README.md

Shodan Function

Aim

This is a simple function which takes IP Addresses and queries, returning the results from https://www.shodan.io/.

It will return the Vulns and Ports open on an IP Address via results.

```
results = {
                "shodan_vulns": "[CVE-2018-1-1]",
                "shodan_ports": "[80, 443]",
                "shodan_url": "https://www.shodan.io/host/1.1.1.1"
            }
```

You will need a paid API key for Shodan - https://developer.shodan.io/billing/signup

Installation

- Ensure you resilient-circuits is setup and communicating with Resilient
- Unzip the file and pip install

```
pip install fn_shodan-1.0.0.tar.gz
```

- Add the configuration to your app.config

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

- Add your shodan API key as specified in the app.config
- Add the example functions to Resilient

```
resilient-circuits customize
```

- You can now reload the Resilient-Circuits and test from the user interface of Resilient
- You will need to create an artifact workflow for it use the following for the pre-processing script and post-processing script as an example

```
inputs.shodan_lookup_host = artifact.value


vulns = results.shodan_vulns
url = results.shodan_url
ports = results.shodan_ports

rendered_text = "Ports: {} \n Vulnerabilities: {} \n Report URL: {}".format(ports,vulns,url)

artifact.description = rendered_text
```