McAfee Threat Intelligence Exchange (TIE) Functions for IBM Resilient

Table of Contents

Release Notes

v1.0.2

- Support added for App Host.

v1.0.1

- Support added for App Host.

v1.0.0

- Initial Release

Overview

Resilient Circuits Components for McAfee TIE Functions

The McAfee TIE Functions for IBM Resilient provides the ability to search McAfee Threat Intelliegence Exchange (TIE) server for information on a specific file hash. This information can come from any of the providers:

- Enterprise
- GTI
- ATD
- MWG

In addition, a system list is returned by the function.

Installation

Requirements

- Resilient platform >= `v35.0.0`
  - To setup up an App Host see: ibm.biz/res-app-host-setup
- An Integration Server running `resilient_circuits>=30.0.0` (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
Function	Read

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
dxlclient_config	Yes	`/home/integration/.resilient/mcafee_tie/dxlclient.config`	*Path to the dxlclient.config file*

More information on the dxlclient.config file and provisioning the system can be found here:

https://opendxl.github.io/opendxl-client-python/pydoc/provisioningoverview.html

https://opendxl.github.io/opendxl-client-python/pydoc/basiccliprovisioning.html#basiccliprovisioning

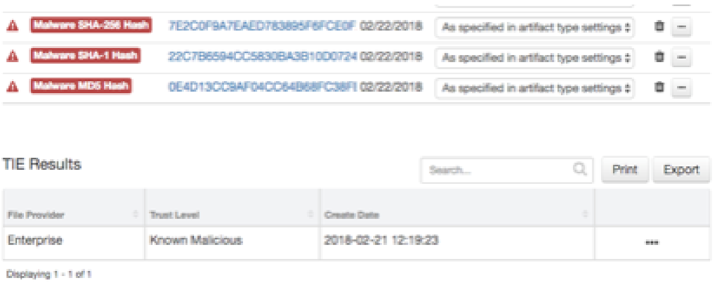
An example of the CLI provisioning command:

```
python -m dxlclient -vv provisionconfig /home/integration/.resilient/fn_mcafee_tie X.X.X.X
client1 -u admin -p password
```

where X.X.X.X is the IP address of the McAfee ePO server or OpenDXL Broker.

Custom Layouts

- Customize the Artifacts Tab page by dragging the TIE Results data table on to it as pictured below or create your own McAfee TIE incident tab and drag the TIE Results on to it:



Malware SHA-256 Hash	7E2C0F9A7EAED783895F6FCE0F	02/22/2018	As specified in artifact type settings	🗑	−
Malware SHA-1 Hash	22C7B6594CC5830BA3B10D0724	02/22/2018	As specified in artifact type settings	🗑	−
Malware MD5 Hash	0E4D13CC9AF04CC64B68FC38FI	02/22/2018	As specified in artifact type settings	🗑	−

TIE Results

File Provider	Trust Level	Create Date	
Enterprise	Known Malicious	2018-02-21 12:19:23	•••

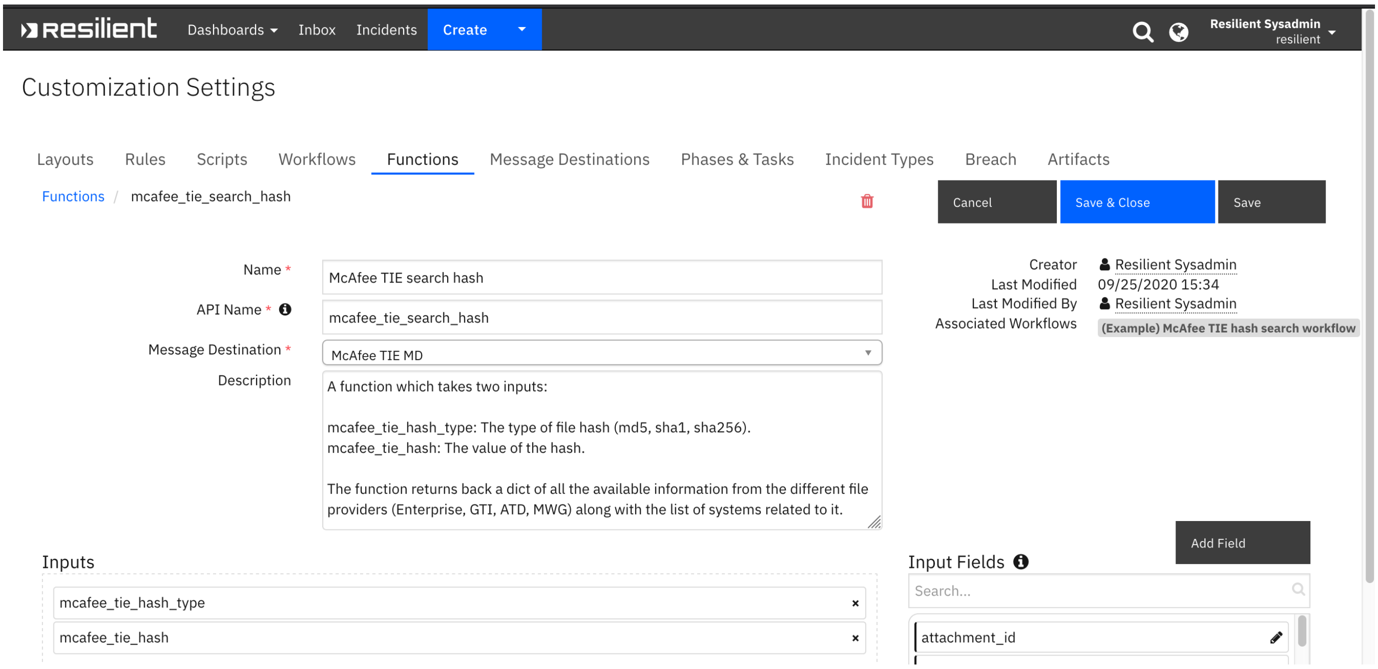
Displaying 1 - 1 of 1

Function - McAfee TIE search hash

A function which takes two inputs:

mcafee_tie_hash_type: The type of file hash (md5, sha1, sha256). mcafee_tie_hash: The value of the hash.

The function returns a JSON object containing the available information from the different file providers (Enterprise, GTI, ATD, MWG) along with the list of systems related to it.



Customization Settings

Functions / mcafee_tie_search_hash

Name * McAfee TIE search hash

API Name * mcafee_tie_search_hash

Message Destination * McAfee TIE MD

Description A function which takes two inputs:

mcafee_tie_hash_type: The type of file hash (md5, sha1, sha256).
mcafee_tie_hash: The value of the hash.

The function returns back a dict of all the available information from the different file providers (Enterprise, GTI, ATD, MWG) along with the list of systems related to it.

Creator Resilient Sysadmin
Last Modified 09/25/2020 15:34
Last Modified By Resilient Sysadmin
Associated Workflows (Example) McAfee TIE hash search workflow

Inputs

mcafee_tie_hash_type ×

mcafee_tie_hash ×

Input Fields

attachment_id

▶ Inputs:

Name	Type	Required	Example	Tooltip
`mcafee_tie_hash`	`text`	No	`-`	The value of the hash
`mcafee_tie_hash_type`	`text`	No	`-`	The type of file hash (md5, sha1, sha256)

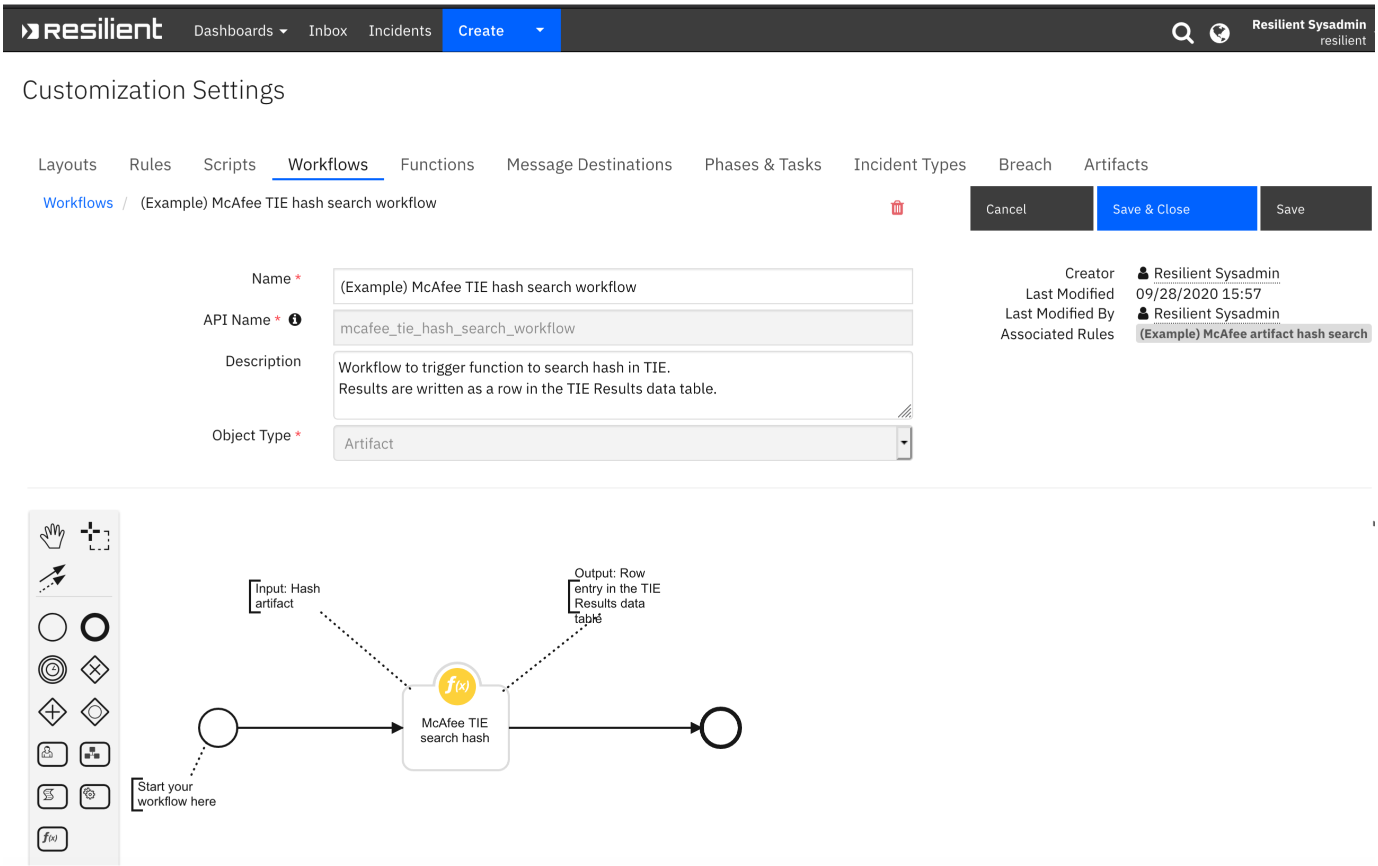
▶ Outputs:

```
results = {
 "GTI":{
    "File Provider":"GTI",
    "Attributes":{

    },
    "Create Date":"2018-02-21 12:17:10",
    "Trust Level":"Known Malicious"
 },
 "ATD":{
    "File Provider":"ATD",
    "Create Date":"2018-03-14 11:53:09",
    "Trust Level":"Most Likely Malicious"
 },
 "MWG":{
    "File Provider":"MWG",
    "Create Date":"2018-03-14 11:53:55",
    "Trust Level":"Most Likely Malicious"
 },
 "Enterprise":{
    "File Provider":"Enterprise",
    "Attributes":{
       "Average Local Rep":"Most Likely Malicious",
       "First Contact":"2018-02-21 12:17:10",
       "Min Local Rep":"Most Likely Malicious",
       "Is Prevalent":"0",
       "File Name Count":"1",
       "Max Local Rep":"Most Likely Malicious"
```

```
      },
      "Create Date":"2018-02-21 12:17:10",
      "Trust Level":"Most Likely Malicious"
   }
   "system_list":[{
     "date": 1519233563,
     "agentGuid": {a00728ff-3187-46c1-97d2-8e0f26ea940b}
   }]
  }
```

▶ Workflows:



Customization Settings

Workflows / (Example) McAfee TIE hash search workflow

Name * (Example) McAfee TIE hash search workflow

API Name * mcafee_tie_hash_search_workflow

Description Workflow to trigger function to search hash in TIE.
Results are written as a row in the TIE Results data table.

Object Type * Artifact

Creator Resilient Sysadmin
Last Modified 09/28/2020 15:57
Last Modified By Resilient Sysadmin
Associated Rules (Example) McAfee artifact hash search

▶ Example Pre-Process Script:

```
if artifact.type == "Malware MD5 Hash":
inputs.mcafee_tie_hash_type = "md5"
inputs.mcafee_tie_hash = artifact.value
elif artifact.type == "Malware SHA-1 Hash":
inputs.mcafee_tie_hash_type = "sha1"
inputs.mcafee_tie_hash = artifact.value
elif artifact.type == "Malware SHA-256 Hash":
inputs.mcafee_tie_hash_type = "sha256"
inputs.mcafee_tie_hash = artifact.value
else:
helper.fail("Artifact hash was not set correctly")
```

▶ Example Post-Process Script:

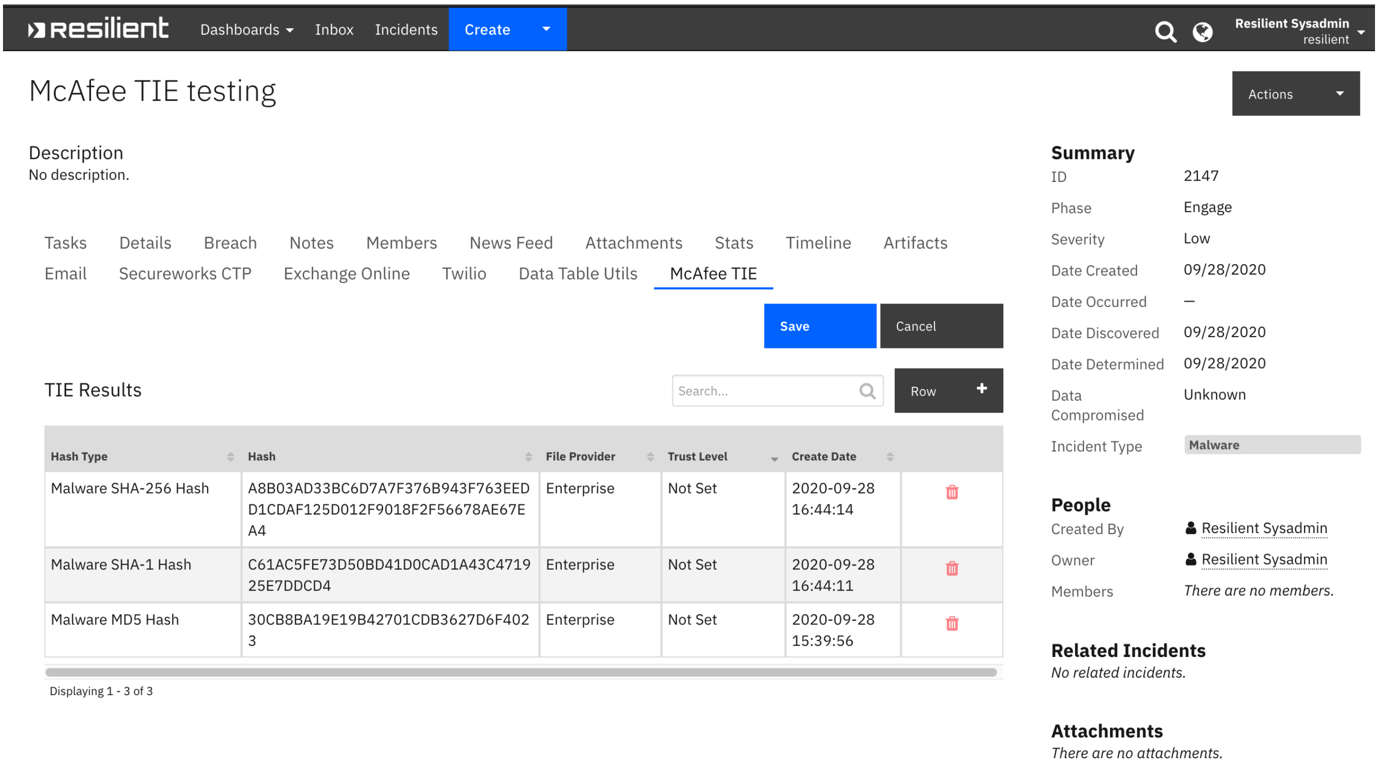
```
"""
Data returned will be in the following structure
```

```
{
 "GTI":{
    "File Provider":"GTI",
    "Attributes":{

    },
    "Create Date":"2018-02-21 12:17:10",
    "Trust Level":"Known Malicious"
 },
 "ATD":{
    "File Provider":"ATD",
    "Create Date":"2018-03-14 11:53:09",
    "Trust Level":"Most Likely Malicious"
 },
 "MWG":{
    "File Provider":"MWG",
    "Create Date":"2018-03-14 11:53:55",
    "Trust Level":"Most Likely Malicious"
 },
 "Enterprise":{
    "File Provider":"Enterprise",
    "Attributes":{
       "Average Local Rep":"Most Likely Malicious",
       "First Contact":"2018-02-21 12:17:10",
       "Min Local Rep":"Most Likely Malicious",
       "Is Prevalent":"0",
       "File Name Count":"1",
       "Max Local Rep":"Most Likely Malicious"
    },
    "Create Date":"2018-02-21 12:17:10",
    "Trust Level":"Most Likely Malicious"
 }
 "system_list":[{
   "date": 1519233563,
   "agentGuid": {a00728ff-3187-46c1-97d2-8e0f26ea940b}
 }]
}
"""

row = incident.addRow("tie_results")
row["hash_type"] = artifact.type
row["hash"] = artifact.value
row["file_provider"] = results["Enterprise"]["File Provider"]
row["trust_level"] = results["Enterprise"]["Trust Level"]
row["tie_create_date"] = results["Enterprise"]["Create Date"]
```

Data Table - TIE Results



McAfee TIE testing

Description

No description.

TIE Results

Hash Type	Hash	File Provider	Trust Level	Create Date
Malware SHA-256 Hash	A8B03AD33BC6D7A7F376B943F763EED D1CDAF125D012F9018F2F56678AE67E A4	Enterprise	Not Set	2020-09-28 16:44:14
Malware SHA-1 Hash	C61AC5FE73D50BD41D0CAD1A43C4719 25E7DDCD4	Enterprise	Not Set	2020-09-28 16:44:11
Malware MD5 Hash	30CB8BA19E19B42701CDB3627D6F402 3	Enterprise	Not Set	2020-09-28 15:39:56

Displaying 1 - 3 of 3

Summary

ID	2147
Phase	Engage
Severity	Low
Date Created	09/28/2020
Date Occurred	—
Date Discovered	09/28/2020
Date Determined	09/28/2020
Data Compromised	Unknown
Incident Type	Malware

People

Created By	Resilient Sysadmin
Owner	Resilient Sysadmin
Members	*There are no members.*

Related Incidents

No related incidents.

Attachments

There are no attachments.

API Name:

tie_results

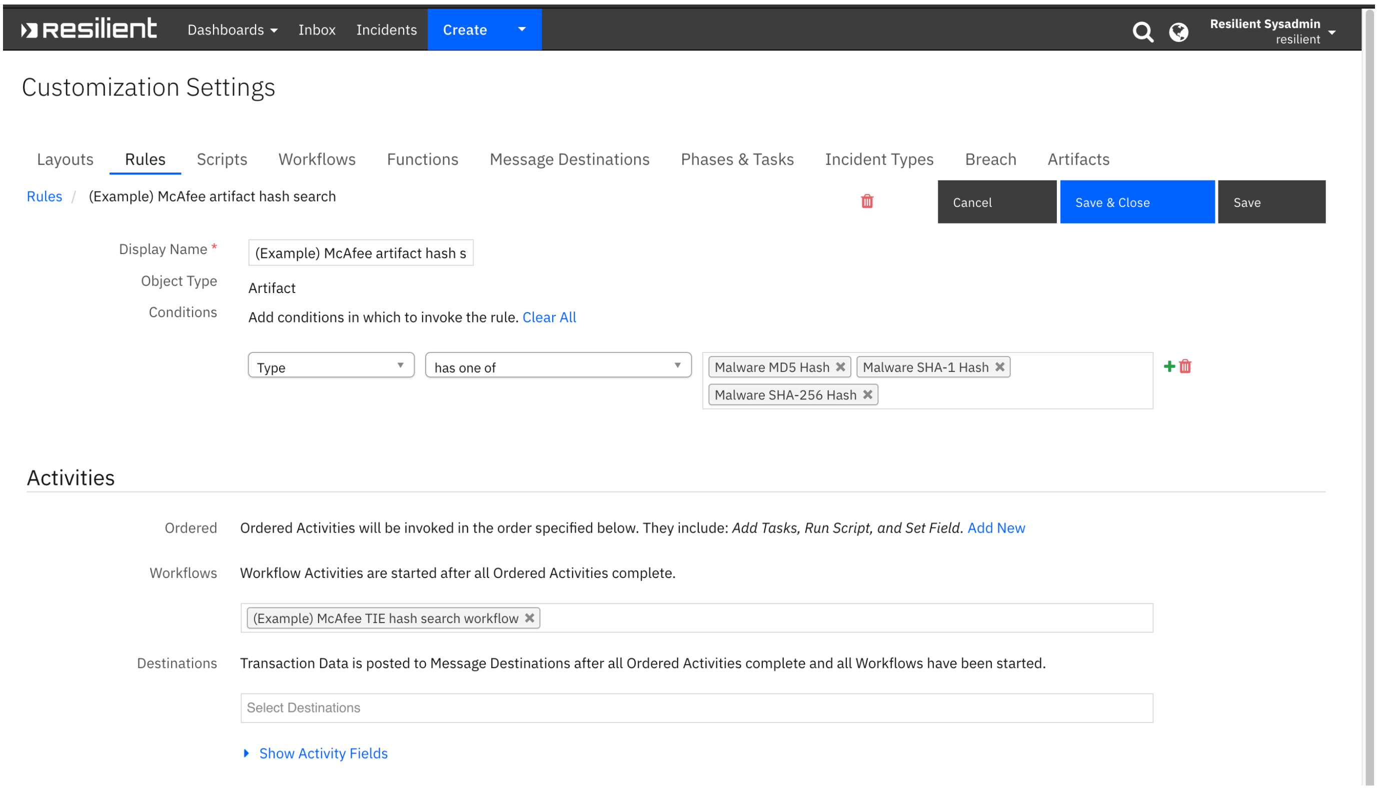
Columns:

Column Name	API Access Name	Type	Tooltip
File Provider	`file_provider`	`text`	-
Hash	`hash`	`text`	-
Hash Type	`hash_type`	`text`	-
Create Date	`tie_create_date`	`text`	-
Trust Level	`trust_level`	`text`	-

Rules

Rule Name	Object	Workflow Triggered
(Example) McAfee artifact hash search	artifact	`mcafee_tie_hash_search_workflow`

▶ Rules:



Customization Settings

Display Name * (Example) McAfee artifact hash s

Object Type Artifact

Conditions Add conditions in which to invoke the rule. Clear All

Type | has one of | Malware MD5 Hash ✖ Malware SHA-1 Hash ✖ Malware SHA-256 Hash ✖

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) McAfee TIE hash search workflow ✖

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

Select Destinations

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 an IBM Supported app. Please search https://ibm.com/mysupport for assistance.