

Joe Sandbox Analysis Function for IBM Resilient

Table of Contents

- [app.config settings](#)
- [Function Inputs](#)
- [Function Output](#)
- [Pre-Process Script](#)
- [Post-Process Script](#)
- [Rules](#)

This package contains a function that can that executes a Joe Sandbox Analysis of an Attachment or Artifact and returns the Analysis Report to IBM Resilient.

The screenshot shows the IBM Resilient interface for customizing a workflow. The top navigation bar includes 'Dashboards', 'Simulations', 'Incidents', and a 'Create' button. The 'Customization Settings' section is active, with tabs for 'Layouts', 'Rules', 'Scripts', 'Workflows', 'Functions', 'Message Destinations', 'Phases & Tasks', 'Incident Types', 'Breach', and 'Artifacts'. The 'Workflows' tab is selected, showing a workflow named 'Example: Joe Sandbox Analysis [Attachment]'. The workflow details include:

- Name:** Example: Joe Sandbox Analysis [Attachment]
- API Name:** example_joe_sandbox_analysis_attachment
- Description:** An example of having an attachment sample analyzed by Joe Sandbox
- Object Type:** Attachment
- Creator:** Admin User
- Last Modified:** 01/22/2019 15:19
- Last Modified By:** Orchestration Engine
- Associated Rules:** Example: Joe Sandbox Analysis [Attachment]

The workflow diagram shows a sequence of steps: a start node (circle with a plus sign) labeled 'Start your workflow here', followed by a function node (rounded rectangle with a yellow 'f' icon) labeled 'Joe Sandbox Analysis', and ending with a circle node.

- Supports an attachment or artifact that is a file, or where the artifact's value contains a URL.
- Allows users to select the type of report, PDF, HTML, or JSON, which is returned from Joe Sandbox.
- Supports a proxy. Just add your proxy details to the [app.config](#) file.
- The function depends on **Joe Security's python module, jbxapi**. See [here](#) for more details

app.config settings:

```
[fn_joe_sandbox_analysis]
# Accept Terms & Conditions
jsb_accept_tac=True

# Your JoeSandbox API Key
```

```
jsb_api_key=

# The analysis URL
jsb_analysis_url=https://jbxcloud.joesecurity.org/analysis

# Amount of time in seconds to wait until checking if the report is ready
again
jsb_analysis_report_ping_delay=120

# This is the max time in seconds the function will wait for the report to
be generated
jsb_analysis_report_request_timeout=1800

# Set if you need to use a proxy to access JSB
#jsb_http_proxy=http://user:pass@10.10.1.10:3128
#jsb_https_proxy=http://user:pass@10.10.1.10:1080
```

Function Inputs:

Function Name	Type	Required	Example	Info
<code>incident_id</code>	Number	Yes	1001	The ID of the current Incident
<code>attachment_id</code>	Number	No	5	The ID of the Attachment to be analyzed
<code>artifact_id</code>	Number	No	6	The ID of the Artifact to be analyzed
<code>jsb_report_type</code>	Select	Yes	"json"	The type of report to be returned from Joe Sandbox. Options are: <code>html</code> , <code>pdf</code> , or <code>json</code>

Function Output:

```
results = {
  "analysis_report_name": "My Malicious Scan Report",
  "analysis_report_id": 123,
  "analysis_report_url":
"https://jbxcloud.joesecurity.org/analysis/123/456",
  "analysis_status": "clean"
}
```

Pre-Process Script:

This example just sets the function inputs.

```
inputs.incident_id = incident.id
inputs.artifact_id = artifact.id
```

Post-Process Script:

This example adds a Note to the Incident and color codes the **analysis_status** depending if it was **malicious** or **clean**

```
color = "#45bc27"

if (results.analysis_status != "clean"):
    color = "#ff402b"

noteText = """"<br>Joe Sandbox analysis <b>{0}</b> complete
           <b>Artifact:</b> '{1}'
           <b>Report URL:</b> <a href='{2}'>{2}</a>
           <b>Detection Status:</b> <b style="color: {3}">{4}
</b>""".format(results.analysis_report_name, artifact.value,
               results.analysis_report_url, color, results.analysis_status)

incident.addNote(helper.createRichText(noteText))
```

Rules

Rule Name	Object Type	Workflow Triggered
Example: Joe Sandbox Analysis [Artifact]	Artifact	Example: Joe Sandbox Analysis [Artifact]
Example: Joe Sandbox Analysis [Attachment]	Attachment	Example: Joe Sandbox Analysis [Attachment]
