

IBM QRadar Integration Guide



Table of Contents

OVERVIEW	3
Features Prerequisites Delpoyment Architecture	
CONFIGURATION	5
CREATING APPLICATION IN OBSERVEIT Configuring ObserveIT App for QRadar QRadar on Cloud	5 7 10
USAGE	12
Application Tuning Viewing Events Dashboard Configuring the Dashboard	
SUPPORT	16
RELEASE NOTES	17



Overview

This document describes the integration of ObserveIT with IBM QRadar software.

FEATURES

The ObserveIT App for IBM QRadar does the following:

- Event Collection: Functions as a custom protocol to connect QRadar to the ObserveIT RESTful API and continuously pull the latest events. ObserveIT App pulls data from ObserveIT into QRadar as follows:
 - o Subscribes to User Interface Activity, User Command Activity, and Alert events
 - o Polls events from multiple ObserveIT instances
- Sample Dashboard: Provides a sample dashboard to highlight insights from your ObserveIT data and includes.
 - o Summary of the most active endpoints and most visited sites
 - o Charts to highlight the riskiest users and top alert categories
 - o Customizable to suit your needs
- Sample Rules: Includes some custom rules to get you started such as:
 - o Mapping the ObserveIT Severity to a corresponding numeric QRadar Severity
 - o Creating offenses from High and Critical Severity Alerts



PREREQUISITES

- Downloaded and install ObserveIT App from the IBM X-Force Exchange
- ObserveIT App communicates with your ObserveIT API directly, typically on port 443.
- ObserveIT (Minimum supported version 7.5.1)
- IBM QRadar (Minimum supported version 7.3.1)

DELPOYMENT ARCHITECTURE

The diagram shows how ObserveIT integrates into an on-prem IBM QRadar.



This shows an integration with QRadar On Cloud (QRoC).





Configuration

You configure ObserveIT App to reach the ObserveIT REST API and retrieve report data.

CREATING APPLICATION IN OBSERVEIT

To integrate ObserveIT with IBM QRadar using RESTful API, you register the application to authenticate access. Oauth2 is the method of authenticating access to the ObserveIT RESTful API.

This procedure describes how to generate a token that you use when you configure ObserveIT TA for QRadar.

1. From the ObserveIT Web Console, click the **1** in the upper-right corner and select **Developer Portal** from the menu.

Notes:

If the **Developer Portal** is not installed by default, you will be prompted to install it.

If the **Developer Portal** fails to properly load, log out of the ObserveIT console and log back in with a local system account rather than an LDAP account.

2. From the **Developer Portal**, select **Credentials** and then click the **Create App** button.

observe <mark>it</mark>			
Elbrary Report API	+ Create App		
Report Analytics API	Application name	Application Id	
Auth API	Splunk	1B617CCD-9952-48F2-8802-24290B5D2B1D	÷/=
Control API	test	B8E27226-3192-432C-BF62-C9F4FC103179	4×1
Activity API			-
Credentials	•		
Documentation			
Getting Started			
Resource Query Language			
Code Examples			
Legal			

The **Create Application** dialog box displays. This is where you register the application.



Create Application	×
Application Name	
qradar	
Allowed Scopes separate by space for multiple scopes, example itreport:*	
*	
Allowed Grants	
✓ Client Credentials	
Password	
Authorization Code	
Refresh Token	
Implicit	
Redirect URIs used for authorization_code and token(implicit) flows	
Redirect URI	
Redirect URI	
Redirect URI	
Cancel Save	

- 3. Do the following:
 - a. In the **Application Name** field, enter a name. It is recommended that you choose a name you can recognize, such as **QRadar**, **QRadar1** etc.
 - b. In Allowed Grants, check Client Credentials.
 - c. Click **Save** and the application is added to the list.



observe <mark>it</mark>			
Library Report API	+ Create App		
Report Analytics API	Application name	Application Id	
Auth API	Splunk	1B617CCD-9952-48F2-8802-24290B5D2B1D	チメ 盲
Control API	test	B8E27226-3192-432C-BF62-C9F4FC103179	4 × 📋
Activity API	qradar	2839002C-8F9F-4037-8D9B-D9CE273BE82C	ケノ言
Credentials			
Documentation			
Getting Started			
Resource Query Language			
Code Examples			
Legal			

4. Click the application you just created. The dialog box for generating a token displays.

qradar	×
Grant Type	
client_credentials -	
Client Id	
2839002C-8F9F-4037-8D9B-D9CE273BE82C	
Client Secret	
FTm6qK85SSc1hltPdH3doUqbgTg3mBMTuWdvkSuhHq	
Scope	
*	
Close	Generate Token

Note the **Client Id** and **Client Secret** values. You will enter them into the configuration screen of the **QRadar add-on**. (See: <u>Configuring ObserveIT App for QRadar</u>.)

CONFIGURING OBSERVEIT APP FOR QRADAR

This procedure describes the registration process in QRadar.



Your ObserveIT instance(s) needs to be registered in the ObserveIT QRadar app. The access token (with the **Client ID** and **Client Secret**) you generated in the ObserveIT **Developer Portal** will be used to authenticate with the API.

1. Open the QRadar Admin screen and scroll down to the bottom. Click the **ObservelT** icon.



The list of ObserveIT instances displays.



ol	oserve <mark>it</mark>		
	Observel	IT Instances	
_	+ Hostname or IP	User Activities 🗘	Alerts \$
	No data a	vailable in table	

2. Click the + button to add your ObserveIT instance.

Configure ObserveIT Instance	×
ObserveIT URL	
https://myobserveit.com	
Verify SSL Certificate	
Client ID	
0EECE782-4DE6-47BB-BBF6-145A635F65	
Client Secret	
Poll Interface Activities	
Poll Command Activities	
Poll Alerts	
Exclude fields with PII	
Save Test C	Cancel

- 3. Complete the **Configure ObserveIT Instance** dialog box.
 - a) Enter the **Client ID** and **Client Secret** values that you copied previously. (See: Creating Application in ObserveIT.)
 - b) Verify SSL Certificate: If your ObserveIT instance is using a self-signed certificate and you are unable to assign it a trusted one, then uncheck the Verify SSL Certificate box. Note that this is a less secure option



- c) Exclude fields with PII: If checked, then any fields that might contain Personally Identifiable Information are not be loaded into QRadar.
 Note: The following fields will be excluded from the user activity and alert data: loginName, secondaryLoginName, endpointName, remoteHostName, windowTitle, accessedUrl, domainName, secondaryDomainName, remoteAddress, sqlUserName
- 4. Click Test before saving to verify the connection between QRadar and ObservelT.

QRADAR ON CLOUD

This section describes the requirements for configuring the ObserveIT app for QRadar in a QRoC environment. A Data Gateway must be installed on your local network to allow the HTTP(S) API requests from the ObserveIT QRadar app to connect to the ObserveIT web console.

1. In the QRoC Admin Console, select "QRoC Self Service".



2. Click Add to add a new proxy mapping.



Filter by Gateway	Search proxyma	pping		o Q	A
	Name	CIDR	Gateway	Status	
G					

3. Configure a proxy mapping to the ObserveIT Web Console and test the connection.

				×		
Home / Data Gateway Proxy Ma Data Gateway Pro	pping oxy Mapping		Proxy Mapping Details Name: Observent			
Filter by Gateway	Search proxymappin		0100			
	Name	CIDR	172.0.0.5/32			
			Gateway:			
			QRadarECG			
			Testing connection:			
			Enter an IP and Port and click the test button to test connection			
			IP Address Port			
			172.0.0.5 443 Test			
			Connection succeeded			
			Close Delete Ed	t i		



4. Configure the ObserveIT app, using the IP address as the hostname in the URL. Unless your ObserveIT certificate has the IP address specifically included as a valid subject alt name, you will need to uncheck the Verify SSL Certificate option.

Configure ObserveIT Insta	nce	3
ObserveIT URL		
https://172.0.0.5		
Verify SSL Certificate		
Client ID		
XXXXXXXXX		-
Client Secret		
•••••		4
Poll Interface Activities		
Poll Command Activities		
Poll Alerts		
Exclude fields with PII		
	Save T	est Cancel

For more details, please visit the IBM Knowledge Center.

https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.qradar.doc_cloud/c_qross_proxy mapping.html

Usage

APPLICATION TUNING

ObserveIT custom properties: Enable indexing and update the pre-parse settings according to the searches and reports you need.

Offenses: By default, all user sessions with one or more High or Critical level alerts will generate an offense, using the session ID as the offense source. You can customize and configure the rules. You may choose to use the loginName or ruleCategory as the offense source depending on how you prefer to manage offenses and investigate alerts.

VIEWING EVENTS

You view events logged as soon as ObserveIT data collection is configured and enabled.



In the Log Activity screen, you see events coming in from the ObserveIT Log Source Group. All fields in the events are parsed into custom event properties.

Dashbo	ard Offenses	Log Activity	Network Activity	Assets R	eports	Risks	Vulnerabilities			System	Time: 5:40 PM
Search	V Quick Searches V	Add Filter	Nave Criteria 🛛 🖗	Save Results 🔗	Cancel 4	✤ False Positive	Rules V Ac	tions ¥			II @
Quie	k Filter 👻									Sea	rch
Curre Log	ent Filters: Source Group is Ob	Viewin servelT (Cle	g real time events ear Filter)	View: Se	elect An	Option: 👻	Display:	Default (Normalized) 🔻			
	Event Name		Log Source	Eve	ent	Time		Low Level Category	Source IP	Source Port	Destinat
	ObservelT User Activi	ity Obse	rveIT_UserInterface	Activity	1 Nov	29, 2018, 5:38	8:48 PM	User Behavior	49.57.50.46	0	169.254.3.3
	ObserveIT User Activi	ity Obse	rveIT_UserInterface	Activity	1 Nov	29, 2018, 5:38	8:48 PM	User Behavior	\$\$ 49.57.50.46	0	169.254.3.3
	ObservelT User Activi	ity Obse	rveIT_UserInterface	Activity	1 Nov	29, 2018, 5:38	8:48 PM	User Behavior	49.57.50.46	0	169.254.3.3
	ObserveIT Alert	Obse	erveIT_Alert_V2		1 Nov	29, 2018, 5:38	8:29 PM	Sense Offense	\$\$ 49.57.50.46	0	169.254.3.3
	ObserveIT Alert	Obse	rveIT_Alert_V2		1 Nov	29, 2018, 5:38	8:29 PM	Sense Offense	49.57.50.46	0	169.254.3.3

From the **Event Details** screen for either User Activity or Alert events, you can click the **View Playback** button to go directly to the player in ObserveIT.

Dashboard Offenses	Log Activity	Network Activity	Assets R	leports Risks	Vulnerabilities					
Return to Event List o	ffense 📀 Map Event	k False Positive	C Extract Proper	ty 🕜 Previous	🔮 Next 🛛 📇 Print	Obfuscation ▼	t View Playback			
Event Information						1				
Event Name	ObserveIT Alert									
Low Level Category	Sense Offense									
Event Description	ObserveIT Alert									
Magnitude			(7)	Relevance	7			Severity	8	Cre
Username	kathy									
Start Time	Nov 29, 2018, 5:3	9:29 PM		Storage Time	Nov 29, 2018, 5	:39:29 PM		Log Source Time	Nov 2	29, 20
Command (custom)	null									
accessedSiteName (custom)	google.com									
accessedUrl (custom)	https://www.google	e.com/gmail/abou	t/#							

Example of player:







DASHBOARD

You can use the QRadar dashboard to review the ObserveIT data.

≡ IBM QRadar			
Dashboard Offenses Log Activity Network Activity Assets	Reports Risks Vulnerabilities		System Time: 7:09 PM
Show Dashboard: ObserveIT Dashboard \$	New Dashboard 💦 Rename Dashboard 😢 Delete Dashboard Add Item 🔻		Next Refresh: 00:00:40 👖 🗾 🥥
ObservelT Top Risky Users (Count)	ObserveIT Top Alert Categories (Count)	888	ObserveIT Most Used Applications (Count)
6/20/18 7:09 PM - 6/21/18 7:09 PM 6 4 2 0 v Legend Vew in Log Activity Vew in Log Activity	20 % 20 % 20 % 60 % Vegend UNACCEPTABLE USE UNAUTHORIZED DBA ACTIVITY DATA EXF Vervin Log Activity	6/20/16 7:09 PM - 6/21/18 7:09 PM	6/20/18 7:09 PM - 6/21/18 7:09 PM
ObservelT Endpoint Activity (Count)	ObservelT Visited Sites (Count)		View in Log Activity
6/20/18 7:09 PM - 6/21/18 7:09 PM		6/21/18 7:09 AM - 6/21/18 7:09 PM	
300	accessedSiteName (custom)	Count	
	test.com	58	
	observeit.com	31	
200	tes.com	2	
	amazonmr.au1.qualtrics.com	1	
	h	1	
100	res	0	
	View in Log Activity		
T and			
- Legeno			
View in Log Activity			

CONFIGURING THE DASHBOARD

To enable the dashboard, you need to configure the Saved Searches.

For each dashboard item, click on the Settings button, then check Capture Time Series Data and click Save.

Show Dashboa	rd:(ObserveIT Dashboard \$)	🗋 New Dashboard 🛛 Prename Dashboard 🛛 S Delete Dashboard 🛛 Add Item 🔻	Refresh Paused: 00:01:00 🕨 🥰 🌘			
ObservelT To	p Risky Users (Count)	ObserveIT Top Alert Categories (Count)	ObserveIT Most Used Applications (Count)			
10	11/22/18 5:26 PM - 11/29/18 5:26 PM Accumulation began 11/29/18 1:58 PM	Value lo Graph: Count Count Chart Type: Bar Chart Chart Display Top: 10 Capture Time Series Data: Save Time Range: Last 3 Days Capture Time Series Data: Count Cou				
5	7 Time Series Data	No results were returned for this item. <u>View in Log Activity</u>	No results were returned for this item			
Time Series Configuration update completed. To include this configuration in your saved search criteria, first close this popup. Click the 'View in Log Activity' or 'View in Network Activity' link below the dashboard item you just saved. On the new page, click 'Save Criteria' from the top tool bar.						
			ÜK			



From the prompt, click View in Log Activity link and the Save Criteria dialog box displays.

Please enter the name of this search below.	Assign Search to Gro	oup(s) 📄 Manage Grou	lps		
Search Name: ObserveIT Top Alert C	Authentica	tion, Identity and User , es is nti\/inus	Activity		
Timespan options:					
Cast Interval (auto refresh)	Specific Interva	I			
	Start Time	11/26/2018	-	5:27 PM	Ŧ
	End Time	11/29/2018	Ŧ	5:27 PM	Ŧ
Include in my Quick Searches	Set as De	efault			

In the Timespan options, select Recent and click OK.

Support

For help using the ObserveIT platform or the ObserveIT App for IBM QRadar, please contact the ObserveIT support organization.

https://www.observeit.com/support/

You can also send an email to <u>integrations@observeit.com</u> with questions about this and other ObserveIT integrations.

Not a customer yet? Start your Free Trial of ObserveIT today!

Free Trial

Start your free trial with ObservelT today. Detect and prevent insider threats in minutes. Reduce your risk, speed up investigations, and streamline compliance.



Release notes

Version	Date	Notes		
2.0.0	2018-11-29	•	New:	
			0	Example Dashboard and Rules
		•	Improved:	
			0	Use new V2 REST API to retrieve events
	2019-05-15	•	New:	
			0	QRoC supported