QRadar MITRE Function

**V1.0.0**

**Release Date: 2/3/2022**

**Overview**

The QRadar MITRE function is meant to provide the MITRE information tied to the QRadar rule that was fired causing the Offense.

This document outlines the functionality of the function as it relates to Resilient running in Python 3. Python 2 not supported.

# Installation

# Integration

# 

# Required Permissions

# 

|  |  |
| --- | --- |
| **Name** | **Permissions** |
| **Org Data** | Read |
| **Function** | Read |

To install the function run the following commands to update the Resilient Environment:

* sudo pip install --upgrade pip
* sudo pip install --upgrade setuptools
* sudo pip install --upgrade resilient-circuits

Then run the following command to install the function:

* sudo pip install --upgrade fn\_qradar\_mitre\_1.0.0.tar.gz

To configure this newly installed function run the following commands per the instructions:

**New environment:**

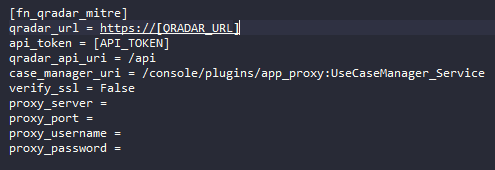
* resilient-circuits config –c

**Existing environment:**

* resilient-circuits config –u –l fn-qradar\_mitre

**Changes to the app.config file.**

* Add the QRadar URL including the HTTPS at the beginning.
* Create an API Token with admin privileges and add that token to your config file.
* If you are using a self-signed cert, Change verify\_ssl to False.
* Finally if you want to use this behind a proxy, enter your proxy information where applicable.



Finish by customizing Resilient for the function.

* resilient-circuits customize –y –l fn-qradar-mitre

Run resilient-circuits or restart the service.

* resilient-circuits run
* systemctl restart resilient\_circuits

# AppHost

To install the App: open Resilient, navigating to the Administration page, Apps tab and select Install:

* Open Resilient, navigating to the Administration page and Apps tab
* select Install, uploading the zip file for fn\_qradar\_mitre, and following the steps to install
* Configure the app.config file as stated above.
* Choose the AppHost server to deploy the app
* Select Deploy

# Release Notes

|  |  |  |
| --- | --- | --- |
| Version | Date | Notes |
| 1.0.0 | 09/2021 | Initial Release |

# Design Changes

# The design that is recommended to layout the new fields and data tables is following:

# New Tab: QRadar

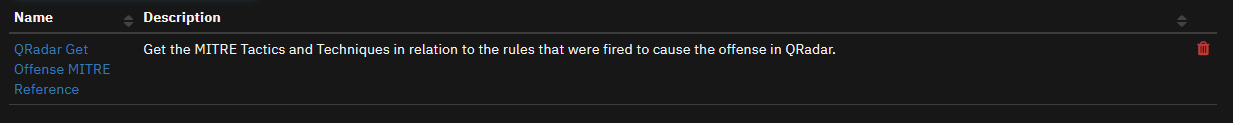
# - Add qradar\_id field

# - Add QRadar Rules and MITRE Tactics and Techniques data table

# 

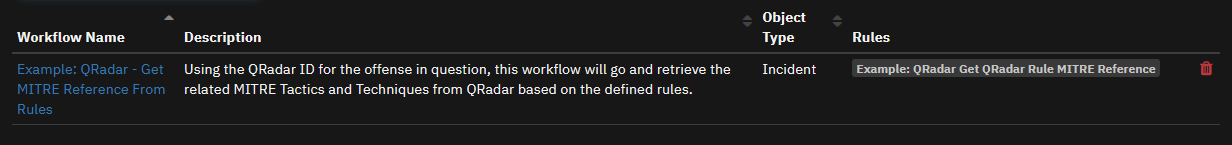
**Function Descriptions**

Once the function has been deployed, you can access use the functions within Resilient. The available functions are pictured below.



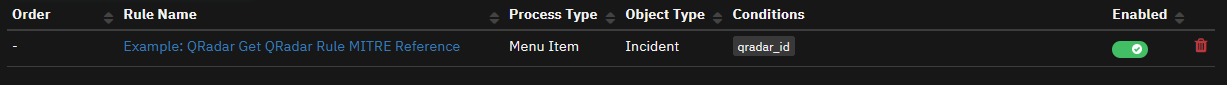
# Workflow Descriptions

The example workflows are meant to be used as a guide to understand how to properly use the function. The pre-process scripts are designed to be used out of the box and there is no need for post-process scripts as there will be no need to data manipulation after the function is complete.



**Rule Descriptions**

The rules are designed to be a guide as to how to setup your rules. They are setup as to only appear on simulation only to cut back on the clutter brought in on live incidents while testing and tweaking this function. If you want to make the example rules available, just remove the simulation requirement.



**Using the Function**

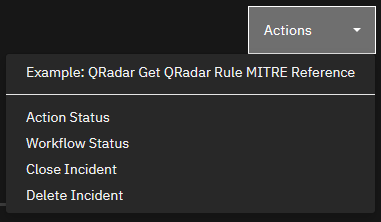
Pulling MITRE Information from QRadar Rule.

Requirements:

The incident must have a value in the qradar\_id field for this action to showup. That ID will be passed to the workflow to pull the correct information.

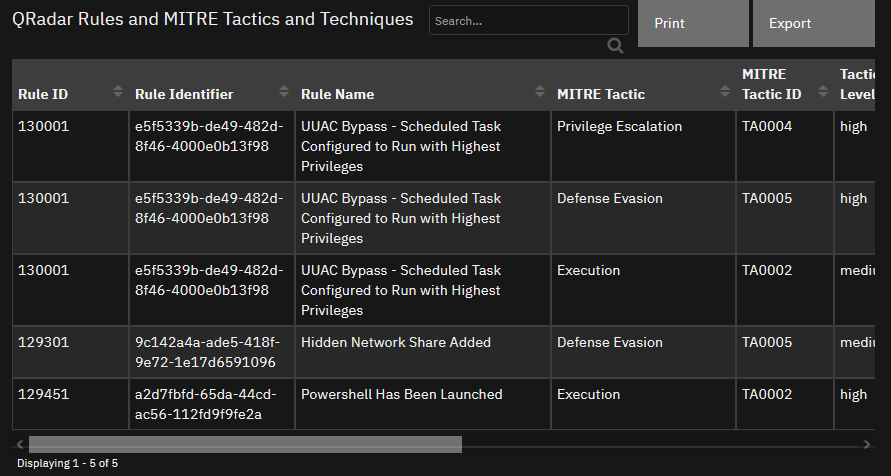
Instructions:

1. Click on the Actions and select the “Example: QRadar Get QRadar Rule MITRE Reference” Menu Item to pull the information from QRadar.



Results:

The “QRadar Rules and MITRE Tactics and Techniques” data table will be filled with each MITRE Tactic and the correlating Techniques that was associated with the rule that was fired causing the offense in QRadar.



**Troubleshooting**

Please feel free to reach out to me on the IBM Community or make a post in the community for any support.