IBM Resilient

Incident Response Platform Integrations

McAfee ATD Functions V1.0.0

Release Date: June 2018

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

This guide describes the McAfee ATD Function.

Overview

The McAfee ATD function contains the ability to analyze a file or URL in ATD and send the result back to the Resilient platform.

This document describes the McAfee ATD function, its customization options, and how to configure it in custom workflows.

Installation

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

- Resilient platform must be version 30 or later.
- You must have a Resilient account available for the integration. This can be any account that has the permission to view and modify administrator and customization settings, and read and update incidents. You must know the account username and password.
- You must have access to the command line of the Resilient appliance, which hosts the Resilient platform; or to a separate integration server where you will deploy and run the functions code. If you are using a separate integration server, you must install Python version 2.7.10 or later, or version 3.6 or later, and "pip". (The Resilient appliance is preconfigured with a suitable version of Python).

Install the Python components

The functions package contains Python components that are 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.

Complete the following steps to install the Python components:

1. Enter the following commands to ensure that the environment is up to date:

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

2. Enter the following command to install the package,

```
sudo pip install --upgrade fn_mcafee_atd-<1.0.0>.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.

Complete the following steps to configure and run the integration:

1. Using sudo, switch to the `integration` user, as follows.

```
sudo su - integration
```

2. Enter one of the following commands to create or update the `resilient-circuits` configuration file:

```
resilient-circuits config -c
```

or

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

3. Edit the `resilient-circuits` configuration file, as follows:

   a. In the [`resilient`] section, ensure that you provide all of the information required to connect to the Resilient platform.

   b. In the [fn_mcafee_atd] section, edit the settings as follows:

```
atd_url=https://<your_atd_server>:<port>
atd_username=<your_atd_username>
atd_password=<your_atd_password>
timeout= #Amount of time in minutes before the function quits and throws
an error.
polling_interval= #Interval in seconds to wait and check to see if the
file has finished being analyzed
vm_profile_list= #Analyzer profile ID
filePriority=[run_now|add_to_q]
atd_trust_cert=[true|false]
```

   Use false for self-signed SSL certificates.

Deploy customizations to the Resilient platform

The package contains the function definition that you can use in workflows and also example workflows and rules that show how to use the function.

1. Use the following command to install these customizations into the Resilient platform:

```
resilient-circuits customize
```

2. Respond to the prompts to deploy the function, message destination, workflow and rule. The following data will be imported.

```
Function inputs: artifact_id, artifact_value, attachment_id, incident_id,
mcafee_atd_report_type, mcafee_atd_url_submit_type, task_id
Message Destination: McAfee ATD Message Destination
Function: McAfee ATD Analyze File, McAfee ATD Analyze URL
Workflow: (Example) McAfee ATD Analyze Artifact File, (Example) McAfee ATD
Analyze Attachment, (Example) McAfee ATD Analyze URL
Rule: (Example) McAfee ATD Analyze Artifact File, (Example) McAfee ATD
Analyze Attachment, (Example) McAfee ATD Analyze URL
```

Run the integration framework

Enter the following command to run the integration manually:

```
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. The following example shows a successful connection to the Resilient platform and loading of components:

```
2018-05-14 14:34:44,161 INFO [app] Configuration file:
/Users/<user>/.resilient/app.config
2018-05-14 14:34:44,162 INFO [app] Resilient server: localhost
2018-05-14 14:34:44,163 INFO [app] Resilient org: TestOrg
2018-05-14 14:34:44,164 INFO [app] Logging Level: INFO
2018-05-14 14:34:44,165 WARNING [co3] Unverified HTTPS requests
(cafile=false).
2018-05-14 14:34:44,756 INFO [component_loader] Loading 1 components
2018-05-14 14:34:44,758 INFO [component_loader]
'fn_mcafee_atd.components.mcafee_atd_analyze_file.FunctionComponent'
loading
2018-05-14 14:34:44,760 INFO [component_loader] Loading
```

```
2018-05-14 14:34:44,761 WARNING [actions_component] Unverified STOMP TLS
certificate (cafile=false)
2018-05-14 14:34:44,771 INFO [stomp_component] Connect to localhost:65001
2018-05-14 14:34:44,773 INFO [actions_component]
'fn_mcafee_atd.components.mcafee_atd_analyze_file.FunctionComponent'
function 'mcafee_atd_analyze_file' registered to
'mcafee_atd_message_destination'
2018-05-14 14:34:44,779 INFO [app] App Started
2018-05-14 14:34:44,781 INFO [actions_component]
'mcafee_atd_analyze_url.FunctionComponent' function
'mcafee_atd_analyze_url' registered to 'mcafee_atd_message_destination'
2018-05-14 14:34:44,782 INFO [component_loader] Loaded and registered
component 'mcafee_atd_analyze_url'
2018-05-14 14:34:44,783 INFO [actions_component]
'mcafee_atd_analyze_file.FunctionComponent' function
'mcafee_atd_analyze_file' registered to 'mcafee_atd_message_destination'
2018-05-14 14:34:44,784 INFO [component_loader] Loaded and registered
component 'mcafee_atd_analyze_file'
2018-05-14 14:34:44,784 INFO [actions_component] STOMP attempting to
connect
2018-05-14 14:34:44,785 INFO [app] Components loaded
2018-05-14 14:34:44,787 INFO [stomp_component] Connect to Stomp...
2018-05-14 14:34:44,788 INFO [client] Connecting to localhost:65001 ...
2018-05-14 14:34:44,802 INFO [client] Connection established
2018-05-14 14:34:44,905 INFO [client] Connected to stomp broker
[session=ID:resilient.localdomain-46697-1525363200980-5:90, version=1.2]
2018-05-14 14:34:44,908 INFO [stomp_component] Connected to
failover:(ssl://localhost:65001)?maxReconnectAttempts=1,startupMaxReconnec
tAttempts=1
2018-05-14 14:34:44,908 INFO [stomp_component] Client HB: 0  Server HB:
15000
2018-05-14 14:34:44,909 INFO [stomp_component] No Client heartbeats will
be sent
2018-05-14 14:34:44,910 INFO [stomp_component] Requested heartbeats from
server.
2018-05-14 14:34:44,911 INFO [actions_component] Subscribe to message
destination 'mcafee_atd_message_destination'
2018-05-14 14:34:44,912 INFO [actions_component] STOMP connected.
2018-05-14 14:34:44,913 INFO [stomp_component] Subscribe to message
destination actions.<org_id>.mcafee_atd_message_destination
```

Configuration of resilient-circuits for restart

For normal operation, `resilient-circuits` must run continuously. The recommended way to do this is to configure it to automatically run at start up. On a Red Hat appliance, you can do this using a `systemd` unit file, such as the one below. You might need to change the paths to your working directory and `app.config`.

1. The unit file must be named `resilient_circuits.service`. To create the file, enter the following command:

```
sudo vi /etc/systemd/system/resilient_circuits.service
```

2. Add the following content to the file:

```
[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.lo
ck
[Install]
WantedBy=multi-user.target
```

3. Ensure that the service unit file is correctly permissioned, as follows:

```
sudo chmod 664 /etc/systemd/system/resilient_circuits.service
```

4. Use the `systemctl` command to manually start, stop, restart and return status on the service:

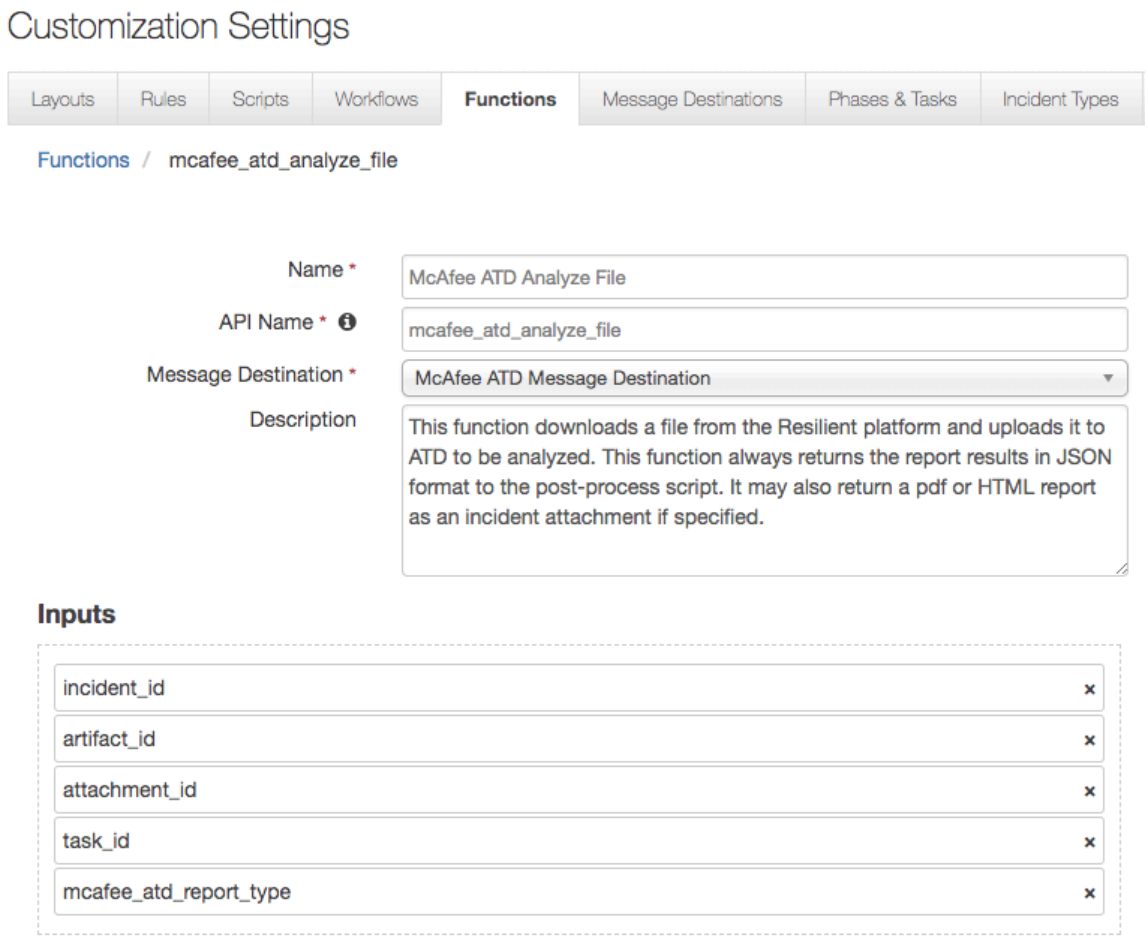
```
sudo systemctl resilient_circuits [start|stop|restart|status]
```

You can view log files for `systemd` and the `resilient-circuits` service using the `journalctl` command, as follows:

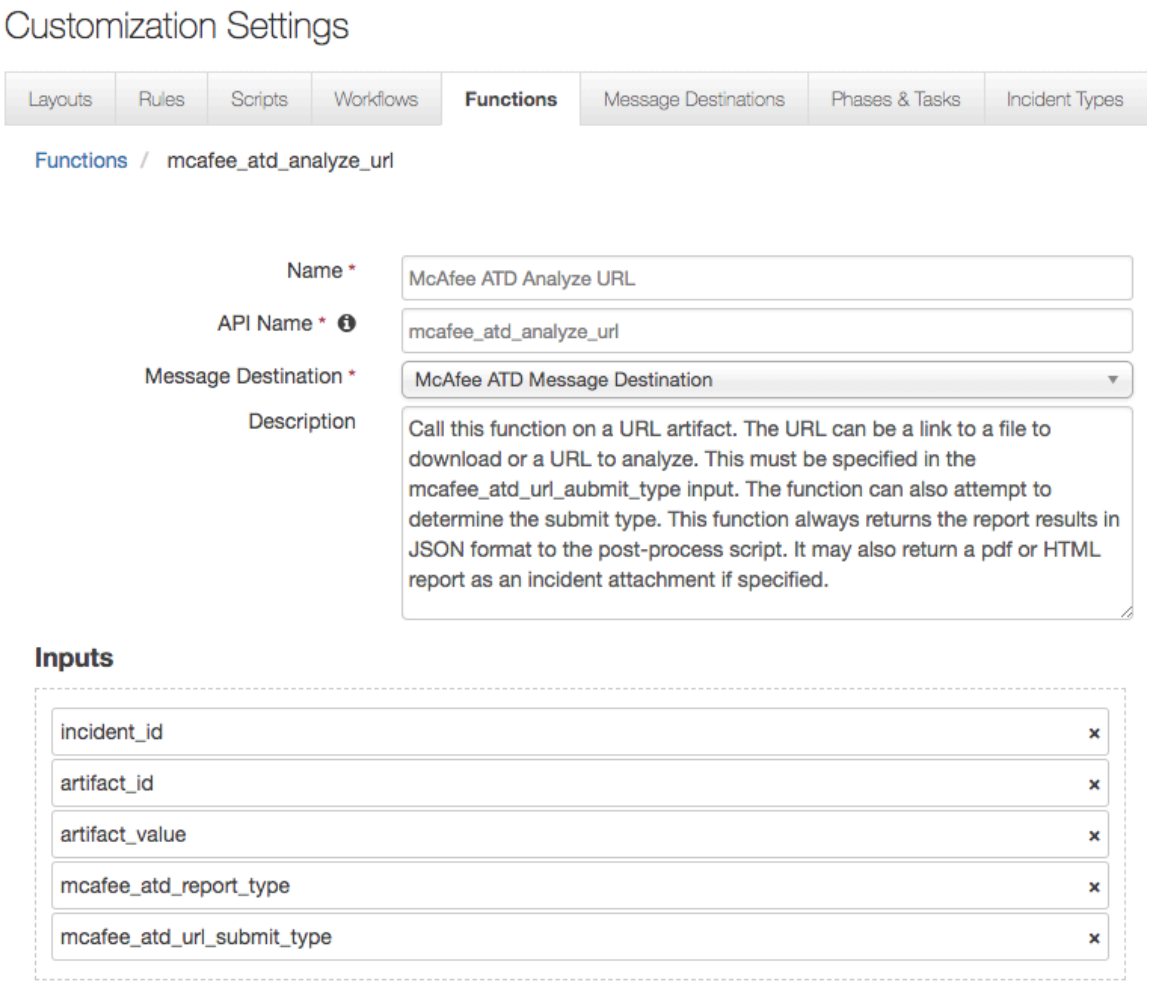
```
sudo journalctl -u resilient_circuits --since "2 hours ago"
```

Function Description

After the function package has been deployed, you can view the functions in the Functions tab in the Resilient platform. You can see function details by clicking the name, as shown in the following screenshots.



The McAfee ATD Analyze File function uploads a file to be analyzed by McAfee ATD and returns the results back to the Resilient platform. Uploading a file is possible from attachments (both incident and task attachments) in addition to artifacts which support attachments. Expected inputs are the incident id, the object id where the file came from (incident attachment, task attachment, or artifact) in addition to the report type.



The McAfee ATD Analyze URL function sends a URL to be analyzed by McAfee ATD and returns the results back to the Resilient platform. Sending the URL is supported when the function is triggered from an artifact which has a URL. URL types supported are URLs which contain the location of a site or URL which is a link to download a file. Inputs to this function include the `incident id`, `artifact id`, `artifact value` (which is the URL), the type of report to return, and finally the submit type for the URL. The submit type refers to the type of URL being sent to ATD. Two types are supported with this function; URL link which just processes the URL inside the analyzer VM and URL download which first downloads a file to be analyzed. The submit type refers to the type of URL being sent to ATD. Two types are supported with this function; URL link, which processes the URL inside the analyzer VM, and URL download, which first downloads a file to be analyzed. The `mcafee_atd_url_submit_type` input has those two options and a third that attempts to determine whether it is based on URL link or URL download, whether the URL ends in a file type, such as .exe. However, this option is not certain to work as expected.

These functions include three example workflows and rules that show how the functions can be used. You can copy and modify these workflows and rules for your own needs.

Do to the nature of workflows, it is only supported that this function can only be called once per workflow per incident. Therefore, the user will have to check the Workflow and Action Status to verify when analysis is complete and the workflow has finished.

For both functions, if a report type of PDF or HTML is chosen for the `mcafee_atd_report_type` input, the report will be added as an attachment to the incident, otherwise as always the report data in JSON format along with the inputs will be returned to the function Post-Process Script. Below is an example of what the response in the Post-Process Script could look like for both functions.

McAfee ATD Analyze File example response


```
{
   "Inputs":{
      "macfee_atd_report_type":"pdf",
      "attachment_id":50,
      "incident_id":2099
   },
   "Run Time":"66.8727591038",
   "Summary":{
      "JSONversion":"1.002",
      "Subject":{
         "size":"167941",
         "sha-1":"AF5FD8F10F6B2BD56F1D4D15B6A895B94485ADF4",
         "Timestamp":"2018-05-15 19:34:09",
         "FileType":"512",
         "sha-
256":"2252DC3FADE1F3DF0DED8CED25B71D6B34DF63D04B9C00E9A9E4F91B05CF51E5",
         "parent_archive":"Not Available",
         "md5":"570E481C2E45DF1918C534E63CA43180",
         "Type":"PE32 executable (GUI) Intel 80386",

"Name":"2252DC3FADE1F3DF0DED8CED25B71D6B34DF63D04B9C00E9A9E4F91B05CF51E5.e
xe"
      },
      "Process":[
         {
            "Reason":"processed by down selectors",

"Name":"2252DC3FADE1F3DF0DED8CED25B71D6B34DF63D04B9C00E9A9E4F91B05CF51E5.e
xe",
            "Severity":"5"
         }
      ],
      "SUMversion":"4.2.2.16",
      "Selectors":[
         {
            "Engine":"Gateway Anti-Malware",
            "Severity":"5",
            "MalwareName":"W32/Rontokbro.gen@MM"
         },
         {
            "Engine":"Anti-Malware",
            "Severity":"5",
            "MalwareName":"W32/Rontokbro.gen@MM"
         },
         {
            "Engine":"Sandbox",
            "Severity":"0",
            "MalwareName":"---"
         }
```

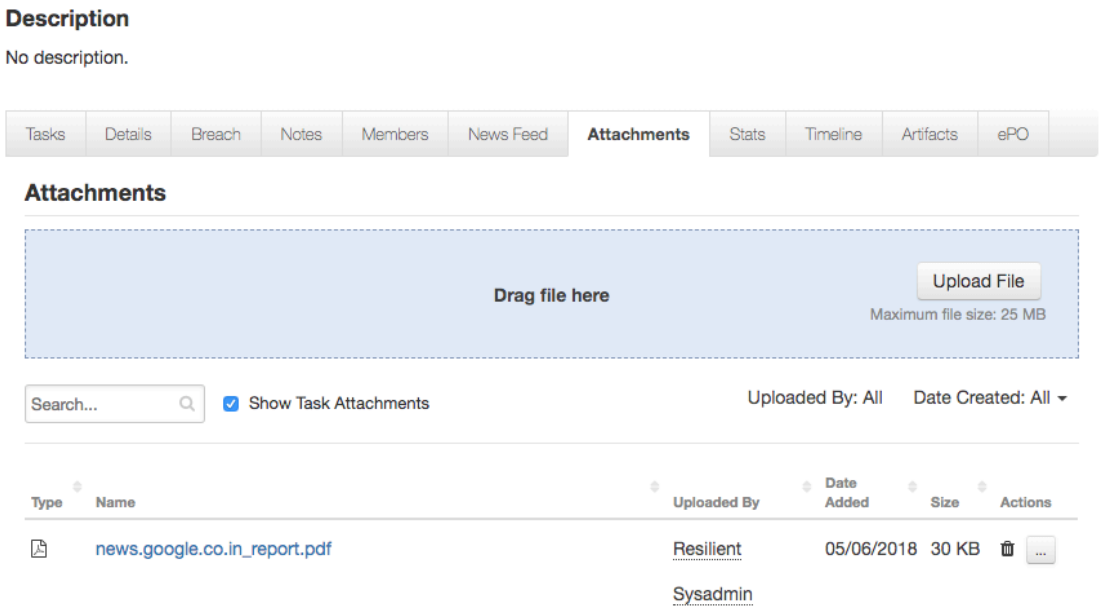
```
      ],
      "hasDynamicAnalysis":"false",
      "Behavior":[
         "Identified as W32/Rontokbro.gen@MM by Gateway Anti-Malware",
         "Identified as W32/Rontokbro.gen@MM by Anti-Malware"
      ],
      "Verdict":{
         "Severity":"5",
         "Description":"The submitted file is not compatible to VM(s) in
the Analyzer Profile"
      },
      "OSversion":"StaticAnalysis",
      "Data":{
         "compiled_with":"Not Available",
         "analysis_seconds":"1",
         "sandbox_analysis":"0"
      },
      "MISversion":"4.2.2.16",
      "DETversion":"4.2.2.180222"
   }
}
```


McAfee ATD Analyze URL example response

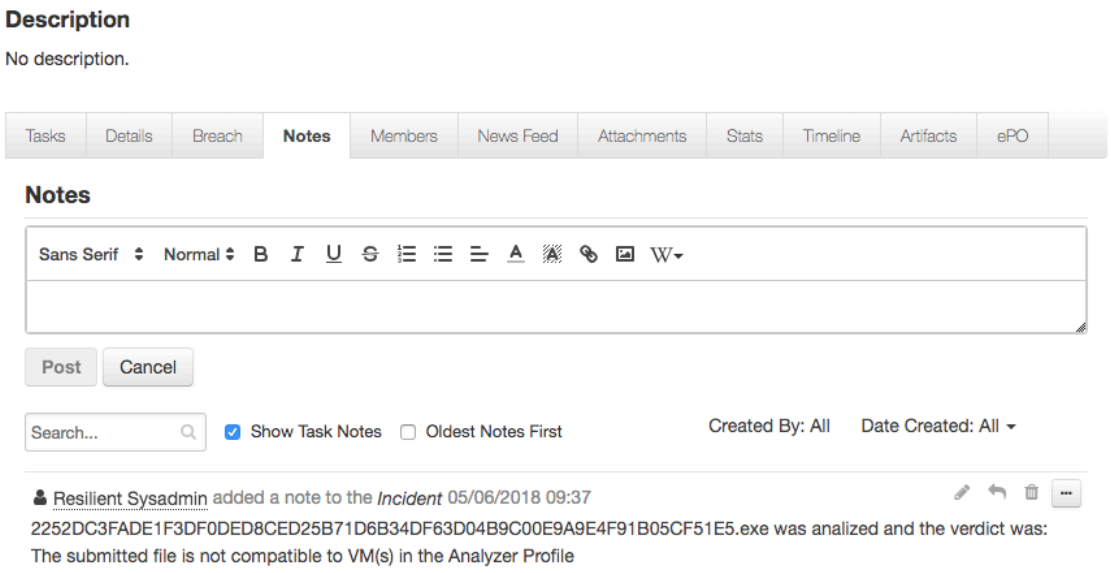

```
{
   "Inputs":{
      "incident_id":2099,
      "artifact_value":"http://news.google.co.in/",
      "artifact_id":65,
      "mcafee_atd_url_submit_type":"Attempt to determine URL submit type",
      "macfee_atd_report_type":"pdf"
   },
   "Run Time":"4.8045668602",
   "Summary":{
      "JSONversion":"1.002",
      "Subject":{
         "size":"25",
         "sha-1":"1E90EDEBA0E12EA5797BBBB524CBC21DAC5B7EEF",
         "Timestamp":"2018-05-15 21:39:15",
         "FileType":"512",
         "sha-
256":"126E9A971CE51CD3ED09034E0526A838DC556584F397CB121B278E08D0890B46",
         "parent_archive":"Not Available",
         "md5":"839F551F97E669DDDB348BDDB907D32C",
         "Type":"application/url",
         "Name":"http://news.google.co.in/"
      },
      "Process":[
         {
            "Reason":"processed by down selectors",
            "Name":"http://news.google.co.in/",
            "Severity":"0"
         }
      ],
      "SUMversion":"4.2.2.16",
      "Selectors":[
         {
            "Engine":"Gateway Anti-Malware",
            "Severity":"0",
            "MalwareName":"---"
```

```
         },
         {
            "Engine":"Anti-Malware",
            "Severity":"0",
            "MalwareName":"---"
         },
         {
            "Engine":"Sandbox",
            "Severity":"0",
            "MalwareName":"---"
         }
      ],
      "hasDynamicAnalysis":"false",
      "Behavior":[
         "Identified as --- by Gateway Anti-Malware",
         "Identified as --- by Anti-Malware"
      ],
      "Verdict":{
         "Severity":"0",
         "Description":"The submitted file is not compatible to VM(s) in
the Analyzer Profile"
      },
      "OSversion":"StaticAnalysis",
      "Data":{
         "compiled_with":"Not Available",
         "analysis_seconds":"1",
         "sandbox_analysis":"0"
      },
      "MISversion":"4.2.2.16",
      "DETversion":"4.2.2.180222"
   }
}
```


The out-of-the-box Workflows can be triggered from attachments and artifacts. If a report type is set, the report is attached as an incident attachment like the following.



Finally, the provided Workflows also adds a note to the incident with the verdict of the file or URL which was analyzed.



Troubleshooting

There are several ways to verify the successful operation of a function, as follows:

- 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` might contain additional information regarding the execution of functions.

- Resilient-Circuits

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

Support

For additional support, contact support@resilientsystems.com.

Including relevant information from the log files will help us resolve your issue.