This template provides an example of what information is needed to make your Resilient CTS successful. It is designed to be flexible, so feel free to change sections to meet your needs, including the title page if you need to add your own logo.***

***For additional examples, see the documentation for various CTS’s.***

***If you have a readme associated with your CTS, you should include a link to your guide and minimize the text in the readme to a brief description. If appropriate, provide a link to your user license.***

***This section is for informational purposes only, so please delete it when you create your own user guide.***

# Introduction

***Provide a description of the CTS. Include any information that users should know about the product as it pertains to the Resilient platform integration. For example:***

As part of the incident response, artifacts (or evidence) may be added to an incident for tracking and analysis. Using the Resilient Custom Threat Service, your product integrates with the Resilient platform so that any network artifacts you add to any Resilient incident automatically performs a lookup to provide additional information regarding the artifacts.

This guide describes how to integrate your product with the Resilient Incident Response Platform.

# Prerequisites

Before registering your product as a threat service with the Resilient platform, verify that your environment conforms to the following prerequisites:

* Resilient platform is version ***xx*** or later.
* Resilient platform is connected to the internet.
* You have a Resilient account to use for the integrations. This can be any account that has the permission to view and modify administrator and customization settings, and read and update incidents. You need to know the account username and password.
* You have access to the command line of the Resilient appliance, which hosts the Resilient platform.
* You have a username and API key, which you can obtain by registering with your company.
* ***Anything else? For example, does your app require that a specific port that needs to be open on the host systems, an additional protocol be supported, and so on?***

# Register the CTS

Perform the following to register your product as a Resilient custom threat service:

1. Log in to the Resilient appliance using an SSH client, such a PuTTY.
2. At the prompt, enter the following command.

sudo resutil threatserviceedit -name productname –resturl 'https://api.productname.com/api/…/?username=xxx&api\_key=yyy'

1. Once completed, test the connectivity using the following command. If the previous step was successful, you should see a success message.

$ sudo resutil threatservicetest -name "product"

1. Log into the Resilient platform as a master administrator then click on your username and select **Administrator Settings** in the drop-down menu.

***Suggest a screenshot of the menu***

1. Click the **Threat Sources** tab and scroll down until you find your product. Make sure that it is set to **ON**.

***Suggest a screenshot of the tab with your product turned to ON***

**NOTE**: If you need to disable your product threat service, you can turn the threat service to OFF.

If you need to remove the threat service, log in to the Resilient appliance using an SSH client and type the following command:

$ sudo resutil threatservicedel -name "product "

# Customer support and feedback

***This is an optional section if you wish to include contact information for your Support group.***