

IBM Resilient SOAR Platform

QRadar Advisor Guide

V2.0.2

Date: September 2020

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2020. All Rights Reserved.

US Government Users Restricted Rights: Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM Resilient SOAR Platform QRadar Integration Guide

Version	Publication	Notes
2.0.2	September 2020	Support added for App Host, support added for proxies, updated deprecated API endpoints, bug fixes
2.0.1	February 2019	Bug fixes for Python 3
2.0	April 2019	Supports the V2.0 release
1.0.1	March 2019	For Watson Search fixed version compatibility with search that returns no data, and fix typo in post-process script
1.0	August 2018	Initial publication.

Table of Contents

- Overview 4
- Check Prerequisites..... 4
- Configure QRadar Advisor 5
 - Cyber Adversary Framework Mapping Application Configuration 6
- Install the Integration 6
- Function descriptions..... 8
 - Example of Watson Search with Local Context.....10
 - Example of Watson Search.....15
 - Example of QRadar Advisor Offense Analysis16
 - Example of mapping QRadar20

Overview

Resilient Functions simplify development of integrations by wrapping each activity into an individual workflow component. These components can be easily installed, then used and combined in Resilient workflows. The Resilient platform sends data to the function component that performs an activity then returns the results to the workflow. The results can be acted upon by scripts, rules, and workflow decision points to dynamically orchestrate the security incident response activities.

This guide describes the QRadar Advisor Integration Function.

Backed by IBM Watson, QRadar Advisor applies artificial intelligence to automatically investigate indicators of compromise (IOC), utilizes cognitive reasoning to provide critical insights, and ultimately accelerates the response cycle. It can augment a security analyst to gain a head start in assessing incidents and reduce the risk of missing threats.

QRadar Advisor Integration Function enables Resilient users to gather Cyber Threat Intelligence (CTI) data from IBM Watson and QRadar. This information is critical for effective identification of potential IOC and quick response to incidents. In addition, this integration receives MITRE ATT&CK information from QRadar Advisor. As a result, an example workflow of this integration depends on the MITRE ATTACK function integration.

QRadar Advisor integration includes four functions:

- Perform a Watson Search on an indicator and retrieve suspicious observables related to it.
- Perform a Watson Search with Local Context on an indicator and retrieve a cyber threat intelligence (CTI) report on it in Structured Threat Information eXpression ([STIX2](#)) format.
- Perform an analysis on a QRadar offense, and retrieve CTI data from QRadar Advisor and IBM Watson in STIX format.
- Map a given QRadar rule to MITRE ATT&CK tactics.

The package also includes workflow examples to demonstrate the usage of the above functions.

The remainder of this document describes the functions and how to configure them in custom workflows or using the configuration file.

Check Prerequisites

Before installing, verify that your environment meets the following prerequisites:

- Resilient platform is version 31 or later.
- You have a Resilient account or API key to use for the integrations. This can be any account or API key that has the permission to view and modify administrator and customization settings, and read and update incidents. You need to know the account username and password or API key and secret.
- If you are not installing on a Resilient platform configured with an App Host, you have access to a Resilient integration server. An *integration server* is the system that you use to deploy integration packages to the Resilient platform. See the [Resilient Integration Server Guide \(PDF\)](#) for more information.

Configure QRadar Advisor

You need to have QRadar Advisor installed to a QRadar server, and fully configured, as shown in the following configuration page.

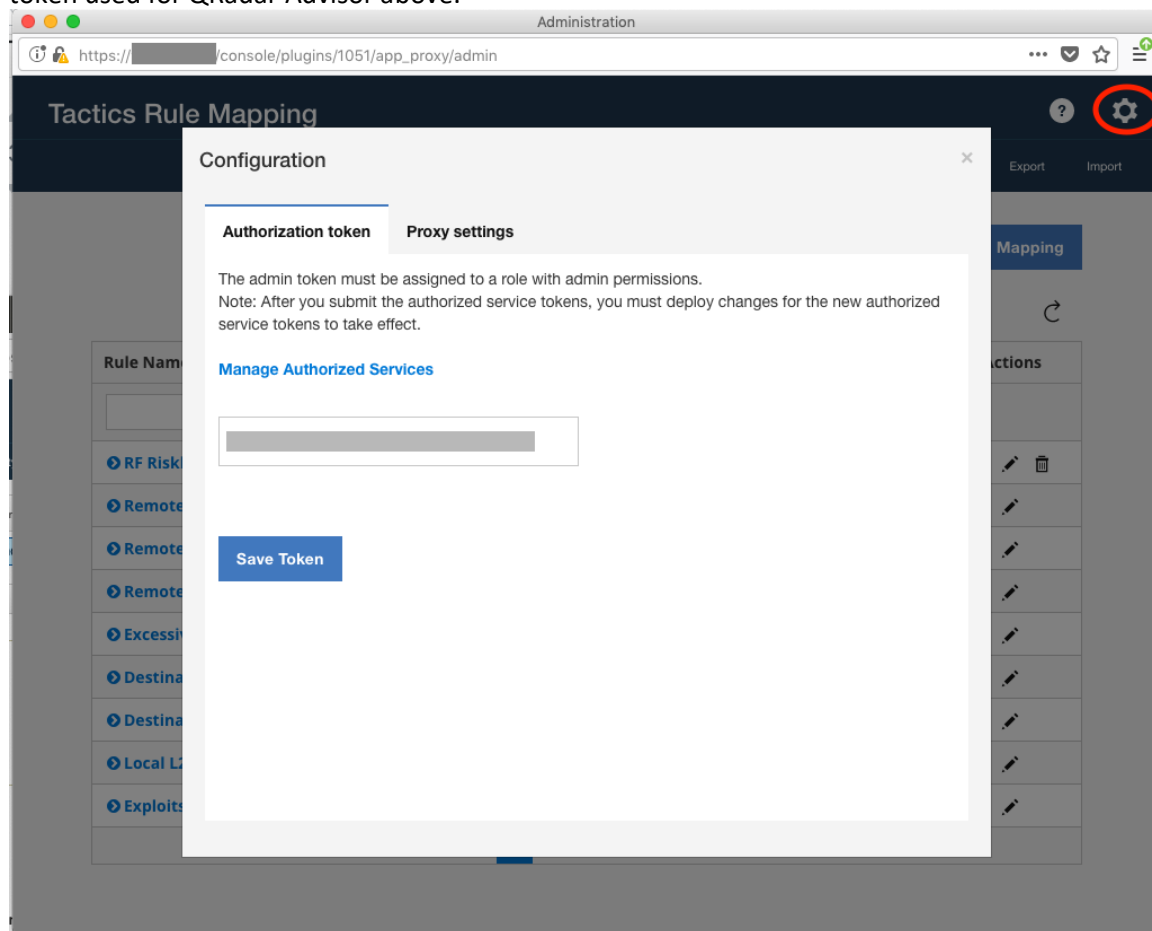
The screenshot shows a web browser window titled "QRadar Advisor with Watson Administration - Mozilla Firefox: IBM Edition". The address bar shows the URL "https://[redacted]/console/plugins/1102/app_proxy/admin". The page header is "IBM QRadar Advisor with Watson Configuration". On the left is a sidebar with a list of configuration steps, each with a green checkmark: Proxy Configuration, XFE Credentials, License Terms, Authorized Service Token, Retention Policy, Property Mapping, Threat Intelligence Mapping, Optimization, Automatic Investigation, Reference Set Export, and Complete. The main content area is titled "Proxy Configuration" with a help icon. It contains the following text: "The QRadar Advisor with Watson app uses the [IBM X-Force Exchange](#) to submit offenses for analysis. Enter details below, if you need to use a secure proxy." Below this is a checkbox for "Use Proxy". Underneath are radio buttons for "HTTPS" (selected) and "SOCKS5". To the right is a checkbox for "Disable Authentication". There are four input fields: "Proxy server", "0" (with a clear button), "Proxy username", and "Proxy password" (with a "Show Password" checkbox). At the bottom is a checkbox for "Enable Custom SSL Certificate Validation" and a blue "Submit" button. In the bottom right corner, there is a link "XFE Credentials" with a right arrow.

To access the QRadar Advisor REST API, you need to know its `app_id`, which you can access by clicking the QRadar Advisor's Configuration icon. For example, in the URL address shown in the configuration page screenshot, the `app_id` is 1102 for this QRadar Advisor instance.

You also need an access token to use the REST API. You can obtain access tokens from the Authorized Service Token section of the Admin page.

Cyber Adversary Framework Mapping Application Configuration

QRadar Advisor 2.0 comes with Cyber Adversary Framework Mapping Application (CAFM). This needs to be properly configured as well. From the Admin page of QRadar, select the Configuration page for CAFM. Click the configuration button on the top right corner, and then enter an authorization token. This token can be the same as the authorization token used for QRadar Advisor above.



Write down the app id for CAFM. It is shown in the URL address of this page. For the example above, the app id for CAFM is 1051. This app id is needed in the app.config file.

Install the Integration

If installing the integration on an integration server, follow the procedures in the [Resilient Integration Server Guide \(PDF\)](#). To complete the installation, you need to perform the following:

1. Edit the [fn_qradar_advisor] section of the resilient-circuits configuration file, as follows:

```
qradar_host=host of your QRadar server with QRadar Advisor installed
qradar_advisor_token=qradar token (res-keyring protected recommended)
qradar_advisor_app_id=qradar app id for qradar advisor
verify_cert=[true|false] whether to validate the QRadar server cert
qradar_cafm_token=qradar token (res-keyring protected recommended)
qradar_cafm_app_id=qradar app id for CAFM
#optional settings
full_search_timeout=timeout for full search in seconds (1200 default)
full_search_period=period for full search in seconds (5 default)
offense_analysis_timeout=timeout for analysis in seconds (1200 default)
offense_analysis_period=period for analysis in seconds (5 default)
# Settings for access to Qradar Advisor via a proxy
#http_proxy=http://proxy:80
#https_proxy=https://proxy:80
```

2. (Recommended) Use res-keyring to store the qradar advisor token:

- a. Instead of storing your token in plaintext, use this instead in your app.config for the token

```
qradar_advisor_token=^qradar_advisor_token  
qradar_cafm_token=^qradar_cafm_token
```

- b. Run the following command from a terminal in the same folder of your app.config

```
res-keyring
```

- c. Follow the prompt to enter your token.

Function descriptions

This package contains the following functions, example workflows and rules that invoke those functions.

Function	Example Workflow	Rule
Watson Search	Example of Watson Search	Watson Search
Watson Search with Local Context	Example of Watson Search with Local Context	Watson Search with Local Context
QRadar Advisor Offense Analysis	Example of QRadar Advisor Offense Analysis	QRadar Advisor Offense Analysis
QRadar Advisor Map Rule	Example of mapping QRadar Rule	Map QRadar rule

In addition, the package contains two custom data tables called “QRadar Advisor analysis results” and “Watson Search with Local Context results”. They are used by the example workflows to show the observables that are extracted from the QRadar Advisor STIX response. Two demo scripts and two associated rules are also included. Each rule is a menu item added to its own data table. The user can click on a rule to create an artifact based on the selected row.

Data Table	Rule	Script
QRadar Advisor analysis results	Create Artifact (QRadar Advisor Analysis)	Create Artifact for QRadar Advisor Analysis Observable
Watson Search with Local Context results	Create Artifact (Watson Search with Local Context)	Create Artifact for Watson Search with Local Context

Once the function package deploys the functions, you can view them in the Resilient platform Functions tab, as shown below.

Customization Settings

Layouts

Rules

Scripts

Workflows

Functions

Message Destinations

Phases & Tasks

Incident Types





Breach

Artifacts

Functions

New Function

Search...

Name	Description	
QRadar Advisor Map Rule	Map rule to MITRE ATT&CK tactic	
QRadar Advisor Offense Analysis	Given a Resilient artifact, this function performs a QRadar Advisor analysis and returns Local, Watson enriched, or Expanded local context (default) results.	
Watson Search	Given a Resilient artifact, this function performs a Watson Search (a QRadar Advisor quick search) and returns a summary.	
Watson Search with Local Context	Given a Resilient artifact, this function performs a Watson Search with Local Context (a QRadar Advisor full search) and returns Local, Watson enriched, or Expanded local context (default) results.	

© Copyright IBM Corporation 2020

The package also includes example workflows and rules that show how the functions can be used. You can copy and modify these workflows and rules for your own needs.

Customization Settings

Layouts

Rules

Scripts

Workflows

Functions

Message Destinations

Phases & Tasks

Incident Types





Breach

Artifacts

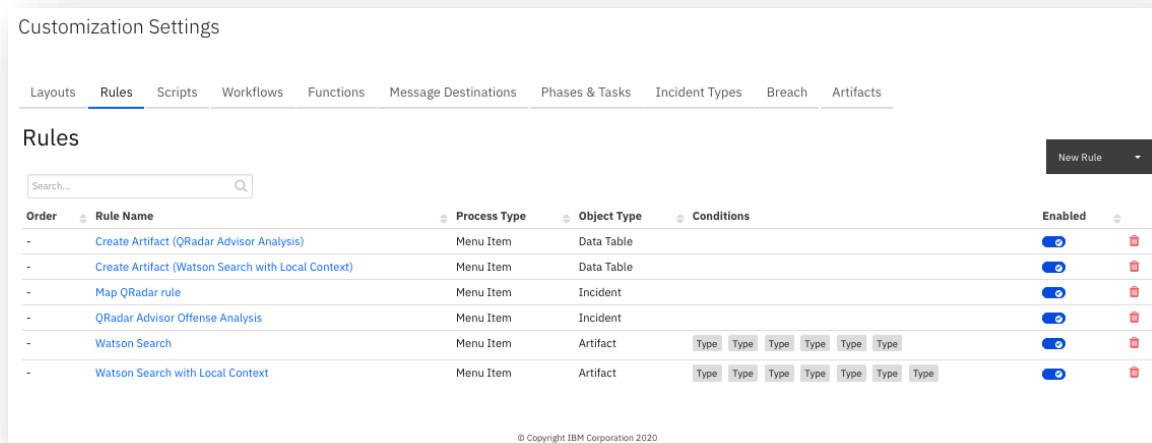
Workflows

New Workflow

Search...

Workflow Name	Description	Object Type	Rules	
Example of mapping QRadar Rule	Map a QRadar rule to MITRE ATT&CK tactic(s) using QRadar Advisor with Watson	Incident	Map QRadar rule	
Example of Watson Search	Performs a Watson Search (a quick search) of observables in QRadar Advisor. Results will be displayed in incident Notes. This sample workflow also creates artifacts for suspicious observables which can be mapped to Resilient artifacts.	Artifact	Watson Search	
Example of Watson Search with Local Context	Performs a Watson Search with Local Context (a full search) of observables in QRadar Advisor. Results will populate a Data Table, create a Task, and generate a HTML representation of the STIX bundles in Notes.	Artifact	Watson Search with Local Context	
Example of QRadar Advisor Offense Analysis	Performs an offense analysis in QRadar Advisor. Results will populate a Data Table, create a Task, and generate a STIX representation in Notes. QRadar Advisor with Watson returns MITRE ATT&CK tactic name.	Incident	QRadar Advisor Offense Analysis	

© Copyright IBM Corporation 2020



The example workflows shown above demonstrate how to use the functions included in the integration package, as explained below.

Example of Watson Search with Local Context

This example workflow invokes the function “Watson Search with Local Context”. The function calls the QRadar Advisor REST API to perform a Watson Search with Local Context on an indicator.

To use this example workflow and rule included in the package for this function, the user needs to create an incident and add an artifact. For this function to work, the artifact type must correspond to one indicator type. QRadar Advisor supports searches on the following indicators:

- IP addresses
- Hashes
- Domains
- URLs
- Persons

QRadar Advisor supports three return stages:

- Stage1: feature hunt
- Stage2: cognitive investigation added on top of the result of stage 1
- Stage3: wider feature hunt added on top of the result of stage 2

The user can specify the desired return stage in the pre-process script of the example workflow.

Customization Settings

Layouts

Rules

Scripts

Workflows

Functions

Message Destinations

Phases & Tasks

Incident Types

Breach

Artifacts

[Workflows](#) / Example of Watson Search with Local Context

Name *

Example of Watson Search with Local Context

API Name *

qradar_advisor_full_search

Description

Performs a Watson Search with Local Context (a full search) of observables in QRadar Advisor. Results will populate a Data Table, create a Task, and generate a HTML.

Object Type *

Artifact

Creator

masterfirst
masterlast
08/01/2018 11:25

Last Modified

08/01/2018 11:25

Last Modified By

masterfirst
masterlast

Associated Rules

Watson Search with Local Context

Hand

Target

Circle

Circle with X

Circle with Plus

Circle with Minus

qradar_advisor_search_value

qradar_advisor_result_stage

Watson Search with Local Context

results.note

results.summary

results.stix

Input

Pre-Process Script

Output

Post-Process Script

Input Parameter

Value

qradar_advisor_search_value

qradar_advisor_result_stage

stage1

stage1

stage2

stage3

The search REST API of QRadar Advisor returns CTI information in Structured Threat Information Expression (STIX 2.0) format. It is normally a STIX bundle with STIX objects. The function processes the STIX data and performs the following:

- Generates a HTML representation of the STIX data
- Extracts observables from the STIX objects
- Generates a summary from the STIX data

The return data from this function includes the raw STIX data in json dictionary format.

In the post-process script, the HTML representation is used to create a note. The observables are used to populate the custom data table, “Watson Search with Local Context results”, and the summary is used to create a task. Note that the raw STIX data is accessible from the post-process script as results.stix, and can be parsed to create custom code.

The screenshot shows the 'Customization Settings' page for a workflow. The 'Workflows' tab is selected. The workflow name is 'Example of Watson Search with Local Context', the API name is 'qradar_advisor_full_search', and the object type is 'Artifact'. The description states: 'Performs a Watson Search with Local Context (a full search) of observables in QRadar Advisor. Results will populate a Data Table, create a Task, and generate a HTML.' The creator is 'masterfirst' and the last modified date is '08/01/2018 11:25'. The associated rule is 'Watson Search with Local Context'.

The workflow diagram shows a process flow starting with an input box containing 'qradar_advisor_search_value' and 'qradar_advisor_result_stage'. This leads to a function block labeled 'Watson Search with Local Context'. The output of this function is a box containing 'results.observables', 'results.note', 'results.summary', and 'results.stix'.

Below the diagram is a code editor showing a Python script for the post-process script. The script includes comments and code for publishing a data table, creating a note, and adding a task.

```

10 # We publish a data table according to the stix
11 date_str = str(Date())
12 for observable in results.observables:
13     qradar_obs = incident.addRow("qradar_advisor_observable_for_artifact")
14     qradar_obs.qradar_advisor_toxicity = observable.toxicity
15     qradar_obs.qradar_advisor_relevance = observable.relevance
16     qradar_obs.qradar_advisor_type = observable.type
17     qradar_obs.qradar_advisor_description = observable.description
18     qradar_obs.artifact_related = artifact.value
19     qradar_obs.full_search_time = date_str
20 # Our STIX tree
21 html = helper.createRichText(results.note)
22 incident.addNote(html)

```

In the following example, a User Account artifact was added to an incident with value “jsmith”. The user can then select Watson Search with Local Context from the artifact menu to search QRadar Advisor for the observable.

The screenshot shows the 'Incident Details' page for a 'Demo incident'. The 'Artifacts' tab is selected. There is an 'Add Artifact' button and a 'Table' view option. Below the table view, there is a search bar and a table of artifacts.

Hits	Related Inci...	Type	Value	Created	Last Modified	Relate?	Actions
0		User Account	jsmith	09/03/2020 11:18	09/03/2020 11:18	As specified in the artifc	🗑️ ⋮

At the bottom of the page, there is a dropdown menu labeled 'Watson Search with Local Context'.

Please note that both Watson Search and Watson Search with Local Context perform queries for information about an indicator. Therefore, only those artifacts that can be mapped into indicators are supported. The types of artifacts that can be searched include:

- DNS Name
- Malware SHA-256 Hash
- Malware SHA-1 Hash
- Malware MD5 Hash
- IP Address
- URL
- User Account

The menu item Watson Search with Local Context is the only one shown for the artifact type listed above.

Note that a full search like this could take up to 15 minutes. Once it is completed, the note created for this indicator can be viewed from the Notes tab of this incident.

Description

demo incident with artifact type User Account

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

custom

Notes

Sans Serif

Normal

B

I

U

Post

Cancel

Search...

☒ Show Task Notes
 ☐ Oldest Notes First

Created By: All

Date Created: All

masterfirst

masterlast

added a note to the Incident 08/01/2018 13:22

jsmith

10.103.22.35

file with name unknown

1ea41812a0114e5c6ae76330e7b4af69

gmuweb.exe

Backdoor.Darkmoon

file with name unknown

Packed.Generic.347

ab.exe

7b0cb4d14d3d8b6ccc7453f7ddb33997

10.103.22.50

file with name unknown

765f46vb.exe

fd4da1b404961e6db45469a27a201f41

Trojan.Gen

file with name unknown

JS.Downloader

d565937b49df96e6a8b88fedcf15d82a

9758W-TERBEDOC-RS62937-15000.zip

Please note that the icons shown in the above note use external URL referencing to the official site for STIX2 icons (https://raw.githubusercontent.com/freetaxii/stix2-graphics/master/icons/png_standard). Therefore, those icons are shown only if the Resilient platform can access the above website.

Also note that some indicators have a link icon at the end. These indicators are basically placeholders for the other (real) indicators with the same value. Think of them as symbolic links in a folder tree.

The data table can be viewed if the user adds the “Watson Search with Local Context results” data table into one tab of an incident. Note that this package includes a rule, “Create Artifact (Watson Search with Local Context)”, which is added to the “Watson Search with Local Context results” data table. This enables the user to create an artifact based on a selected row from this data table as shown below.

Artifact Searched	Search Time	Description	Type	Toxicity	Relevance	
jsmith	Wed Aug 01 17:22:14 UTC 2018	1ea41812a0114e5c6ae76330e7b4af69	file	very-low	medium	...
jsmith	Wed Aug 01 17:22:14 UTC 2018	10.103.22.35	ipv4-addr	very-low	medium	...
jsmith	Wed Aug 01 17:22:14 UTC 2018	Trojan.Gen	malware	very-high	medium	...
jsmith	Wed Aug 01 17:22:14 UTC 2018	JS.Downloader	malware	very-high	medium	...
jsmith	Wed Aug 01 17:22:14 UTC 2018	a26fb483371ba5b77b5be7b3f8c74cf4	file	very-low	medium	...
jsmith	Wed Aug 01 17:22:14 UTC 2018	765f46vb eye	file	very-low	medium	...

The newly created task can be viewed from the Tasks tab.

Description

No description.

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

QRadar

Splunk

Tasks

0% Complete

Filter: All

Selected

Add Task

Task Name	Owner	Due Date	Flags	Actions
Initial				
<div> <div>Review Watson full search of artifact: jsmith</div> <div>Unassigned</div> <div>No due date</div> <div>0 0</div> <div>...</div> </div>				
Respond				
Respond - (Data Breach - Organizational)				
<div> <div>Investigate exposure of PI</div> <div>Unassigned</div> <div>No due date</div> <div>0 0</div> <div>...</div> </div>				

Since Watson Search with Local Context could potentially take a long time to complete depending on the performance of QRadar Advisor, additional configuration settings are available in the app.config file.

Setting	Explanation
full_search_timeout	Timeout in seconds. It is the time the function waits for the result returned from QRadar Advisor. It is optional, and defaulted to 1200 seconds if absent.
full_search_period	In seconds. It specifies how often the function checks the search status. It is optional, and defaulted to 5 seconds if absent.

Example of Watson Search

This example workflow invokes the function “Watson Search”. The function calls the QRadar Advisor REST API to perform a quick search on an indicator.

To use this example workflow, the user creates an incident and then adds an artifact with the desired artifact type as shown in the Watson Search with Local Context function.

The QRadar Advisor REST API for Watson Search returns data in JSON format. The JSON dictionary contains two lists, one for suspicious_observables, and the other for other_observables. In the post-process script of this example workflow, the suspicious_observables are mapped to default artifact types, using a dictionary defined there. The user can easily map observables to custom artifacts by modifying the dictionary mapping.

Note the other_observables are not used in this example workflow. If user wants to make use of them, they can be accessed in the post-process script as results.other_observables.

In the following example, a Watson Search on the artifact, “domain.com”, is initiated when selecting Watson Search from the artifact menu

Description
Demo incident

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline **Artifacts** Email QRadar Advisor

Add Artifact Table Graph

Value: All Type: All Date Created: All Has Attachment: All Has Hits: All More...

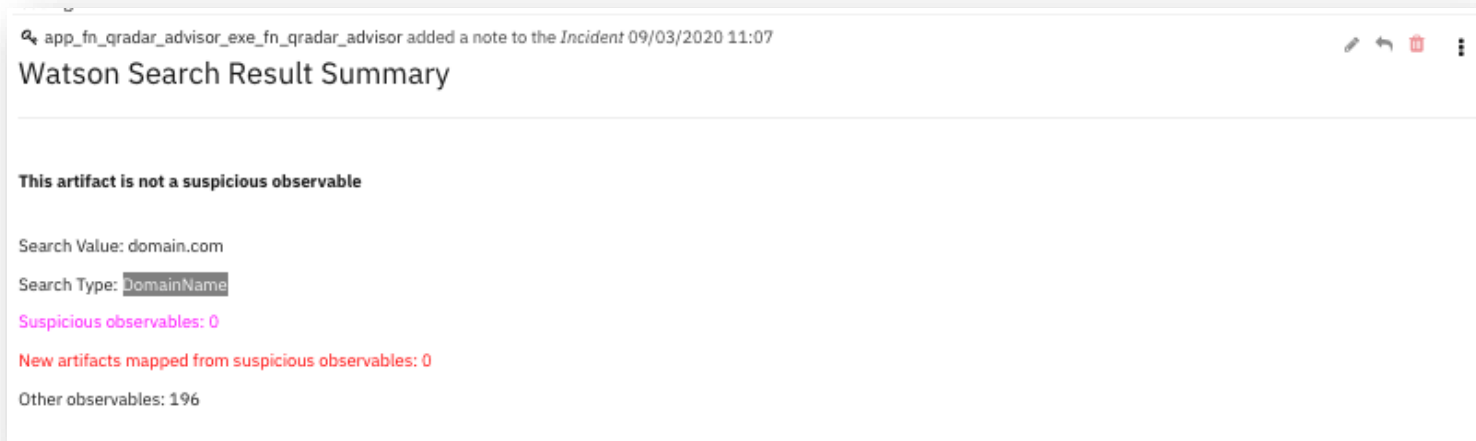
Columns Search...

Hits	Related Inci...	Type	Value	Created	Last Modified	Relate?	Actions
0		DNS Name	domain.com	09/03/2020 11:06	09/03/2020 11:06	As specified in the artifa	

Items per page 25 1-1 of 1 item

Watson Search
Watson Search with Local Context

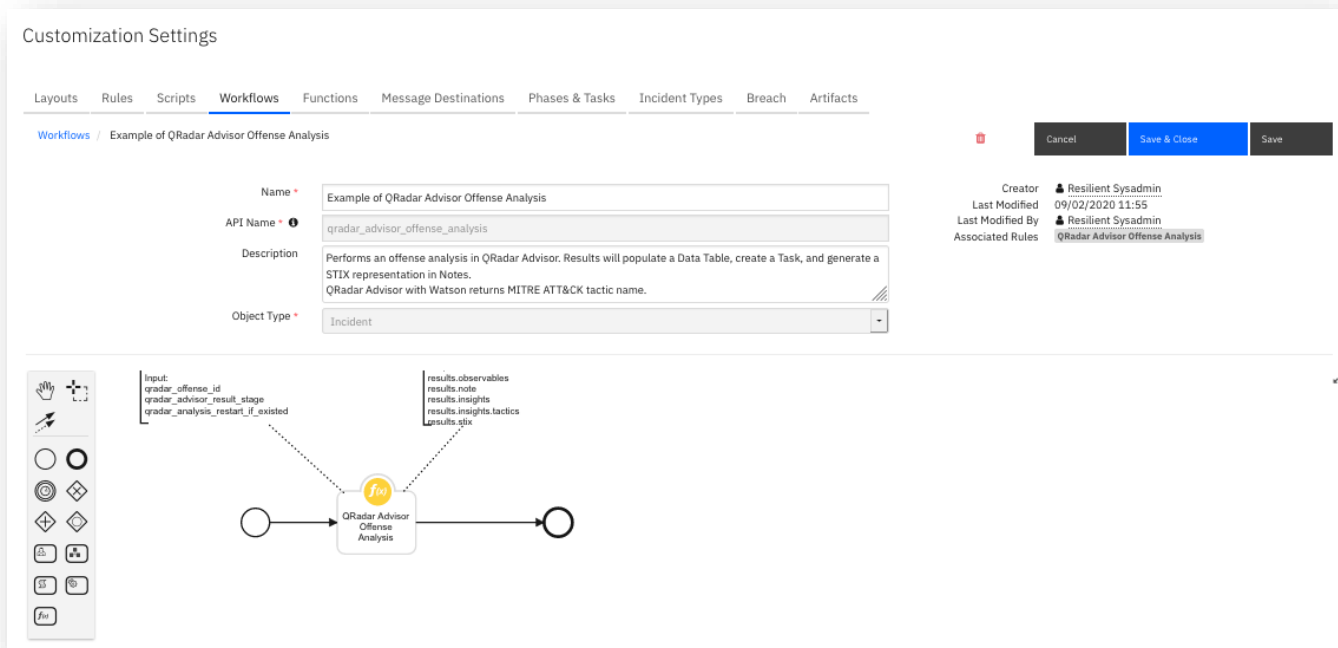
For this example, the Watson Search of “domain.com” does not return any suspicious observables. As a result, no new artifacts are added. A note was added to the incident to summarize this.



Example of QRadar Advisor Offense Analysis

This example workflow invokes two functions.

Function	Explanation	Outputs
QRadar Advisor Offense Analysis	Call QRadar Advisor API to perform the following: <ul style="list-style-type: none"> get the insights of a QRadar Advisor offense. perform analysis of the offense. 	<ul style="list-style-type: none"> QRadar Advisor Observable data table Incident note Task



The QRadar Advisor return of insights is in JSON format, and the result of an analysis is in STIX format.

Similar to the Watson Search with Local Context, the QRadar Advisor Offense Analysis generates a HTML representation of the STIX data. It also extracts observables from the STIX objects.

Just like Watson Search with Local Context, the user can also specify the return stage from the pre-process script of the example workflow.

Input	Pre-Process Script	Output	Post-Process Script
Input Parameter		Value	
qradar_offense_id		<input type="text"/>	
qradar_advisor_result_stage		stage3	
qradar_analysis_restart_if_existed ⓘ		Yes	

One more setting is qradar_analysis_restart_if_existed. If this flag is set to Yes, the function restarts a new analysis even if a previous result exists for this offense.

In the post-process script of the “QRadar Advisor Offense Analysis”, the HTML representation is used to create a note. The observables are used to populate the “QRadar Advisor analysis results” data table. The insights are used to create a task. The MITRE ATT&CK tactic information is written to a custom field, “mitre_tactic_name”, which is displayed in this example as “MITRE ATT&CK Tactic name.”

```
22 qradar_obs.qradar_advisor_type = observable.type
23 qradar_obs.qradar_advisor_description = observable.description
24
25 # Pass insights data (with MITRE ATTACK tactics information) to following function
26 # using workflow.properties.qraw_offense_insights. Refer to the Output tab please
27
28 # Our STIX tree or error status.
29 html = helper.createRichText(results.note)
30 incident.addNote(html)
31
32 # if process_insights:
33 #     # If we didn't get a 404 (no observables) status process for insights.
34 #     # Task
35     task_title = "Review QRadar Advisor Analysis for Offense " + str(incident.properties.qradar_id)
36     task_summary = results.insights.insights + "\n\n" + results.insights.stage3_insights
37     incident.addTask(task_title, "Initial", task_summary)
38
39     #
40     # MITRE tactic information
41     #
42     tactics = results.insights["tactics"]
43
44     mitre_tactic_names = []
45     if tactics is not None:
46         for tactic in tactics:
47             #
48             # Note, even though QRAW calls it tactic_id, it is more a tactic name
49             #
50             mitre_tactic_names.append(tactic["tactic_id"])
51     #
52     # Qradar id does not exist, but we have the tactic information. Create a task to include the insights
```

The raw STIX data from QRadar Advisor is accessible from the post-process script as results.stix, if the user wants to create custom code to parse the STIX data.

To use the example workflow, a Resilient incident must have a valid QRadar offense ID stored in a custom field, qradar_id. In the following example, the incident is linked to QRadar offense 2696.

The offense analysis begins upon selection of the rule “QRadar Advisor Offense Analysis” from the Action menu of the incident.

QRadar Offense analysis 2696

Description
No description.

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Artifacts Email **QRadar Advisor**

qradar_id 2696
qradar_rule —
MITRE ATT&CK Tactic name —

QRadar Advisor analysis results

Description	Type	Toxicity	Relevance
There is no data for this table			

Summary

ID 20
Phase Re
Severity Low
Date Created 09/03/2020 12:18
Date Occurred —
Date Discovered 09/03/2020 12:18
Data Compromised Unknown
Incident Type —

People

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

Related Incidents
No related incidents.

Actions

- Map QRadat rule
- QRadar Advisor Offense Analysis**
- Action Status
- Workflow Status
- Close Incident
- Delete Incident

A normal analysis can take up to 20 minutes. Once completed, the HTML representation is shown in the Notes tab.

Notes

Sans Serif Normal B I U W.

Post Cancel

Search... ☒ Show Task Notes ☐ Oldest Notes First Created By: All Date Created: All

Resilient Sysadmin added a note to the incident 09/03/2020 12:38

- userD
 - 192.168.0.17
- 193.184.16.214
 - 192.168.0.17
- 89.223.26.52
 - 192.168.0.17

x-mitre-tactic Command and Control

There are 5 objects and 2 links.

Observables are added to the data table, “QRadar Advisor analysis results”. A menu rule is included for this data table. Users can use it to create a new artifact based on the selected row.

The MITRE ATT&CK tactic name(s) are assigned to the custom field “MITRE ATT&CK Tactic name”.

QRadar Offense analysis 2696

Description

No description.

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

Email

QRadar Advisor

qradar_id

2696

qradar_rule

—

MITRE ATT&CK Tactic name

Command and Control

Edit

QRadar Advisor analysis results

Search...

Print

Export

Description	Type	Toxicity	Relevance	
userD	identity	very-low	very-high	⋮
193.184.16.214	ipv4-addr	very-low	medium	⋮
192.168.0.17	ipv4-addr	very-low	medium	⋮
89.223.26.52	ipv4-addr	high	medium	⋮
Command and Control	x-mitre-tactic	—	—	⋮

Displaying 1 - 5 of 5

A task is created based on the insights returned from QRadar Advisor. The insights are kept in the instruction of the task.

QRadar Offense analysis 2696

Description
No description.

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

Email

QRadar Advisor

0% Complete

Filter: Active

Selected

Add Task

Task Name	Instructions	Flags	Actions
Initial			
<div><div><div></div><div></div></div><div><div>Review QRadar Advisor Analysis for Offense 2696</div></div></div>	Watson has analyzed this offense and a total of three observables. The reasoning process has not found any additional indicators that are related to this offense. No data points were found to be linked with the offense. One indicator was related to suspicious activity, and all indicators were active. In particular, one IP address has been found, which is known to be suspicious or malicious.	<div><div></div><div></div></div>	<div><div></div><div></div></div>
Respond			
<div><div><div></div><div></div></div><div><div>Respond - (Data Breach - Organizational)</div></div></div> <div><div><div></div><div></div></div><div><div>*Investigate Exposure of Personal Information/Data</div></div></div>	Unassigned	No due date	<div><div></div><div></div></div>

Since an analysis could potentially take a long time to complete depending on the performance of QRadar Advisor, additional configuration settings are available in the app.config file.

Setting	Explanation
offense_analysis_timeout	Timeout in seconds. It is the time the function waits for the result returned from QRadar Advisor. It is optional, and defaults to 1200 seconds if absent.
offense_analysis_period	In seconds. It specifies how often the function checks the analysis status. It is optional, and defaults to 5 seconds if absent.

Example of mapping QRadar

This example workflow invokes the following function.

Function	Explanation	Outputs
QRadar Advisor Map Rule	Call the QRadar CAMF API to map a given QRadar rule to a MITRE tactic.	MITRE ATT&CK Tactic name

Customization Settings

Layouts Rules Scripts **Workflows** Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

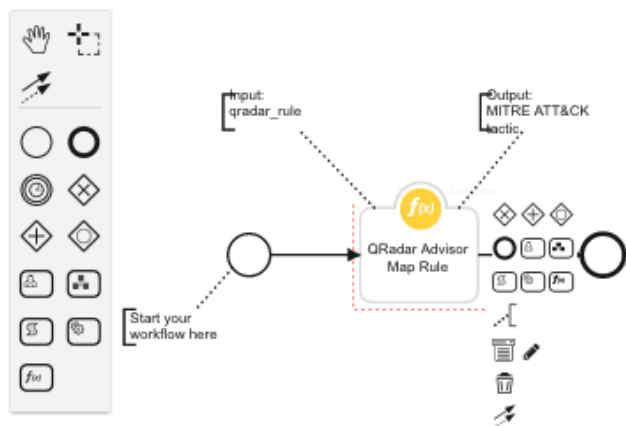
Workflows / Example of mapping QRadar Rule

Name * Example of mapping QRadar Rule

API Name * qradar_advisor_map_rule

Description Map a QRadar rule to MITRE ATT&CK tactic(s) using QRadar Advisor with Watson

Object Type * Incident



Input Pre-Process Script Output Post-Process Script

Language: Python Theme **light** Mode **Default** Tab Size **2** [- Font](#) [+ Font](#)

```
1 inputs.qradar_rule_name = incident.properties.qradar_rule
```

To use this workflow example, a user needs to enter a QRadar rule into the custom field `qradar_rule` first, then select “Map QRadar rule”.

Description
Tactic mapping

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Artifacts Email **QRadar Advisor**

qradar_rule

MITRE ATT&CK Tactic name

RF Risklist Source Log

—

Edit

QRadar Advisor analysis results

Search...

Print

Export

Description	Type	Toxicity	Relevance
There is no data for this table			

Showing 0 to 0 of 0 entries

Summary

ID

20

Phase

Re

Severity

Low

Date Created

09/02/2020 13:20

Date Occurred

—

Date Discovered

09/02/2020 13:20

Data Compromised

Unknown

Incident Type

—

People

Created By

Owner

Members

Resilient Sysadmin

Resilient Sysadmin

There are no members.

Related Incidents

No related incidents.

Map QRadar rule

QRadar Advisor Offense Analysis

Action Status

Workflow Status

Close Incident

Delete Incident

In the above example, there is an example QRadar rule named “RF Risklist Source Log”. This rule detects if a local host contacts an external IP that is in a reference set called “RF Risklist”. If so, it stores the local IP into a reference set. QRadar Advisor maps this rule to a MITRE ATT&CK tactic called “Initial Access” and the returned name is entered into the custom field MITRE ATT&CK Tactic name.

Description

Tactic mapping

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

Email

QRadar Advisor

qradar_rule ⓘ

MITRE ATT&CK Tactic name ⓘ

RF Risklist Source Log

Initial Access

Edit

QRadar Advisor analysis results

Search...

Print

Export

Description ⓘ

Type ⓘ

Toxicity ⓘ

Relevance ⓘ

There is no data for this table

Showing 0 to 0 of 0 entries