None

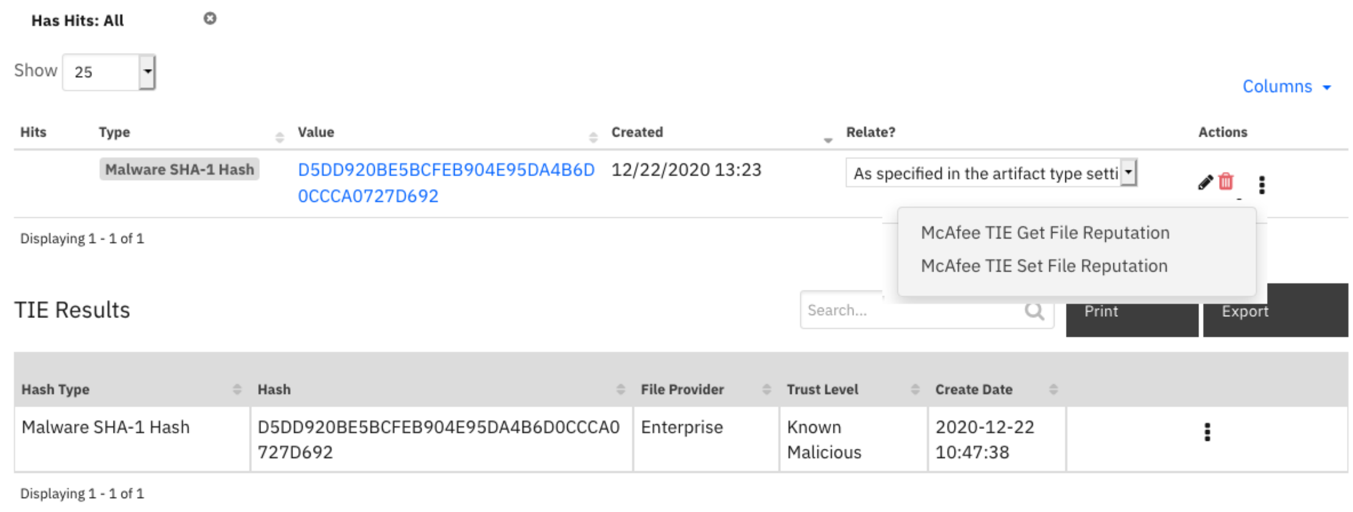
Table of Contents

Release Notes

Version	Date	Notes
1.1.0	12/2020	Added Feature: Set Reputation
1.0.2	09/2020	Bug fixes
1.0.1	05/2020	App Host support
1.0.0	05/2018	Initial Release

Overview

Resilient Circuits Components for McAfee TIE Functions



Has Hits: All
Show 25
Columns
McAfee TIE Get File Reputation
McAfee TIE Set File Reputation
Search...
Print
Export

Hits	Type	Value	Created	Relate?	Actions
	Malware SHA-1 Hash	D5DD920BE5BCFEB904E95DA4B6D0CCCA0727D692	12/22/2020 13:23	As specified in the artifact type setti	

Displaying 1 - 1 of 1

TIE Results

Hash Type	Hash	File Provider	Trust Level	Create Date	
Malware SHA-1 Hash	D5DD920BE5BCFEB904E95DA4B6D0CCCA0727D692	Enterprise	Known Malicious	2020-12-22 10:47:38	

Displaying 1 - 1 of 1

The McAfee TIE Functions for IBM Resilient provides the ability to search and set file reputation within McAfee Threat Intelligence 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.

Key Features

- Search for hashes in McAfee TIE
- Set file reputation trust levels on file hashes

Requirements

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

Resilient platform

The Resilient platform supports two app deployment mechanisms, App Host and integration server.

If deploying to a Resilient platform with an App Host, the requirements are:

- Resilient platform >= `36.0.5634`.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

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

- Resilient platform >= `36.0.5634`.
- 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>=30.0.0`.
- If using an API key account, make sure the account provides the following minimum permissions:

Name	Permissions
Org Data	Read
Function	Read

The following Resilient platform guides provide additional information:

- *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 Knowledge Center at ibm.biz/resilient-docs. On this web page, select your Resilient platform version. On the follow-on page, you can find the *App Host Deployment Guide* or *Integration Server Guide* by expanding **Resilient 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 >= 1.4.
- Cloud Pak is configured with an App Host.
- The app is in a container-based format (available from the AppExchange as a `zip` file).

The following Cloud Pak guides provide additional information:

- *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 Knowledge Center table of contents, select Case Management and Orchestration & Automation > **System administrator**.

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

Proxy Server

The app supports a proxy server. See the DXL Configuration file for settings.

Installation

Install

- To install or uninstall an App or Integration on the *Resilient platform*, see the documentation at ibm.biz/resilient-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.

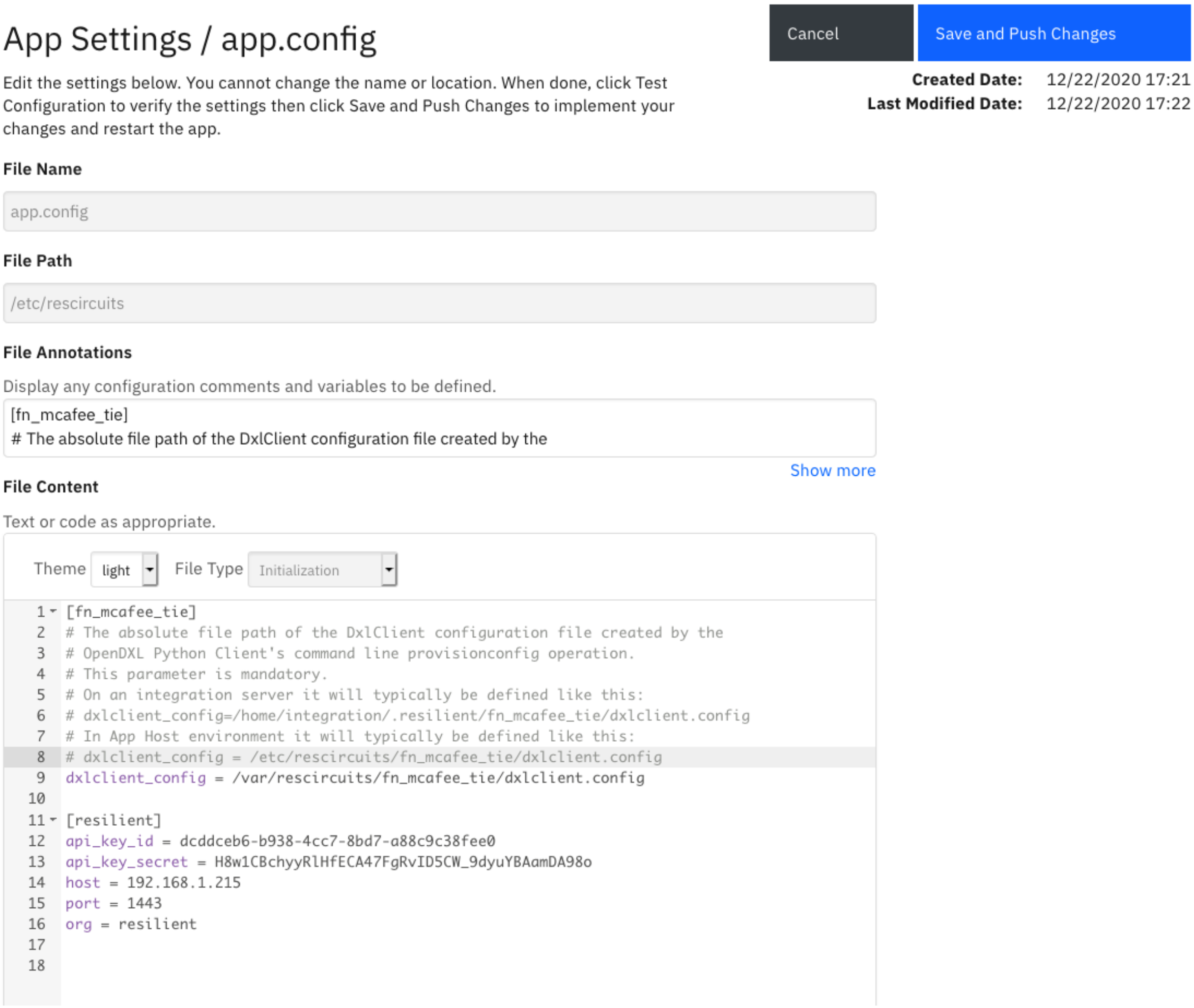
App Configuration

The following table provides the settings you need to configure the app. These settings are made in the app.config file. See the documentation discussed in the Requirements section for the procedure.

Config	Required	Example	Description
dxlclient_config	Yes	`/var/rescircuits/fn_macafee_tie/dxlclient.config`	*DXLClient configuration file. See the OpenDXL documentation for instructions on how to set.*

App Host Configuration

Since McAfee TIE references it's own configuration file, this file needs to be added to the files available to the container running this app for App Host. This is done by referring to the location of config file as `/var/rescircuits/fn_macafee_tie/dxlclient.config` within the container and then including that file in the files available to the app. See the snapshot below for an example.



Edit the settings below. You cannot change the name or location. When done, click Test Configuration to verify the settings then click Save and Push Changes to implement your changes and restart the app.

Created Date: 12/22/2020 17:21
Last Modified Date: 12/22/2020 17:22

File Name

app.config

File Path

/etc/rescircuits

File Annotations

Display any configuration comments and variables to be defined.

[fn_mcafee_tie]
The absolute file path of the DxlClient configuration file created by the

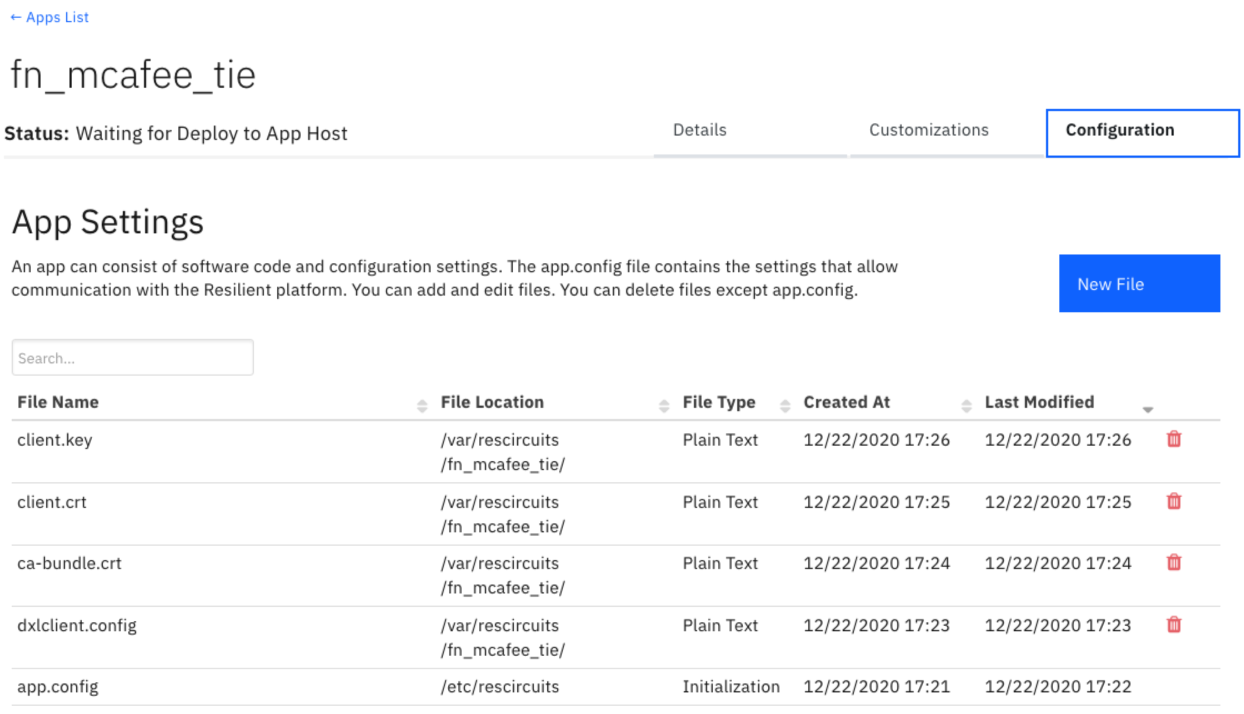
File Content

Text or code as appropriate.

```
[fn_mcafee_tie]
# The absolute file path of the DxlClient configuration file created by the
# OpenDXL Python Client's command line provisionconfig operation.
# This parameter is mandatory.
# On an integration server it will typically be defined like this:
# dxlclient_config=/home/integration/.resilient/fn_mcafee_tie/dxlclient.config
# In App Host environment it will typically be defined like this:
# dxlclient_config = /etc/rescircuits/fn_mcafee_tie/dxlclient.config
dxlclient_config = /var/rescircuits/fn_mcafee_tie/dxlclient.config

[resilient]
api_key_id = dcddceb6-b938-4cc7-8bd7-a88c9c38fee0
api_key_secret = H8w1CBchyyRlHfECA47FgRvID5CW_9dyuYBAamDA98o
host = 192.168.1.215
port = 1443
org = resilient
```

In addition to the dxlclient.config file, three certificate files need to be added to the app: ca-bundle.crt, client.crt, client.key. These files were built when you generated the dxlclient.config file and will be included in the same folder location. Be aware that all references to the folder (ex. `/var/rescircuits/fn_macafee_tie/`) must be specified the same way. That is, all references to the file path should contain the trailing slash or all references should leave it off.



← Apps List

fn_mcafee_tie

Status: Waiting for Deploy to App Host

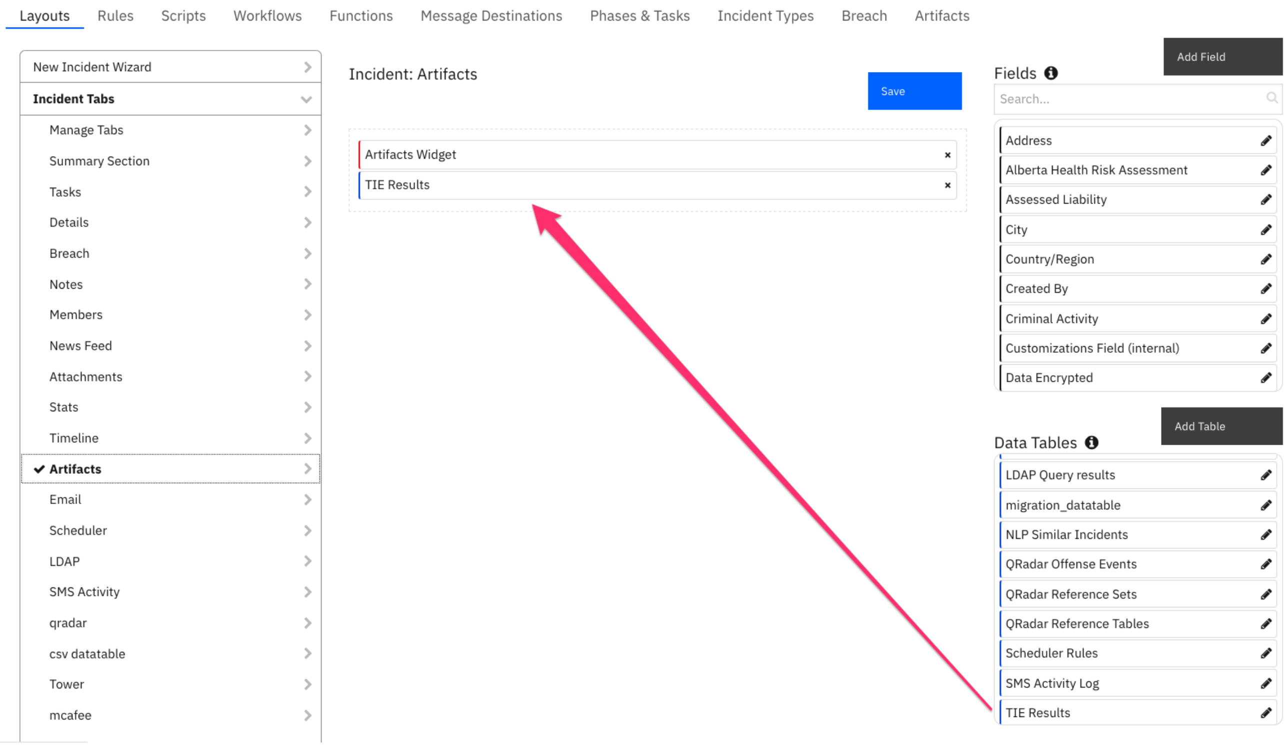
App Settings

An app can consist of software code and configuration settings. The app.config file contains the settings that allow communication with the Resilient platform. You can add and edit files. You can delete files except app.config.

File Name	File Location	File Type	Created At	Last Modified
client.key	/var/rescircuits /fn_mcafee_tie/	Plain Text	12/22/2020 17:26	12/22/2020 17:26
client.crt	/var/rescircuits /fn_mcafee_tie/	Plain Text	12/22/2020 17:25	12/22/2020 17:25
ca-bundle.crt	/var/rescircuits /fn_mcafee_tie/	Plain Text	12/22/2020 17:24	12/22/2020 17:24
dxlclient.config	/var/rescircuits /fn_mcafee_tie/	Plain Text	12/22/2020 17:23	12/22/2020 17:23
app.config	/etc/rescircuits	Initialization	12/22/2020 17:21	12/22/2020 17:22

Custom Layouts

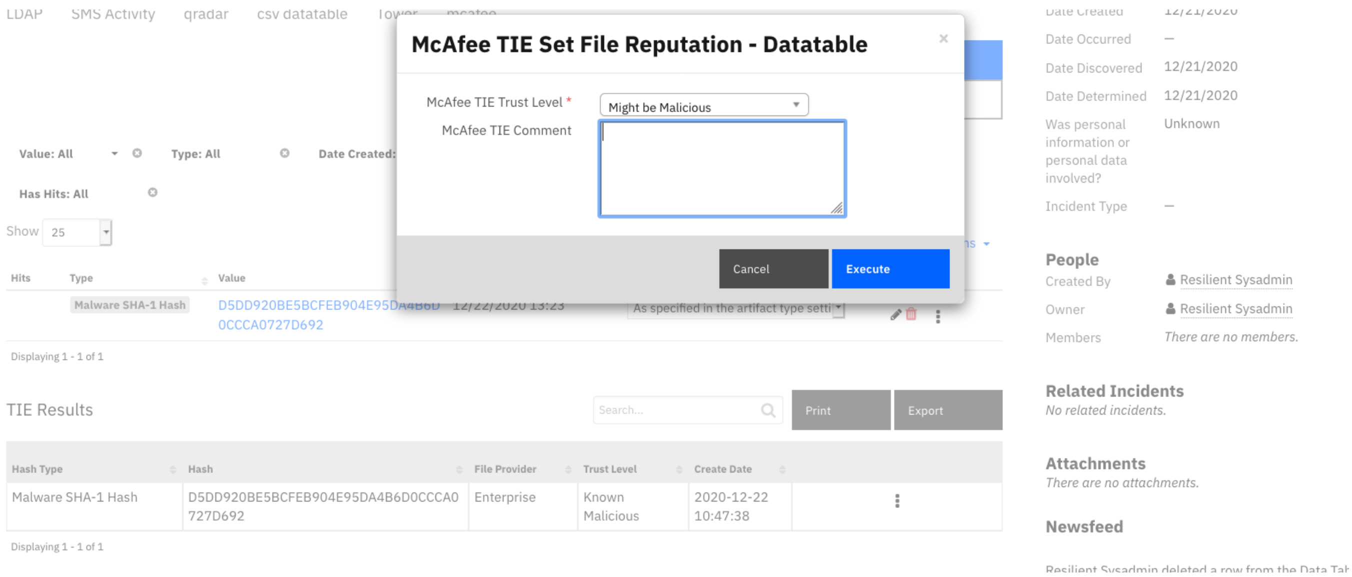
- Import the Data Table, TIE Results, like the screenshot below. Your setup may use a different tab:



Function - McAfee TIE: Set File Reputation

Set a file's reputation. This works on MD5, SH1 and SHA256 hashes.

Manual action rules are available from an artifact or from the TIE Results datatable.



McAfee TIE Set File Reputation - Datatable

McAfee TIE Trust Level * : Might be Malicious
McAfee TIE Comment:

Hits	Type	Value		
	Malware SHA-1 Hash	D5DD920BE5BCFEB904E95DA4B6D0CCCA0727D692	12/22/2020 13:23	As specified in the artifact type setti

Displaying 1 - 1 of 1

TIE Results

Hash Type	Hash	File Provider	Trust Level	Create Date	
Malware SHA-1 Hash	D5DD920BE5BCFEB904E95DA4B6D0CCCA0727D692	Enterprise	Known Malicious	2020-12-22 10:47:38	⋮

Displaying 1 - 1 of 1

Date Created	12/21/2020
Date Occurred	–
Date Discovered	12/21/2020
Date Determined	12/21/2020
Was personal information or personal data involved?	Unknown
Incident Type	–

People

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

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

Resilient Sysadmin deleted a row from the Data Tab

▶ Inputs:

Name	Type	Required	Example	Tooltip
`mcafee_tie_comment`	`text`	No	`-`	-
`mcafee_tie_filename`	`text`	No	`-`	Used for new reputation entries
`mcafee_tie_hash`	`text`	Yes	`D5DD920BE5BCFEB904E95DA4B6D0CCCA0727D692`	The value of the hash
`mcafee_tie_hash_type`	`text`	Yes	`md5`	The type of file hash (md5, sha1, sha256)
`mcafee_tie_trust_level`	`select`	Yes	`Most Likely Malicious`	-

▶ Outputs:

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    'hashes': {
      'sha1': 'd5dd920be5bcfeb904e95da4b6d0ccca0727d692'
    },
    'oldReputations': {
      3: {
        'createDate': 1608652058,
        'providerId': 3,
        'trustLevel': 50,
        'attributes': {
          '2101652': '1',
          '2123156': '0',
          '2098277': '0',
          '2102165': '1608652058',
          '2114965': '1',
          '2111893': '4',
          '2139285': '216172786408751223'
        }
      },
      1: {
        'createDate': 1608652105,
        'providerId': 1,
        'trustLevel': 1,
        'attributes': {
          '2120340': '2134902792'
        }
      }
    },
    'newReputations': {
      3: {
        'createDate': 1608652058,
        'providerId': 3,
        'trustLevel': 99,
        'attributes': {
          '2101652': '1',
          '2123156': '0',
          '2098277': '0',
          '2102165': '1608652058',
          '2114965': '1',
          '2111893': '4',
          '2139285': '216172786408751223'
        }
      },
      1: {
        'createDate': 1608652105,
        'providerId': 1,
        'trustLevel': 1,
        'attributes': {
          '2120340': '2134902792'
        }
      }
    },
    'updateTime': 1608669082
  },
  'raw': '{"hashes": {"sha1": "d5dd920be5bcfeb904e95da4b6d0ccca0727d692"}, "oldReputations": {"3":
{"createDate": 1608652058, "providerId": 3, "trustLevel": 50, "attributes": {"2101652": "1", "2123156":
"0", "2098277": "0", "2102165": "1608652058", "2114965": "1", "2111893": "4", "2139285":
"216172786408751223"}}, "1": {"createDate": 1608652105, "providerId": 1, "trustLevel": 1, "attributes":
{"2120340": "2134902792"}}}, "newReputations": {"3": {"createDate": 1608652058, "providerId": 3,
"trustLevel": 99, "attributes": {"2101652": "1", "2123156": "0", "2098277": "0", "2102165": "1608652058",
"2114965": "1", "2111893": "4", "2139285": "216172786408751223"}}, "1": {"createDate": 1608652105,
"providerId": 1, "trustLevel": 1, "attributes": {"2120340": "2134902792"}}}, "updateTime": 1608669082}',
  'inputs': {
    'mcafee_tie_hash_type': 'Malware SHA-1 Hash',
    'mcafee_tie_hash': 'D5DD920BE5BCFEB904E95DA4B6D0CCCA0727D692',
    'mcafee_tie_trust_level': {
      'id': 880,
      'name': 'Known Trusted'
    },
    'mcafee_tie_comment': None
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-mcafee-tie',
    'package_version': '1.1.0',
    'host': 'Marks-MacBook-Pro.local',
    'execution_time_ms': 5048,
    'timestamp': '2020-12-22 15:31:27'
  }
}
```

▶ Example Pre-Process Script:

```
inputs.mcafee_tie_trust_level = str(rule.properties.mcafee_tie_trust_level)
inputs.mcafee_tie_comment = rule.properties.mcafee_tie_comment.content
inputs.mcafee_tie_filename = rule.properties.mcafee_tie_filename
inputs.mcafee_tie_hash_type = artifact.type
inputs.mcafee_tie_hash = artifact.value
```

▶ Example Post-Process Script:

```
note = "McAfee TIE File Reputation: {}, Hash: {}".format(results.inputs['mcafee_tie_trust_level']
['name'], results.inputs['mcafee_tie_hash'])
if results.content:
    incident.addNote("Set reputation successfull\n{}".format(note))
else:
    incident.addNote("Set reputation unsuccessfull\n{}".format(note))
```

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 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.

screenshot: fn-mcafee-tie-search-hash

▶ Inputs:

Name	Type	Required	Example	Tooltip
`mcafee_tie_hash`	`text`	Yes	`DB1AEC5222075800EDA75D7205267569679B424E5C58A28102417F46D3B5790D`	The value of the hash
`mcafee_tie_hash_type`	`text`	Yes	`sha-256`	The type of file hash (md5, sha1, sha256)

▶ Outputs:

```
results = {
  'version': '1.0',
  'success': True,
  'reason': None,
  'content': {
    'mcafee_topic_name': '/mcafee/event/epo/threat/response',
    'mcafee_dxl_payload': '{"hashes": [{"type": "md5", "value": "Dk0TzJrwTMZLaPw4/goNrA=="}],
"providerId": 3, "trustLevel": 1}',
    'mcafee_publish_method': 'Service',
    'mcafee_wait_for_response': 'No'
  },
  'raw': '{"mcafee_topic_name": "/mcafee/event/epo/threat/response", "mcafee_dxl_payload": "
{\\"hashes\\": [{\\"type\\": \\"md5\\", \\"value\\": \\"Dk0TzJrwTMZLaPw4/goNrA==\\"}], \\"providerId\\":
3, \\"trustLevel\\": 1}", "mcafee_publish_method": "Service", "mcafee_wait_for_response": "No"}',
  'inputs': {
    'mcafee_publish_method': {
      'id': 205,
      'name': 'Service'
    },
    'mcafee_topic_name': '/mcafee/event/epo/threat/response',
    'mcafee_dxl_payload': '{"hashes": [{"type": "md5", "value": "Dk0TzJrwTMZLaPw4/goNrA=="}],
"providerId": 3, "trustLevel": 1}',
    'mcafee_wait_for_response': {
      'id': 203,
      'name': 'No'
    }
  },
  'metrics': {
    'version': '1.0',
    'package': 'fn-mcafee-opendxl',
    'package_version': '1.2.0',
    'host': 'Marks-MacBook-Pro.local',
    'execution_time_ms': 0,
    'timestamp': '2020-12-22 15:31:49'
  },
  'mcafee_topic_name': '/mcafee/event/epo/threat/response',
  'mcafee_dxl_payload': '{"hashes": [{"type": "md5", "value": "Dk0TzJrwTMZLaPw4/goNrA=="}], "providerId":
3, "trustLevel": 1}',
  'mcafee_publish_method': 'Service',
  'mcafee_wait_for_response': 'No'
}
```

▶ 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:

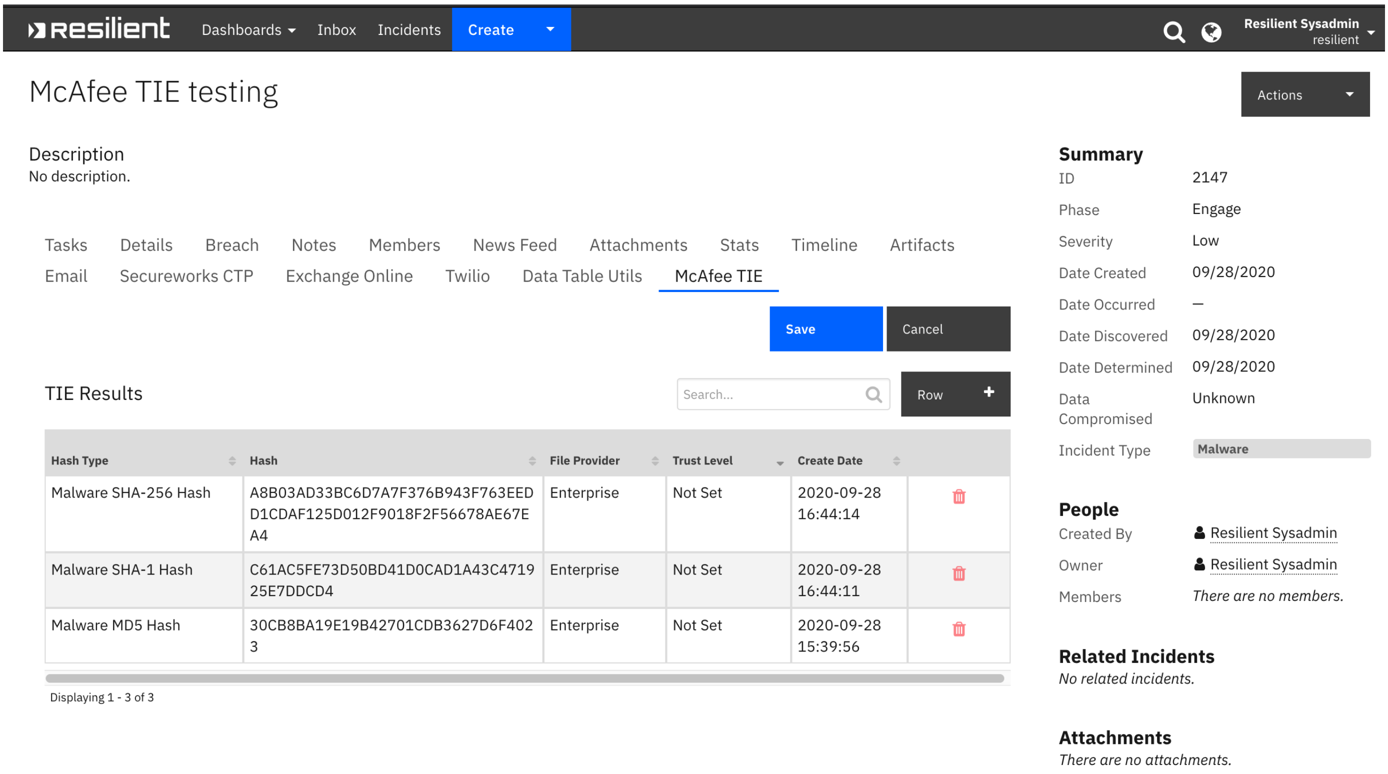
```
"""
Data returned will be in the following structure


{
   "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	A8B03AD33BC6D7A7F376B943F763EEDD1CDAF125D012F9018F2F56678AE67EA4	Enterprise	Not Set	2020-09-28 16:44:14
Malware SHA-1 Hash	C61AC5FE73D50BD41D0CAD1A43C471925E7DDCD4	Enterprise	Not Set	2020-09-28 16:44:11
Malware MD5 Hash	30CB8BA19E19B42701CDB3627D6F4023	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
McAfee TIE Set File Reputation	artifact	`mcafee_tie_set_file_reputation`
McAfee TIE Set File Reputation - Datatable	tie_results	`mcafee_tie_set_reputation__datatable`
McAfee TIE Get File Reputation	artifact	`mcafee_tie_get_file_reputation`

Troubleshooting & Support

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

For Support

This is an IBM supported app. Please search https://ibm.com/mysupport for assistance.