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`

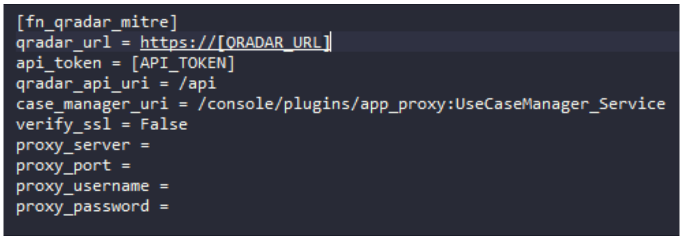
Existing environment:

- `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.



```
[fn_qradar_mitre]
qradar_url = https://[QRADAR_URL]
api_token = [API_TOKEN]
qradar_api_uri = /api
case_manager_uri = /console/plugins/app_proxy:UseCaseManager_Service
verify_ssl = False
proxy_server =
proxy_port =
proxy_username =
proxy_password =
```

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

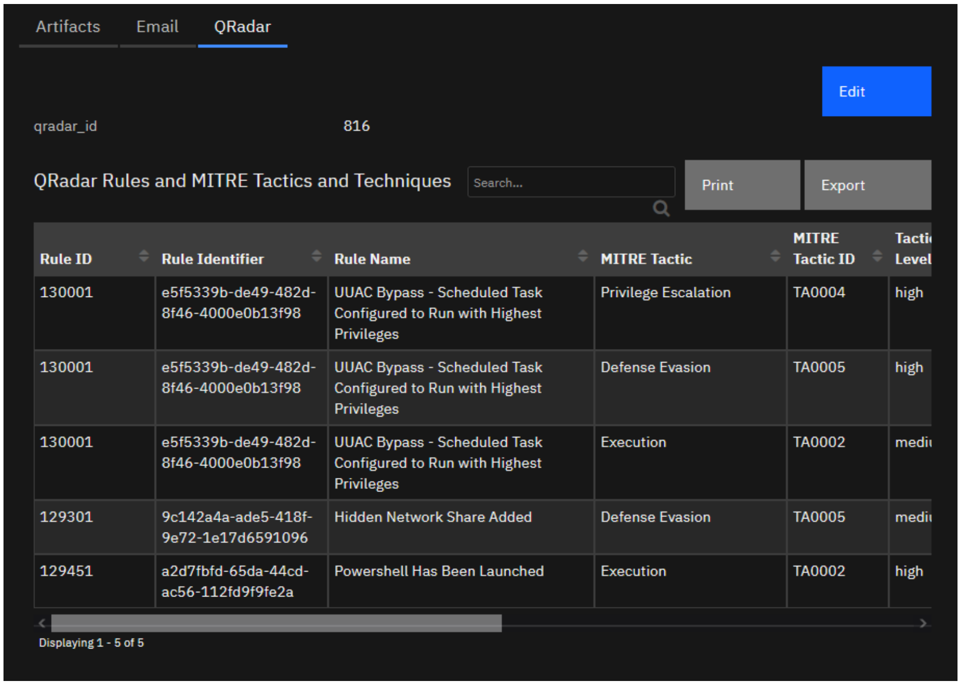
Version	Date	Notes
1.0.0	09/2021	Initial Release

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



qradar_id 816

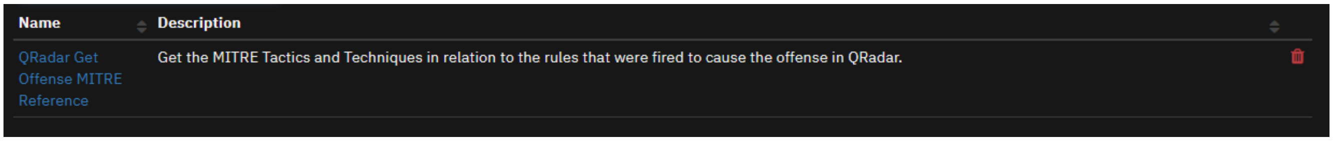
QRadar Rules and MITRE Tactics and Techniques

Rule ID	Rule Identifier	Rule Name	MITRE Tactic	MITRE Tactic ID	Tacti Level
130001	e5f5339b-de49-482d-8f46-4000e0b13f98	UUAC Bypass - Scheduled Task Configured to Run with Highest Privileges	Privilege Escalation	TA0004	high
130001	e5f5339b-de49-482d-8f46-4000e0b13f98	UUAC Bypass - Scheduled Task Configured to Run with Highest Privileges	Defense Evasion	TA0005	high
130001	e5f5339b-de49-482d-8f46-4000e0b13f98	UUAC Bypass - Scheduled Task Configured to Run with Highest Privileges	Execution	TA0002	medi
129301	9c142a4a-ade5-418f-9e72-1e17d6591096	Hidden Network Share Added	Defense Evasion	TA0005	medi
129451	a2d7fbfd-65da-44cd-ac56-112fd9f9fe2a	Powershell Has Been Launched	Execution	TA0002	high

Displaying 1 - 5 of 5

Function Descriptions

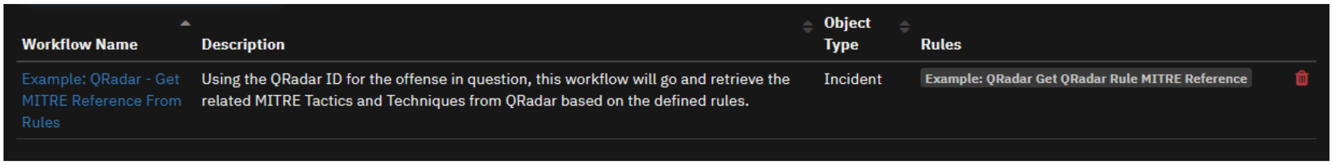
Once the function has been deployed, you can access use the functions within Resilient. The available functions are pictured below.



Name	Description
QRadar Get Offense MITRE Reference	Get the MITRE Tactics and Techniques in relation to the rules that were fired to cause the offense in QRadar.

Workflow Descriptions

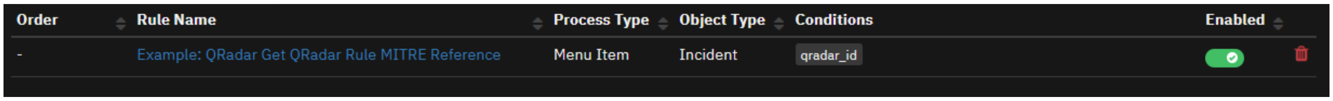
The example workflows are meant to be used as a guide to understand how to properly use the function. The pre-process scripts are designed to be used out of the box and there is no need for post-process scripts as there will be no need to data manipulation after the function is complete.



Workflow Name	Description	Object Type	Rules
Example: QRadar - Get MITRE Reference From Rules	Using the QRadar ID for the offense in question, this workflow will go and retrieve the related MITRE Tactics and Techniques from QRadar based on the defined rules.	Incident	Example: QRadar Get QRadar Rule MITRE Reference

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.



Order	Rule Name	Process Type	Object Type	Conditions	Enabled
-	Example: QRadar Get QRadar Rule MITRE Reference	Menu Item	Incident	qradar_id	✓

Using the Function

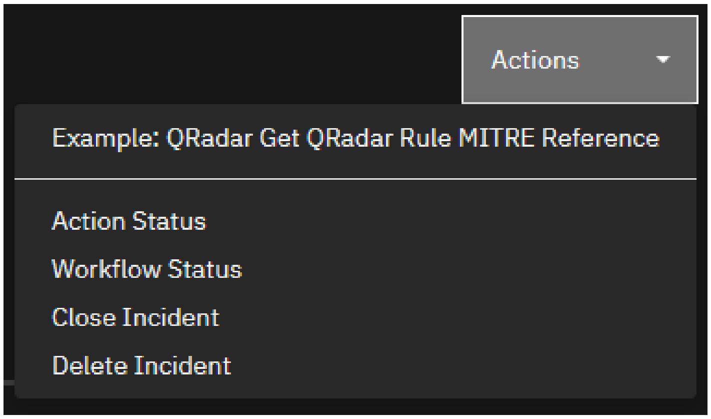
Pulling MITRE Information from QRadar Rule.

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:

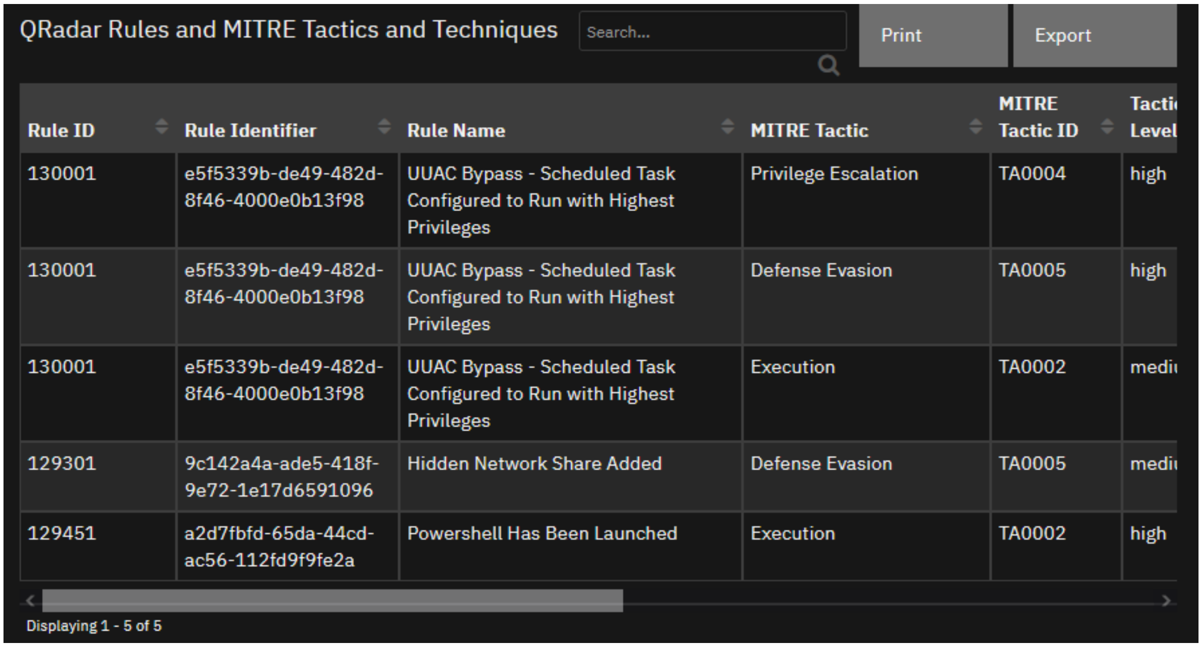
1. Click on the Actions and select the "Example: QRadar Get QRadar Rule MITRE Reference" Menu Item to pull the information from QRadar.



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.



Rule ID	Rule Identifier	Rule Name	MITRE Tactic	MITRE Tactic ID	Tacti Level
130001	e5f5339b-de49-482d-8f46-4000e0b13f98	UUAC Bypass - Scheduled Task Configured to Run with Highest Privileges	Privilege Escalation	TA0004	high
130001	e5f5339b-de49-482d-8f46-4000e0b13f98	UUAC Bypass - Scheduled Task Configured to Run with Highest Privileges	Defense Evasion	TA0005	high
130001	e5f5339b-de49-482d-8f46-4000e0b13f98	UUAC Bypass - Scheduled Task Configured to Run with Highest Privileges	Execution	TA0002	medi
129301	9c142a4a-ade5-418f-9e72-1e17d6591096	Hidden Network Share Added	Defense Evasion	TA0005	medi
129451	a2d7fbfd-65da-44cd-ac56-112fd9f9fe2a	Powershell Has Been Launched	Execution	TA0002	high

Displaying 1 - 5 of 5

Troubleshooting

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