

# SNDBOX Sandbox Analyzer Function for IBM Resilient

## Table of Contents

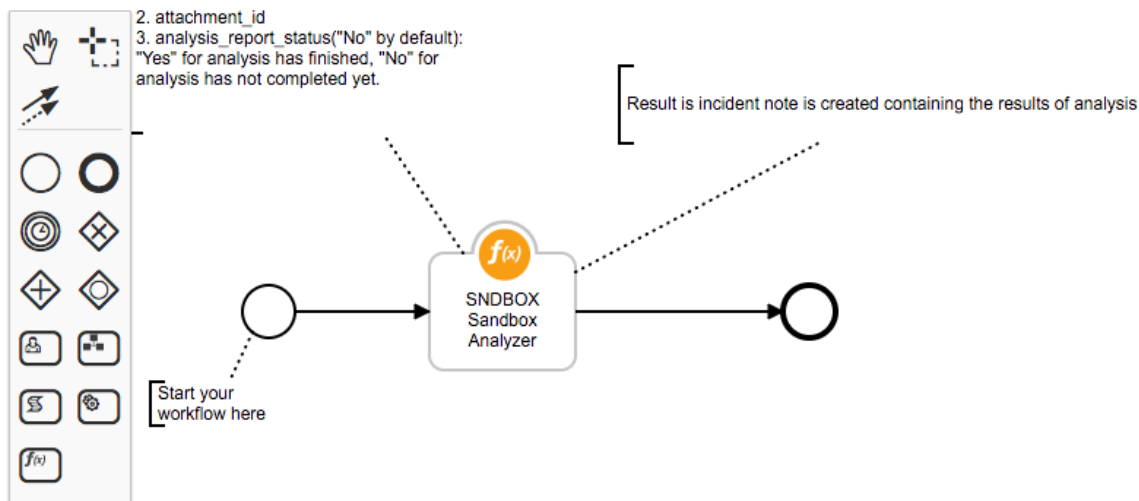
---

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

////////////////////////////////////

This package contains a function that executes a SNDBOX Malware Sandbox Analysis using SNDBOX Cloud APIs, also included are two example workflows and two example rules that demonstrate how to use this function.

Name *	Example: SNDBOX Sandbox Analyzer [Attachment]
API Name * ⓘ	example_sndbox_sandbox_analyzer_attachment
Description	This workflow takes an attachment file as input and calls the SNDBOX platform function to determine if the file contains malware. The analysis result is returned in an incident note.
Object Type *	Attachment



## Notes

- an attachment or artifact must be a file. Please refer <https://app.sndbox.com/docs/files> for the supported file list.
  - The report only supports Type of JSON. HTML and PDF are not supported.
- ////////////////////////////////////

# app.config settings:

```
# Your SNDBOX Analyzer API Key
sndbox_api_key=

# Your SNDBOX Server URL, using https://api.sndbox.com if empty.
sndbox_analyzer_url=https://api.sndbox.com

# Amount of time in seconds to wait until timeout.
sndbox_analyzer_report_request_timeout=300
```

# Function Inputs:

Function Name	Type	Required	Example	Info
incident_id	Number	Yes	1001	The ID of the current Incident
attachment_id	Number	No	5	The ID of the Attachment to be analyzed
artifact_id	Number	No	6	The ID of the Artifact to be analyzed
analyzer_report_status	Boolean	Yes	No	Has the analysis report generated successfully. Options are: Yes or No

# Function Output:

```
results = {
    "analysis_report_status": analyzer_report_status,
    "incident_id": incident_id,
    "artifact_id": artifact_id,
    "attachment_id": attachment_id,
    "sample_final_result": sample_final_result
}
```

# Pre-Process Script:

#### Example: SNDBOX Sandbox Analyzer [Attachment]

```
inputs.incident_id = incident.id
inputs.attachment_id = attachment.id
```

#### Example: SNDBOX Sandbox Analyzer [Artifact]

```
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**

```
def font_color(score):
    color = "green"
    try:
        if float(score) >= 0.56:
            color = "red"
    except:
        pass
    return color

def sample_score(score):
    return round(score * 100) if score else 0

if not results.sandbox_analysis_report_status:
    noteText = u"""Successful submit <b>{}</b> to SNDBOX Platform. However it will
    artifact.value)

else:
    noteText = u"""Successful submit <b>{}</b> to SNDBOX Platform. Check the resu
    artifact.value)

    for sample in results.sample_final_result:
        noteText += u"""-----
        color = font_color(sample["sample_report"]["score"])
        noteText += u"""<br>SNDBOX Sandbox Analysis: <b>{sample_filename}</b> com
            SNDBOX Online Attachment: <a href={sample_online_report}>{samp
            SNDBOX Analyzer result: Score: <b style= "color:{color}">{sam
        """.format(sample_filename=sample["sample_report"]["name"],
                    sample_online_report=sample["sample_report"]["sample_ur
                    color=color,
                    sample_score=sample_score(sample["sample_report"]["scor

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

**Example of adding a incident note from post-processing scripts:**

 Resilient Sysadmin added a note to the *Incident* 06/18/2019 17:20

Successful submit **d560119a1d85e53ebfa82154d7358726\_ms\_creation.doc** to SNDBOX Platform. Check the results below:

SNDBOX Sandbox Analysis: **d560119a1d85e53ebfa82154d7358726\_ms\_creation.doc** complete.

SNDBOX Online Attachment: <https://app.sandbox.com/sample/b837767c-41a0-4be0-be76-bc5d542fe209>

SNDBOX Analyzer result: Score: **100.0**

# Rules

Rule Name	Object Type	Workflow Triggered
Example: SNDBOX Sandbox Analysis [Artifact]	Artifact	Example: SNDBOX Sandbox Analyzer [Artifact]

Rules / Example: SNDBOX Sandbox Analyzer [Artifact]



Cancel

Save & Close

Save

Display Name \*

Example: SNDBOX Sandbox Analyz

Object Type

Artifact

Conditions

Add conditions in which to invoke the rule. [Clear All](#)

☐ All ☒ Any ☐ Advanced

example: 1 OR (2 AND 3)



Type

is equal to

Email Attachment



Type

is equal to

Log File



Type

is equal to

Other File



## Activities

Ordered

Ordered Activities will be invoked in the order specified below. They include: *Add Tasks*, *Run Script*, and *Set Field*. [Add New](#)

Workflows

Workflow Activities are started after all Ordered Activities complete.

Example: SNDBOX Sandbox Analyzer [Artifact] x

Destinations

Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

[Show Activity Fields](#)

Rule Name	Object Type	Workflow Triggered2
Example: SNDBOX Sandbox Analyzer [Attachment]	Attachment	Example: SNDBOX Sandbox Analyzer [Attachment]



Cancel

Save & Close

Save

Display Name \*

Example: SNDBOX Sandbox Analyz

Object Type

Attachment

Conditions

Add conditions in which to invoke the rule. [Add New](#)

Activities

Ordered

Ordered Activities will be invoked in the order specified below. They include: *Add Tasks, Run Script, and Set Field.* [Add New](#)

Workflows

Workflow Activities are started after all Ordered Activities complete.

Example: SNDBOX Sandbox Analyzer [Attachment] x

Destinations

Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

Show Activity Fields