fn_phish_tank

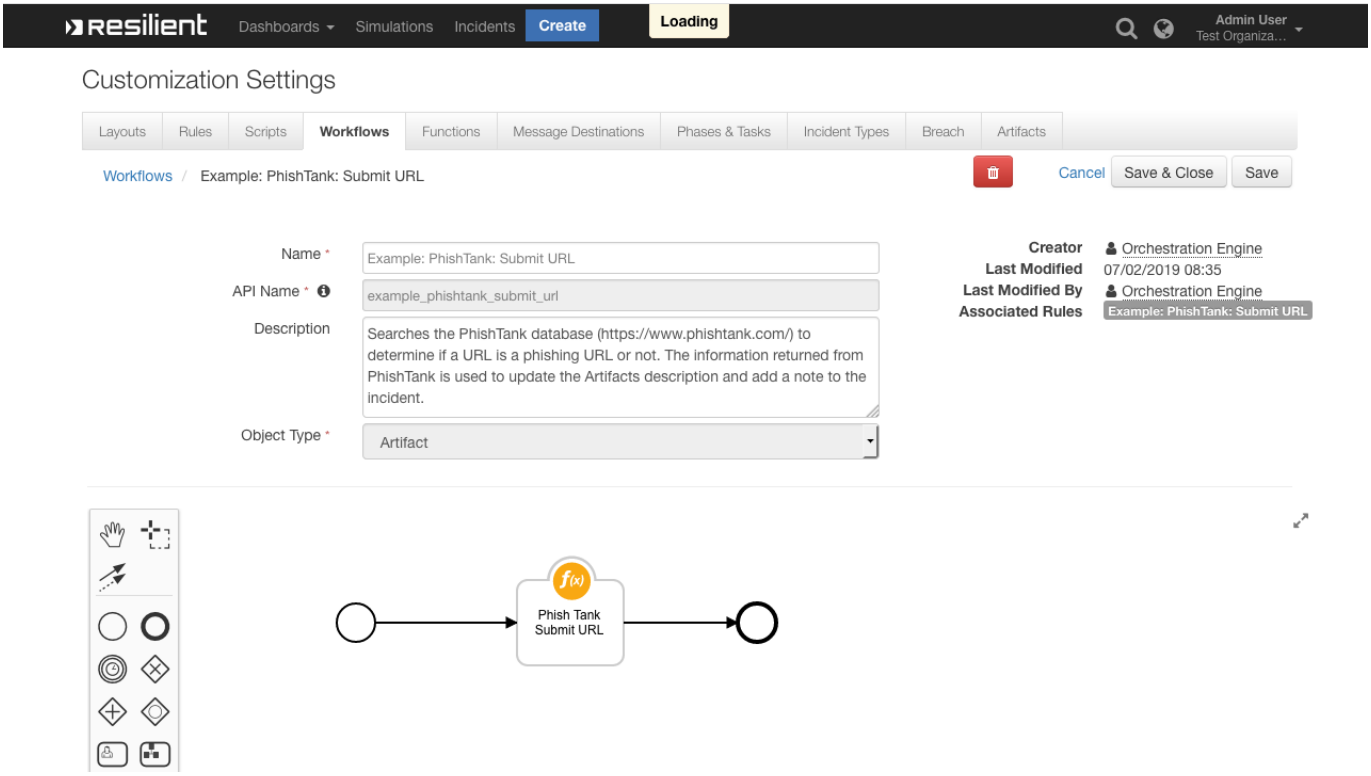
Table of Contents

Release Notes

Version	Date	Notes
1.0.2	08/2024	Rebuilt the app for server v40
1.0.2	06/2022	Default URL fixes
1.0.0	07/2021	Initial Release

Overview

PhishTank Lookup URL Function for IBM Resilient



Searches the PhishTank database (https://www.phishtank.com/) to determine if a URL is a phishing URL or not.

```
The information returned from PhishTank is used to update the Artifacts
description and add a note to the incident.
```

Requirements

This app supports the IBM Security QRadar SOAR Platform and the IBM Security QRadar SOAR for IBM Cloud Pak for Security.

SOAR platform

The SOAR platform supports two app deployment mechanisms, Edge Gateway (also known as App Host) and integration server.

If deploying to a SOAR platform with an App Host, the requirements are:

- SOAR platform >= `40.0.6554`.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

If deploying to a SOAR platform with an integration server, the requirements are:

- SOAR platform >= `40.0.6554`.
- The app is in the older integration format (available from the AppExchange as a `zip` file which contains a `tar.gz` file).
- Integration server is running `resilient_circuits>=30.0.0`.
- If using an API key account, make sure the account provides the following minimum permissions:

Name	Permissions

Name	Permissions
Org Data	Read
Function	Read

The following SOAR platform guides provide additional information:

- *Edge Gateway Deployment Guide* or *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *Integration Server Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *System Administrator Guide*: provides the procedure to install, configure and deploy apps.

The above guides are available on the IBM Documentation website at ibm.biz/soar-docs. On this web page, select your SOAR platform version. On the follow-on page, you can find the *Edge Gateway Deployment Guide*, *App Host Deployment Guide*, or *Integration Server Guide* by expanding **Apps** in the Table of Contents pane. The System Administrator Guide is available by expanding **System Administrator**.

Cloud Pak for Security

If you are deploying to IBM Cloud Pak for Security, the requirements are:

- IBM Cloud Pak for Security >= `1.10.15`.
- Cloud Pak is configured with an Edge Gateway.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

The following Cloud Pak guides provide additional information:

- *Edge Gateway Deployment Guide* or *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings. From the Table of Contents, select Case Management and Orchestration & Automation > **Orchestration and Automation Apps**.
- *System Administrator Guide*: provides information to install, configure, and deploy apps. From the IBM Cloud Pak for Security IBM Documentation table of contents, select Case Management and Orchestration & Automation > **System administrator**.

These guides are available on the IBM Documentation website at ibm.biz/cp4s-docs. From this web page, select your IBM Cloud Pak for Security version. From the version-specific IBM Documentation page, select Case Management and Orchestration & Automation.

Proxy Server

The app **does** support a proxy server.

Python Environment

Python 3.9, 3.11, and 3.12 are officially supported. When deployed as an app, the app runs on Python 3.11. Additional package dependencies may exist for each of these packages:

- python-dateutil>=2.8.0
- requests>=2.21.0
- resilient-lib>=32.0.140
- resilient_circuits>=30.0.0

Installation

Install

- To install or uninstall an App or Integration on the *SOAR platform*, see the documentation at ibm.biz/soar-docs.
- To install or uninstall an App on *IBM Cloud Pak for Security*, see the documentation at ibm.biz/cp4s-docs and follow the instructions above to navigate to Orchestration and Automation.

App Configuration

The following table provides the settings you need to configure the app. These settings are made in the app.config file. See the documentation discussed in the Requirements section for the procedure.

Config	Required	Example	Description
phish_tank_api_key	Yes	``	
phish_tank_api_url	Yes	`https://checkurl.phishtank.com/checkurl/`	
proxy	Yes	``	

Integration Server

- Download the `fn_phish_tank.zip`
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip fn_phish_tank-x.x.x.zip
```

- **Change Directory** into the unzipped Directory:

```
$ cd fn_phish_tank-x.x.x
```

- **Install** the package:

```
$ pip install fn_phish_tank-x.x.x.tar.gz
```

- Import the **configurations** into your app.config file:

```
$ resilient-circuits config -u
```

- Import the fn_phish_tank **customizations** into the Resilient platform:

```
$ resilient-circuits customize -y -l fn-phish-tank
```

- Open the config file, scroll to the bottom and edit your fn_phish_tank configurations:

```
$ nano ~/.resilient/app.config
```

Config	Required	Example	Description
phish_tank_api_url	Yes	`https://checkurl.phishtank.com/checkurl/`	PhishTank API Access URL
phish_tank_api_key	Yes	-	PhishTank API Key
proxy	No	`127.0.0.1`	Proxy Server Address. Default is `None`

- **Save** and **Close** the app.config file.
- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-phish-tank
```

- **Run** resilient-circuits or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

Uninstall

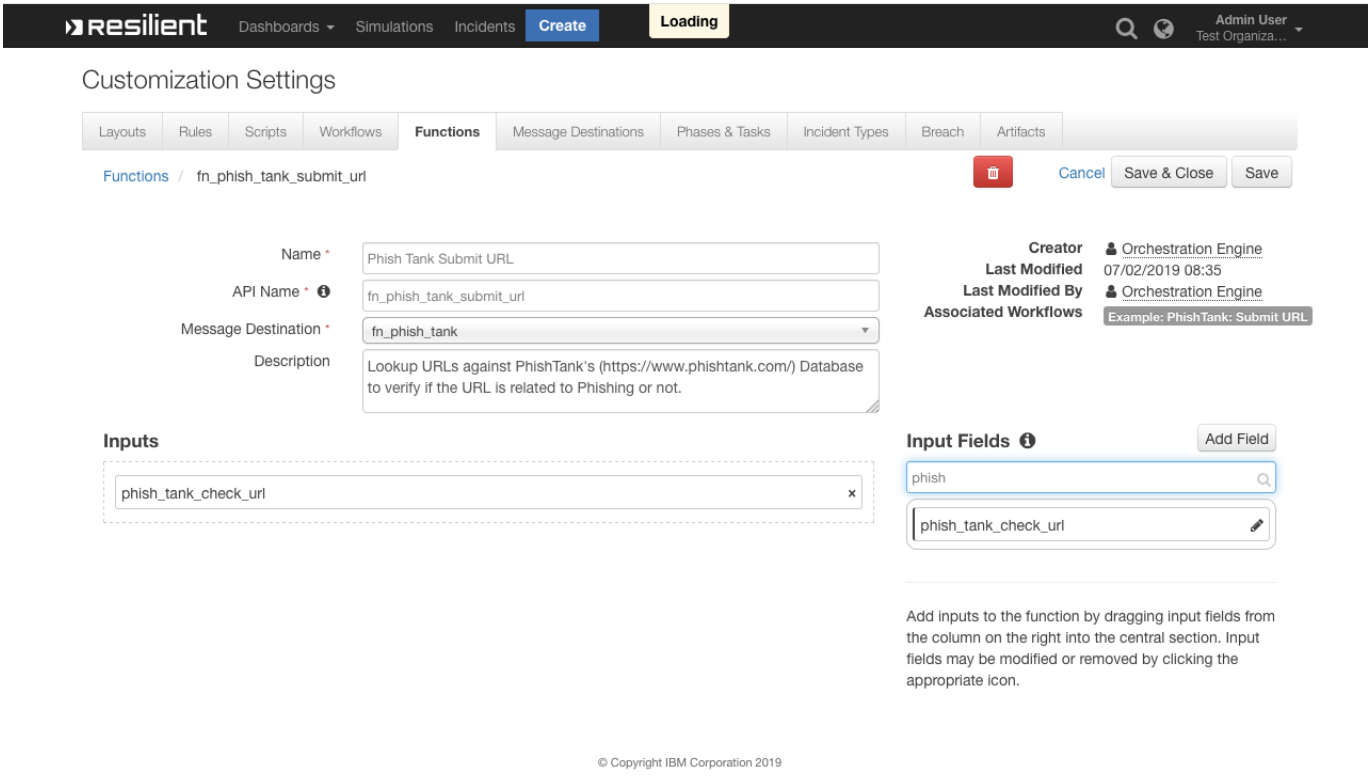
- SSH into your Integration Server
- **Uninstall** the package:

```
$ pip uninstall fn-phish-tank
```

- Open the config file, scroll to the [fn_phish_tank] section and remove the section or prefix `#` to comment out the section.
- **Save** and **Close** the app.config file.

Function - Phish Tank Submit URL

Searches the PhishTank database (https://www.phishtank.com/) to determine if a URL is a phishing URL or not. The information returned from PhishTank is used to update the Artifacts description and add a note to the incident.



▶ Inputs:

Name	Type	Required	Example	Tooltip
`phish_tank_check_url`	`text`	Yes	`http://www.example.com`	URL to lookup in PhishTank's Database

▶ Outputs:

> **NOTE:** This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
    # TODO: Generate an example of the Function Output within this code block.
    # To get the output of a Function:
    #   1. Run resilient-circuits in DEBUG mode: $ resilient-circuits run --
loglevel=DEBUG
    #   2. Invoke the Function in SOAR
    #   3. Gather the results using: $ resilient-sdk codegen -p fn_phish_tank -
-gather-results
    #   4. Run docgen again: $ resilient-sdk docgen -p fn_phish_tank
    # Or simply paste example outputs manually here. Be sure to remove any
personal information
}
```

▶ Example Function Input Script:

```
# Get the url from the Artifact's Value
inputs.phish_tank_check_url = artifact.value
```

▶ Example Function Post Process Script:

```
def append_artifact_description(the_artifact, the_text):
  """Appends the_text to the_artifact.description safely
  handling unicode"""

  new_description = u""

  if the_artifact.description is None:
    current_description = None
  else:
    current_description = the_artifact.description.get("content", None)

  if current_description is not None:
    new_description = u"{0}<br>---<br>{1}".format(unicode(current_description),
unicode(the_text))

  else:
    new_description = u"{0}".format(unicode(the_text))

  the_artifact.description = helper.createRichText(new_description)


if results.success:

  # Get the PhishTank Results
  phish_tank_results = results.content.get("results", {})
  url = phish_tank_results.get("url", u"")
  in_database = phish_tank_results.get("in_database", False)
  is_verified = phish_tank_results.get("verified", False)
  is_valid = phish_tank_results.get("valid", False)

  # Define the comment and msg to be appended to the Artifact's Description
  comment = u""
  msg = u"""<b>PhishTank Lookup</b> has complete
            <br><b>URL:</b> {0}</b>
            <br><b>Found in Database:</b> {1}""".format(url,
unicode(in_database))

  if not in_database:
    comment = u"Nothing known about this url"

  else:
    phish_id = phish_tank_results.get("phish_id")
    phish_detail_page_url = phish_tank_results.get("phish_detail_page")

    msg = u"""{0}
          <br><b>Phish ID:</b> {1}
          <br><b>Valid Phish:</b> {2}
          <br><b>Verified:</b> {3}
```

```
            <br><b>Link to PhishTank: <a href={4}>{4}</a></b>""".format(msg,
phish_id, u"Yes" if is_valid else u"No", u"Yes" if is_verified else "No",
phish_detail_page_url)

    if is_verified and is_valid:
      comment = u"Verified: Is a phishing site"

    elif is_verified and not is_valid:
      comment = u"This site is not a phishing site"

    elif not is_verified:
      comment = u"This url has not been verified"

  msg = u"""{0}<br><br><b>Comment:</b> {1}""".format(msg, comment)

  append_artifact_description(artifact, msg)
  incident.addNote(helper.createRichText(msg))
```

Rules

Rule Name	Object	Workflow Triggered	Condition
Example: PhishTank: Submit URL	artifact	`example_phishtank_submit_url`	`artifact.type equals URL`

Troubleshooting & Support

Refer to the documentation listed in the Requirements section for troubleshooting information.

For Support

This is a IBM Community provided app. Please search the Community ibm.biz/soarsupport for assistance.