Resilient Circuits Components for function: fn_rsa_netwitness

Resilient Functions simplify development of integrations by wrapping each activity into an individual workflow component. These components can be easily installed, then used and combined in Resilient workflows. The Resilient platform sends data to the function component that performs an activity then returns the results to the workflow. The results can be acted upon by scripts, rules, and workflow decision points to dynamically orchestrate the security incident response activities.

The RSA NetWitness functions query for metadata and return pcap and log files for specific times and sessions.

Release Notes

Release History

Version	Date	Notes
1.1.3	6/2021	Fix for convert_to_nw_time
1.1.2	6/2021	Updated execute_call to execute_call_v2
1.1.1	6/2021	Bug fix for json logs output

Contents:

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)

To package for distribution,

```
python ./fn_rsa_netwitness/setup.py sdist
```

To install the package

```
pip install dist/fn_rsa_netwitness-x.x.x.tar.gz
```

After installation, the package will be loaded by resilient-circuits run. To uninstall,

```
pip uninstall fn-rsa-netwitness
```

Requirements:

- resilient-circuits

Installation:

Run the following command to import this function into IBM resilient

```
resilient-circuits customize -y -l fn-rsa-netwitness
```

To configure this function run and following command

```
resilient-circuits config -u -l fn-rsa-netwitness
```

Then edit the app.config file and provide the following NetWitness configurations:

```
 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]
```

Optionally, run selftest to test the integration you configured with the following command

```
resilient-circuits selftest -l fn-rsa-netwitness
```

Run Resilient Circuits

```
resilient-circuits run
```