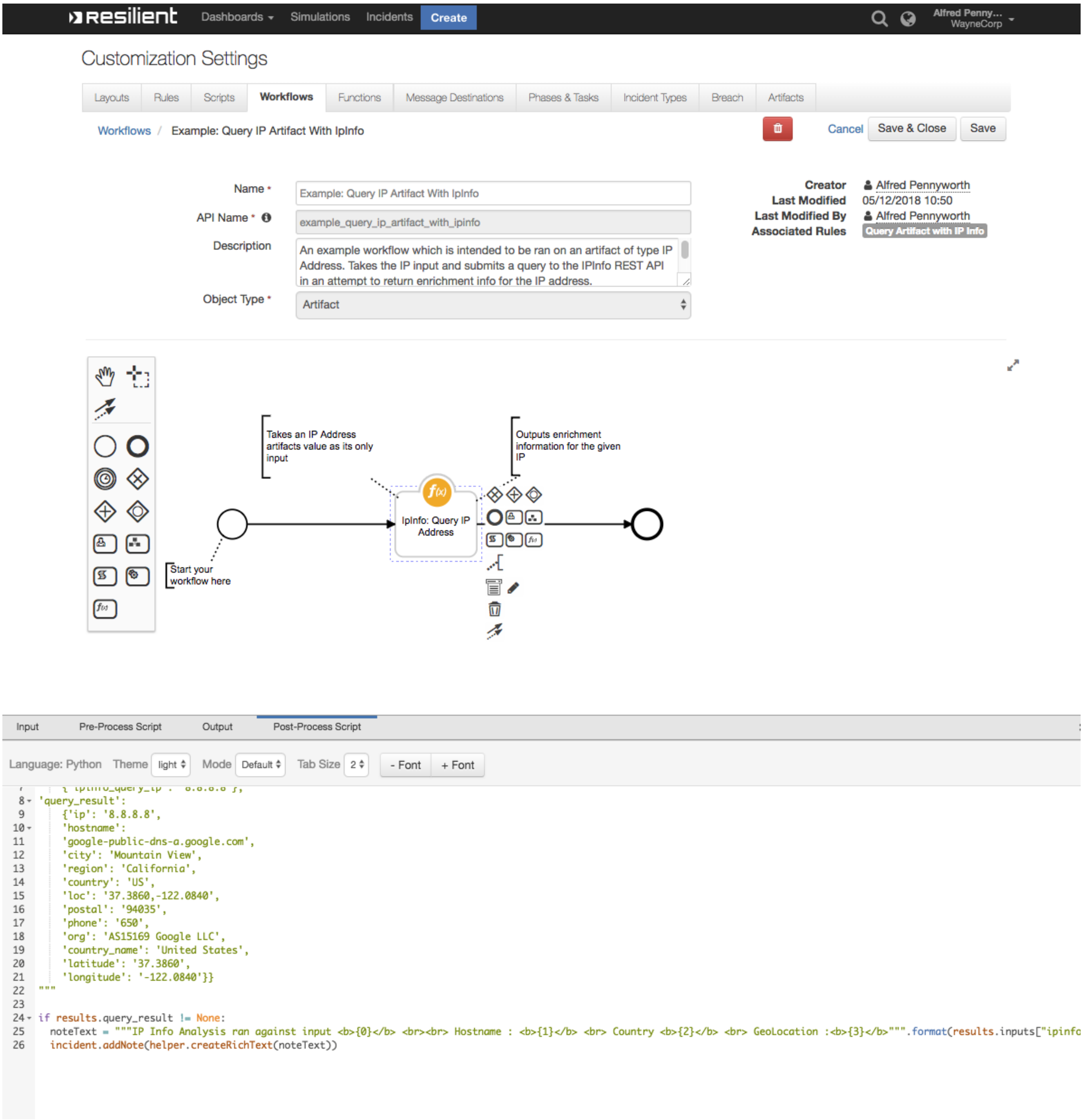
Resilient Integration with IPInfo

This package contains one function which provides enrichment information for an IP Address Artifact by querying that artifact in the IPInfo Database. Takes in an input of an IP address and then queries for information such as the location, ASN and hostname of the IP if any. Results are saved in a rich text note.



Customization Settings

Workflows / Example: Query IP Artifact With IpInfo

Name * Example: Query IP Artifact With IpInfo

API Name * example_query_ip_artifact_with_ipinfo

Description An example workflow which is intended to be ran on an artifact of type IP Address. Takes the IP input and submits a query to the IPInfo REST API in an attempt to return enrichment info for the IP address.

Object Type * Artifact

Creator Alfred Pennyworth

Last Modified 05/12/2018 10:50

Last Modified By Alfred Pennyworth

Associated Rules Query Artifact with IP Info

Takes an IP Address artifacts value as its only input
Outputs enrichment information for the given IP
IpInfo: Query IP Address
Start your workflow here

Language: Python Theme light Mode Default Tab Size 2

```
    {'ipinfo_query_ip': '8.8.8.8'},
'query_result':
    {'ip': '8.8.8.8',
    'hostname':
    'google-public-dns-a.google.com',
    'city': 'Mountain View',
    'region': 'California',
    'country': 'US',
    'loc': '37.3860,-122.0840',
    'postal': '94035',
    'phone': '650',
    'org': 'AS15169 Google LLC',
    'country_name': 'United States',
    'latitude': '37.3860',
    'longitude': '-122.0840'}}
"""

if results.query_result != None:
  noteText = """IP Info Analysis ran against input <b>{0}</b> <br><br> Hostname : <b>{1}</b> <br> Country <b>{2}</b> <br> GeoLocation :<b>{3}</b>""".format(results.inputs["ipinfo
  incident.addNote(helper.createRichText(noteText))
```

app.config settings:

The only config value required by this integration package is an access token for IP Info's API

```
[fn_ipinfo]
ipinfo_access_token=123asb
```

Function Inputs:

Function Name	Type	Required	Example
`ipinfo_query_ip`	`String`	Yes	`'8.8.8.8'`

Pre-Process Script:

```
inputs.ipinfo_query_ip = artifact.value
```

Post-Process Script:

This example **adds a Note to the Incident.**

```
if results.query_result != None:
  noteText = """IP Info Analysis ran against input <b>{0}</b> <br><br>
Hostname : <b>{1}</b> <br> Country <b>{2}</b> <br> GeoLocation :<b>{3}
</b>""".format(results.inputs["ipinfo_query_ip"],
results.query_result['hostname'], results.query_result['country'],
results.query_result['loc'])
  incident.addNote(helper.createRichText(noteText))
```

Output :

```
{
'success': True,
'inputs':
    {'ipinfo_query_ip': '8.8.8.8'},
'query_result':
    {'ip': '8.8.8.8',
    'hostname':
    'google-public-dns-a.google.com',
    'city': 'Mountain View',
    'region': 'California',
    'country': 'US',
    'loc': '37.3860,-122.0840',
    'postal': '94035',
    'phone': '650',
    'org': 'AS15169 Google LLC',
    'country_name': 'United States',
    'latitude': '37.3860',
        'longitude': '-122.0840'}}
```

Rules

Rule Name	Object Type	Workflow Triggered
Query Artifact with IP Info	`Artifact`	`Example: Query IP Artifact With IpInfo`