# **IBM** Resilient



## **Incident Response Platform Integrations**

Splunk Function V1.0.3

Release Date: August 2020

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.

This guide describes the Splunk Integration functions.

#### **Overview**

The Splunk function, fn\_splunk\_integration, provides an automated way of managing bidirectional actions between Resilient artifact items and Splunk items in threat intelligence collections.

The Splunk integration with the Resilient platform package provides the following:

- Search function to query a Splunk intelligence collection for threat items.
- Update function to change the status of a Splunk ES notable event.
- Add function to create a new threat intelligence item in a given Splunk collection.
- Delete function to disable a threat intelligence item from a given Splunk collection.

Together with the above functions, this package includes example workflows that demonstrate how to call those functions, rules that start the example workflows, and custom fields and data tables updated by the example workflows.

The remainder of this document describes each included function, how to configure them in custom workflows, and any additional customization options.

#### Installation

Before installing, verify that your environment meets the following prerequisites:

- Resilient platform is version 35.2 or later.
- You have access to a Resilient integration server or an App Host environment.
- Splunk version 6.6 or later.
- Splunk ES 4.7.2 or later (only required for the function to update a Splunk ES notable event).

#### **App Host Installation**

All the components for running this integration in a container already exist when using the App Host app.

To install,

- \* Navigate to Administrative Settings and then the Apps tab.
- \* Click the Install button and select the downloaded file: app-fn\_splunk\_integration-x.x.zip.
- \* Go to the Configuration tab and edit the app.config file, editing the URL and access credentials for Splunk, making any additional setting changes.

```
[fn_splunk_integration]
host=<splunk url>
port=<8089 or the customized port>
username=<splunk access user>
splunkpassword=<splunk access password, key-ring protection recommended>
verify_cert=[true|false]
```

#### **Integration Server Installation**

The functions package contains Python components that will be called by the Resilient platform to execute the functions during your workflows. These components run in the 'resilient-circuits' integration framework.

The package also includes Resilient customizations that will be imported into the platform later.

Ensure that the environment is up to date:

```
sudo pip install --upgrade pip
sudo pip install --upgrade setuptools
sudo pip install --upgrade resilient-circuits
```

To install the package, you must first unzip it then install the package as follows:

```
sudo pip install app-fn_splunk_integration-<version>.tar.gz
```

## **Configure the Python components**

The 'resilient-circuits' components run as an unprivileged user, typically named 'integration'. If you do not already have an 'integration' user configured on your appliance, create it now.

Perform the following to configure and run the integration:

1. Using 'sudo', become the integration user.

```
sudo su - integration
```

2. From the account used for Integrations, use one of the following commands to configure the Splunk settings. Use –c to create new environments or –u to update existing environments:

```
resilient-circuits config -c -l fn-splunk-integration
```

#### OR

resilient-circuits config -u -l fn-splunk-integration

- 3. Edit the .resilient/app.config configuration.
  - a. In the [resilient] section, ensure that you provide all the information needed to connect to the Resilient platform.
  - b. In the [fn splunk integration] section, edit the settings as required.

```
host=<splunk url>
port=<8089 or the customized port>
username=<splunk access user>
splunkpassword=<splunk access password, key-ring protection recommended>
verify_cert=[true|false]
```

Use "false" for self-signed certificates.

#### Deploy customizations into the Resilient platform

The package contains function definitions that you can use in workflows, and also includes example workflows and rules that show how to use these functions. Install these customizations to the Resilient platform with the following command:

```
resilient-circuits customize -l fn-splunk-integration
```

You will be prompted to import the functions and associated message destinations, workflows, and so on. Note that users can arrange custom fields and data tables in the Layout to suit their particular needs.

#### Run the integration framework

Run the integration manually with the following command:

```
resilient-circuits run
```

The resilient-circuits command starts, loads its components, and continues to run until interrupted. If it stops immediately with an error message, check your configuration values and retry.

## Configuration of resilient-circuits for restartability

For normal operation, resilient-circuits must run <u>continuously</u>. The recommended way to do this is to configure the service to automatically run at startup. On a Red Hat appliance, this is done using a systemd unit file such as the one below. You may need to change the paths to your working directory and app.config.

The unit file should be named 'resilient circuits.service':

```
sudo vi /etc/systemd/system/resilient circuits.service
```

#### The contents:

```
[Unit]
```

```
Description=Resilient-Circuits Service
After=resilient.service
Requires=resilient.service
[Service]
Type=simple
User=integration
WorkingDirectory=/home/integration
ExecStart=/usr/local/bin/resilient-circuits run
Restart=always
TimeoutSec=10
Environment=APP_CONFIG_FILE=/home/integration/.resilient/app.config
Environment=APP_LOCK_FILE=/home/integration/.resilient/resilient_circuits.
lock
[Install]
WantedBy=multi-user.target
```

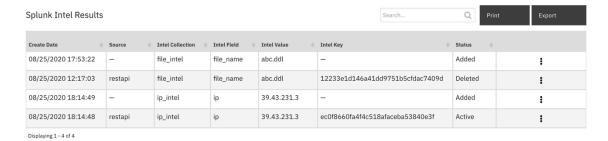
Ensure that the service unit file is correctly permissioned:

```
sudo chmod 664 /etc/systemd/system/resilient circuits.service
```

## **Upgrades**

When upgrading from previous versions, a new datatable, <code>splunk\_itel\_results</code>, replaces the previous table. Please update your layout to reflect the use of this new datatable.

Its use has also changed, including add intel operations and reflecting the status of a collection entry ("Active" or "Deleted").



## **Function Descriptions**

In the Customization Settings section of the Resilient platform, you can verify that the following Splunk specific functions, workflows, datatable, and rules are available by clicking their respective tabs.

Here are the details about how each function is used in the example workflows and rules.

#### **Splunk Search**

This function performs a query to fetch data from the Splunk server.

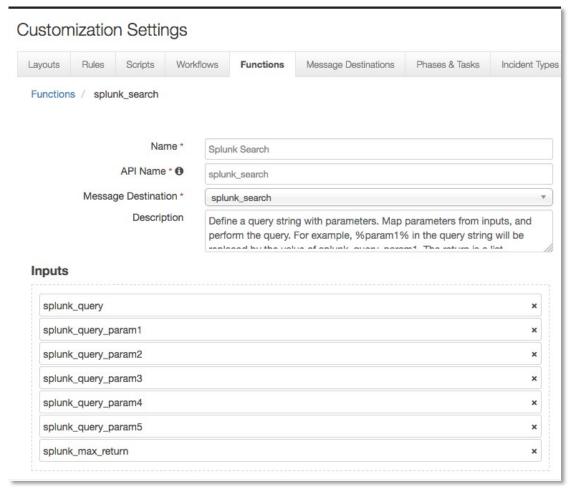


Figure 1: Splunk Search

As shown above, this function takes the following parameters:

- splunk\_query: Query to perform. It contains demo template queries that you can select from within the workflow. The demo queries contain parameters which are replaced by the splunk\_query\_param[n] below. For example, one demo query is: SELECT %param1% FROM events WHERE username=%param2% LAST %param3% MINUTES. Users can then set values for splunk\_query\_param1, splunk\_query\_param2, and splunk\_query\_param3 in the workflow.
- splunk query param[n]: parameters used in the query.
- splunk max return: specifies how many events to return from Splunk.

The example workflow (object type = Artifact) that calls this function is "Example of searching an artifact in Splunk ES". The Input tab of this function is shown in Figure 2. It shows the mapping of the parameters; for example, %param1% in the query is mapped to the appropriate Splunk collection, such as ip\_intel.

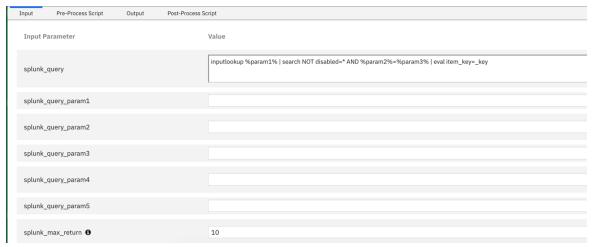


Figure 2: Example of searching an artifact in Splunk ES

In the Pre-Process Script, the %param3% is set to the value of the artifact associated with this workflow and the collection is determined by a lookup table of artifact values and Splunk collection information.

```
lookup map = {
 "DNS Name": ("ip intel", "domain"),
  "Email Attachment": None,
  "Email Attachment Name": ("file intel", "file name"),
 "Email Body": None,
 "Email Recipient": None,
 "Email Sender": ("email intel", "src user"),
 "Email Sender Name": ("email intel", "src user"),
 "Email Subject": ("email intel", "subject"),
 "File Name": ("file_intel", "file_name"),
 "File Path": None,
 "HTTP Request Header": None,
 "HTTP Response Header": None,
 "IP Address": ("ip intel", "ip"),
 "Log File": None,
 "MAC Address": None,
 "Malware Family/Variant": None,
 "Malware MD5 Hash": ("file intel", "file hash"),
 "Malware Sample": None,
 "Malware Sample Fuzzy Hash": ("file intel", "file hash"),
 "Malware SHA-1 Hash": ("file intel", "file hash"),
 "Malware SHA-256 Hash": ("file intel", "file hash"),
 "Mutex": None,
 "Network CIDR Range": None,
 "Other File": None,
 "Password": None,
 "Port": None,
 "Process Name": ("process intel", "process"),
 "Registry Key": ("registry intel", "registry value name"),
 "RFC 822 Email Message File": None,
 "Service": ("service_intel", "service"),
 "String": None,
 "System Name": ("service intel", "service"),
 "URI Path": None,
 "URL": ("http intel", "url"),
 "URL Referer": ("http_intel", "http_referrer"),
 "User Account": None,
 "User Agent": ("http intel", "http user agent")
```

A rule "Search Splunk ES for an artifact" is also included to call the provided workflow.

With these components in place, if an IP Address artifact is added, users can click the Actions button, and the above rule appears as shown in Figure 4. By clicking the menu item, this search function is activated. The search result from Splunk is used to update the custom data table called "splunk\_results" shown in Figure 5. The definition of this data table is also included in the package.

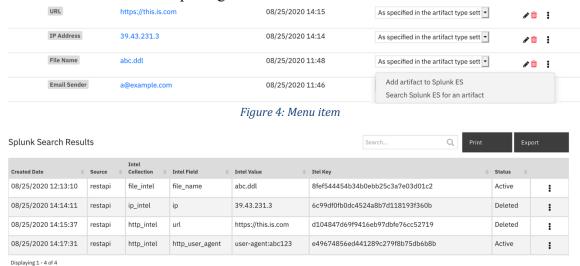


Figure 5: Data table

## Splunk Add Intelligence Item

This function adds a new threat intelligence item to a given collection.

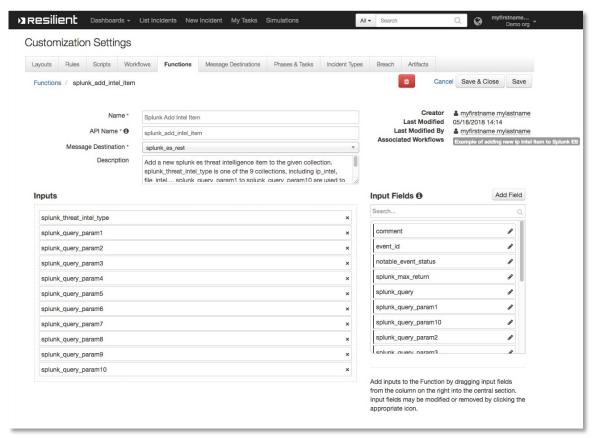


Figure 6: Splunk Add Intelligence Item

Here, splunk\_threat\_intel\_type is the name of the Splunk threat intelligence collection, and splunk\_query\_param1 to splunk\_query\_param10 are inputs used to create a python dictionary that adds a new threat intelligence item to a given collection.

In the Input tab of the example workflow for artifact, splunk\_threat\_intel\_type is set to ip\_intel, and splunk\_query\_param1 to ip. In the Pre-Process Script, splunk\_query\_param2 is the value of the associated artifact. For an IP address artifact, a

python dictionary: {"ip": "the\_associated\_artifact\_value"}, and a new item is added to the ip\_intel collection.

An example rule, "Add artifact to Splunk ES", calls this example workflow. As a result, a user can click on this menu item to add an artifact to the appropriate collection of Splunk ES, such as ip intel.



Figure 7: Rule and Menu Item

#### **Splunk Delete Intelligence Item**

This function is used to disable a threat intelligence item from a given collection. A workflow, "Example of deleting an artifact in Splunk ES", calls this function, and is activated by a rule called "Delete artifact from Splunk ES".

The rule is a menu item to a row in the included data table. As shown in Figure 8, a row contains the intel\_item\_key corresponding to this intelligence item. This menu item calls the function to delete the item associated with that item key.



*Figure 8: Data table row with data including intel\_item\_key* 

#### **Splunk ES Notable Event**

This function updates the status and comment of a given notable event, using the event\_id stored in an incident. It can be used together with the "Resilient Integration for Splunk ES" addon.

An incident escalated from the "Resilient Integration for Splunk and Splunk ES" addon contains a custom property called splunk\_notable\_event\_id. In the workflow, the status of the incident is mapped to the status of notable event. Also, a comment is given in the Input tab. As a result, this menu item updates the notable event identified by this event id accordingly.

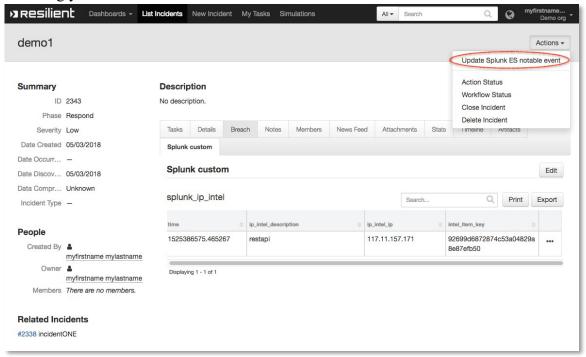


Figure 10: Update Splunk ES Notable Event

## **Troubleshooting**

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

• Resilient 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.

• Resilient 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.

Resilient Logs

By default, Resilient 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 <code>.resilient/app.config</code> file under the section <code>[resilient]</code> and the property <code>logdir</code>. The default file name is <code>app.log</code>. Each function will create progress information. Failures will show up as errors and may contain python trace statements.

## **Support**

For additional support, contact <u>support@resilientsystems.com</u>. Including relevant information from the log files will help us resolve your issue.