fn-misp for IBM Resilient

Table of Contents

Release Notes

Version 3.0.1

- App Host support
- Proxy support

Version 3.0.0

- There have been significant changes to the app for version 3, the community built a python3 compatible version of the app. This meant there was 2 different version in circulation.
- This version of the app is designed to reunify the fn-misp apps. To support both python2 and python3 automatically - using the latest recommended libraries from the MISP community.
- Finally, the Lookup Att&ck function has been removed, as MISP now stores Att&ck information as Tags - this is returned via the search attribute function, so no special function is required.
- The old separate apps are packaged inside the app directory, marked as ARCHIVE. They are unsupported and just for code documentation purposes.

Version 1.6.1

- Fixed Issue with verify certs
- Added support for tags in search attribute
- Workflow update to show use of parsing tags, e.g. TLP etc
- Packaged as zip for easy install (no unzip required)

Version 1.5.1

- Full documentation for Att&ck Support

Version 1.5.0

- Added MITRE Att&ck support

Version 1.0.0

- Initial Release

Overview

Creates Events, Attributes and Sightings in MISP from incidents and artifacts in Resilient.

The purpose of this package is to allow the creation of an event in MISP from an incident in Resilient. This could represent a multiple-to-one or a one-to-one relationship. Once the event is created, attributes can be populated to it. For artifacts which have a hit in MISP, one can create a sighting back to MISP to show threat intelligence teams the indicator has been seen in the wild. Additional search functions allow one to search all attributes and return sightings from an event. This package does not replace or supersede the MISP Custom Threat Service, the aim is to supplement it and create a bi-directional connection and integration. The package is built in a flexible way so it can be used with any real rule or workflow configuration. Sample rules and workflows are provided. Custom attribute types can be mapped from the workflow pre-processing script of the function. See the sample workflows for sample payloads returned.

Key Features

- Create Events in MISP from Resilient Incidents
- Add or list MISP sightings from Resilient
- Create tags and attributes from Resilient Aritfacts

Installation

Requirements

- Resilient platform >= `v35.2.32`
- App Host >= `v1.2.132` (if using App Host)
  - To setup up an App Host see: ibm.biz/res-app-host-setup
- An Integration Server running `resilient_circuits>=32.0` (if using an Integration Server)
  - To set up an Integration Server see: ibm.biz/res-int-server-guide
  - If using an API key account, minimum required permissions are:

Name	Permissions
Org Data	Read, Edit
Function	Read

- Proxy supported: Yes

Install

- To install or uninstall an App using the App Host see ibm.biz/res-install-app
- To install or uninstall an Integration using the Integration Server see the ibm.biz/res-install-int

---

App Configuration

The following table describes the settings you need to configure in the app.config file. If using App Host, see the Resilient System Administrator Guide. If using the integration server, see the Integration Server Guide.

Config	Required	Example	Description
misp_url	Yes	`10.10.10.10:5000`	*IP or URL of the MISP instance along with the http port*
misp_key	Yes	`someAPIkey`	*API key to access the MISP API*
verify_cert	Yes	`True`	*Secure connection*
https_proxy	No	https://your.proxy.com	*https proxy for connecting to MISP*
http_proxy	No	http://your.proxy.com	*http proxy for connecting to MISP*

Function - MISP Create Event

Create a MISP event from an incident

▶ Inputs:

Name	Type	Required	Example	Tooltip
`misp_analysis_level`	`number`	No	–	initial =0, ongoing=1, complete=2
`misp_distribution`	`number`	No	–	Organization only=0
`misp_event_name`	`text`	Yes	–	-
`misp_threat_level`	`number`	No	–	high=1, medium=2, low=3

▶ Outputs:

```
results = {
    "success": True,
    "content":
        {
          "Event": {
            "id": "66",
            "orgc_id": "1",
            "org_id": "1",
            "date": "2020-09-25",
            "threat_level_id": "1",
            "info": "Example Event",
```

```
            "published": false,
            "uuid": "17538fd2-54da-4280-bd98-25ba6723ea92",
            "attribute_count": "0",
            "analysis": "1",
            "timestamp": "1601060754",
            "distribution": "1",
            "proposal_email_lock": false,
            "locked": false,
            "publish_timestamp": "0",
            "sharing_group_id": "0",
            "disable_correlation": false,
            "extends_uuid": "",
            "event_creator_email": "admin@admin.test",
            "Org": {
              "id": "1",
              "name": "ORGNAME",
              "uuid": "00e8cf4b-ba62-4edb-a990-90049cd53df2",
              "local": true
            },
            "Orgc": {
              "id": "1",
              "name": "ORGNAME",
              "uuid": "00e8cf4b-ba62-4edb-a990-90049cd53df2",
              "local": true
            },
            "Attribute": [],
            "ShadowAttribute": [],
            "RelatedEvent": [],
            "Galaxy": [],
            "Object": []
          }
        }
}
```


▶ Workflows

▶ Example Pre-Process Script:

```
#inputs.misp_analysis_level = 0
#inputs.misp_distribution = 0
#inputs.misp_threat_level = 2
inputs.misp_event_name = incident.name
```

▶ Example Post-Process Script:


```
# {'success': True, 'content': {'Event': {'id': '4', 'orgc_id': '1',
'org_id': '1', 'date': '2019-03-23', 'threat_level_id': '1', 'info': 'misp
2', 'published': False, 'uuid': '5c96475a-3170-48e7-b0b5-0138ac110002',
'attribute_count': '0', 'analysis': '2', 'timestamp': '1553352538',
'distribution': '0', 'proposal_email_lock': False, 'locked': False,
```

```
'publish_timestamp': '0', 'sharing_group_id': '0', 'disable_correlation':
False, 'extends_uuid': '', 'event_creator_email': 'admin@admin.test',
'Org': {'id': '1', 'name': 'ORGNAME', 'uuid': '5c963124-caa0-4dee-a783-
00b6ac110002'}, 'Orgc': {'id': '1', 'name': 'ORGNAME', 'uuid': '5c963124-
caa0-4dee-a783-00b6ac110002'}, 'Attribute': [], 'ShadowAttribute': [],
'RelatedEvent': [], 'Galaxy': [], 'Object': []}}}
incident.properties.misp_event_id = results.content['Event']['id']
```

Function - MISP Sighting List

List all sightings associated with an event

▶ Inputs:

Name	Type	Required	Example	Tooltip
misp_event_id	number	No	-	-

▶ Outputs:

```
results = {
          "success": true,
          "content": [
            {
              "Sighting": {
                "id": "5",
                "attribute_id": "5",
                "event_id": "27",
                "org_id": "1",
                "date_sighting": "1601061492",
                "uuid": "1ec3931f-c718-4913-9f45-b5ec5eb97ed4",
                "source": "IBM Resilient SOAR",
                "type": "0"
              },
              "Organisation": {
                "name": "ORGNAME"
              }
            }
          ]
}
```

▶ Workflows

▶ Example Pre-Process Script:

```
inputs.misp_event_id = incident.properties.misp_event_id
```

▶ Example Post-Process Script:

```
content = results.content
incident.addNote(u"Sightings for associated event.\n{}".format(content))
```

Function - MISP Create Sighting

Create a MISP sighting from an incident artifact

▶ Inputs:

Name	Type	Required	Example	Tooltip
misp_sighting	text	No	–	-

▶ Outputs:

```
results = {
          "success": true,
          "content": {
            "Sighting": {
              "id": "5",
              "attribute_id": "5",
              "event_id": "27",
              "org_id": "1",
              "date_sighting": "1601061492",
              "uuid": "1ec3931f-c718-4913-9f45-b5ec5eb97ed4",
              "source": "IBM Resilient SOAR",
              "type": "0"
            }
          }
}
```

▶ Workflows

▶ Example Pre-Process Script:

```
inputs.misp_sighting = artifact.value
```

▶ Example Post-Process Script:

```
# Result: {'success': True, 'content': {'message': 'Sighting added'}}
existing_description = artifact.description.content+'\n' if
artifact.description else ""

#if results.content[0].get('errors'):
#  artifact.description = u"{}MISP Attribute failure:
```

```
{}".format(existing_description, results.content[0]['errors']['value'])
#else:
artifact.description = u"{}MISP Attribute created:
{}".format(existing_description, results.content['message'])
```

Function - MISP Search Attribute

Search MISP event attributes for a given match on an artifact

▶ Inputs:

Name	Type	Required	Example	Tooltip
misp_attribute_value	text	No	-	-

▶ Outputs:


```
results = {
            "success": true,
            "content": [
                {
                  "Event": {
                    "id": "66",
                    "orgc_id": "1",
                    "org_id": "1",
                    "date": "2020-09-25",
                    "threat_level_id": "1",
                    "info": "Example Event",
                    "published": false,
                    "uuid": "17538fd2-54da-4280-bd98-25ba6723ea92",
                    "attribute_count": "1",
                    "analysis": "1",
                    "timestamp": "1601062027",
                    "distribution": "1",
                    "proposal_email_lock": false,
                    "locked": false,
                    "publish_timestamp": "0",
                    "sharing_group_id": "0",
                    "disable_correlation": false,
                    "extends_uuid": "",
                    "event_creator_email": "admin@admin.test",
                    "Org": {
                      "id": "1",
                      "name": "ORGNAME",
                      "uuid": "00e8cf4b-ba62-4edb-a990-90049cd53df2",
                      "local": true
                    },
                    "Orgc": {
                      "id": "1",
                      "name": "ORGNAME",
                      "uuid": "00e8cf4b-ba62-4edb-a990-90049cd53df2",
```

```
                    "local": true
                  },
                  "Attribute": [
                    {
                      "id": "6",
                      "type": "text",
                      "category": "Other",
                      "to_ids": false,
                      "uuid": "b4e6230a-98a2-4935-9706-f5ebc6a1b628",
                      "event_id": "66",
                      "distribution": "5",
                      "timestamp": "1601062027",
                      "comment": "",
                      "sharing_group_id": "0",
                      "deleted": false,
                      "disable_correlation": false,
                      "object_id": "0",
                      "object_relation": null,
                      "first_seen": null,
                      "last_seen": null,
                      "value": "example attribute",
                      "Galaxy": [],
                      "ShadowAttribute": []
                    }
                  ],
                  "ShadowAttribute": [],
                  "RelatedEvent": [],
                  "Galaxy": [],
                  "Object": []
                }
              }
            ],
            "tags": []
}
```


▶ Workflows

▶ Example Pre-Process Script:

```
inputs.misp_attribute_value = artifact.value
```

▶ Example Post-Process Script:


```
# Result: {"response": {"Attribute":
[{"id":"3","event_id":"3","object_id":"0","object_relation":null,"category
":"Network activity","type":"ip-dst","to_ids":false,"uuid":"666a6890-fddd-
4a5d-a474-
22c85c6a1ce5","timestamp":"1553352781","distribution":"5","sharing_group_i
d":"0","comment":"","deleted":false,"disable_correlation":false,"value":"8
.8.8.8","Event":
```

```
{"org_id":"1","distribution":"0","id":"3","info":"misp","orgc_id":"1","uui
d":"5c96443b-1dcc-42fc-910a-01afac110002"}}]}}
existing_description = artifact.description.content+'\n' if
artifact.description else ""

if not results.success:
artifact.description = u"{}No matching attribute
found".format(existing_description)
else:
matched = []
for match in results.content:
    matched.append(u"Event: {}, ID: {}, Tags: {}".format(match['Event']
['info'], match['Event']['id'], results.tags))

artifact.description = u"{} Attribute Search Matches:\n
{}".format(existing_description, '\n'.join(matched))
```

Function - MISP Create Tag

Creates a Tag

▶ Inputs:

Name	Type	Required	Example	Tooltip
misp_attribute_value	text	No	-	-
misp_event_id	number	No	-	-
misp_tag_name	text	No	-	-
misp_tag_type	select	No	-	-

▶ Outputs:

```
results = {
    "success": True
}
```

▶ Workflows

▶ Example Pre-Process Script:

```
inputs.misp_attribute_value = artifact.value
inputs.misp_event_id = incident.properties.misp_event_id
inputs.misp_tag_name = "tlp:white"
```

▶ Example Post-Process Script:

None

Function - MISP Create Attribute

Create a MISP attribute from an incident artifact

▶ Inputs:

Name	Type	Required	Example	Tooltip
misp_attribute_type	text	No	–	-
misp_attribute_value	text	No	–	-
misp_event_id	number	No	–	-

▶ Outputs:


```
results = {
            "success": true,
              "content": {
                "Attribute": {
                  "id": "7",
                  "event_id": "6",
                  "object_id": "0",
                  "object_relation": null,
                  "category": "Network activity",
                  "type": "hostname",
                  "value1": "ibm.com",
                  "value2": "",
                  "to_ids": true,
                  "uuid": "943207c1-a8f1-40f1-9566-1eaa3c2fcfb9",
                  "timestamp": "1601062824",
                  "distribution": "5",
                  "sharing_group_id": "0",
                  "comment": "",
                  "deleted": false,
                  "disable_correlation": false,
                  "first_seen": null,
                  "last_seen": null,
                  "value": "ibm.com"
                },
                "AttributeTag": []
              }
}
```


▶ Workflows

▶ Example Pre-Process Script:

```
inputs.misp_attribute_value = artifact.value
inputs.misp_event_id = incident.properties.misp_event_id


resilient_to_misp_map = {
  "DNS Name": "domain",
  "Email Attachment": "email-attachment",
  "Email Body": "email-body",
  "Email Recipient": "email-dst",
  "Email Sender": "email-src",
  "Email subject": "email-subject",
  "File Name": "filename",
  "DNS Name": "hostname",
  "MAC Address": "mac-address",
  "Malware MD5 Hash": "md5",
  "Port": "port",
  "Malware SHA-1 Hash": "sha1",
  "Malware SHA-256 Hash": "sha256",
  "URI Path": "uri",
  "URL": "url",
  "Threat CVE ID": "vulnerability",
  "IP Address": "ip-dst"
}

try:
misp_type = resilient_to_misp_map[artifact.type]
inputs.misp_attribute_type = misp_type
except Exception, e:
helper.fail(u"You do not have this artifact type {} mapped to a type in
MISP - Ask your Admin".format(artifact.value))
raise e
```

▶ Example Post-Process Script:

```
# Result: {'success': True, 'content': [{'Attribute': {'id': '3',
'event_id': '3', 'object_id': '0', 'object_relation': None, 'category':
'Network activity', 'type': 'ip-dst', 'value1': '8.8.8.8', 'value2': '',
'to_ids': False, 'uuid': '666a6890-fddd-4a5d-a474-22c85c6a1ce5',
'timestamp': '1553352781', 'distribution': '5', 'sharing_group_id': '0',
'comment': '', 'deleted': False, 'disable_correlation': False, 'value':
'8.8.8.8'}}]}
# Result: {'success': True, 'content': [{'name': 'Could not add
Attribute', 'message': 'Could not add Attribute', 'url':
'/attributes/add', 'errors': {'value': ['A similar attribute already
exists for this event.']}}]}
existing_description = artifact.description.content+'\n' if
artifact.description else ""

if results.content[0].get('errors'):
```

```
artifact.description = u"{}MISP Attribute failure:
{}".format(existing_description, results.content[0]['errors']['value'])
else:
artifact.description = u"{}MISP Attribute created:
{}".format(existing_description, results.content[0]['Attribute']
['category'])
```

Custom Fields

Label	API Access Name	Type	Prefix	Placeholder	Tooltip
MISP Event Id	misp_event_id	text	properties	-	-

Rules

Rule Name	Object	Workflow Triggered
Example: Create MISP Event	incident	example_misp_create_event
Example: MISP Sighting List	incident	example_misp_sighting_list
Example: Create MISP Sighting	artifact	example_misp_create_sighting
Example: Create MISP Attribute	artifact	example_misp_create_attribute
Example: MISP Search Attribute	artifact	example_misp_search_attribute

Troubleshooting & Support

If using the app with an App Host, see the Resilient System Administrator Guide and the App Host Deployment Guide for troubleshooting procedures. You can find these guides on the IBM Knowledge Center, where you can select which version of the Resilient platform you are using.

If using the app with an integration server, see the Integration Server Guide

For Support

This is a IBM Community Provided App. Please search the Community https://ibm.biz/resilientcommunity for assistance.