RSA NetWitness PoC Integration

This integration contains two functions `NetWitness Query Event Session` and `NetWitness Query`. Disclaimer, this has not been tested and may include some minor bugs.

Installation

`pip install fn_rsa_netwitness-1.0.0.tar.gz`

Import functions, workflows, rules, etc

`resilient-circuits customize` The following will be what is imported:

```
    # This import data contains:
    #   Action fields:
    #     netwitness_query
    #     nw_event_session_id
    #   Function inputs:
    #     incident_id
    #     nw_event_session_id
    #     nw_query
    #   DataTables:
    #     logs_and_packets
    #   Message Destinations:
    #     rsa_netwitness_message_destination
    #   Functions:
    #     netwitness_query
    #     netwitness_query_event_session
    #   Workflows:
    #     netwitness_get_event_session_logs
    #     netwitness_query
    #   Rules:
    #     NetWitness get session logs
    #     NetWitness Query
```

Config

`resilient-circuits config -u` This will add the following section to the existing `app.config`

```
[fn_rsa_netwitness]
nw_url=<https://test.nw_server.com>
nw_port=<default port for communication, might be 50005? >
nw_user=<nw_username>
nw_password=<nw_password>
cafile=[true|false]
```

NetWitness Query Event Session

This function is inspired from a PS integration which had working code. This function is triggered when the incident rule `NetWitness get session logs` is triggered. It prompts for imput in a modal popup for the session ids you wish to get the pcap data on. This can take multiple session IDs by adding a comma separated string of the required session IDs.

When run this function will populate the data table `Logs and Packets` with the log data of the pcap file from the session IDs.

This function will also attempt to download the entire pcap file and upload it to the incident as an attachment.

NetWitness Query

This function is triggered from the incident rule `NetWitness Query` and will prompt you for a query string when run. The query string can be anything NetWitness supports (ie: return session IDs when the ip address was xx.xx.xx.xx between two dates).

When session IDs are returned this function works best and will take the list of session IDs and use them to gather the pcap file for these IDs and attach it to the incident.