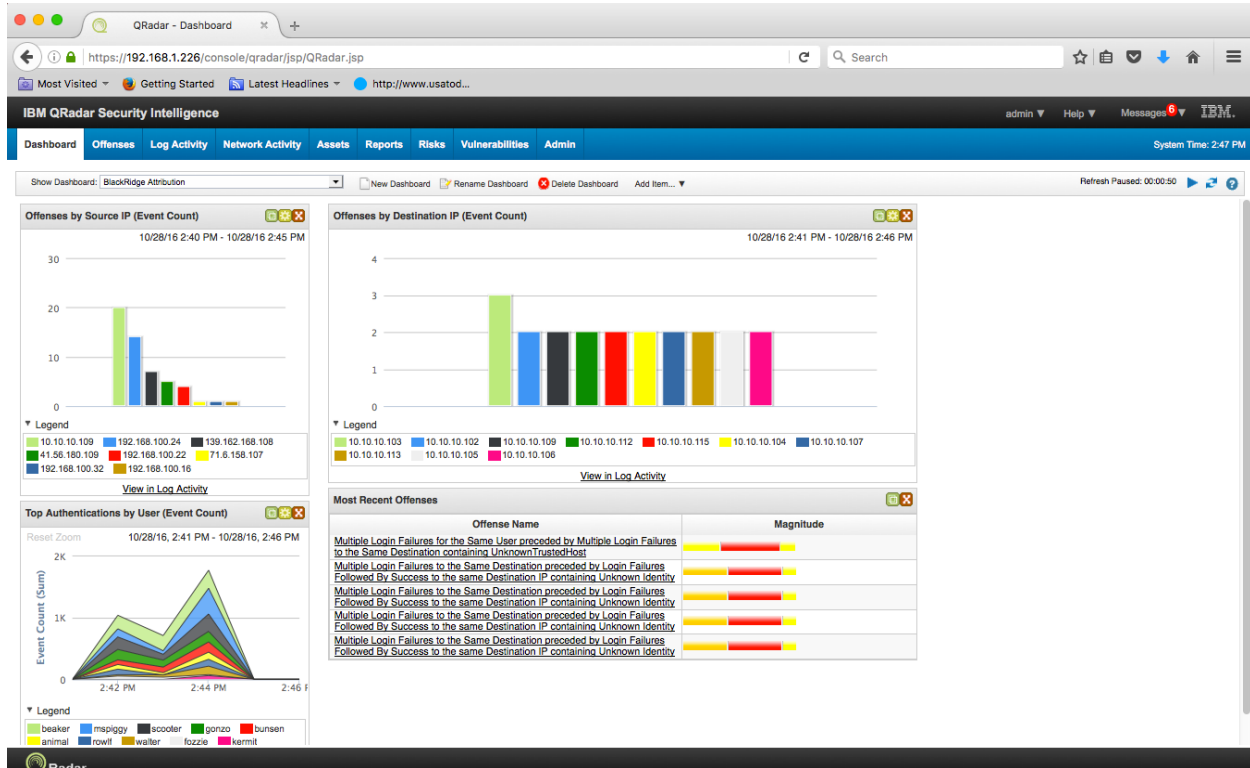


BlackRidge Application for IBM Security QRadar SIEM

Introduction

The BlackRidge App for QRadar enables the processing of BlackRidge TAC Gateway Syslog messages about network connection attempts.



Supported QRadar versions:

- 7.2.8

The BlackRidge App for QRadar enables the processing of BlackRidge security messages. This provides identity attribution of unauthorized network connection attempts to QRadar to enable the earliest possible detection, by administrators, of potential breaches, and compromised or rogue insiders and third parties. The app comes with a predefined set of dashboards which provide ready-made graphs for popular Syslog messages from BlackRidge gateways.

Installation

The following are the prerequisites for installing the BlackRidge App for QRadar:

- BlackRidge TAC Gateway v3.0 or higher
- Admin account to BlackRidge TAC Gateway
- QRadar admin username and password

Install the BlackRidge TAC Gateway App for QRadar from [IBM App Exchange for QRadar](#)

Gateway Configuration

Run the following steps on your BlackRidge TAC Gateway as the admin user:

- `/etc/syslog/add`
 - Purpose: Add a remote Syslog server entry
 - Options
 - name - the label for the Syslog entry for configuration management in the BlackRidge Gateway
 - server - the IP address to send Syslog messages to
 - port - the port to send the Syslog messages to (Default is 514)
 - pri - the priority to send - recommend using "all"
 - Example: `/etc/syslog/add name=QRadar_Server server=192.168.1.75 port=514 pri=all`

```
[admin@BRGW-40[bump0]]:/etc/syslog/> add name=QRadar_Server server=19.168.1.75 port=514 pri=all
The syslog rule was successfully added.
Syslog was successfully restarted.
[admin@BRGW-40[bump0]]:/etc/syslog/> show

Syslog Format: LEEF (IBM standard)
Syslog Debug: Disabled

# Name          Facility      Priority      Server        Port
1 QRadar_Server kern,local0   *            19.168.1.75   514
admin@BRGW-40[bump0]]:/etc/syslog/>
```

- `/etc/syslog/cfg`
 - Purpose: Configure the format of the Syslog message
 - Options
 - No options - running this command will prompt a menu
 - Example: `/etc/syslog/cfg`

```
[admin@BRGW-40[bump0]]:/etc/syslog/> cfg

Please choose which format you want for syslog entries:
    0 - BlackRidge default
    1 - LEEF (IBM standard)
[Number associated with the format you wish to use? 1
The syslog format was successfully configured.
admin@BRGW-40[bump0]]:/etc/syslog/>
```

QRadar Configuration

- Download the BlackRidge App for QRadar zip file to a local drive on your computer
- Login to QRadar UI
- Click on the 'Admin' tab
- Click on 'System Configuration' 'Extensions Management'
- In the 'Extensions Management' window, click on the 'Add' button in the top right corner
- Click on 'Browse' and find the BlackRidge App for QRadar zip file.
- Click on 'Add'
- Review the content that will be installed as part of the extension and click on 'Install'.
- In the 'Admin' tab, click on 'Data Sources' 'Log Sources'
- Click on 'Add'
- Enter the Log Source details as shown in this screenshot

Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources.

Log Source Name	BlackRidge Simulator
Log Source Description	BlackRidge Simulator
Log Source Type	BlackRidge App for QRadar
Protocol Configuration	Forwarded
Log Source Identifier	172.19.13.2
Enabled	☒
Credibility	5
Target Event Collector	eventcollector0 :: qradar
Coalescing Events	☒
Incoming Payload Encoding	UTF-8
Store Event Payload	☒
Log Source Language	
Log Source Extension	BlackRidgeTACGatewayCustom_ext
Extension Use Condition	Parsing Override

Please select any groups you would like this log source to be a member of:

- Change the 'Log Source Identifier' to the IP address of the BlackRidge TAC Gateway or the server running the BlackRidge Syslog Simulator
- Click on 'Save'
- In the 'Log Sources' window, click on the log source you just created and ensure that the "Enabled" field shows True. If it displays 'False', click on the 'Enable/Disable' button to Enable your log source

Search For: All Log Source Groups ☒ Enable/Disable ☒ Delete

☒ Extensions ☐ Parsing Order ☒ Assign

You have 1 of an allowable 750 active Log Sources as defined by your license

Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier
BR	BR	Error	Syslog		BlackRidgeTACGateway	True	172.19.13.3
Threeco...	Threeco...	Disabled	Syslog		3Com 8800 Series Switch	False	127.0.0.1
VPNGat...	VPNGat...	Disabled	Syslog		Nortel VPN Gateway	False	172.19.13.2
VPNGat...	VPNGat...	Disabled	Syslog		Nortel VPN Gateway	False	172.19.13.3

- If your BlackRidge Gateway or simulator is now run with the QRadar IP Address as the Syslog destination, you should start seeing events under 'Log Activity' tab.

IBM QRadar Security Intelligence										admin ▾ Help ▾		Messages 5 ▾ IBM.					
Dashboard		Offenses		Network Activity		Assets		Reports		Risks		Vulnerabilities		Admin		System Time: 5:15 PM	
Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾																	
Trusted Host NoAuth Accept	BR	1 Jan 6, 2017, 5:15:44...	Access Permitted	192.168.100.40	51328	10.10.10.202	80	scooter									
Trusted Host NoAuth Accept	BR	1 Jan 6, 2017, 5:15:44...	Access Permitted	192.168.100.40	51328	10.10.10.203	80	scooter									
Trusted Host NoAuth Accept	BR	1 Jan 6, 2017, 5:15:44...	Access Permitted	192.168.100.40	51328	10.10.10.200	80	scooter									
Trusted Host NoAuth Accept	BR	1 Jan 6, 2017, 5:15:44...	Access Permitted	192.168.100.40	51328	10.10.10.201	80	scooter									
Unknown Trusted Host	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	213.24.132.109	22	none									
Key No Longer Active	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	213.24.132.109	80	N/A									
Unknown Trusted Host	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	41.56.180.109	22	none									
Key No Longer Active	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	41.56.180.109	80	N/A									
Protected Resource Insert	BR	1 Jan 6, 2017, 5:15:44...	Access Permitted	192.168.100.40	51328	10.10.10.115	22	scooter									
Unknown Identity	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	192.168.100.40	51328	10.10.10.115	22	none									
Unknown Trusted Host	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	41.56.180.104	22	none									
Key No Longer Active	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	41.56.180.104	80	N/A									
Unknown Trusted Host	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	41.56.180.105	22	none									
Key No Longer Active	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.115	51328	41.56.180.105	80	N/A									
Trusted Host Insert	BR	1 Jan 6, 2017, 5:15:44...	Access Permitted	192.168.100.40	51328	10.10.10.115	22	scooter									
Protected Resource Accept	BR	1 Jan 6, 2017, 5:15:44...	Access Permitted	192.168.100.40	51328	10.10.10.115	22	scooter									
Unknown Trusted Host	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.114	51328	213.24.132.109	80	none									
Key No Longer Active	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.114	51328	213.24.132.109	80	N/A									
Unknown Trusted Host	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.114	51328	41.56.180.109	80	none									
Key No Longer Active	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.114	51328	41.56.180.109	80	N/A									
Key No Longer Active	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.114	51328	41.56.180.104	80	N/A									
Unknown Trusted Host	BR	1 Jan 6, 2017, 5:15:44...	Access Denied	10.10.10.114	51328	41.56.180.105	80	none									

License

This IBM Security App Exchange Partner Agreement ("Agreement") between BlackRidge Technology, Inc ("BLACKRIDGE" or "Supplier") and International Business Machines Corporation ("IBM") establishes the terms between the parties for Licensed Works provided to IBM and its Affiliates to be made available and distributed by IBM and its Affiliates to its customers ("Published") via the IBM Security App Exchange("Exchange").