MCAFEE THREAT INTELLIGENCE EXCHANGE – RESILIENT THREAT SERVICE INTEGRATION GUIDE

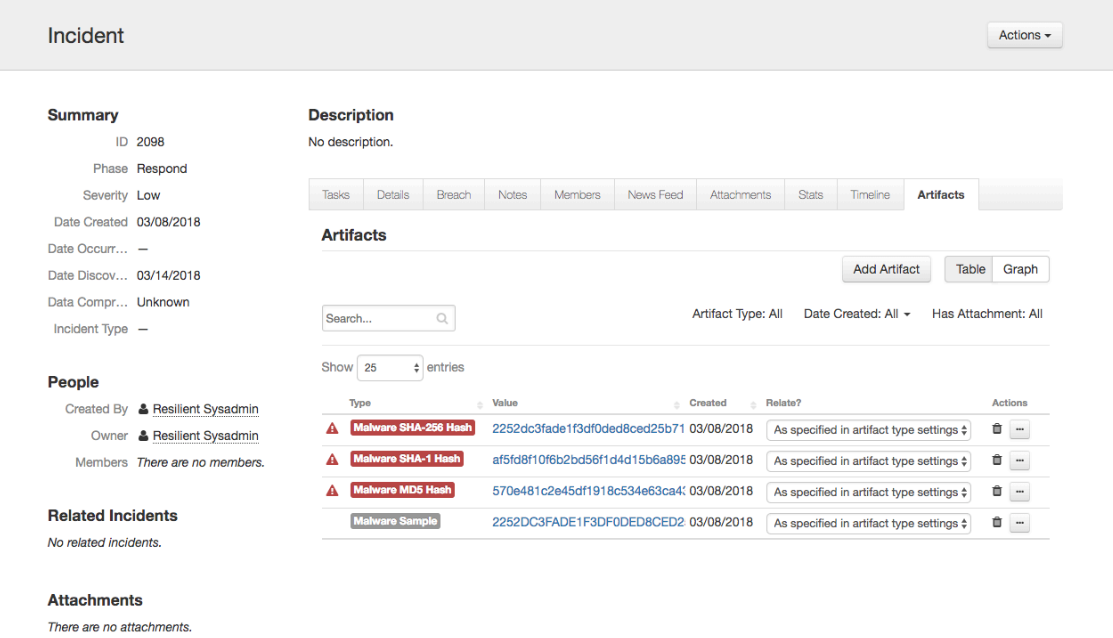
V1.0

Table of Contents

1. Introduction

As part of the incident response, artifacts (or evidence) may be added to an incident for tracking and analysis.

This integration provides automatic investigation of file reputation, using McAfee Threat Intelligence Exchange, for Resilient artifacts. When a malware sample is uploaded to the Resilient incident, its hashes (MD5, SHA1 and SHA256) are automatically sent to threat intelligence lookup. Also, when a file hash is directly entered into the Resilient platform, or added to the incident by an automated source such as a SIEM, these hashes are also automatically investigated.



Summary

ID	2098
Phase	Respond
Severity	Low
Date Created	03/08/2018
Date Occurr…	—
Date Discov…	03/14/2018
Data Compr…	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.

Description

No description.

Artifacts

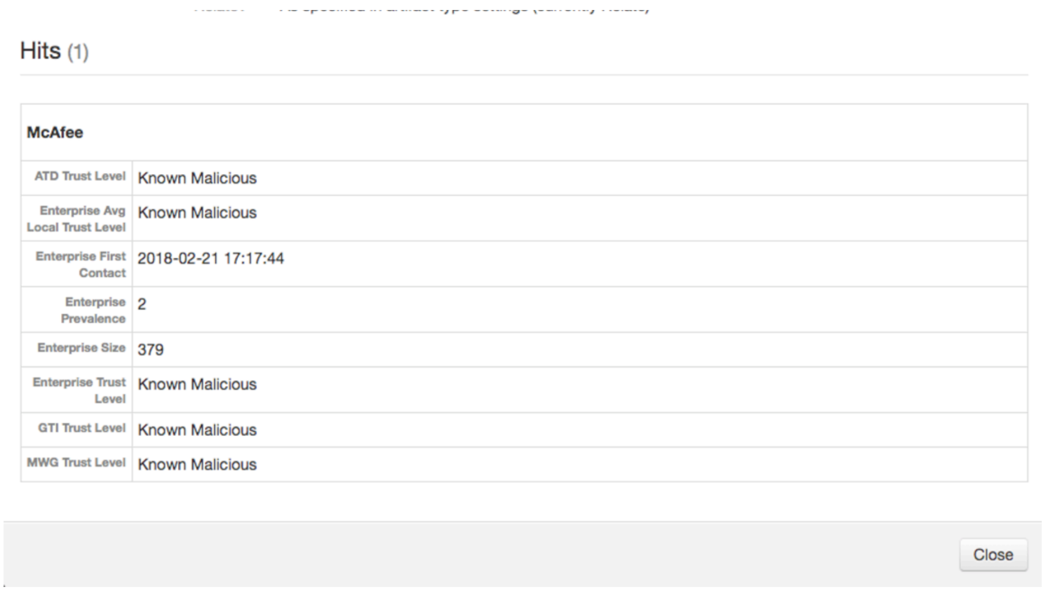
Artifact Type: All   Date Created: All   Has Attachment: All

Show 25 entries

	Type	Value	Created	Relate?	Actions
⚠	Malware SHA-256 Hash	2252dc3fade1f3df0ded8ced25b71	03/08/2018	As specified in artifact type settings	🗑 ···
⚠	Malware SHA-1 Hash	af5fd8f10f6b2bd56f1d4d15b6a895	03/08/2018	As specified in artifact type settings	🗑 ···
⚠	Malware MD5 Hash	570e481c2e45df1918c534e63ca4	03/08/2018	As specified in artifact type settings	🗑 ···
	Malware Sample	2252DC3FADE1F3DF0DED8CED2	03/08/2018	As specified in artifact type settings	🗑 ···

When a file reputation is most likely malicious, the McAfee Threat Intelligence Exchange threat service provides the following information:

- Enterprise Trust Level,
- Enterprise Average Local Trust Level,
- Enterprise Prevalence,
- Enterprise Size,
- Enterprise First Contact Date,
- GTI (Global Threat Intelligence) Trust Level,
- GTI Prevalence,
- GTI First Contact,
- ATD (McAfee Advanced Threat Defense) Trust Level,
- MWG (McAfee Web Gateway) Trust Level



Hits (1)

McAfee

ATD Trust Level	Known Malicious
Enterprise Avg Local Trust Level	Known Malicious
Enterprise First Contact	2018-02-21 17:17:44
Enterprise Prevalence	2
Enterprise Size	379
Enterprise Trust Level	Known Malicious
GTI Trust Level	Known Malicious
MWG Trust Level	Known Malicious

2. Installation

Before registering McAfee Threat Intelligence Exchange as a threat service with the Resilient platform, verify that your environment conforms to the following prerequisites:

- Resilient platform is version 28 or later.
- Resilient platform is connected to the internet.
- You have a Resilient account to use for the custom threat service. For Resilient platforms at version 28 or earlier, this must be the Master Administrator account. For Resilient platform version 29 or later, this can be any account that has the permission to create incidents and view and modify administrator and customization settings. You need to know the account username and password.
- You have access to the command line of the Resilient appliance, which hosts the Resilient platform.
- You have configured McAfee TIE, and network connectivity to enable the DXL (Data Exchange Layer) connection between the Resilient platform and your McAfee TiE server.

2.1. Install the Python components

The integration is a Web Service, called by the Resilient platform to query each artifact. It runs in the ‘resilient-circuits’ integration framework. Three components are required for this:

- rc-webserver, a web server component,
- rc-cts, a custom threat service lookup component,
- rc-cts-mcafeetie, the integration with McAfee Threat Intelligence Exchange.

Each of these components is included with the ZIP file that you downloaded. Additionally, the ZIP file contains current versions of the ‘resilient’ and ‘resilient-circuits’ components that make up the framework, and the OpenDXL Python Client.

Perform the following to install the integration on the Resilient appliance:

1. Copy the ZIP file to the appliance using SCP. The file should be copied to the home directory of the ‘resadmin’ user.
2. Log in to the Resilient appliance as ‘resadmin’ using an SSH client, such as PuTTY.
3. At the prompt, unzip the integration.

   ```
   unzip mcafeetie-1.0.0.zip
   ```

4. Change to the mcafeetie subdirectory and install the Python packages.

   ```
   cd mcafeetie-1.0.0

   sudo pip install -r requirements.txt --find-links .
   ```

2.2. Configure and Provision the OpenDXL Client

Before installing the integration, you must configure OpenDXL. This is the data exchange layer that allows communication with McAfee products including McAfee TIE.

Provisioning can be done using the OpenDXL Python Client’s command line interface (CLI), the OpenDXL Broker Management Console, or an external certificate authority.

Refer to the OpenDXL instructions for more details.

2.3. Configure and Run the Python components

The ‘resilient-circuits’ components run as an unprivileged user, typically named `integration`. If you do not already have an `integration` user configured on your appliance, create it now.

Perform the following to configure and run the integration:

1. Using ‘sudo’, become the integration user.

   ```
   sudo su - integration
   ```

2. Create or update the Resilient-circuits configuration file.

   ```
   resilient-circuits config -u
   ```

3. Edit the resilient-circuits configuration file.

   a. In the [resilient] section, ensure that you provide all the information needed to connect to the Resilient platform.

   b. In the [webserver] section, change the values to suit your preference if necessary.

   ```
   [webserver]
   # IP or DNS for the web server. Default is localhost.
   # server=0.0.0.0

   # Port for the web server. Default is 9000.
   # port=9000

   # Set the web server to use secure protocol. secure=1 means HTTPS, and secure=0 means HTTP. Default is 0
   # secure=1

   # The cert file is the private key certificate for the TLS server. This is required if secure=1. Default is None.
   # certfile=~/.resilient/ssl.cer
   ```

   c. In the [mcafee] section, be sure to specify the correct path to the OpenDXLclient configuration file.

   ```
   [mcafee]
   dxlclient_config=/home/resilient/.resilient/mcafee_tie/dxlclient.config
   ```

4. Run the integration with the following command:

   ```
   resilient-circuits run
   ```

The resilient-circuits command starts, loads its components, and continues to run until interrupted. If it stops immediately with an error message, check your configuration values and retry.

3. Register the Threat Service

Perform the following to register the integration as a Resilient threat service:

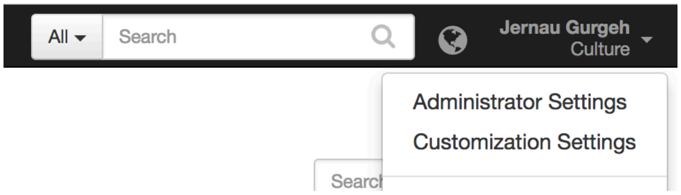
1. Log in to the Resilient appliance using an SSH client, such a PuTTY.
2. At the prompt, enter the following command.

```
sudo resutil threatserviceedit -name "McAfee Threat Intelligence Exchange" –
resturl 'http://localhost:9000/cts/mcafeetie'
```

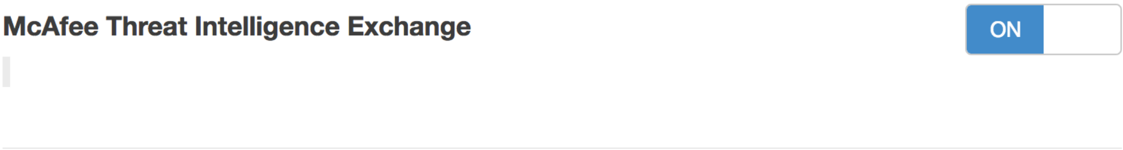
3. Once completed, test the connectivity using the following command. If the previous step was successful, you should see a success message.

```
sudo resutil threatservicetest -name " McAfee Threat Intelligence
Exchange"
```

4. Log into the Resilient platform using the Resilient account defined in Prerequisites then click on your username and select **Administrator Settings** in the drop-down menu.



5. Click the **Threat Sources** tab and scroll down until you find McAfee Threat Intelligence Exchange. Make sure that it is set to **ON**.



McAfee Threat Intelligence Exchange ON

NOTE: If you need to disable your product threat service, you can turn the threat service to OFF.

If you need to remove the threat service, log in to the Resilient appliance using an SSH client and type the following command:

```
sudo resutil threatservicedel -name "McAfee Threat Intelligence Exchange"
```

4. Customer Support and Feedback

See the McAfee Threat Intelligence Exchange (TIE) DXL Python Client Library Documentation for installation instructions, API documentation, and examples. For bugs, questions and discussions please use the GitHub Issues web site.

Support for the Resilient platform is available from support@resilientsystems.com*.*