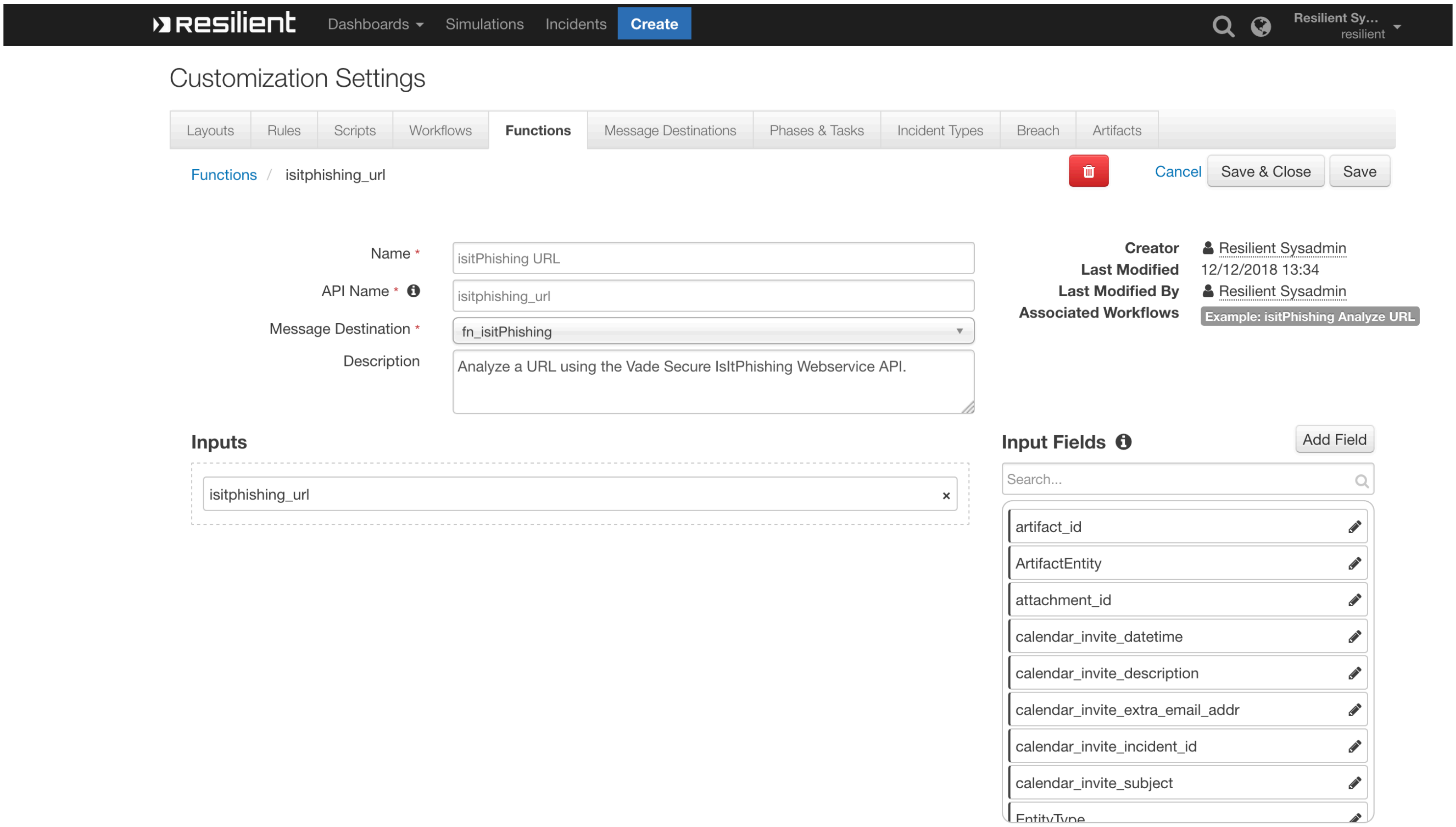
Resilient Integration with IsItPhishing

This package contains two functions that call the Vade Secure IsItPhishing Webservice API to analyze a URL or to analyze an HTML document. Also included are 3 example workflows and rules to demonstrate how to invoke and use the functions.



Customization Settings

Functions / isitphishing_url

Name * isitPhishing URL

API Name * isitphishing_url

Message Destination * fn_isitPhishing

Description Analyze a URL using the Vade Secure IsItPhishing Webservice API.

Creator Resilient Sysadmin

Last Modified 12/12/2018 13:34

Last Modified By Resilient Sysadmin

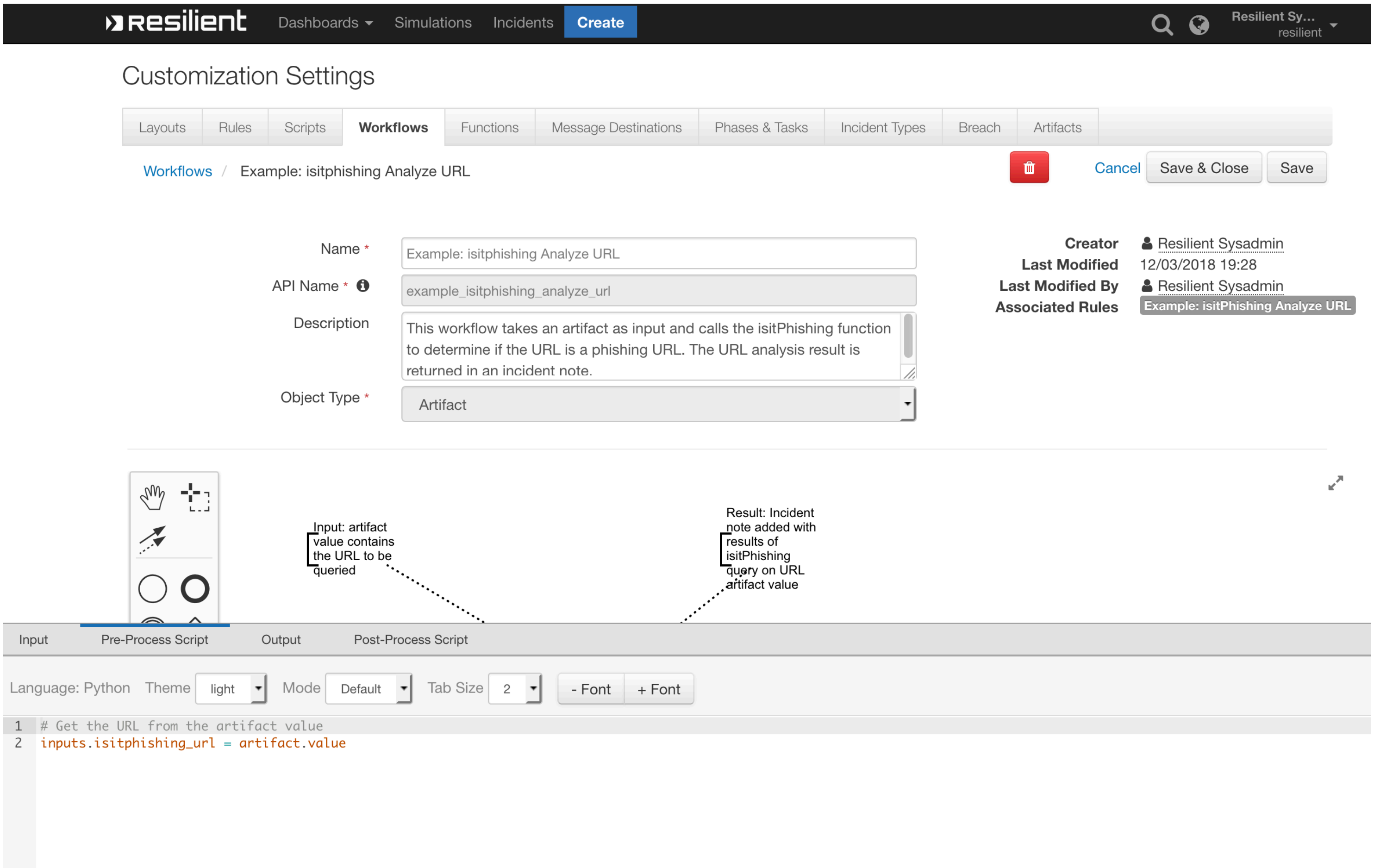
Associated Workflows Example: isitPhishing Analyze URL

Inputs

isitphishing_url

Input Fields

- artifact_id
- ArtifactEntity
- attachment_id
- calendar_invite_datetime
- calendar_invite_description
- calendar_invite_extra_email_addr
- calendar_invite_incident_id
- calendar_invite_subject
- EntityType



Customization Settings

Workflows / Example: isitphishing Analyze URL

Name *	Example: isitphishing Analyze URL
API Name *	example_isitphishing_analyze_url
Description	This workflow takes an artifact as input and calls the isitPhishing function to determine if the URL is a phishing URL. The URL analysis result is returned in an incident note.
Object Type *	Artifact

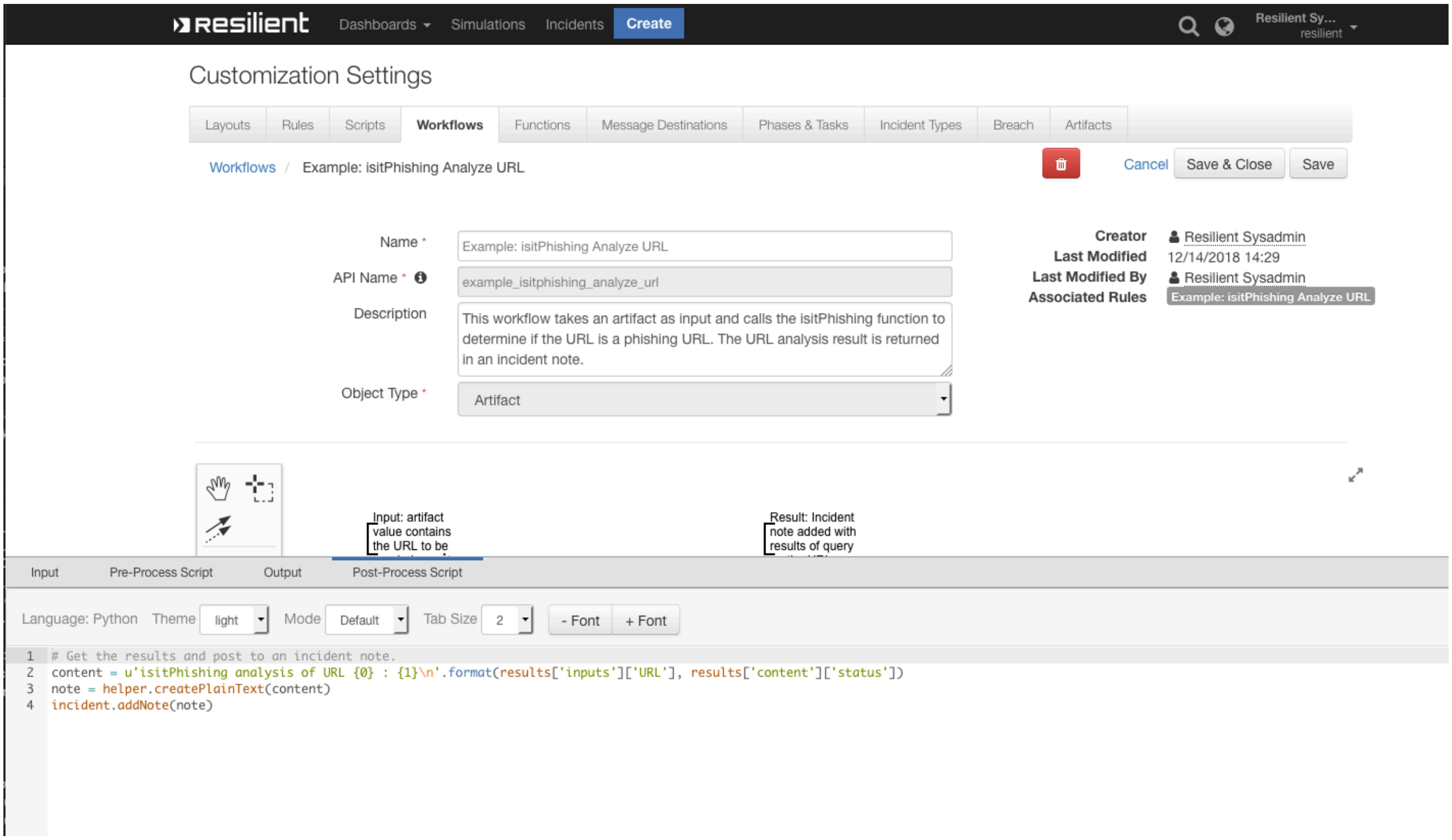
Creator	Resilient Sysadmin
Last Modified	12/03/2018 19:28
Last Modified By	Resilient Sysadmin
Associated Rules	Example: isitPhishing Analyze URL

Input: artifact value contains the URL to be queried

Result: Incident note added with results of isitPhishing query on URL artifact value

Language: Python Theme light Mode Default Tab Size 2

```
# Get the URL from the artifact value
inputs.isitphishing_url = artifact.value
```



Customization Settings

Workflows / Example: isitPhishing Analyze URL

Name *	Example: isitPhishing Analyze URL
API Name *	example_isitphishing_analyze_url
Description	This workflow takes an artifact as input and calls the isitPhishing function to determine if the URL is a phishing URL. The URL analysis result is returned in an incident note.
Object Type *	Artifact

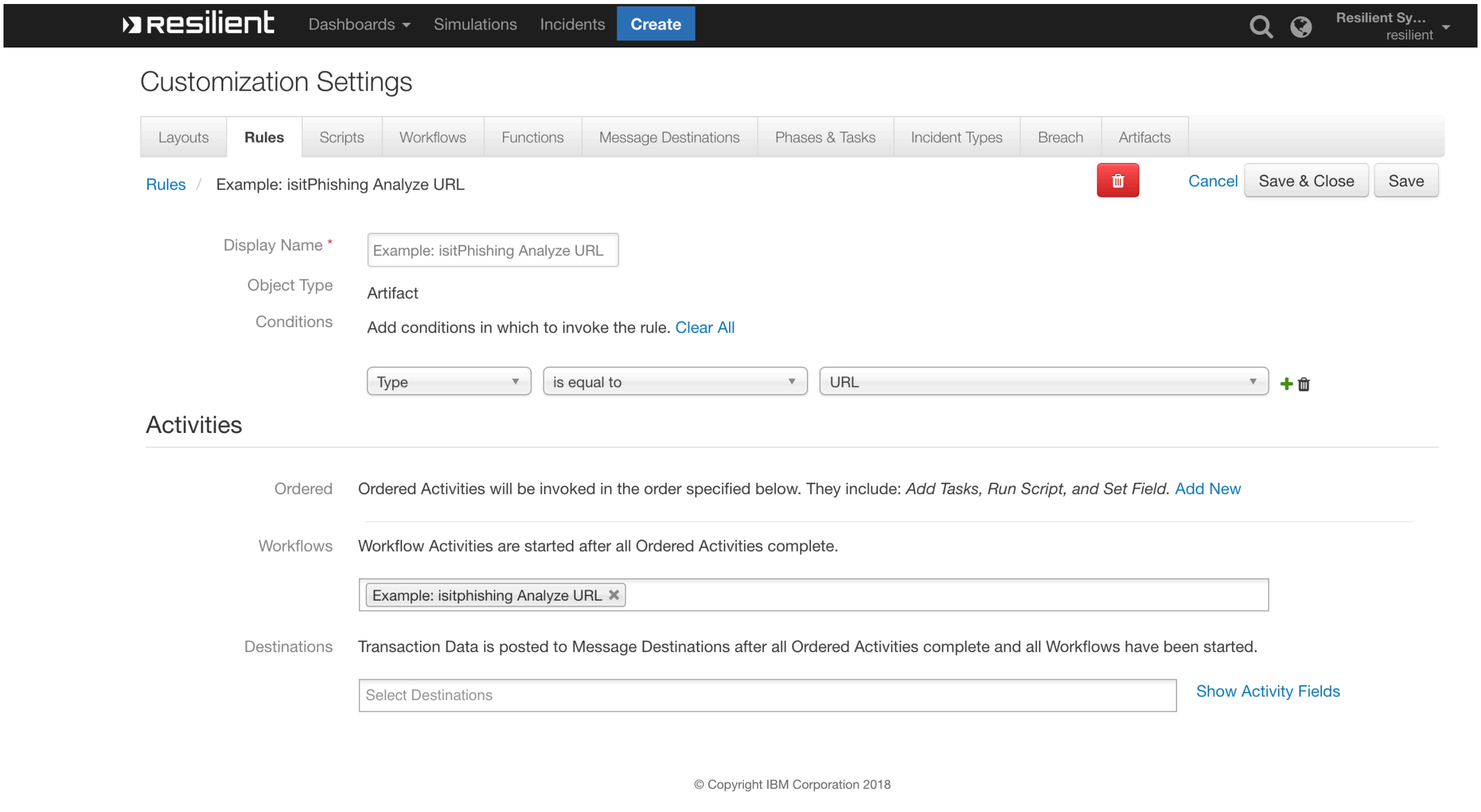
Creator	Resilient Sysadmin
Last Modified	12/14/2018 14:29
Last Modified By	Resilient Sysadmin
Associated Rules	Example: isitPhishing Analyze URL

Input: artifact value contains the URL to be

Result: Incident note added with results of query

Language: Python Theme light Mode Default Tab Size 2

```
# Get the results and post to an incident note.
content = u'isitPhishing analysis of URL {0} : {1}\n'.format(results['inputs']['URL'], results['content']['status'])
note = helper.createPlainText(content)
incident.addNote(note)
```



Customization Settings

Rules / Example: isitPhishing Analyze URL

Display Name * Example: isitPhishing Analyze URL

Object Type Artifact

Conditions Add conditions in which to invoke the rule. Clear All

Type ▾ is equal to ▾ URL ▾

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: *Add Tasks, Run Script, and Set Field.* Add New

Workflows Workflow Activities are started after all Ordered Activities complete.

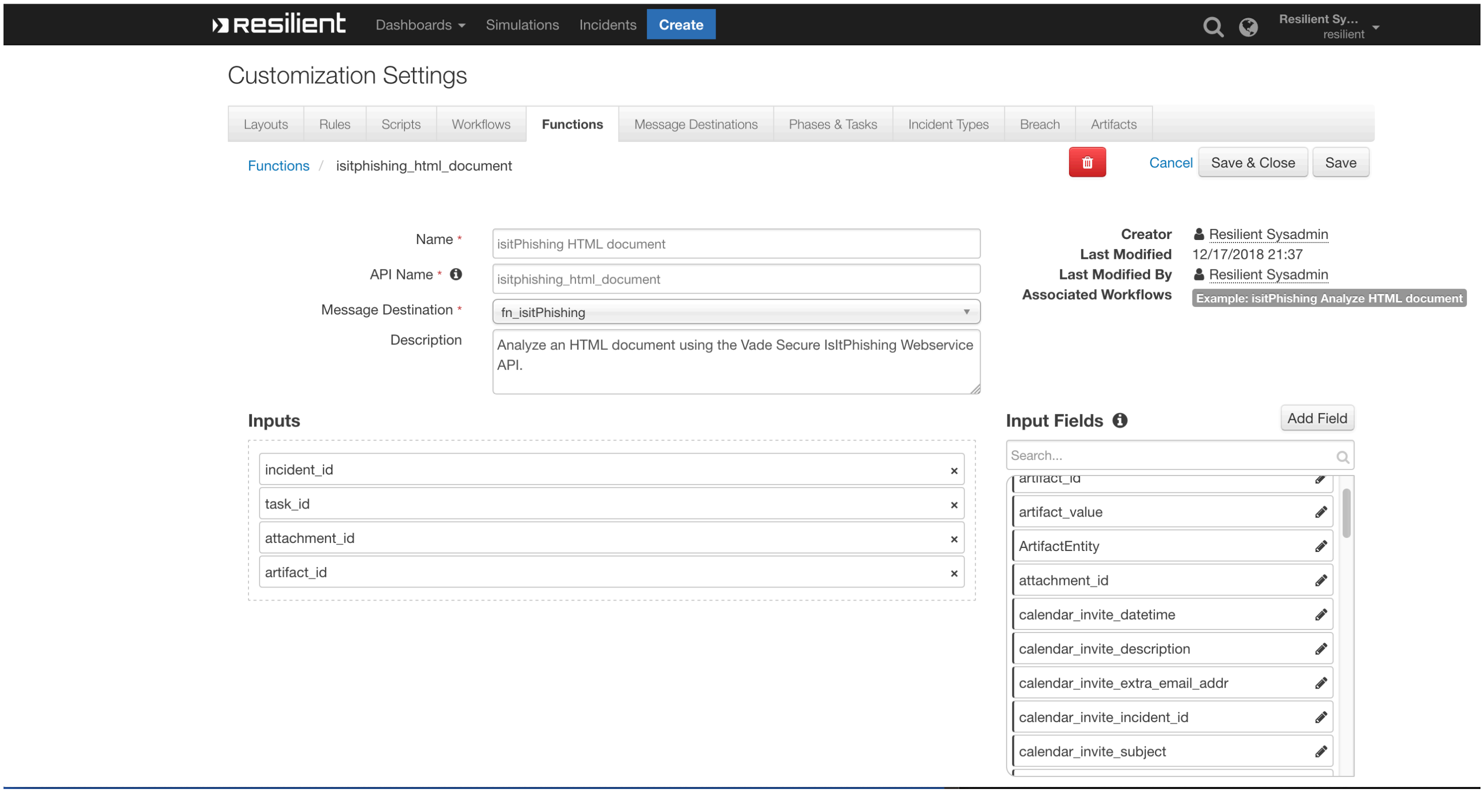
Example: isitphishing Analyze URL ✖

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

Show Activity Fields

© Copyright IBM Corporation 2018



Customization Settings

Functions / isitphishing_html_document

Name * isitPhishing HTML document

API Name * isitphishing_html_document

Message Destination * fn_isitPhishing ▾

Description Analyze an HTML document using the Vade Secure IsItPhishing Webservice API.

Creator Resilient Sysadmin

Last Modified 12/17/2018 21:37

Last Modified By Resilient Sysadmin

Associated Workflows Example: isitPhishing Analyze HTML document

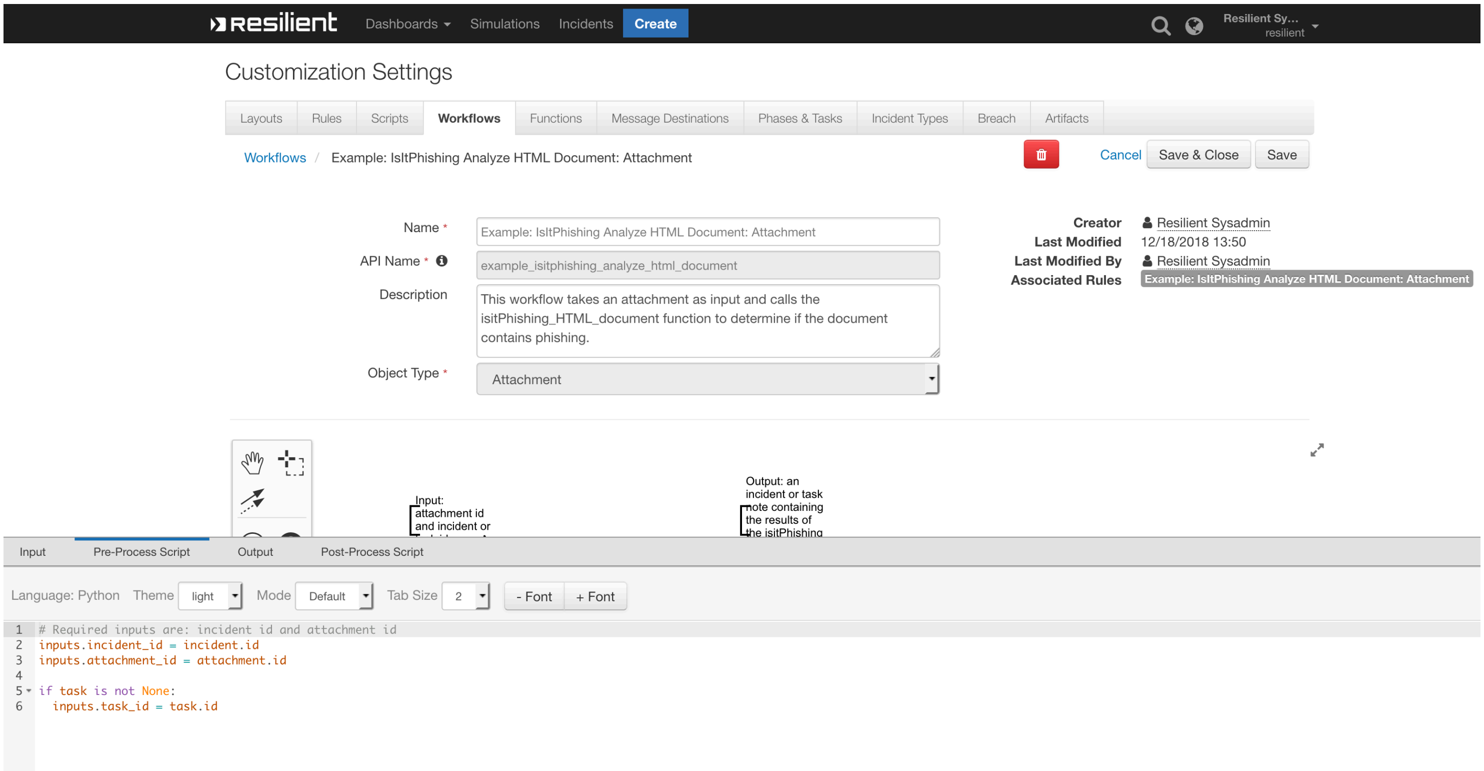
Inputs

- incident_id ×
- task_id ×
- attachment_id ×
- artifact_id ×

Input Fields

Search...

- artifact_id
- artifact_value
- ArtifactEntity
- attachment_id
- calendar_invite_datetime
- calendar_invite_description
- calendar_invite_extra_email_addr
- calendar_invite_incident_id
- calendar_invite_subject



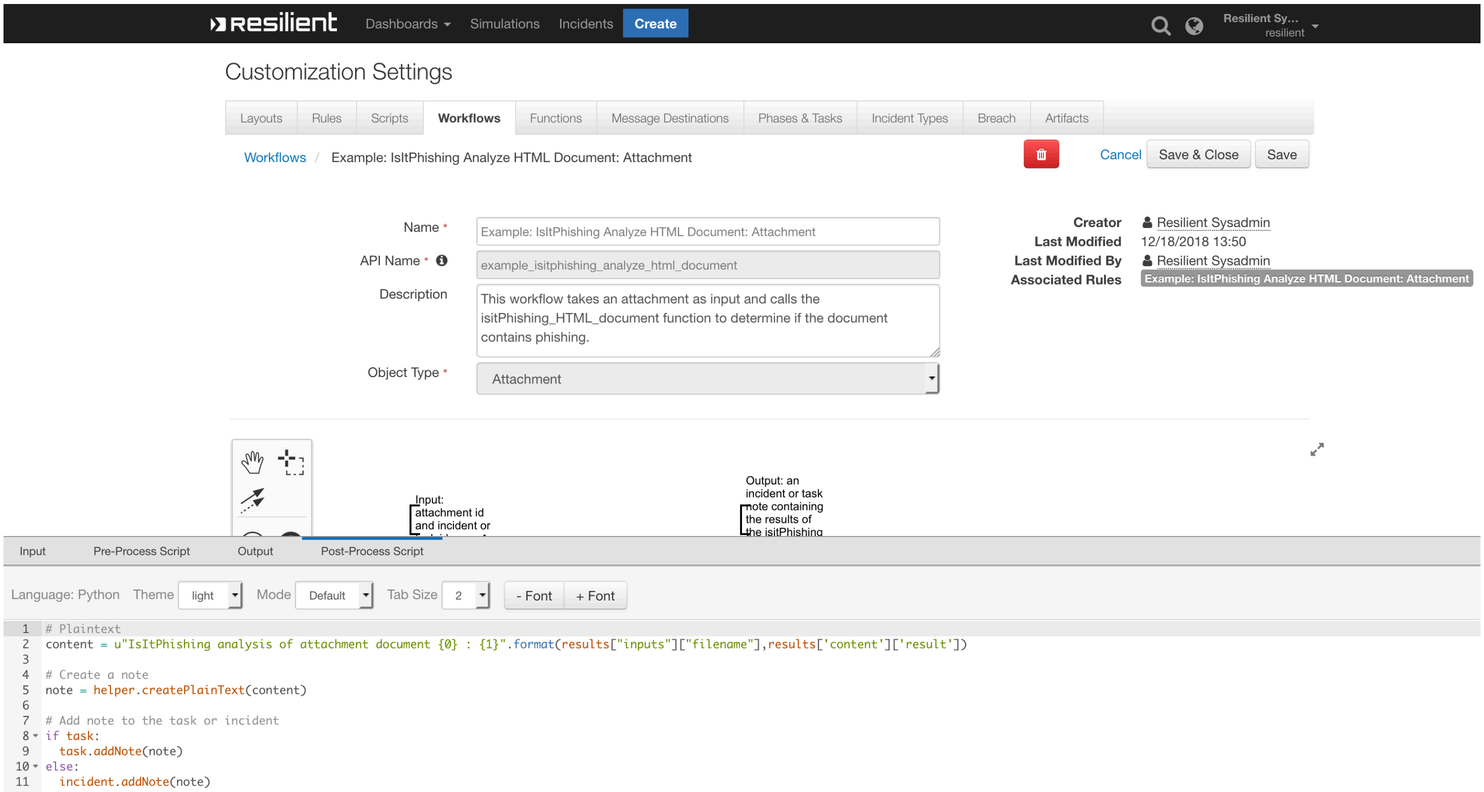
Name *	Example: IsItPhishing Analyze HTML Document: Attachment
API Name *	example_isitphishing_analyze_html_document
Description	This workflow takes an attachment as input and calls the isitPhishing_HTML_document function to determine if the document contains phishing.
Object Type *	Attachment

Creator	Resilient Sysadmin
Last Modified	12/18/2018 13:50
Last Modified By	Resilient Sysadmin
Associated Rules	Example: IsItPhishing Analyze HTML Document: Attachment

Language: Python Theme light Mode Default Tab Size 2

```
# Required inputs are: incident id and attachment id
inputs.incident_id = incident.id
inputs.attachment_id = attachment.id

if task is not None:
  inputs.task_id = task.id
```



Name *	Example: IsItPhishing Analyze HTML Document: Attachment
API Name *	example_isitphishing_analyze_html_document
Description	This workflow takes an attachment as input and calls the isitPhishing_HTML_document function to determine if the document contains phishing.
Object Type *	Attachment

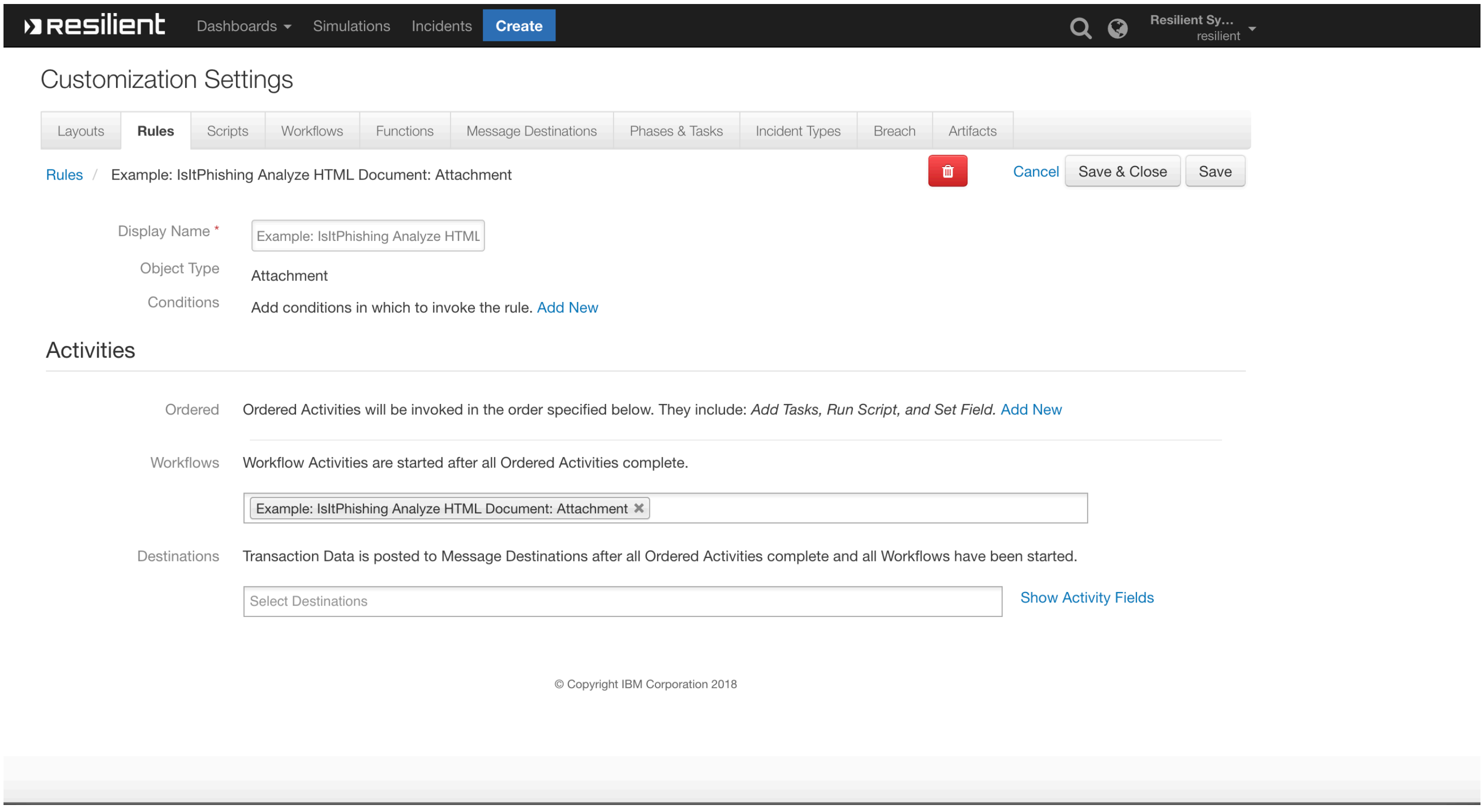
Creator	Resilient Sysadmin
Last Modified	12/18/2018 13:50
Last Modified By	Resilient Sysadmin
Associated Rules	Example: IsItPhishing Analyze HTML Document: Attachment

Language: Python Theme light Mode Default Tab Size 2

```
# Plaintext
content = u"IsItPhishing analysis of attachment document {0} : {1}".format(results["inputs"]["filename"],results['content']['result'])

# Create a note
note = helper.createPlainText(content)

# Add note to the task or incident
if task:
  task.addNote(note)
else:
  incident.addNote(note)
```



Customization Settings

Rules / Example: IsItPhishing Analyze HTML Document: Attachment

Display Name * Example: IsItPhishing Analyze HTML

Object Type Attachment

Conditions Add conditions in which to invoke the rule. Add New

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: *Add Tasks, Run Script, and Set Field.* Add New

Workflows Workflow Activities are started after all Ordered Activities complete.

Example: IsItPhishing Analyze HTML Document: Attachment ✖

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

Show Activity Fields

© Copyright IBM Corporation 2018

app.config settings:

```
[fn_isitPhishing]
# Define the Vade Secure IsItPhishing Webservice API endpoint
#
isitPhishing_api_url=https://ws.isitphishing.org/api/v2
#
# You need a license key to use the Vade Secure IsItPhishing API.
# This key will be provided to you by Vade Secure, and has the following format:
# <NAME>:<LICENSE>
isitPhishing_name=xxxx
isitPhishing_license=xxxx
```

Function: isitPhishing_url

Function Inputs:

Function Parameter	Type	Required	Example	Info
`isitPhishing_url`	`String`	Yes	`"http://www.thisisaphishingurl.com "`	N/A

Function Output:

```
results = {
  analysis: {
    status: "PHISHING"
  },
  inputs: {
    URL: "URL_to_analyze"
  }
}
```

Pre-Process Script:

```
# Get the URL from the artifact value
inputs.isitphishing_url = artifact.value
```

Post-Process Script: Example: IsItPhishing Analyze URL:

```
# Get the results and post to an incident note.
content = u'IsItPhishing analysis of URL {0} : {1}\n'.format(results['inputs']['URL'], results['analysis']['status'])
note = helper.createPlainText(content)
incident.addNote(note)
```

Rules: Example: isitPhishing Analyze URL:

Rule Name	Object Type	Workflow Triggered	Conditions
Example: IsItPhishing Analyze URL	`Artifact`	`Example: IsItPhishing Analyze URL`	Artifact type is URL

Function: isitPhishinghtmldocument

Function Inputs:

Function Parameter	Type	Required
`incident_id`	`Number`	Yes
`task_id`	`Number`	No
`attachment_id`	`Number`	No
`artifact_id`	`Number`	No

Function Output:

```

results = {
  analysis: {
    result : "PHISHING"
  },
  inputs: {
    incident_id": incident_id,
    "task_id": task_id,
    "attachment_id": attachment_id,
    "artifact_id": artifact_id
  }
}
```

Pre-Process Script for Attachment:

```
# Required inputs are: incident id and attachment id
inputs.incident_id = incident.id
inputs.attachment_id = attachment.id

if task is not None:
  inputs.task_id = task.id
```

Post-Process Script for Attachment:

```
# Get the results and post to an incident note.
content = u"IsItPhishing analysis of attachment document {0} : {1}".format(results["input
s"]["filename"],results['content']['result'])
note = helper.createPlainText(content)
incident.addNote(note)
```

Rule for Attachment:

Rule Name	Object Type	Workflow Triggered
Example: IsItPhishing Analyze HTML Document: Attachment	`Attachment`	`Example: IsItPhishing Analyze HTML document: Attachment`

Pre-Process Script for Artifact:

```
# Required inputs are: incident id and attachment id
inputs.incident_id = incident.id
inputs.artifact_id = artifact.id
```

Post-Process Script for Artifact:

```
# Get the results and post to an incident note.
content = u"IsItPhishing analysis of artifact document {0} : {1}".format(results["inputs"
]["filename"],results['content']['result'])

note = helper.createPlainText(content)

incident.addNote(note)
```

Rule for Artifact:

Rule Name	Object Type	Workflow Triggered
Example: IsItPhishing Analyze HTML Document: Artifact	`Artifact`	`Example: IsItPhishing Analyze HTML document: Artifact`

Install and run

To package for distribution,

`python ./fn_isitPhishing/setup.py sdist`

The resulting .tar.gz file can be installed using

```
pip install <filename>.tar.gz
```

To run the integration:

```
resilient-circuits run
```