

Resilient Content Package for QRadar Advisor and MITRE ATT&CK™

Description

This content package contains a single resource file with the following workflows:

1. Example of QRadar Advisor Offense Analysis with MITRE
2. Retrieve analysis and insights from QRadar Advisor, together with MITRE ATT&CK tactic
3. Retrieve MITRE ATT&CK techniques related to the tactic above
4. Example of mapping QRadar rule to tactic
5. Retrieve mapping of a QRadar rule to MITRE ATT&CK tactic(s) from QRadar Advisor
6. Retrieve MITRE ATT&CK techniques related to the tactic above

Package Dependences

The workflows in this package depend on the following integration packages - QRadar Advisor integration 2.0 - QRadar integration 2.0 (optional) - MITRE integration 1.0

Import

First of all, ensure that the above integration packages have been installed. Download the *resqrawmitre* package. Unzip it if necessary(`tar -xvf resqrawmitre.tar`). In Resilient server, go to Administrator Settings->Organization->Import->Import Settings and select the *qraw_mitre.res* file downloaded above.

Administrator Settings

[Users](#) [Groups](#) [Roles](#) [Workspaces](#) [Timeframes](#) [Network](#) [Organization](#) [Threat Sources](#) [Notifications](#)

General

[Details](#)

[Settings](#)

Email Connections

[Inbound](#) >

Migrate Settings

[Import](#)

[Import History](#)

[Export](#)

[Export History](#)

Import Settings

No file selected

[+ Import Settings](#)

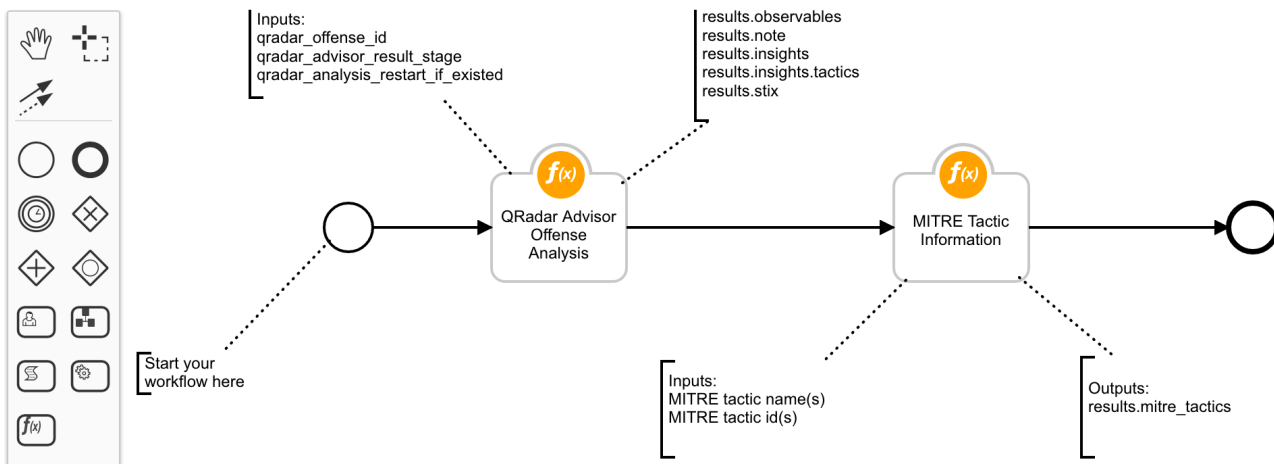
Select a file from which you would like to import settings to this organization.

Usage

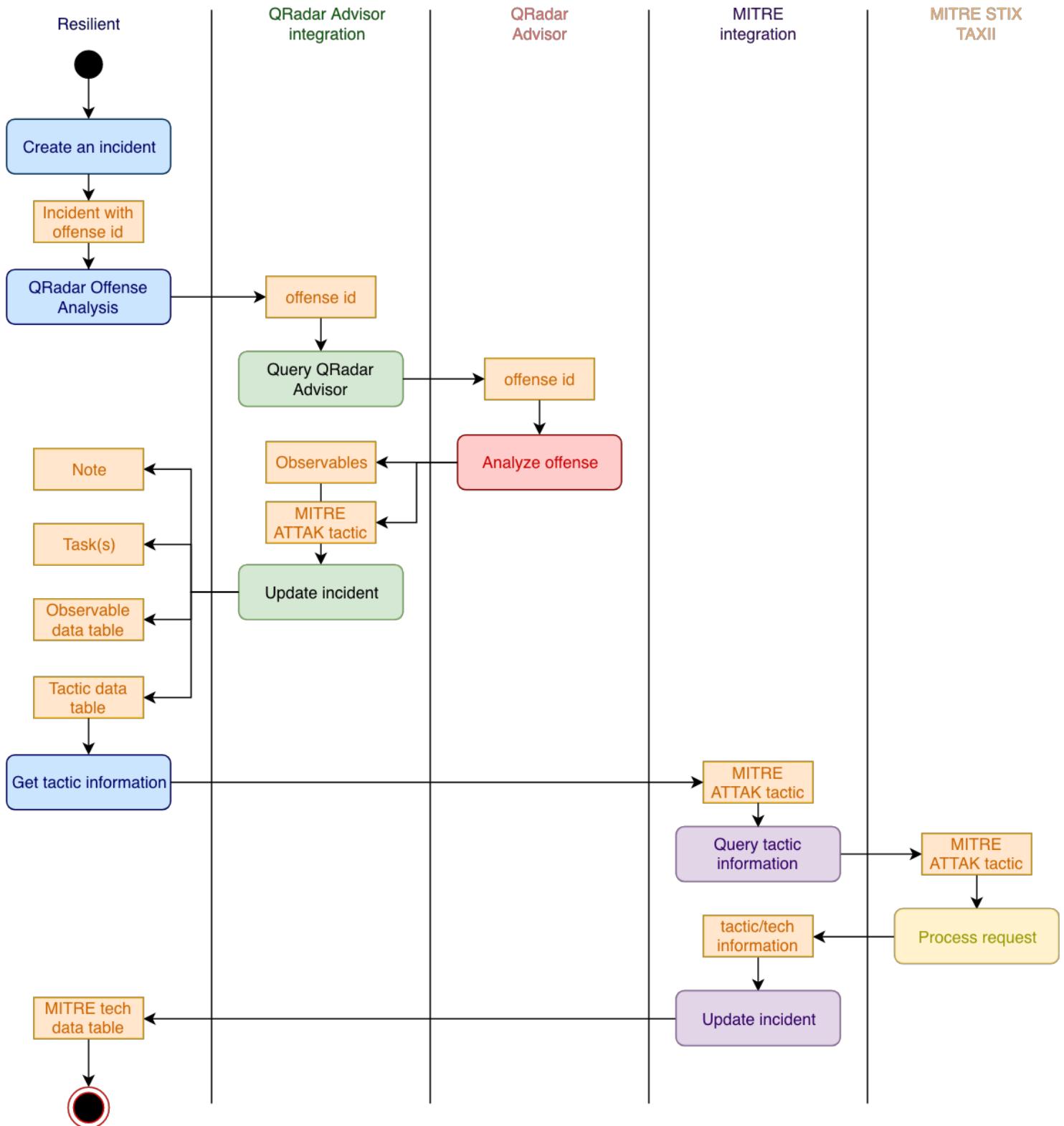
Once the resource file is successfully imported, the workflows included in the file are ready for use.

Example of QRadar Advisor Offense Analysis with MITRE

This workflow invokes two functions from two integration packages.



The "QRadar Advisor Offense Analysis" is a function from the QRadar Advisor integration, and "MITRE Tactic Information" is a function from the MITRE integration. The data flow is shown below



Here, a user starts from an incident with a QRadar offense id. In the following example, the incident is escalated from QRadar offense 23.

Description

No description.

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

analysis

full search

QRadar Advisor

QRaw MITRE

qradar_id

23

Edit

MITRE ATT&CK of Incident

Search...

Print

Export

ATT&CK Tactic	Tactic Code	Confidence	Reference	
Command and Control	TA0011	60	https://attack.mitre.org/tactics/TA0011/	...

Displaying 1 - 1 of 1

MITRE ATT&CK Techniques

Search...

Print

Export

Tactic	Technique name	Technique id	References	Description	Detection	
Command and Control	Port Knocking	T1205	https://attack.mitre.org/techniques/T1205 https://www.giac.org/paper/gchq/	Port Knocking is a well-established method used by both defenders and adversaries to hide open ports from access. To enable a port, an adversary sends a series of packets with certain characteristics before the	Record network packets sent to and from the system, looking for extraneous packets that do not belong to established flows.	...

Summary

ID

2211

Phase

Respond

Severity

Low

Date Created

03/08/2019

Date Occurred

—

Date Discovered

03/08/2019

Was personal information or personal data involved?

Unknown

Incident Type

—

People

Created By

masterfirst masterlast

Owner

masterfirst masterlast

Members

There are no members.

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

Note for convenience, a tab was created to hold all the related information here. To do analysis for the related offense, select Actions->"QRadar Advisor Offense Analysis with MITRE", to start this workflow. The first function, "QRadar Advisor Offense Analysis", is called to get the analysis and insights of the offense from QRadar Advisor. The insights contains MITRE ATT&CK tactic information, shown in the "MITRE ATT&CK of Incident" data table. In this example, QRadar Advisor returns a tactic called "Command and Control", together with a confidence value of 60 (over 100).


With this information, the second function "MITRE Tactic Information" is called. This function retrieves the following information from the MITRE STIX TAXII server: - Tactic ID - Reference link to tactic - Techniques related to this tactic The information is populated into the "MITRE ATT&CK Techniques" data table.

Note that from the "MITRE ATT&CK Techniques" data table, the user can easily create a task for a selected technique, by clicking a data table menu item.

Command and Control	Multi-hop Proxy	T1188	https://attack.mitre.org/techniques/T1188	To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source.	When observing use of Multi-hop proxies, the actual command and control servers could allow correlating incoming and outgoing flows to trace malicious traffic back to its source. Multi-hop proxies can also be detected by alerting on traffic to known anonymity networks (such as [Tor])(https://attack.mitre.org/software/S0183) or known adversary infrastructure that uses this technique.	...
---------------------	-----------------	-------	---------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----

Create Task for MITRE ATT&CK technique

A new task is created with description, detection, and mitigation for the selected technique.

 MITRE ATT&CK Technique: Port Knocking

Complete and Close

...

DetailsNotesMembersAttachments

Details

Edit

This task is optional

Mark Task Required

OwnerUnassigned

Due Date

Date Closed

Instructions

Creatormasterfirst masterlast

Date Initiated03/08/2019 09:25

Description

Detection

Mitigation

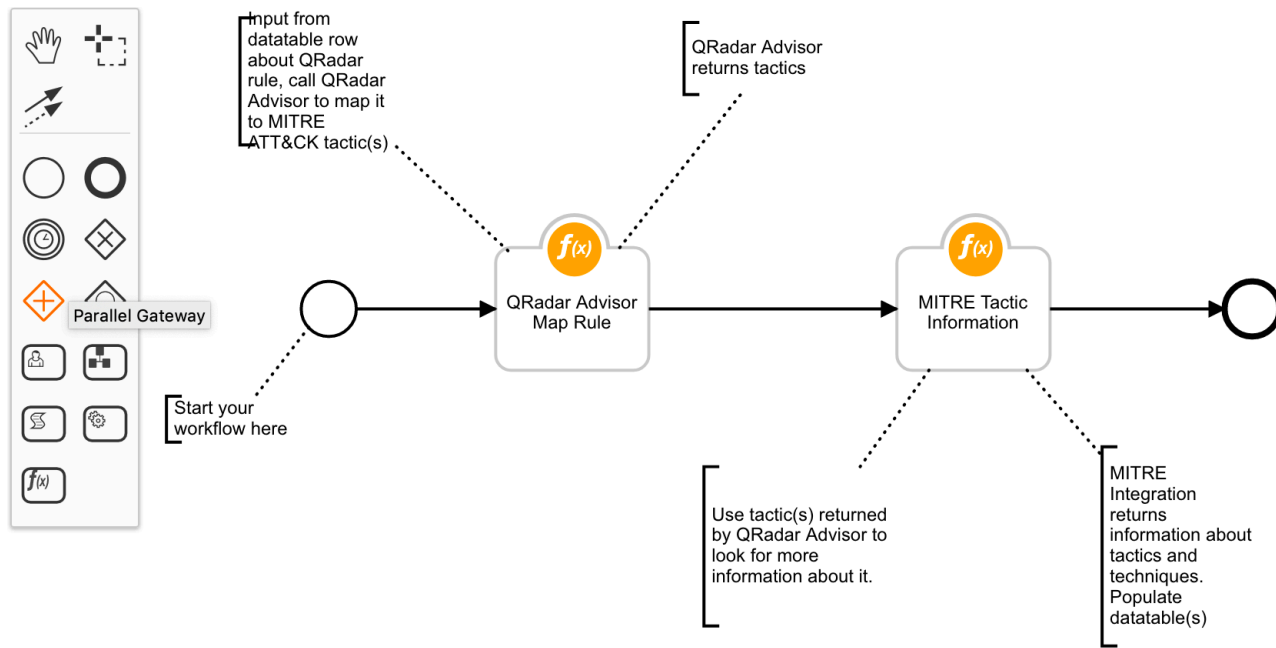
Port Knocking is a well-established method used by both defenders and adversaries to hide open ports from access. To enable a port, an adversary sends a series of packets with certain characteristics before the port will be opened. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports, but can involve unusual flags, specific strings or other unique characteristics. After the sequence is completed, opening a port is often accomplished by the host based firewall, but could also be implemented by custom software. This technique has been observed to both for the dynamic opening of a listening port as well as the initiating of a connection to a listening server on a different system. The observation of the signal packets to trigger the communication can be conducted through different methods. One means, originally implemented by Cd00r (Citation: Hartrell cd00r 2002), is to use the libpcap libraries to sniff for the packets in question. Another method leverages raw sockets, which enables the malware to use ports that are already open for use by other programs.

Record network packets sent to and from the system, looking for extraneous packets that do not belong to established flows.

Mitigation of some variants of this technique could be achieved through the use of stateful firewalls, depending upon how it is implemented.

Example of mapping QRadar rule to tactic

This workflow also contains two functions.



The "QRadar Advisor Map Rule" is a function from the QRadar Advisor integration, and the "MITRE Tactic Information" is a function from the MITRE integration.

This workflow can be used together with the "Example of finding all QRadar reference sets for artifact" workflow from the QRadar integration 2.0. These two workflows can make a complete use case.

This use case starts with an artifact. The dataflow is shown below.

Show25

Type	Value	Created	Relate?	Actions
IP Address	192.168.0.155	03/08/2019 09:30	As specified in the artifact type setti	<div><div></div><div></div></div>

QRadar Reference Set

Search

Reference Set	Item Value	Source
RF Risklist Source	192.168.0.155	RF Risklist Source L

Delete from QRadat Reference Set

Find in QRadat Reference Set

Find QRadat Reference Sets

QRadar Add to Reference Set

QRadar Move from suspect to blocked

Watson Search

Watson Search with Local Context

The result is shown in the "QRadar Reference Set" data table. Note that the "Source" column (if not empty)shows the QRadat rule that added this IP into the reference set. In this example, a rule called "RF Risklist Source Log" monitors source IPs that contact external malicious sites, and log the source IPs into a Reference Set called "RF Risklist Source". This IP address (192.168.0.155) is in that Reference Set.

Once the "QRadar Reference Set" data table is populated with data, user can select "Map rule to MITRE tactic".

QRadar Reference Set

Search...PrintExport

Reference Set	Item Value	Source	
RF Risklist Source	192.168.0.155	RF Risklist Source Log	...

Displaying 1 - 1 of 1

Map rule to MITRE tactic

This manual item invokes the "Example of mapping QRadat rule to tactic" workflow of this package.

The workflow first call "QRadar Advisor Map Rule" function to map the rule to MITRE ATT&CK tactic. The result is shown in the "MITRE ATT&CK of Artifact" data table.

MITRE ATT&CK of Artifact

Search...PrintExport

Artifact	MITRE ATT&CK Tactic	Tactic Code	Confidence	Reference	
192.168.0.155	Initial Access	TA0001	low	https://attack.mitre.org/tactics/TA0001/	...

Displaying 1 - 1 of 1

In this example, QRadat Advisor maps the rule "RF Risklist Source Log" into a MITRE ATT&CK tactic called "Initial Access".

With this tactic information, the workflow makes a second call to the MITRE integration function, "MITRE Tactic Information" to get all the MITRE ATT&CK techniques related to this tactic. Similar to the first workflow, technique information is shown in the "MITRE ATT&CK Techniques" data table. From here, the user can create

tasks for selected techniques.

Uninstall

Manually delete the followings: 1. Rules - "Map rule to MITRE tactic" - "QRadar Advisor Offense Analysis with MITRE" 2. Data tables - MITRE ATT&CK of Artifact 3. Workflows - Example of QRadar Advisor Offense Analysis with MITRE - Example of mapping QRadar rule to tactic