Utility Functions for IBM SOAR

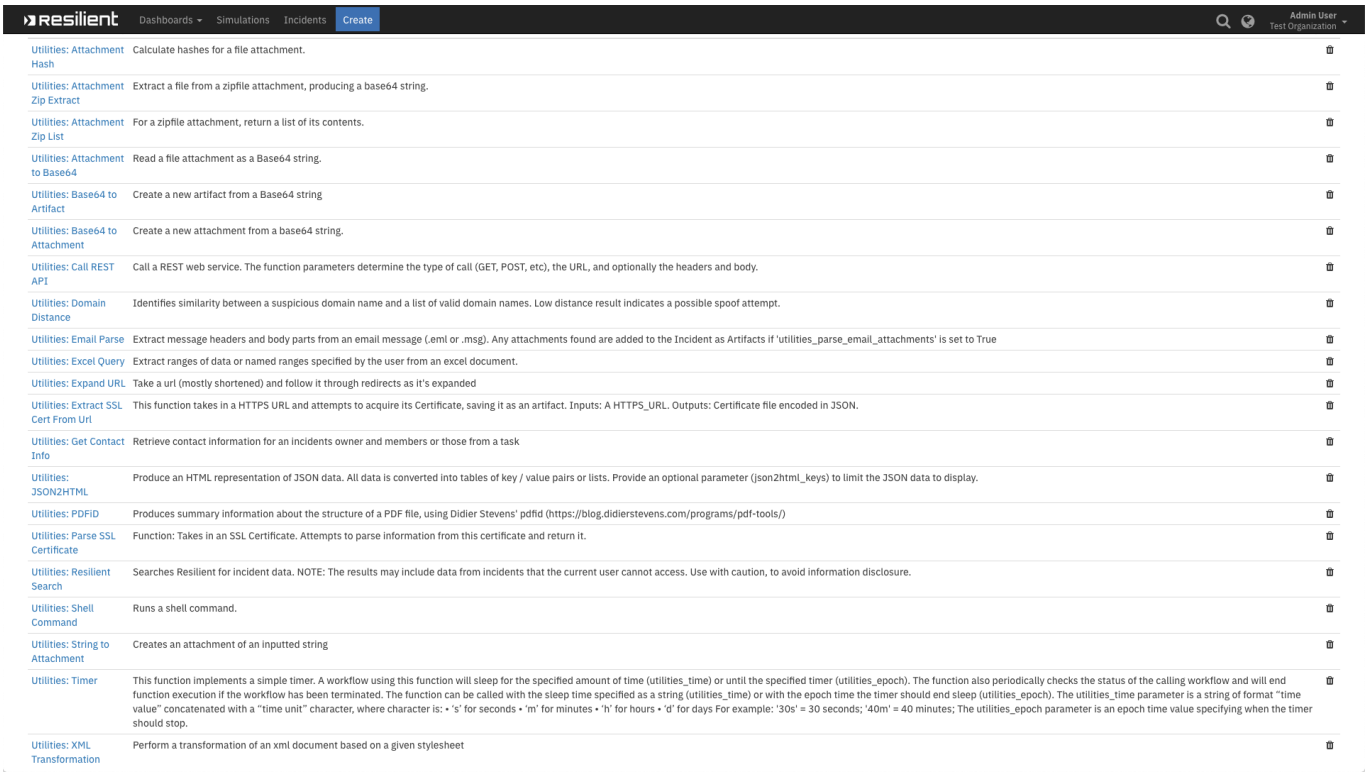
Release Notes

Release History

Version	Date	Notes
2.1.0	3/2022	• Support for PATCH method • Add rule to get owner contact info for Tasks • Bug fix for utilities_pdfid
2.0.6	7/2021	pin dependency 'chardet' at v4.0.0
2.0.2	2/2021	bug fixes for Shell Command
2.0.1	9/2020	bug fixes
2.0.0	7/2020	Numerous fixes, improved Rules and workflows and only Python 3 supported
1.0.15	5/2020	Bug fixes, App Host Support
1.0.14	5/2020	Shell Command support for Remote Linux Execution

Overview

Useful workflow functions for common automation and integration activities in the SOAR platform



SOAR functions simplify development of integrations by wrapping each external activity into an individual workflow component. These components can be easily installed, then used and combined in SOAR workflows. The SOAR 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

---

Requirements

- SOAR platform >= `v42.0`
- An Integration Server running `resilient_circuits>=30.0.0`
  - To set up an Integration Server see: ibm.biz/res-int-server-guide

---

Installation

- Download the `fn_utilities.zip`.
- Copy the `.zip` to your Integration Server and SSH into it.
- **Unzip** the package:

```
$ unzip fn_utilities-x.x.x.zip
```

- **Change Directory** into the unzipped directory:

```
$ cd fn_utilities-x.x.x
```

- **Install** the package:

```
$ pip install fn_utilities-x.x.x.tar.gz
```

- Import the **configurations** into your app.config file:

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

- Import the fn_utilities **customizations** into the SOAR platform:

```
$ resilient-circuits customize -y -l fn-utilities
```

- Open the config file, scroll to the bottom and edit your fn_utilities configurations:

```
$ nano ~/.resilient/app.config
```

Config	Required	Example	Description
shell_escaping	No	`sh`	For safety, shell_command parameter values are escaped. Set this to `sh` (Bash) or `ps` (PowerShell).
remote_powershell_extensions	No	`ps1, psm1`	A CSV list of extensions a remote PowerShell is trusted to run.
remote_auth_transport	No	`ntlm`	Transport authentication method for a remote PowerShell. Can be NTLM or basic.
max_timer	No	`30d`	Max Timer sleep time. The input string is of format “time value” concatenated with a “time unit” character, where character is: ‘s’ for seconds, ‘m’ for minutes, ‘h’ for hours ‘d’ for days. For example: '30s' = 30 seconds; '40m' = 40 minutes;

- **Save** and **Close** the app.config file.

- [Optional]: Run selftest to test the Integration you configured:

```
$ resilient-circuits selftest -l fn-utilities
```

- **Run** resilient-circuits or restart the Service on Windows/Linux:

```
$ resilient-circuits run
```

Uninstall

- SSH into your Integration Server.
- **Uninstall** the package:

```
$ pip uninstall fn-utilities
```

- Open the config file, scroll to the [fn_utilities] section and remove the section or prefix # to comment out the section.
- **Save** and **Close** the app.config file.

Troubleshooting

There are several ways to verify the successful operation of a function.

SOAR Action Status

- When viewing an incident, use the Actions menu to view **Action Status**.
- By default, pending and errors are displayed.
- Modify the filter for actions to also show Completed actions.
- Clicking on an action displays additional information on the progress made or what error occurred.

SOAR Scripting Log

- A separate log file is available to review scripting errors.
- This is useful when issues occur in the pre-processing or post-processing scripts.
- The default location for this log file is: `/var/log/resilient-scripting/resilient-scripting.log`.

SOAR Logs

- By default, SOAR logs are retained at `/usr/share/co3/logs`.
- The `client.log` may contain additional information regarding the execution of functions.

Resilient-Circuits

- The log is controlled in the `.resilient/app.config` file under the section [resilient] and the property `logdir`.
- The default file name is `app.log`.
- Each function will create progress information.
- Failures will show up as errors and may contain python trace statements.

Support

Name	Version	Author	Support URL
fn_utilities	1.0.10	IBM SOAR	http://ibm.biz/soarcommunity