RSA NetWitness PoC Integration

This integration contains five functions `NetWitness Get Meta ID ranges`, `NetWitness Get Meta Values`, `NetWitness Query`, `NetWitness Retrieve Log Data`, `NetWitness Retrieve PCAP Data`.

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:

```
#   Action fields:
#     netwitness_end_time
#     netwitness_query
#     netwitness_start_time
#   Function inputs:
#     incident_id
#     nw_data_format
#     nw_end_time
#     nw_event_session_ids
#     nw_meta_id1
#     nw_meta_id2
#     nw_query
#     nw_results_size
#     nw_session_id1
#     nw_session_id2
#     nw_start_time
#   Message Destinations:
#     rsa_netwitness_message_destination
#   Functions:
#     netwitness_get_meta_id_ranges
#     netwitness_get_meta_values
#     netwitness_query
#     netwitness_retrieve_log_data
#     netwitness_retrieve_pcap_data
#   Workflows:
#     example_netwitness_get_meta_values
#     example_netwitness_retrieve_log_file
#     example_netwitness_retrieve_pcap_file
#     example_netwitness_retrieve_pcap_file_time
#   Rules:
#     (Example) NetWitness Get Meta Values
#     (Example) NetWitness Retrieve Log File
#     (Example) NetWitness Retrieve PCAP File
#     (Example) NetWitness Retrieve PCAP File (Time)
```

Config

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

```
[fn_rsa_netwitness]
nw_packet_server_url=<http://test.nw_packet_server.com:50104>
nw_packet_server_user=<nw_packet_server_username>
nw_packet_server_password=<nw_packet_server_password>
nw_packet_server_verify=[true|false]

nw_log_server_url=<http://test.nw_log_server.com:50102>
nw_log_server_user=<nw_log_server_username>
nw_log_server_password=<nw_log_server_password>
nw_log_server_verify=[true|false]
```

How to use the NetWtiness Functions

1. Import necessary customization data into the Resilient Platform. (Note the example workflow `example_netwitness_retrieve_log_file` relies on the function `Utilities: String to Attachment` from the `fn_utilities` package and must be inported first):

   ```
   resilient-circuits customize
   ```

2. Update and edit app.config:

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

3. Start Resilient Circuits:

   ```
   resilient-circuits run
   ```

4. Trigger a rule.