

IBM® Storage

Cyber Resilient Infrastructure Detect, Protect, and Mitigate Threats Against Brocade SAN FOS with IBM QRadar

IBM Storage Team



© Copyright International Business Machines Corporation 2022.

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

Contents

About this document	1
Executive summary	1
Scope	2
Introduction	2
Brocade SAN Fabric Operating System	2
IBM QRadar	3
Prerequisites	3
Solution overview	4
Control path use cases	5
Lab setup	5
Sample use case demonstration	13
Summary	16
About the author	16
Acknowledgments	16
Resources	16
Notices	17
Trademarks	18
Terms and conditions for product documentation	19
Applicability	19
Commercial use	19
Rights	19
Privacy policy considerations	19



About this document

Enterprise networks are large and rely on numerous connected endpoints to ensure smooth operational efficiency. However, they also present a challenge from a security perspective.

The focus of this Blueprint is to demonstrate an early threat detection against the network fabric that is powered by Brocade that uses IBM® QRadar®. It also protects the same if a cyberattack or an internal threat by rouge user within the organization occurs.

The publication also describes how to configure the syslog that is forwarding on Brocade SAN FOS. Finally, it explains how the forwarded audit events are used for detecting the threat and runs the custom action to mitigate the threat.

Executive summary

The financial effects of cyberattacks continue to rise. Cyberattacks can occur in various ways. They can take the form of malware or ransomware that is targeted at stealing confidential data or holding valuable information for ransom.

Sometimes, these attacks are designed to destroy confidential data to cripple organizations. In many cases, it was observed that the data breaches involve internal threat actors.

A *fabric* refers collectively to the equipment and configuration that implements a network. A *network fabric* describes the network topology in which components pass data to each other through interconnecting switches.

Brocade SAN switches are immensely popular because of the robustness, simplified configuration, and ease of management. To support most the Brocade switch implementations, IBM QRadar integrated the support for the events that were produced by SAN-FOS by using the QRadar device support module (DSM).

Detecting a threat before it starts can help speed recovery even more. IBM Security™ QRadar is a Security Information and Event Management (SIEM) and threat management system that monitors activities. It looks for signs that can indicate the start of an attack, such as logins from unusual IP addresses or outside business hours or multiple login failures from a single IP.

Scope

The focus of this publication is to proactively start a cyber resilience workflow from IBM QRadar to block an IP address when multiple failed logins on Brocade switch are detected.

As part of early threat detection, a sample rule that is used by IBM QRadar is shown. A Python script that also is used as a response to block the user's IP address in the switch is provided.

Customers are encouraged to create control path or data path use cases, customized IBM QRadar rules, and custom response scripts that are best-suited to their environment.

The use cases, QRadar rules, and Python script that are presented here are templates only and cannot be used as-is in an environment.

Introduction

Combining the capabilities of Brocade SAN FOS and IBM QRadar enables enterprises to build comprehensive cyber resilience solutions that address the Detect function of the NIST framework and the Respond and Protect function.

The Brocade SAN FOS can log all administrative activities in the access logs. To identify and detect potential malicious access and for compliance auditing purpose, such access logs must be integrated with the SIEM solution.

By combining Brocade SAN FOS administration access logs, application logs, network or server logs, flow and packet data IBM QRadar can provide complete protection for the enterprise data.

Brocade SAN Fabric Operating System

All Brocade switch products are based on a foundation of innovative, industry-leading core technologies that are built into the Brocade Fabric Operating System (FOS). This operating system manages all hardware resources, and processes is optimized to improve performance, efficiency, and availability of each switch and the fabric that is formed by the interconnected switches.

Brocade FOS enables the ability to proactively monitor millions of physical-layer, protocol-layer, and application-layer data points in real time. In combination with Brocade SANnav, it also translates the information that is gathered into actionable insights about the performance and health of the storage area network (SAN).

In addition, Brocade FOS supports various authentication, encryption, and management tools to protect fabrics and data from unauthorized access.

By partnering with IBM QRadar and their SIEM solutions, Brocade SANs can be further integrated into a user's secure infrastructure strategy.

IBM QRadar

IBM® QRadar® is a leading Security Information and Event Management (SIEM) solution that can monitor, inspect, detect, and derive insights for identifying potential threats to the data that is stored on IBM Spectrum® Scale-managed systems. It is one of the most popular SIEM solutions on the market today. It provides powerful cyber resilience and threat detection features, such as centralized visibility, flexible deployment, automated intelligence, machine learning, and proactive threat hunting.

The data management and storage features of IBM Spectrum Scale, combined with the log analysis, deep inspection, and detection of threats that are provided by IBM QRadar, offer an excellent platform for hosting unstructured business data, reducing the effect of cyberthreats, and increasing cyber resilience.

IBM QRadar can detect malicious patterns by using several data sources and analysis tools and techniques. These tools include access logs, heuristics, and correlation with logs from other systems, such as network logs or server logs, network flow and packet data, and even unknown threat vector detection by using IBM Watson® for Security resources. Its open architecture enables third-party interoperability so that many solutions can be integrated, which makes it even more scalable and robust.

Prerequisites

The following prerequisites must be met for the solution:

- A user with Administrator privileges is created on the Brocade switch or centralized authentication, such as LDAP or Active Directory. This user is used by IBM QRadar® system to securely log on to storage system by using SSH to perform various actions. We suggest creating qradaradmin user for this task.
- Password-less authentication is set up between IBM QRadar and Brocade switch, which is the public key from a user on IBM QRadar that is added to the qradaradmin user that is defined on Brocade SAN FOS. Figure 3 on page 5 shows the `sshutil` command, which is used to perform this action at the switch.
- To authenticate the qradaradmin user by using the public key that is shared with Brocade SAN FOS, the private key of the same user from IBM QRadar is added to `/opt/qradar/bin/ca_jail/home/customactionuser/.ssh` folder.
- The firewall rules between IBM QRadar and Brocade SAN FOS are adjusted to allow traffic on 514/tcp or 514/udp.

Note: IBM QRadar accepts incoming events on both TCP/UDP protocols on port 514. The choice of the protocol that is used for communication depends on the organization's guidelines.

Solution overview

Organizations can face threats in multiple ways: compromised user credentials by using sphere fishing attack, a rouge user within the organization, or cyberattacks, such as brute force attempts or ransomware. Any of these threats poses grave risks to the infrastructure that is used within an organization.

Fabric or network components are the backbone of any infrastructure. Although it is not common for normal users to access the switch hardware, nothing stops a curious or threat actor from unknowingly or knowingly starting a brute force attack.

Figure 1 shows a typical infrastructure within the organization, wherein the application hosts and storage are connected by using fabric interconnects.

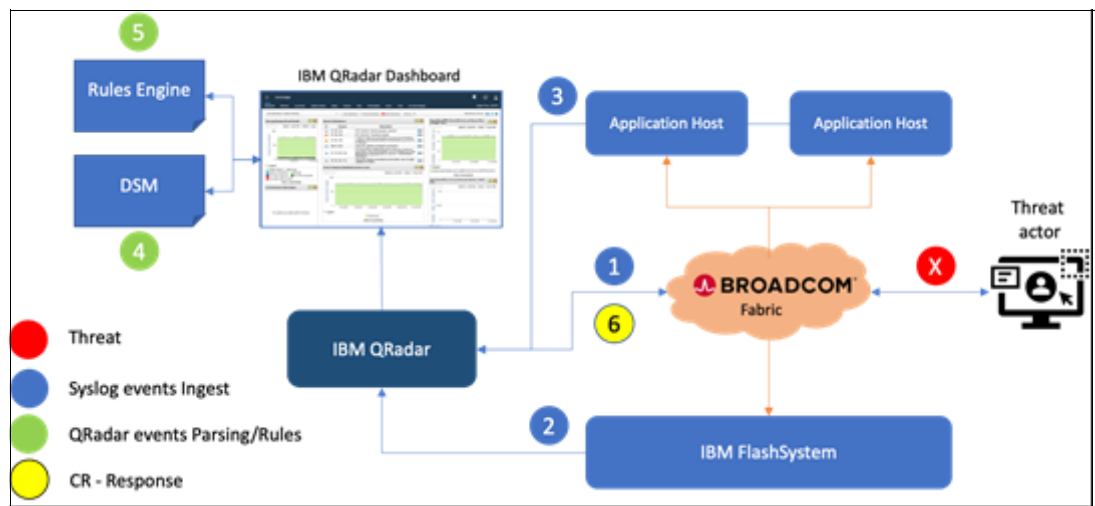


Figure 1 Solution overview

As part of the solution to perform an early threat detection, the switch appliance is configured to forward the audit logs by using syslog configuration. Also, the audit or system logs are forwarded from IBM FlashSystem® and other hosts within the infrastructure.

Armed with the audit information from all devices, IBM QRadar now has a complete view of device topologies. Any threat that originates from any of the devices can now be detected in real time.

When a curious user or a threat actor makes multiple failed login attempts to the switch appliance, IBM QRadar receives the failed login attempt as event. IBM QRadar's device support module supports Brocade SAN FOS immediately. The data from the received events is automatically parsed, stored in the local database, and presented in the QRadar dashboard in a tabular format under various headings.

Because the information is now locally available, IBM QRadar's rules wizard is used to create various rules to match the threat and start a predefined response. In our example, because the received events were from failed login attempts, the IP address that is associated with the events was blocked so no further connections can be made.

To block the IP address, a Python script is used to log on to the switch and create a switch policy with a "deny" rule specification for the program that was used in login attempt.

In the following sections, we discuss various use cases in which these responses can be repeated.

Control path use cases

Some of the threats that otherwise go unnoticed are described in this section. Although the following list is not exhaustive, but these threats can be used as a starting point by the security or compliance officer. Attacks on switch infrastructure are uncommon, but cannot be entirely ruled out:

- Multiple failed login attempts by a user or administrator.
- Administrator logins outside business hours or a maintenance window.
- Same administrative user log in detected from different locations or IP address at the same time.
- A less privileged user attempts to elevate privileges by using administrator commands post login in the switch.

Lab setup

This section describes the steps that are involved in creating the lab setup.

Although most switches allow changes by using the CLI or REST API interfaces we used CLI commands in our lab setup. Therefore, access was enabled to port 22 to switch and a user with administrator privileges also was defined.

Complete the following steps:

1. Define a new administrator user on the switch. (In our example, we added the `qradaradmin` user.) You are prompted for the password during this creation process (see Figure 2).

```
ssh admin@129.40.101.137
IBM_2498_F48_110:admin> userconfig --add qradaradmin -r admin
```

Figure 2 Defining `qradaradmin` user in switch local database

2. Import the public key from the IBM QRadar host.

In this step, it is assumed that a public/private SSH key pair was generated on the IBM QRadar host (see Figure 3).

```
IBM_2498_F48_110:admin> sshutil importpubkey
Enter user name for whom key is imported: qradaradmin
Enter IP address: 129.40.101.137
Enter remote directory:/root/.ssh
Enter public key name(must have .pub suffix):id_rsa.pub
```

Figure 3 Importing QRadar root user's public key to `qradaradmin`

3. Create the syslog configuration to forward the audit log events to IBM QRadar host (see Figure 4).

```
IBM_2498_F48_110:admin> syslogadmin -set -ip 129.40.103.20 -port 514
-facility syslog.1
IBM_2498_F48_110:admin> syslogadmin --show -ip
syslog.1      129.40.103.20
```

Figure 4 Create syslog facility on the switch

Post-configuration of syslog facility on the switch, QRadar starts receiving events. QRadar's DSM support for SAN FOS appliances normalizes the event data on which the QRadar administrator defines rules to identify threat and starts a response. The following section shows these configuration changes on QRadar.

Configuring QRadar host

Complete the following steps:

1. Copy the private key of the IBM QRadar user to the `/opt/qradar/bin/ca_jail/home/customactionuser/.ssh` folder. Figure 5 shows the location and permissions on the `id_rsa` file.

```
[root@qradar /opt/qradar/bin/ca_jail/home/customactionuser/.ssh]# ls -la
total 16
drwx----- 2 customactionuser root      71 Jul  6 05:49 ./
drwxrwxr-x  3 customactionuser customactionuser 18 Jun 29 19:59 ../
-rw----- 1 customactionuser root      83 Jul  6 05:38 config
-rw----- 1 customactionuser root    3243 Jul  6 05:49 id_rsa
-rw----- 1 customactionuser root     756 Jul  6 05:55 id_rsa.pub
-rw----- 1 customactionuser root     531 Jul  6 01:39 known_hosts
```

Figure 5 The `.ssh` folder path for `customactionuser`

The private key must be copied because IBM QRadar creates a false root (chroot environment) to provide a pristine, yet isolated environment for user-provided scripts.

2. Log in to QRadar as the `admin` user and click the **Admin** tab. Then, click **Define Actions** under the **Custom Actions** section. Finally, click **Add** to define the custom action (see Figure 6).

Figure 6 Defining the custom action

- Under the scripts parameter section, define parameters under Fixed Property and Network Event Property (see Figure 7).

Script Parameters

Parameter Name:

☐ Fixed Property
☒ Network Event Property

Property:

Add
Remove Selected

Name	Type	Value
switch-ip-address	Fixed Property	129.40.101.137
offending-ip	Network Event Property	sourceip
offending-command	Network Event Property	Command

Figure 7 Script Parameters window

When defining the Network Event Property, the drop-down list provides different properties from which the administrator can choose. In our example, we restrict the selection choice only to sourceip and Command properties. Save all of the defined properties and acknowledge the dialog box to deploy the change.

- Click the **Admin** tab again and then, click **Deploy Changes** to deploy the script in the QRadar environment (see Figure 8).

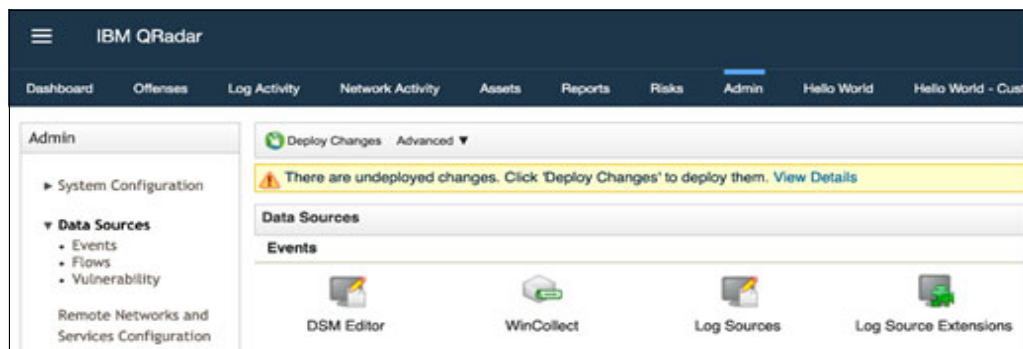


Figure 8 Deploying changes from Admin tab

- Click the **Log Activity** tab and then, click **Add filter** and enter the switch IP address as the value for the Source or Destination IP property (see Figure 9).

Figure 9 Adding filter to events only from switch IP address

Figure 10 shows the filtered events.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Successful logout	Brocade-129_40_101_137	1	Dec 10, 2021, 7:27:1...	Misc Logout	129.40.101.137	0	129.40.101.137	0	N/A	1
sshutil operation	Brocade-129_40_101_137	1	Dec 10, 2021, 7:23:4...	Information	129.40.101.137	0	129.40.101.137	0	N/A	1
sshutil operation	Brocade-129_40_101_137	1	Dec 10, 2021, 7:23:4...	Information	129.40.101.137	0	129.40.101.137	0	N/A	1
User Login	SIM Audit-2 :: gradar	1	Dec 10, 2021, 7:23:4...	SIM User Authentication	129.40.101.137	0	129.40.103.20	0	root	1
User Logout	SIM Audit-2 :: gradar	1	Dec 10, 2021, 7:23:4...	SIM User Authentication	129.40.101.137	0	129.40.103.20	0	root	1
A command was executed on console	Brocade-129_40_101_137	1	Dec 10, 2021, 7:21:3...	Information	129.40.101.137	0	129.40.101.137	0	N/A	1

Figure 10 Filtered events

- Click **Rules** and choose the **Rules menu** option to open the Rules window. Click **Actions** and choose the **New Event Rule** menu option (see Figure 11).

Figure 11 Choosing the New Event Rule option

- In the rules wizard window, click the **Events** radio button to define an event rule and then, click **Next** to start the Rules Wizard Stack Editor.

- The Rules Test Stack Editor window shows various rules, which includes the option to define conditions. Use the (+) sign in the green circle to add the rule. Any condition object, such as these log sources, is shown as a hyperlink (see Figure 12).

Figure 12 Rule Test Stack Editor window

When the value or condition is selected or applied, the condition object is changed to reflect the value (see Figure 13).

Figure 13 Rule completed with condition object or value

When choosing the value for QID object, make sure to select the QID number that matches the QID value that is shown on the event (see Figure 14).

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Failed Login	Brocade-129_40_101_137	1	Dec 12, 2021, 11:44:...	User Login Failure	9.43.49.96	0	129.40.101.137	0	N/A	High

Event Information									
Event Name	Failed Login								
Low Level Category	User Login Failure								
Event Description	Indicates a failed login attempt occurred.								
Magnitude	High	(3)	Relevance	1	Severity	3	Credibility	5	
Username	N/A								
Start Time	Dec 12, 2021, 11:44:14 PM	Storage Time	Dec 12, 2021, 11:44:14 PM	Log Source Time	Dec 12, 2021, 11:44:14 PM				
Command (custom)	ssh								
Domain	Default Domain								

Additional Information			
Protocol	255	QID	77502065
Log Source	Brocade-129_40_101_137	Event Count	1

Figure 14 QID value for a specific event

Figure 15 shows a fully defined rule in the Rules Stack Editor window.

The screenshot shows the 'Rule Wizard: Rule Test Stack Editor' window. At the top, it asks 'Which tests do you wish to perform on incoming events?' with a 'Test Group' dropdown set to 'All' and an 'Export as Building Block' button. Below this is a list of tests with checkboxes and green checkmarks. The selected test is 'when at least this many events are seen with the same event properties in this many minutes'. Below the list, there is a section for the rule definition: 'Rule (Click on an underlined value to edit it). Invalid tests are highlighted and must be fixed before rule can be saved.' The rule is defined as 'Apply block-ip-post-multiple-failed-logins on events which are detected by the Local system'. It includes three conditions: 'and when the event(s) were detected by one or more of Brocade-129_40_101_137', 'and when the event QID is one of the following (77502065) Failed Login', and 'and when at least this many events are seen with the same event properties in this many minutes'. Below the rule definition, there is a section for selecting groups: 'Please select any groups you would like this rule to be a member of:'. The groups listed are Anomaly, Asset Reconciliation Exclusion, Authentication, Botnet, and Category Definitions. At the bottom, there is a 'Notes' section with the text 'Brute force login attempt detected'. The bottom of the window has navigation buttons: '<< Back', 'Next >>', 'Finish', and 'Cancel'.

Figure 15 Fully defined rule with notes

9. Click **Next** to define the Rule Action attributes, such as Severity, Credibility, Relevance, and Offense, that are based on event-violating attributes. Use the same window to define the Rule Response. In our example, we select the **block-ip** Custom Action (see Figure 16). This custom action was added earlier.

The screenshot shows the 'Rule Wizard: Rule Response' window. It is divided into four main sections:

- Rule Action**: This section is for choosing the action(s) to take when an event occurs. It includes checkboxes for Severity, Credibility, and Relevance, each with a 'Set to' dropdown and a value of 4. There is also a checkbox for 'Ensure the detected event is part of an offense'. Below this, there is a dropdown for 'Index offense based on' set to 'Source IP', a checkbox for 'Annotate this offense' with the value 'Offending IP Blocked', and a checkbox for 'Include detected events by Source IP from this point forward, in the offense, for : 300 second(s)'. At the bottom of this section are checkboxes for 'Annotate event' and 'Bypass further rule correlation event'.
- Rule Response**: This section is for choosing the response(s) to make when an event triggers this rule. It includes checkboxes for 'Dispatch New Event', 'Email', 'Send to Local Syslog', 'Send to Forwarding Destinations', 'Notify', 'Add to a Reference Set', 'Add to Reference Data', 'Remove from a Reference Set', 'Remove from Reference Data', 'Trigger Scan', and 'Execute Custom Action'. The 'Execute Custom Action' checkbox is checked, and the 'Custom Action to execute' dropdown is set to 'block-ip'.
- Response Limiter**: This section is for configuring the frequency with which you want this rule response to respond. It includes a checkbox for 'Respond no more than 1 time(s) per 10 minute(s) per Rule', which is checked.
- Enable Rule**: This section includes a checkbox for 'Enable this rule if you want it to begin watching events right away.', which is checked.

Figure 16 Defining rule attributes

10. Click **Next**. The last window that is shown here is the Rule Summary window, which displays the rule (see Figure 17).

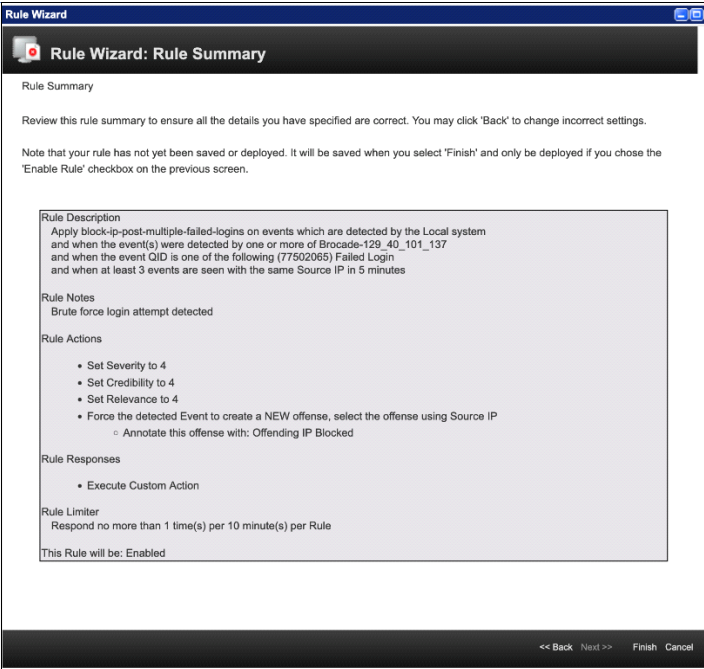


Figure 17 Rule Summary window

Understanding log source

This section describes how to work with the log source, which is automatically defined for audit events that are received from Brocade SAN FOS.

When log forwarding is enabled on Brocade SAN FOS by using the `syslogadmin` command, IBM QRadar starts receiving the events. The received events are listed in IBM QRadar’s Log Activity window (see Figure 18).

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
ipfilter policy(ies) saved	Brocade-129.40.101.137	2	Nov 12, 2021, 4:18:58 AM	Policy Change	129.40.101.137	0	129.40.101.137	0	N/A	100
A command was executed on console	Brocade-129.40.101.137	6	Nov 12, 2021, 4:18:53 AM	Information	129.40.101.137	0	129.40.101.137	0	N/A	100
Successful logout	Brocade-129.40.101.137	2	Nov 12, 2021, 4:18:54 AM	Misc Logout	129.40.101.137	0	129.40.101.137	0	N/A	100
Previous message repeated	Brocade-129.40.101.137	1	Nov 12, 2021, 4:18:58 AM	Information	129.40.101.137	0	129.40.101.137	0	N/A	100
Successful Login	Brocade-129.40.101.137	1	Nov 12, 2021, 4:18:56 AM	User Login Success	129.40.103.20	0	129.40.101.137	0	N/A	100
Successful Login	Brocade-129.40.101.137	1	Nov 12, 2021, 4:18:53 AM	User Login Success	129.40.103.20	0	129.40.101.137	0	N/A	100
Failed Login	Brocade-129.40.101.137	1	Nov 12, 2021, 4:18:51 AM	User Login Failure	9.206.136.159	0	129.40.101.137	0	N/A	100
Failed Login	Brocade-129.40.101.137	1	Nov 12, 2021, 4:18:47 AM	User Login Failure	9.206.136.159	0	129.40.101.137	0	N/A	100

Figure 18 IBM QRadar Log Activity window

To see the log source definition, click the **Admin** tab, and then, select the **Log Source** option. A list is displayed that includes user-defined and automatic log sources that are available on the system. Select the row that matches the log source name and click **View**. The automatically defined log source for Brocade SAN FOS is shown (see Figure 19).

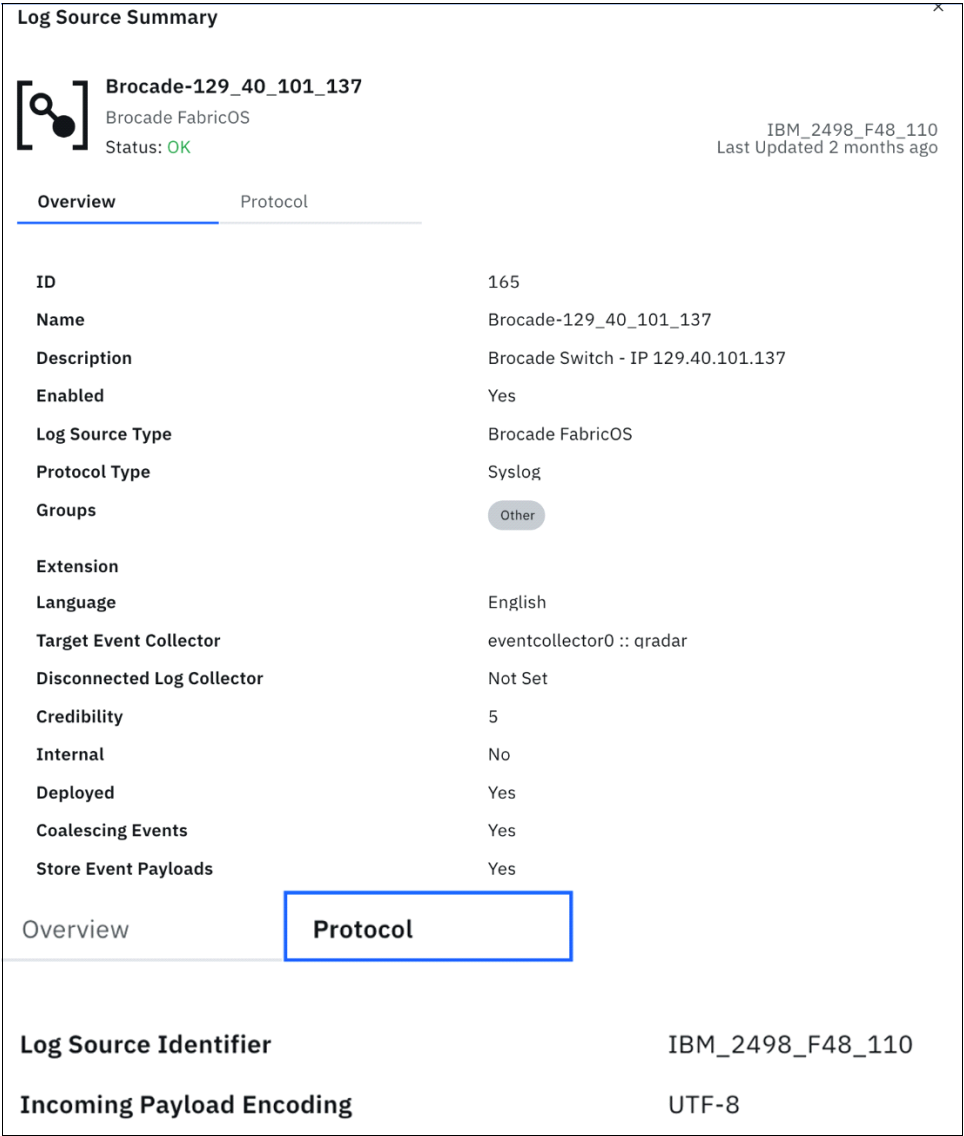


Figure 19 QRadar Log Source Summary window

Sample use case demonstration

To demonstrate the cyber resiliency workflow by using the configuration that we built so far, a sample use case of a brute force login attack was generated from within the network.

After the QRadar rules engine identifies the threat, it starts the predefined response. The response in this case is to block the offending IP address by defining a new switch policy that is based on the active policy.

The new policy that is defined includes the deny rule for the offending IP and includes another rule to enable logging in from any IP by using the same protocol.

Figure 20 shows the policies that are active on the switch.

```
[root@qradar ~]# ssh qradaradmin@129.40.101.137
IBM_2498_F48_110:qradaradmin> ipfilter --show

Name: default_ipv4, Type: ipv4, State: active
Rule    Source IP          Protocol  Dest Port  Action
1       any                    tcp       22         permit
2       any                    tcp       23         permit
3       any                    tcp       80         permit
4       any                    tcp       443        permit
5       any                    udp       161        permit
6       any                    udp       123        permit
7       any                    tcp       600 - 1023 permit
8       any                    udp       600 - 1023 permit

Name: default_ipv6, Type: ipv6, State: active
Rule    Source IP          Protocol  Dest Port  Action
1       any                    tcp       22         permit
2       any                    tcp       23         permit
3       any                    tcp       80         permit
4       any                    tcp       443        permit
5       any                    udp       161        permit
6       any                    udp       123        permit
7       any                    tcp       600 - 1023 permit
8       any                    udp       600 - 1023 permit
```

Figure 20 Existing switch policies

Next, we generate a brute force login attack on the switch (see Figure 21).

```
sha@Shashanks-MBP QRadar-Brocade % ssh qradaradmin@129.40.101.137
Warning: Permanently added '129.40.101.137' (ECDSA) to the list of known hosts.
qradaradmin@129.40.101.137's password:
Permission denied, please try again.
qradaradmin@129.40.101.137's password:
Permission denied, please try again.
qradaradmin@129.40.101.137's password:
qradaradmin@129.40.101.137: Permission denied (publickey,password).
```

Figure 21 Brute force login attack

All failed login attempt events are logged in QRadar (see Figure 22).

Failed Login	Brocade-129_40_101_137	1 Nov 12, 2021, 4:18:51 AM	User Login Failure	19.206.136.159	0	129.40.101.137	0	N/A	N/A
Failed Login	Brocade-129_40_101_137	1 Nov 12, 2021, 4:18:47 AM	User Login Failure	19.206.136.159	0	129.40.101.137	0	N/A	N/A
Failed Login	Brocade-129_40_101_137	1 Nov 12, 2021, 4:18:42 AM	User Login Failure	19.206.136.159	0	129.40.101.137	0	N/A	N/A

Figure 22 Failed login events that were received in QRadar

The response to block the offending IP when three consecutive failed login events are observed in 5 minutes.

Figure 23 shows more events that were captured in QRadar. The Python script is configured as the rule response, logs in to the switch by using the QRadar admin user, copies the active policy, and inserts the blocking rule.

Note: The value of 3 for the number of failed events is a user-defined value. It is added as part of the rule in the lab for demonstration purposes only.

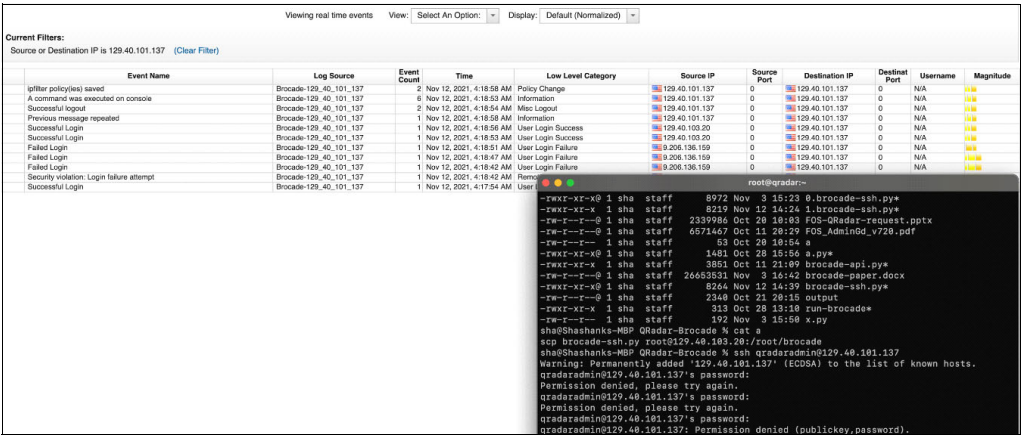


Figure 23 Brute force login attack and QRadar response events

The switch now has a new defined policy that shows the newly defined rule with the deny attribute (see Figure 24).

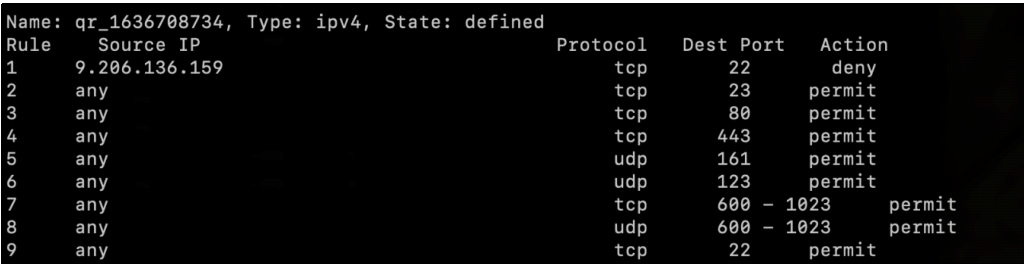


Figure 24 New policy defined on switch

For demonstration purposes, we defined the policy only; it was *not* enabled.

The sample script that is provided with this publication shows how the new policy rules are created. For more information about downloading the sample script from GitHub, see “Resources” on page 16.

Note: Readers should customize the sample script and sample rules per their needs. They also should confirm the response that is generated in the test environment before implementing changes in the production environment to avoid any disruptions. Do *not* implement the script in your environment.

Summary

The solution that is described in this paper shows the integration of IBM QRadar and Brocade SAN FOS for early threat detection and generating response to block the attacker IP by defining a new policy in the switch.

About the author

Shashank Shingornikar is a Storage Solutions Architect with IBM Systems, ISDL Lab Pune, India, for over 12 years. He has worked extensively with IBM Storage products, such as IBM Spectrum Virtualize, IBM FlashSystems, and IBM Spectrum Scale building solutions that combine Oracle and Red Hat OpenShift features. Currently, he is working on demonstrating Cyber resilience solutions with IBM® QRadar and IBM Storage Systems. Before joining IBM, Shashank has worked in the Netherlands on various HA/DR/Cluster/Replication solutions for database technologies, such as Oracle, MSSQL, and MySQL.

Acknowledgments

The author wishes to thank the following contributors for making the infrastructure available and their valuable guidance:

Andrew Greenfield
IBM Team

Brian Larsen
Marcus Thordal
Van Tran
Brocade Team

Resources

For more information, see the following resources:

- IBM QRadar:
<http://www.ibm.com/docs/en/qsip>
- Adding custom actions to IBM QRadar:
<http://ibm.com/docs/en/qsip/7.4?topic=tasks-adding-custom-actions>
- Broadcom switch documentation:
 - <http://www.broadcom.com/products/ethernet-connectivity/switching>
 - <http://www.broadcom.com/products/fibre-channel-networking>
- NIST Framework:
<http://www.nist.gov>
- GitHub link to download the script:
<https://github.com/IBM/ibm-qradar-brocade>

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

IBM®


IBM FlashSystem®

IBM Security™

IBM Spectrum®

IBM Watson®

QRadar®

Redbooks (logo) ®

The following terms are trademarks of other companies:

OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.



© Copyright IBM Corporation

March 2022

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



Please recycle

ISBN 0738460265

REDP-5672-00