

Parent/Child Relationships

Table of Contents

- [Release Notes](#)
 - [Overview](#)
 - [Key Features](#)
 - [Requirements](#)
 - [SOAR platform](#)
 - [Cloud Pak for Security](#)
 - [Python Environment](#)
 - [Installation](#)
 - [Install](#)
 - [App Configuration](#)
 - [Custom Layouts](#)
 - [Function - Relations: Assign Parent](#)
 - [Function - Relations: Auto Close Child Incidents](#)
 - [Function - Relations: Copy Task](#)
 - [Function - Relations: Remove Child Relation](#)
 - [Function - Relations: Sync Artifact](#)
 - [Function - Relations: Sync Child Table Data](#)
 - [Function - Relations: Sync DataTable Data](#)
 - [Function - Relations: Sync Notes](#)
 - [Function - Relations: Sync Task Notes](#)
 - [Data Table - Relations Child Incidents](#)
 - [Custom Fields](#)
 - [Custom Artifact Types](#)
 - [Rules](#)
 - [Troubleshooting & Support](#)
-

Release Notes

Version	Date	Notes
1.0.0	07/2020	Initial Release
1.0.1	05/2021	Add AppHost Support Patch: Verification of Parent Incident before creating relation
1.0.2	04/2023	Support for Python 3.9 Support for CP4S Patch: Verification of Parent and Child Incidents are different Patch: Changed rules to only sync incident notes
2.0.0	09/2023	New Function: Copy Task to Children New Function: Sync Task Notes from Copied Tasks New Function: Sync Artifact Data to Parent and Children New Function: Sync DataTable Data to Parent and Children Enhancement: Added functionality to all note syncing to allow conversations, meaning notes and replies to notes for better collaboration

Overview

The Relations function is meant to provide the ability to allow parent/child relations levels within Resilient to link incidents “manually”. This package consists of 9 Functions, 9 Workflows, and 11 Rules along with 2 new fields and 1 new data table.

If you would like the Playbook variants of these instead of the workflows, Checkout the link below:

<https://github.com/TheIRGurus/Playbooks/tree/main/Incident%20Relations%20Playbooks>

This document outlines the functionality of function as it relates to Resilient.

Builds Relationships of Incidents within IBM Security SOAR



App used within the SOAR platform allowing the relationship building of incidents as Children and Parents.

The app will also allow syncing of notes between the incidents with a relationship, auto closing child incidents of a closed parent, and syncing changes in child status with the parent DataTable that shows all children.

Key Features

- Assign Parent incident to Child
- Remove Child Relation if established incorrectly
- Sync Notes between Parent and Child
 - Child Notes sync automatically
 - Parent Notes sync manually
- Parent incident contains Data Table of Children incidents
- Sync Child incident data automatically to Parent Data Table
- Copy Tasks from the Parent Incident to the Children
- Sync Notes from the Copied Tasks between Parent and Child
 - Child Notes sync automatically
 - Parent Notes sync manually
- Syncing of Artifacts between Parent to Children
- Auto-close Child incidents on Parent incident closure

Requirements

No application specific configuration settings are required.

This app supports the IBM Security QRadar SOAR Platform and the IBM Security QRadar SOAR for IBM Cloud Pak for Security.

SOAR platform

The SOAR platform supports two app deployment mechanisms, Edge Gateway (formerly App Host) and integration server.

If deploying to a SOAR platform with an Edge Gateway, the requirements are:

- SOAR platform >= **46.0.8131**.
- The app is in a container-based format (available from the AppExchange as a **zip** file).

If deploying to a SOAR platform with an integration server, the requirements are:

- SOAR platform >= **46.0.8131**.
- The app is in the older integration format (available from the AppExchange as a **zip** file which contains a **tar.gz** file).
- Integration server is running **resilient-circuits**>=48.0.0.
- If using an API key account, make sure the account provides the following minimum permissions:

Name	Permissions
Org Data	Read
Function	Read
All Incidents	Read
All Incidents Status	Edit

Name	Permissions
All Incidents Fields	Edit
All Incidents Notes	Edit

The following SOAR platform guides provide additional information:

- *Edge Gateway Deployment Guide* or *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *Integration Server Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings.
- *System Administrator Guide*: provides the procedure to install, configure and deploy apps.

The above guides are available on the IBM Documentation website at ibm.biz/soar-docs. On this web page, select your SOAR platform version. On the follow-on page, you can find the *Edge Gateway Deployment Guide*, *App Host Deployment Guide*, or *Integration Server Guide* by expanding **Apps** in the Table of Contents pane. The System Administrator Guide is available by expanding **System Administrator**.

Cloud Pak for Security

If you are deploying to IBM Cloud Pak for Security, the requirements are:

- IBM Cloud Pak for Security >= 1.8.
- Cloud Pak is configured with an Edge Gateway.
- The app is in a container-based format (available from the AppExchange as a [zip](#) file).

The following Cloud Pak guides provide additional information:

- *Edge Gateway Deployment Guide* or *App Host Deployment Guide*: provides installation, configuration, and troubleshooting information, including proxy server settings. From the Table of Contents, select Case Management and Orchestration & Automation > **Orchestration and Automation Apps**.
- *System Administrator Guide*: provides information to install, configure, and deploy apps. From the IBM Cloud Pak for Security IBM Documentation table of contents, select Case Management and Orchestration & Automation > **System administrator**.

These guides are available on the IBM Documentation website at ibm.biz/cp4s-docs. From this web page, select your IBM Cloud Pak for Security version. From the version-specific IBM Documentation page, select Case Management and Orchestration & Automation.

Python Environment

Python 3.6 and Python 3.9 are supported. Additional package dependencies may exist for each of these packages:

- resilient-circuits>=48.0.0

Installation

Install

- To install or uninstall an App or Integration on the *SOAR platform*, see the documentation at ibm.biz/soar-docs.
- To install or uninstall an App on *IBM Cloud Pak for Security*, see the documentation at ibm.biz/cp4s-docs and follow the instructions above to navigate to Orchestration and Automation.

App Configuration

No application specific configuration settings are required.

Custom Layouts

- Import the Data Tables and Custom Fields like the screenshot below:

If Relation Level is: Parent

New Tab: Child Incidents

- Add Relations Child Incidents data table

Summary Section:

- Add Relation Level

Tasks

Details

Child Incidents

QRadar

SEP

Areas/Users Involved

Artifacts

Notes

Attachments

News Feed

Timeline

Relations Child Incidents

Search...

Print

Export

Edit

Incident ID	Incident Name	Incident Status	
5146	Child Incident 1	Closed	
5147	Child Incident 2	Closed	
5166	Child Incident 4	Closed	

Relation Level

Parent

Status

Closed

Phase

Initial

Severity

High

Incident Disposition

Confirmed

Data Compromised

Unknown

Resolution

Resolved

Incident Classification

Security

Incident Type

Reported Phish

FQUAL Association

—

NIST Attack Vectors

E-mail

People

If Relation Level is: Child

Summary Section:

- Add Relation Level
- Parent ID

Summary

ID

5146

Relation Level

Child

Parent ID

5169

Status

Closed

Phase

Initial

Severity

Info

Function - Relations: Assign Parent

Create a parent/child relationship between the 2 incidents provided.

Name *

Relations: Assign Parent

API Name * ⓘ

relations_assign_parent

Message Destination *

fn_relations

Description

Create a parent/child relationship between the 2 incidents provided.

Inputs

relations_child_incident_id

relations_parent_incident_id

► Inputs:

Name	Type	Required	Example	Tooltip
relations_child_incident_id	number	Yes	-	-
relations_parent_incident_id	number	Yes	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```

results = {
  "content": {
    "child_artifact_results": {
      "content": {
        "actions": [
          {
            "enabled": false,
            "id": 23,
            "name": "Update Data Table Row"
          },
          {
            "enabled": false,
            "id": 96,
            "name": "Example: XML Transformation"
          },
          {
            "enabled": false,
            "id": 21,
            "name": "Get Data Table Rows"
          },
          {
            "enabled": false,
            "id": 91,
            "name": "Example: Shell Command"
          },
          {
            "enabled": false,
            "id": 92,
            "name": "Example: String to Attachment"
          },
          {
            "enabled": false,
            "id": 20,
            "name": "Get Data Table Row"
          },
          {
            "enabled": false,
            "id": 17,
            "name": "Delete Data Table Rows"
          },
          {
            "enabled": false,
            "id": 16,
            "name": "Delete Data Table Row"
          },
          {
            "enabled": false,
            "id": 100,
            "name": "Add Row to Datatable"
          },
          {
            "enabled": false,
            "id": 27,

```

```
    "name": "Defender Find Machine by DNS name"
  },
  {
    "enabled": false,
    "id": 28,
    "name": "Defender Find Machines by File Hash"
  },
  {
    "enabled": false,
    "id": 29,
    "name": "Defender Find Machines by Internal IP Address"
  },
  {
    "enabled": false,
    "id": 30,
    "name": "Defender Get File Information"
  },
  {
    "enabled": false,
    "id": 42,
    "name": "Defender Set Indicator"
  },
  {
    "enabled": false,
    "id": 75,
    "name": "Example: (Artifact) Attachment to Base64"
  },
  {
    "enabled": false,
    "id": 429,
    "name": "Example: Network Utilities Domain Distance"
  },
  {
    "enabled": false,
    "id": 430,
    "name": "Example: Network Utilities Expand URL"
  },
  {
    "enabled": false,
    "id": 431,
    "name": "Example: Network Utilities Extract SSL Certificate from URL"
  },
  {
    "enabled": false,
    "id": 81,
    "name": "Example: Email Parsing (Artifact)"
  },
  {
    "enabled": false,
    "id": 79,
    "name": "Example: Call REST API"
  },
  {
    "enabled": false,
    "id": 432,
    "name": "Example: Network Utilities Linux Shell Command"
  },
  {
    "enabled": false,
    "id": 433,
    "name": "Example: Network Utilities Local Shell Command"
  },
  {
    "enabled": false,
    "id": 76,
    "name": "Example: Artifact Hash"
```

```
},
{
  "enabled": false,
  "id": 434,
  "name": "Example: Network Utilities Windows Shell Command"
},
{
  "enabled": false,
  "id": 83,
  "name": "Example: Expand URL"
},
{
  "enabled": false,
  "id": 84,
  "name": "Example: Extract SSL Certificate"
},
{
  "enabled": false,
  "id": 87,
  "name": "Example: JSON2HTML"
},
{
  "enabled": false,
  "id": 88,
  "name": "Example: Parse SSL Certificate"
},
{
  "enabled": false,
  "id": 210,
  "name": "Example: LDAP Utilities: Remove User(s) from Group(s)"
},
{
  "enabled": false,
  "id": 225,
  "name": "QRadar Move from Sample Blocked to Sample Suspected"
},
{
  "enabled": false,
  "id": 80,
  "name": "Example: Domain Distance"
},
{
  "enabled": false,
  "id": 213,
  "name": "Example: LDAP Utilities: Toggle Access"
},
{
  "enabled": false,
  "id": 214,
  "name": "Example: LDAP Utilities: Update"
},
{
  "enabled": false,
  "id": 191,
  "name": "Example: Exchange Online Get User Profile"
},
{
  "enabled": false,
  "id": 194,
  "name": "Example: Exchange Online Query Messages on Artifact"
},
{
  "enabled": false,
  "id": 205,
  "name": "Schedule a Rule/Playbook to Run - Artifact"
},
},
```

```
{
  "enabled": false,
  "id": 267,
  "name": "Example: urlscan.io"
},
{
  "enabled": false,
  "id": 381,
  "name": "Example: Relations - Sync Artifact"
},
{
  "enabled": false,
  "id": 209,
  "name": "Example: LDAP Utilities: Add User(s) to Group(s)"
},
{
  "enabled": false,
  "id": 211,
  "name": "Example: LDAP Utilities: Search"
},
{
  "enabled": false,
  "id": 212,
  "name": "Example: LDAP Utilities: Set Password"
},
{
  "enabled": false,
  "id": 365,
  "name": "Run whois query against Artifact (RDAP)"
},
{
  "enabled": false,
  "id": 364,
  "name": "Run rdap query against Artifact"
},
{
  "enabled": true,
  "id": 221,
  "name": "Find All QRadar Reference Sets"
},
{
  "enabled": true,
  "id": 222,
  "name": "Find in QRadar Reference Set"
},
{
  "enabled": false,
  "id": 223,
  "name": "QRadar Add to Reference Set"
},
{
  "enabled": true,
  "id": 224,
  "name": "QRadar Add to Reference Table"
}
],
"attachment": null,
"created": 1693442727342,
"creator_principal": {
  "display_name": "AppBuilder",
  "id": 49,
  "name": "6bf8c47e-77a6-41ad-ad22-1004f7eee7cb",
  "type": "apikey"
},
"description": "Parent Incident ID in Relationship",
"global_artifact": [],
```



```

    "global_info": null,
    "hash": "99e5ebfa1cbebdd970bb3d841bb645d8bee76c375a637406859e2a8425951177",
    "hits": [],
    "id": 3828,
    "inc_id": 2802,
    "inc_name": "Child 3",
    "inc_owner": 1,
    "ip": {
      "destination": null,
      "source": null
    },
    "last_modified_by": {
      "display_name": "AppBuilder",
      "id": 49,
      "name": "6bf8c47e-77a6-41ad-ad22-1004f7eee7cb",
      "type": "apikey"
    },
    "last_modified_time": 1693442727362,
    "parent_id": null,
    "pending_scan_result": false,
    "pending_sources": [],
    "perms": {
      "delete": true,
      "read": true,
      "write": true
    },
    "playbooks": [
      {
        "display_name": "Relations: Sync Artifact",
        "playbook_handle": 138
      },
      {
        "display_name": "Scheduler: Schedule a Job (Artifact) (PB)",
        "playbook_handle": 131
      }
    ],
    "properties": null,
    "related_incident_count": null,
    "relating": true,
    "type": 1040,
    "value": "2799"
  },
  "success": true
},
"notes_synced": 1,
"parent_artifact_results": {
  "content": "Parent Already in Artifacts",
  "success": false
},
"table_addition_results": {
  "content": {
    "actions": [],
    "cells": {
      "relations_incident_id": {
        "id": "relations_incident_id",
        "row_id": 6786,
        "value": "\u003cdiv class=\"rte\"\u003e\u003cdiv\u003e\u003ca href=\"#incidents/2802\" target=\"_blank\"\u003e2802\u003c/a\u003e\u003c/div\u003e\u003c/div\u003e"
      },
      "relations_incident_name": {
        "id": "relations_incident_name",
        "row_id": 6786,
        "value": "Child 3"
      },
      "relations_incident_status": {
        "id": "relations_incident_status",

```

```
        "row_id": 6786,
        "value": "Active"
      }
    },
    "id": 6786,
    "inc_id": 2799,
    "inc_name": "Parent",
    "inc_owner": "john_doe@company.com",
    "playbooks": [],
    "table_name": "Relations Child Incidents",
    "type_id": 1043,
    "version": 1
  },
  "success": true
}
},
"inputs": {
  "relations_child_incident_id": 2802,
  "relations_parent_incident_id": 2799
},
"metrics": {
  "execution_time_ms": 11502,
  "host": "IBM-PF36KPAV",
  "package": "fn-relations",
  "package_version": "2.0.0",
  "timestamp": "2023-08-30 20:45:34",
  "version": "1.0"
},
"raw": null,
"reason": null,
"success": true,
"version": 2.0
}
```

► Example Pre-Process Script:

```
inputs.relations_child_incident_id = incident.id
inputs.relations_parent_incident_id = rule.properties.relations_parent_incident
```

► Example Post-Process Script:

None

Function - Relations: Auto Close Child Incidents

Close child incidents when the parent incident is closed.

Name *

Relations: Auto Close Child Incidents

API Name * ⓘ

relations_auto_close_child_incidents

Message Destination *

fn_relations

Description

Close child incidents when the parent incident is closed.

Inputs

relations_parent_incident_id

► Inputs:

Name	Type	Required	Example	Tooltip
relations_parent_incident_id	number	Yes	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "incidents": [
      2801,
      2800
    ]
  },
  "inputs": {
    "relations_parent_incident_id": 2799
  },
  "metrics": {
    "execution_time_ms": 10038,
    "host": "IBM-PF36KPAV",
    "package": "fn-relations",
    "package_version": "2.0.0",
    "timestamp": "2023-08-30 21:12:37",
    "version": "1.0"
  },
  "raw": null,
  "reason": null,
  "success": true,
  "version": 2.0
}
```

► Example Pre-Process Script:

```
inputs.relations_parent_incident_id = incident.id
```

► Example Post-Process Script:

```
None
```

Function - Relations: Copy Task

Copy a task from a Parent Incident down to the Children.

Name *

API Name * ⓘ

Message Destination *

Description

Relations: Copy Task

relations_copy_task

fn_relations

Copy a task from a Parent Incident down to the Children.

Inputs

relations_parent_incident_id

task_id

► Inputs:

Name	Type	Required	Example	Tooltip
relations_parent_incident_id	number	Yes	-	-
task_id	number	No	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "children": [
      2797,
      2796,
      2798
    ],
    "task": {
      "due_date": 1693454400000,
      "instructions": "\u003cdiv class=\"rte\"\u003e\u003cdiv\u003eThis is a instruction list for the new task!\u003c/div\u003e\u003cdiv\u003c/div\u003e",
      "name": "Task 615 from Parent: New Task for the Kids",
      "phase_id": "Containment \u0026 Remediation",
      "required": true
    }
  },
  "inputs": {
    "relations_parent_incident_id": 2795,
    "task_id": 615
  },
  "metrics": {
    "execution_time_ms": 7216,
    "host": "IBM-PF36KPAV",
    "package": "fn-relations",
    "package_version": "2.0.0",
    "timestamp": "2023-08-30 23:29:46",
    "version": "1.0"
  },
  "raw": null,
  "reason": null,
```

```
"success": true,
"version": 2.0
}
```

► Example Pre-Process Script:

```
inputs.relations_parent_incident_id
```

► Example Post-Process Script:

```
None
```

Function - Relations: Remove Child Relation

Used to remove the relation child relation from a Child incident as well as removing the parent relation from the Parent incident if it no longer has children.

Name *

Relations: Remove Child Relation

API Name * ⓘ

relations_remove_child_relation

Message Destination *

fn_relations

Description

Used to remove the relation child relation from a Child incident as well as removing the parent relation from the Parent incident if it no longer has children.

Inputs

relations_child_incident_id

relations_remove_notes

► Inputs:

Name	Type	Required	Example	Tooltip
relations_child_incident_id	number	Yes	-	-
relations_remove_notes	boolean	Yes	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "child_incident": 2800,
    "parent_incident": 2799
  },
  "inputs": {
    "relations_child_incident_id": 2802,
    "relations_remove_notes": true
  },
  "metrics": {
    "execution_time_ms": 15068,

```

```
    "host": "IBM-PF36KPAV",
    "package": "fn-relations",
    "package_version": "2.0.0",
    "timestamp": "2023-08-30 20:44:47",
    "version": "1.0"
  },
  "raw": null,
  "reason": null,
  "success": true,
  "version": 2.0
}
```

► Example Pre-Process Script:

```
inputs.relations_child_incident_id = incident.id
inputs.relations_remove_notes = rule.properties.relations_remove_notes
```

► Example Post-Process Script:

```
None
```

Function - Relations: Sync Artifact

Sync Artifacts from the incident where the artifact is currently to the parent or child.

Name *

API Name * ⓘ

Message Destination *

Description

Relations: Sync Artifact

relations_sync_artifact

fn_relations

Sync Artifacts from the incident where the artifact is currently to the parent or child.

Inputs

incident_id

artifact_id

► Inputs:

Name	Type	Required	Example	Tooltip
artifact_id	number	No	-	-
incident_id	number	Yes	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "artifact": {
```

```
    "description": "Artifact Synced from incident 2795. created from Sentinel entity: cb1a7e68-4ff3-9aef-4224-e2b3b5adbdbc",
    "type": "String",
    "value": "windowssvmos2"
  },
  "incidents": [
    2797,
    2796,
    2798
  ]
},
"inputs": {
  "artifact_id": 3805,
  "incident_id": 2795
},
"metrics": {
  "execution_time_ms": 5944,
  "host": "IBM-PF36KPAV",
  "package": "fn-relations",
  "package_version": "2.0.0",
  "timestamp": "2023-08-30 23:27:26",
  "version": "1.0"
},
"raw": null,
"reason": null,
"success": true,
"version": 2.0
}
```

► Example Pre-Process Script:

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

► Example Post-Process Script:

None

Function - Relations: Sync Child Table Data

Update data within the Parent Table if the Child data changes.

Name *

Relations: Sync Child Table Data

API Name * ⓘ

relations_sync_child_table_data

Message Destination *

fn_relations

Description

Update data within the Parent Table if the Child data changes.

Inputs

relations_child_incident_id

relations_parent_incident_id

► Inputs:

Name	Type	Required	Example	Tooltip
relations_child_incident_id	number	Yes	-	-
relations_parent_incident_id	number	Yes	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "response": {
      "actions": [],
      "cells": {
        "relations_incident_id": {
          "id": "relations_incident_id",
          "row_id": 6786,
          "value": "\u003cddiv class=\"rte\"\u003e\u003cddiv\u003e\u003ca href=\"#incidents/2802\" target=\"_blank\"\u003e2802\u003c/a\u003e\u003c/div\u003e\u003c/div\u003e"
        },
        "relations_incident_name": {
          "id": "relations_incident_name",
          "row_id": 6786,
          "value": "Child 3"
        },
        "relations_incident_status": {
          "id": "relations_incident_status",
          "row_id": 6786,
          "value": "Closed"
        }
      },
      "id": 6786,
      "inc_id": 2799,
      "inc_name": "Parent",
      "inc_owner": "john_doe@company.com",
      "playbooks": [],
      "table_name": "Relations Child Incidents",
      "type_id": 1043,
      "version": 4
    }
  },
  "inputs": {
    "relations_child_incident_id": 2802,
    "relations_parent_incident_id": 2799
  }
}
```



```
    },
    "metrics": {
      "execution_time_ms": 2219,
      "host": "IBM-PF36KPAV",
      "package": "fn-relations",
      "package_version": "2.0.0",
      "timestamp": "2023-08-30 21:58:36",
      "version": "1.0"
    },
    "raw": null,
    "reason": null,
    "success": true,
    "version": 2.0
  }
}
```

► Example Pre-Process Script:

```
import re

regex = re.compile(r'#incidents/(\d+)')

inputs.relations_parent_incident_id =
int(re.findall(regex,incident.properties.relations_parent_id[ 'content' ])[0])
inputs.relations_child_incident_id = incident.id
```

► Example Post-Process Script:

```
None
```

Function - Relations: Sync DataTable Data

A Function used to Sync DataTable Data from the incident where it resides to the parent or child.

Name *

API Name * ⓘ

Message Destination *

Description

Relations: Sync DataTable Data

relations_sync_datatable_data

fn_relations

A Function used to Sync DataTable Data from the incident where it resides to the parent or child.

Inputs

incident_id

relations_datatables

relations_exclude_datatables

relations_row_data

► Inputs:

Name	Type	Required	Example	Tooltip
------	------	----------	---------	---------

Name	Type	Required	Example	Tooltip
incident_id	number	Yes	-	-
relations_datatables	text	Yes	data_table_api1,data_table_api2 OR All	A comma seperated list of DataTable API Names to sync, or just "All" if syncing everything.
relations_exclude_datatables	text	No	data_table_api1,data_table_api2,data_table_api3	A Comma Seperated list of DataTable API Names that are to be excluded from the Sync. Meant to be used when syncing "All" DataTables.
relations_row_data	text	No	-	The entire row output of a DataTable Row for syncing specific Rows individually.

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "datatables": [
      "ldap_users"
    ],
    "incidents": [
      2797,
      2796,
      2798
    ],
    "rows": null
  },
  "inputs": {
    "incident_id": 2795,
    "relations_datatables": "ldap_users",
```

```
    "relations_exclude_datatables": "dt_relations_child_incidents"
  },
  "metrics": {
    "execution_time_ms": 5321,
    "host": "IBM-PF36KPAV",
    "package": "fn-relations",
    "package_version": "2.0.0",
    "timestamp": "2023-08-30 23:41:19",
    "version": "1.0"
  },
  "raw": null,
  "reason": null,
  "success": true,
  "version": 2.0
}
```

► Example Pre-Process Script:

```
inputs.incident_id = incident.id
inputs.relations_datatables = rule.properties.relations_datatables_to_sync
if rule.properties.relations_datatables_to_exclude:
    inputs.relations_exclude_datatables = 'dt_relations_child_incidents,' +
rule.properties.relations_datatables_to_exclude
else:
    inputs.relations_exclude_datatables = 'dt_relations_child_incidents'
```

► Example Post-Process Script:

```
None
```

Function - Relations: Sync Notes

Sync notes from the incident where the note is currently to the parent or child.

Name *

API Name * ⓘ

Message Destination *

Description

Relations: Sync Notes

relations_sync_notes

fn_relations

Sync notes from the incident where the note is currently to the parent or child.

Inputs

incident_id

relations_note_id

► Inputs:

Name	Type	Required	Example	Tooltip
incident_id	number	Yes	-	-

Name	Type	Required	Example	Tooltip
<code>relations_note_id</code>	number	Yes	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "new_note": {
      "text": {
        "content": "Note from Parent Incident: \u003ca href=\"#incidents/2799\"
target=\"_blank\" \u003e2799\u003c/a\u003e\u003cbr\u003eNote ID: 609\u003cbr\u003eOn Date: 08/30/2023
20:43:40\u003cbr\u003eBy: John Doe\u003cbr\u003e\u003cbr\u003e\u003cdiv
class=\"rte\" \u003e\u003cdiv\u003eReply to the privileged note!\u003c/div\u003e\u003c/div\u003e\",
        "format": "html"
      }
    }
  },
  "inputs": {
    "incident_id": 2799,
    "relations_note_id": 609
  },
  "metrics": {
    "execution_time_ms": 5574,
    "host": "IBM-PF36KPAV",
    "package": "fn-relations",
    "package_version": "2.0.0",
    "timestamp": "2023-08-30 20:43:56",
    "version": "1.0"
  },
  "raw": null,
  "reason": null,
  "success": true,
  "version": 2.0
}
```

► Example Pre-Process Script:

```
inputs.relations_note_id = note.id
inputs.incident_id = incident.id
```

► Example Post-Process Script:

None

Function - Relations: Sync Task Notes

Sync Task notes from a copied Task back to parent originating Task.

Name *

API Name * ⓘ

Message Destination *

Description

Relations: Sync Task Notes

relations_sync_task_notes

fn_relations

Sync Task notes from a copied Task back to parent originating Task.

Inputs

task_id

relations_note_id

► Inputs:

Name	Type	Required	Example	Tooltip
relations_note_id	number	Yes	-	-
task_id	number	No	-	-

► Outputs:

NOTE: This example might be in JSON format, but `results` is a Python Dictionary on the SOAR platform.

```
results = {
  "content": {
    "new_note": {
      "parent_id": "409",
      "text": {
        "content": "Response from Child Incident: \u003ca href=\"\#incidents/2796\"
target=\"_blank\" \u003e\u003ca/a\u003e\u003cbr\u003eTask: \u003ca href=\"\#incidents/2796?
taskId=617\u0026tabName=comments\" target=\"_blank\" \u003eTask 615 from Parent: New Task for the
Kids\u003c/a\u003e\u003cbr\u003eNote ID: 413\u003cbr\u003eOn Date: 08/30/2023
23:31:03\u003cbr\u003eBy: John Doe\u003cbr\u003e\u003cbr\u003e\u003cdiv
class=\"rte\" \u003e\u003cdiv\u003eSure looks like you can!\u003c/div\u003e\u003c/div\u003e",
        "format": "html"
      }
    }
  },
  "inputs": {
    "relations_note_id": 413,
    "task_id": 617
  },
  "metrics": {
    "execution_time_ms": 4242,
    "host": "IBM-PF36KPAV",
    "package": "fn-relations",
    "package_version": "2.0.0",
    "timestamp": "2023-08-30 23:31:10",
    "version": "1.0"
  },
  "raw": null,
  "reason": null,
  "success": true,
  "version": 2.0
}
```

► Example Pre-Process Script:

```
inputs.relations_note_id note.id
inputs.task_id = task.id
```

► Example Post-Process Script:

```
None
```

Data Table - Relations Child Incidents

Relations Child Incidents

Search...

Print

Export

Incident ID	Incident Name	Incident Status	
2800	Child 1	Closed	⋮
2801	Child 2	Closed	⋮
2802	Child 3	Closed	⋮

Displaying 1 - 3 of 3

API Name:

dt_relations_child_incidents

Columns:

Column Name	API Access Name	Type	Tooltip
Incident ID	relations_incident_id	textarea	-
Incident Name	relations_incident_name	text	-
Incident Status	relations_incident_status	select	-

Custom Fields

Label	API Access Name	Type	Prefix	Placeholder	Tooltip
Relation Level	relations_level	select	properties	-	Is this incident considered a Parent or Child incident?
Parent ID	relations_parent_id	textarea	properties	-	Incident Number of the Parent Incident

Custom Artifact Types

Display Name	API Access Name	Description
Related Parent Incident	related_parent_incident	Incident ID of the parent of all related incidents to create a relation within Resilient incidents manually.

Rules

Rule Name	Object	Workflow Triggered
Example: Relations - Assign Parent Incident	incident	example_relations_assign_parent
Example: Relations - Close Child Incidents	incident	example_relations_auto_close_child_incidents
Example: Relations - Remove Child Relation	incident	example_relations_remove_child_relation
Example: Relations - Send Task to Children	task	example_relations_send_task_to_children
Example: Relations - Sync Artifact	artifact	example_relations_sync_artifact_to_parentchild
Example: Relations - Sync DataTable Data	incident	example_relations_sync_datatable_data_to_parentchild
Example: Relations - Sync Notes with Child	note	example_relations_sync_notes_to_parentchild
Example: Relations - Sync Notes with Parent	note	example_relations_sync_notes_to_parentchild
Example: Relations - Sync Task Note to Child	note	example_relations_sync_task_notes_to_parentchild
Example: Relations - Sync Task Notes to Parent	note	example_relations_sync_task_notes_to_parentchild
Example: Relations - Update Child Incident Parent Data Table	incident	example_relations_update_child_table_data

Troubleshooting & Support

Refer to the documentation listed in the Requirements section for troubleshooting information.

For Support

This is a IBM Community provided App. Please search the Community ibm.biz/soarcommunity for assistance.