Contents

Objective: 2

Description: 2

Project steps: 2

1-Introduction 2

2-Environment Setup: 2

Prerequisites: 2

Installation: 2

3-Configuring Log Sources: 3

Adding Log Sources: 3

4-Implementing Virus Detection Use Case 5

Scenario Description: 5

Data Simulation: 6

Rule Testing: 6

5-Dashboard: 7

Dashboards: 7

6-Conclusion 9

Summary of the project: 9

Conclusion: 9

IBM QRadar Configuration and Virus Detection Use cases

Objective: To configure IBM QRadar SIEM for monitoring and detecting virus activity within an organization's network. The project will cover the initial setup, configuration, and implementation of a virus detection use case.

Description: This project demonstrates the setup and configuration of IBM QRadar SIEM, including integration with network devices, log sources, and creation of custom rules to detect virus activity. The project includes a practical use case for detecting virus infections and generating alerts

Project steps:

1-Introduction

- Overview of the project
- Importance of SIEM in cyber security
- Objectives and expected outcomes

2-Environment Setup:

Prerequisites:

- IBM QRadar SIEM (installed and configured)

250 GB Free storage for VM and 16GB RAM or at least 8 GB RAM for VM.

- Access to network devices and log sources (e.g., firewalls, antivirus software)

Installation:

- Steps to install IBM QRadar (if not already installed)
- Configuration of basic settings (time zone, network settings, etc.)

1. Double-click on the QRadar file.

2. From the popup, please name your VM and set the path (enter the name in the first line; the default path will display on the second line).

3. Right-click on the new VM and select "Properties."

4. Increase the RAM allocation to a minimum of 8GB.

5. Change the network adapter setting from "Bridging" to "Host-only."

6. Click the "Add" button to add another network adapter (set to the default NAT).

7. Click "OK" and power on the VM.

8. A login credential screen will appear (type "root" as the username and press Enter).

9. Set your root user password, press Enter, retype the same password, and press Enter again.

10. Type ./setup in the command prompt and press Enter.

11. Press Enter again.

12. Press "Q" and then press Enter.

13. Press "Y" and press Enter.

14. Now, sit back and relax until it displays the completion message and prompts for the admin password.

15. In case of failure, repeat steps from 1 to 4.

Note: If, during installation, your screen goes black or enters screen saver mode, press the space bar to activate it again.

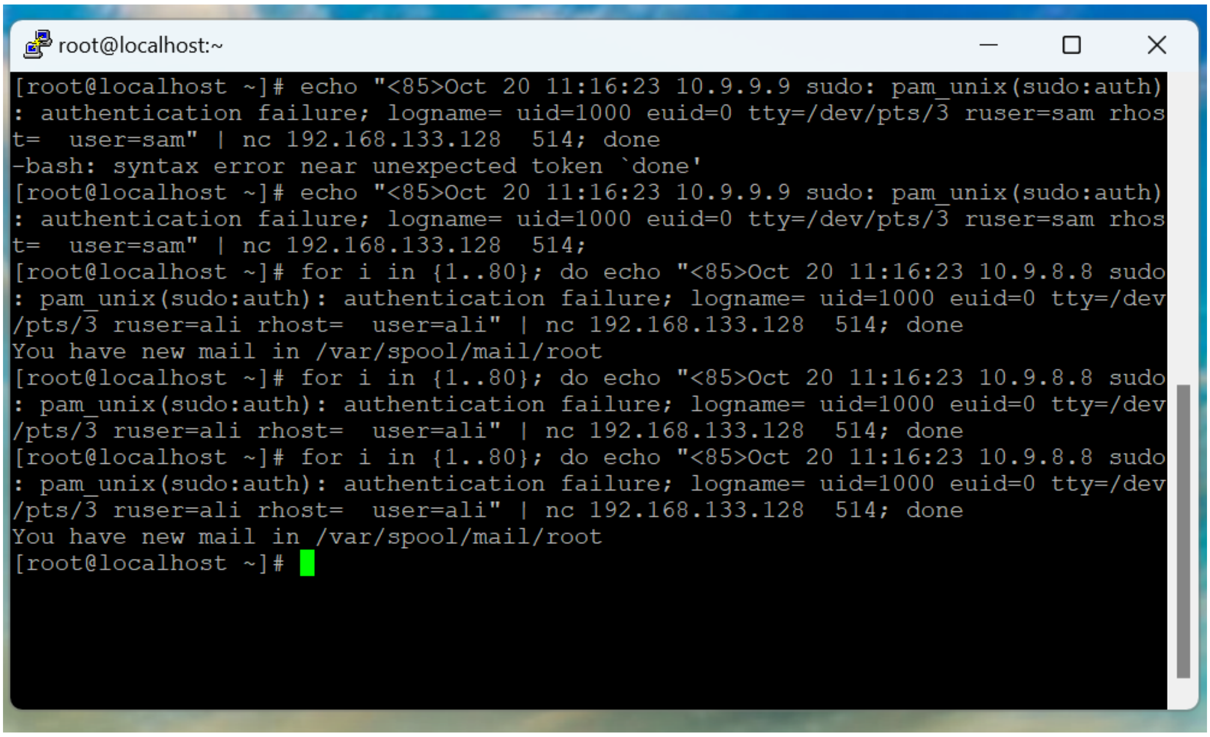
3-Configuring Log Sources:

Adding Log Sources:

- Steps to add log sources (e.g., firewalls, antivirus logs) (use case logs file)
- Configuring log source parameters (IP address, protocol, port, etc.)

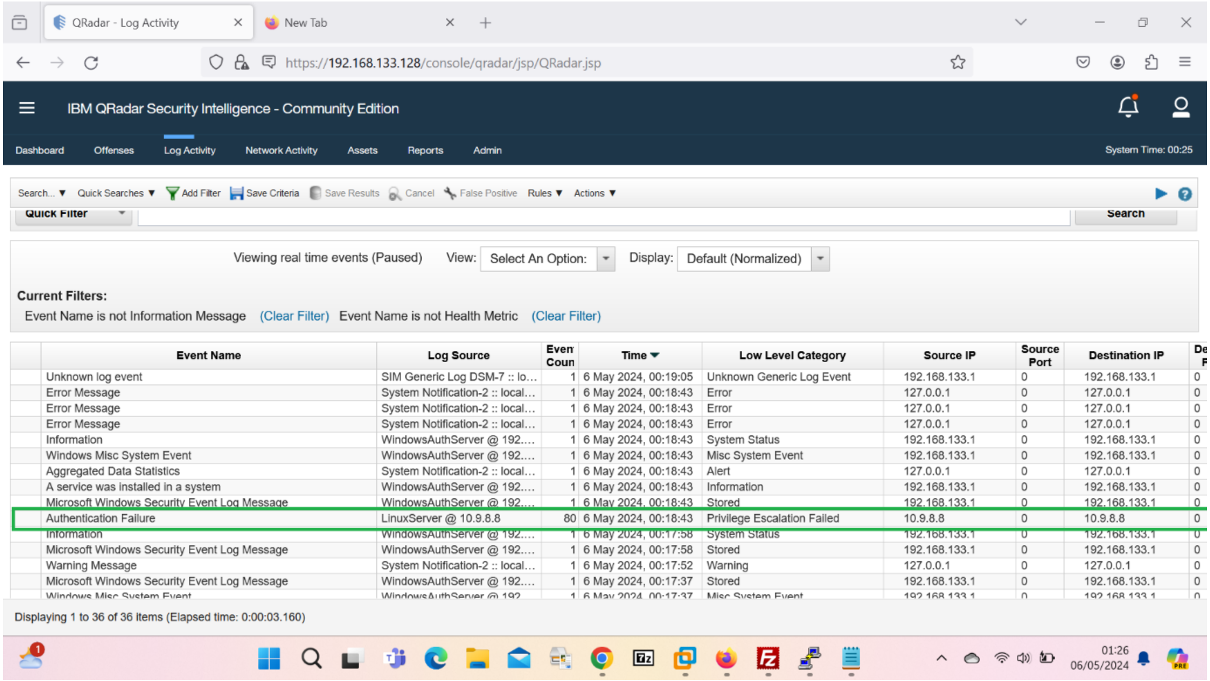
Verifying Log Source Integration:

- Ensuring log sources are correctly sending logs to QRadar
- Checking log source status in QRadar dashboard



```
[root@localhost ~]# echo "<85>Oct 20 11:16:23 10.9.9.9 sudo: pam_unix(sudo:auth)
: authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/3 ruser=sam rhos
t=  user=sam" | nc 192.168.133.128  514; done
-bash: syntax error near unexpected token `done'
[root@localhost ~]# echo "<85>Oct 20 11:16:23 10.9.9.9 sudo: pam_unix(sudo:auth)
: authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/3 ruser=sam rhos
t=  user=sam" | nc 192.168.133.128  514;
[root@localhost ~]# for i in {1..80}; do echo "<85>Oct 20 11:16:23 10.9.8.8 sudo
: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev
/pts/3 ruser=ali rhost=  user=ali" | nc 192.168.133.128  514; done
You have new mail in /var/spool/mail/root
[root@localhost ~]# for i in {1..80}; do echo "<85>Oct 20 11:16:23 10.9.8.8 sudo
: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev
/pts/3 ruser=ali rhost=  user=ali" | nc 192.168.133.128  514; done
[root@localhost ~]# for i in {1..80}; do echo "<85>Oct 20 11:16:23 10.9.8.8 sudo
: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev
/pts/3 ruser=ali rhost=  user=ali" | nc 192.168.133.128  514; done
You have new mail in /var/spool/mail/root
[root@localhost ~]# 
```

Putty connection and sending logs



Viewing real time events (Paused) View: Select An Option: Display: Default (Normalized)

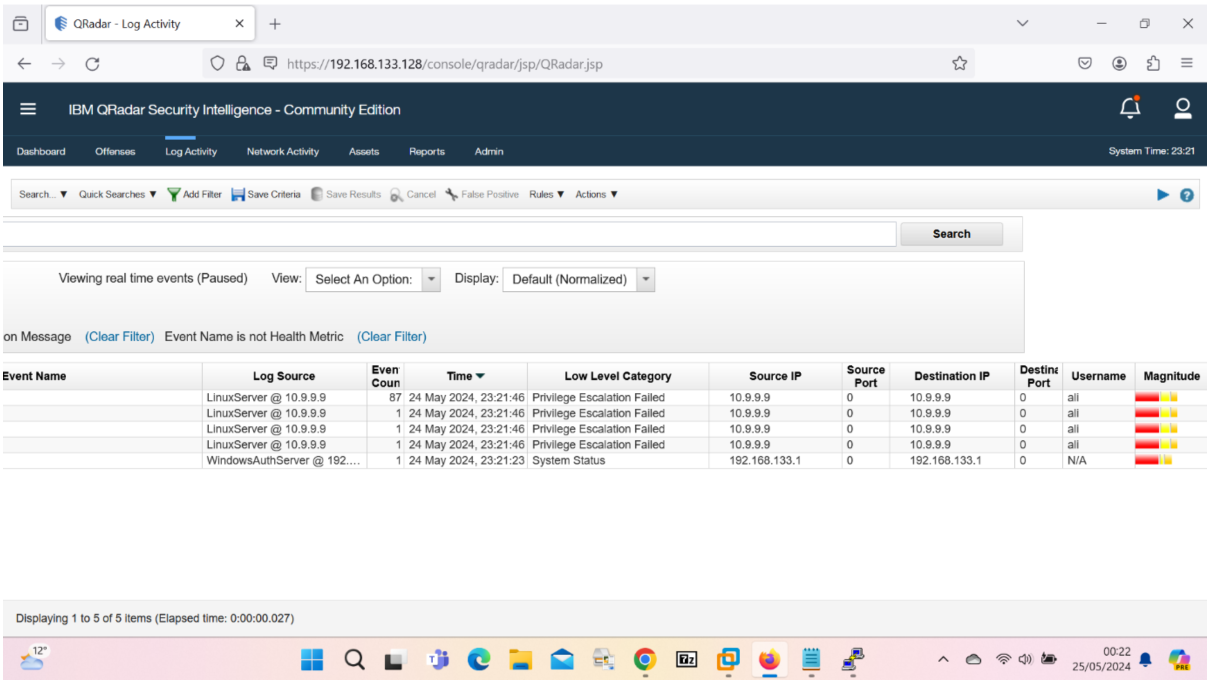
Current Filters:

Event Name is not Information Message (Clear Filter) Event Name is not Health Metric (Clear Filter)

	Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	De F
	Unknown log event	SIM Generic Log DSM-7 :: lo…	1	6 May 2024, 00:19:05	Unknown Generic Log Event	192.168.133.1	0	192.168.133.1	0
	Error Message	System Notification-2 :: local…	1	6 May 2024, 00:18:43	Error	127.0.0.1	0	127.0.0.1	0
	Error Message	System Notification-2 :: local…	1	6 May 2024, 00:18:43	Error	127.0.0.1	0	127.0.0.1	0
	Error Message	System Notification-2 :: local…	1	6 May 2024, 00:18:43	Error	127.0.0.1	0	127.0.0.1	0
	Information	WindowsAuthServer @ 192.…	1	6 May 2024, 00:18:43	System Status	192.168.133.1	0	192.168.133.1	0
	Windows Misc System Event	WindowsAuthServer @ 192.…	1	6 May 2024, 00:18:43	Misc System Event	192.168.133.1	0	192.168.133.1	0
	Aggregated Data Statistics	System Notification-2 :: local…	1	6 May 2024, 00:18:43	Alert	127.0.0.1	0	127.0.0.1	0
	A service was installed in a system	WindowsAuthServer @ 192.…	1	6 May 2024, 00:18:43	Information	192.168.133.1	0	192.168.133.1	0
	Microsoft Windows Security Event Log Message	WindowsAuthServer @ 192.…	1	6 May 2024, 00:18:43	Stored	192.168.133.1	0	192.168.133.1	0
	Authentication Failure	LinuxServer @ 10.9.8.8	80	6 May 2024, 00:18:43	Privilege Escalation Failed	10.9.8.8	0	10.9.8.8	0
	Information	WindowsAuthServer @ 192.…	1	6 May 2024, 00:17:58	System Status	192.168.133.1	0	192.168.133.1	0
	Microsoft Windows Security Event Log Message	WindowsAuthServer @ 192.…	1	6 May 2024, 00:17:58	Stored	192.168.133.1	0	192.168.133.1	0
	Warning Message	System Notification-2 :: local…	1	6 May 2024, 00:17:52	Warning	127.0.0.1	0	127.0.0.1	0
	Microsoft Windows Security Event Log Message	WindowsAuthServer @ 192.…	1	6 May 2024, 00:17:37	Stored	192.168.133.1	0	192.168.133.1	0
	Windows Misc System Event	WindowsAuthServer @ 192	1	6 May 2024, 00:17:37	Misc System Event	192.168.133.1	0	192.168.133.1	0

Displaying 1 to 36 of 36 items (Elapsed time: 0:00:03.160)

Log send 80 times

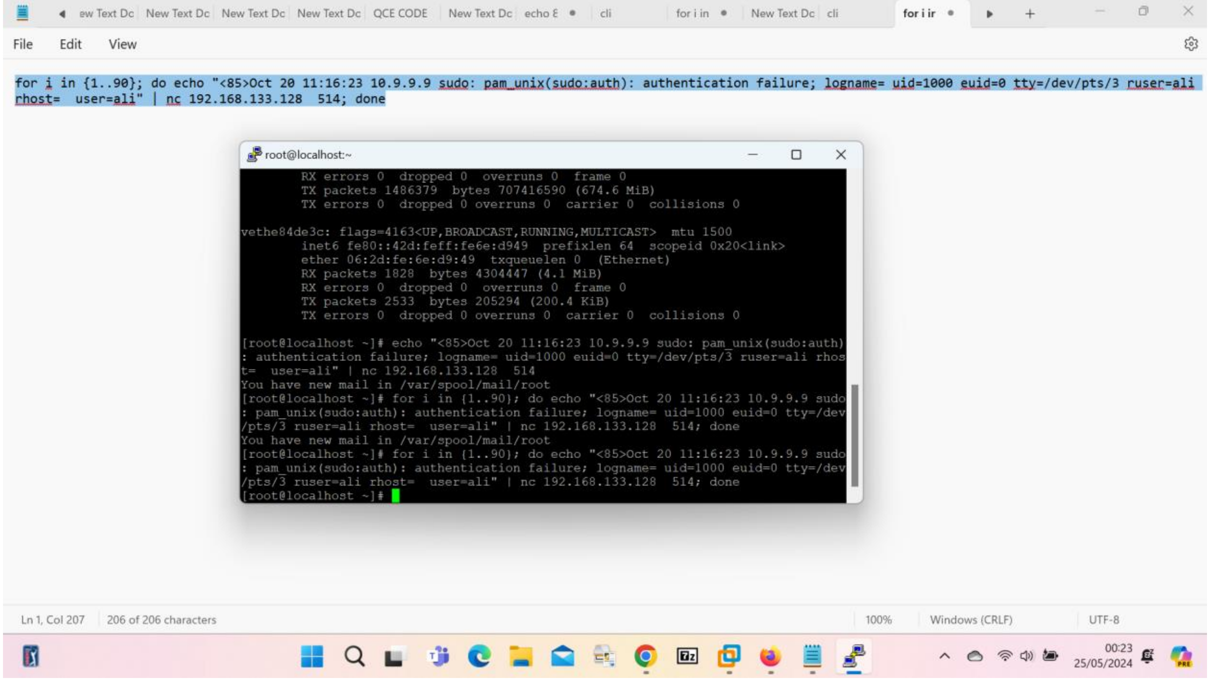


Viewing real time events (Paused) View: Select An Option: Display: Default (Normalized)

on Message (Clear Filter) Event Name is not Health Metric (Clear Filter)

Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
	LinuxServer @ 10.9.9.9	87	24 May 2024, 23:21:46	Privilege Escalation Failed	10.9.9.9	0	10.9.9.9	0	ali	
	LinuxServer @ 10.9.9.9	1	24 May 2024, 23:21:46	Privilege Escalation Failed	10.9.9.9	0	10.9.9.9	0	ali	
	LinuxServer @ 10.9.9.9	1	24 May 2024, 23:21:46	Privilege Escalation Failed	10.9.9.9	0	10.9.9.9	0	ali	
	LinuxServer @ 10.9.9.9	1	24 May 2024, 23:21:46	Privilege Escalation Failed	10.9.9.9	0	10.9.9.9	0	ali	
	WindowsAuthServer @ 192....	1	24 May 2024, 23:21:23	System Status	192.168.133.1	0	192.168.133.1	0	N/A	

Displaying 1 to 5 of 5 items (Elapsed time: 0:00:00.027)



```
for i in {1..90}; do echo "<85>Oct 20 11:16:23 10.9.9.9 sudo: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/3 ruser=ali
rhost=  user=ali" | nc 192.168.133.128  514; done
```

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1486379  bytes 707416590 (674.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vethe84de3c: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::42d:feff:fe6e:d949  prefixlen 64  scopeid 0x20<link>
        ether 06:2d:fe:6e:d9:49  txqueuelen 0  (Ethernet)
        RX packets 1828  bytes 4304447 (4.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2533  bytes 205294 (200.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost ~]# echo "<85>Oct 20 11:16:23 10.9.9.9 sudo: pam_unix(sudo:auth)
: authentication failure; logname= uid=1000 euid=0 tty=/dev/pts/3 ruser=ali rhos
t=  user=ali" | nc 192.168.133.128  514
You have new mail in /var/spool/mail/root
[root@localhost ~]# for i in {1..90}; do echo "<85>Oct 20 11:16:23 10.9.9.9 sudo
: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev
/pts/3 ruser=ali rhost=  user=ali" | nc 192.168.133.128  514; done
You have new mail in /var/spool/mail/root
[root@localhost ~]# for i in {1..90}; do echo "<85>Oct 20 11:16:23 10.9.9.9 sudo
: pam_unix(sudo:auth): authentication failure; logname= uid=1000 euid=0 tty=/dev
/pts/3 ruser=ali rhost=  user=ali" | nc 192.168.133.128  514; done
[root@localhost ~]#
```

Sample log

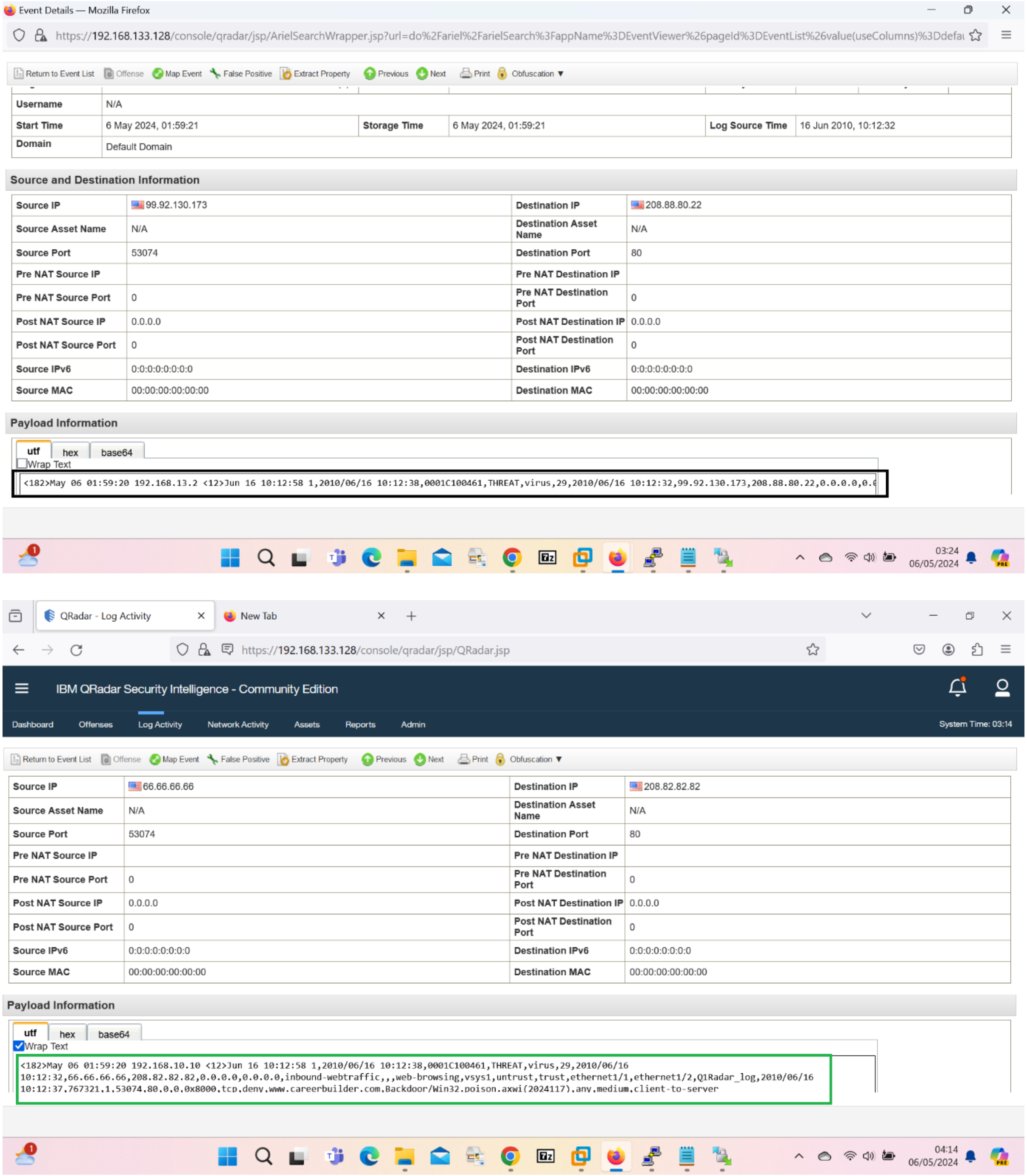
4-Implementing Virus Detection Use Case

Scenario Description:

- Description of the virus detection scenario (e.g., detection of a known virus signature)

Data Simulation:

- Simulating virus activity (e.g., using sample virus logs, generating test events)


Event Details — Mozilla Firefox
https://192.168.133.128/console/qradar/jsp/ArielSearchWrapper.jsp?url=do%2Fariel%2FarielSearch%3FappName%3DEventViewer%26pageId%3DEventList%26value(useColumns)%3Ddefau
Return to Event List
Offense
Map Event
False Positive
Extract Property
Previous
Next
Print
Obfuscation ▼

Username	N/A				
Start Time	6 May 2024, 01:59:21	Storage Time	6 May 2024, 01:59:21	Log Source Time	16 Jun 2010, 10:12:32
Domain	Default Domain				

Source and Destination Information

Source IP	99.92.130.173	Destination IP	208.88.80.22
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	53074	Destination Port	80
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP	0.0.0.0	Post NAT Destination IP	0.0.0.0
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

```
<182>May 06 01:59:20 192.168.13.2 <12>Jun 16 10:12:58 1,2010/06/16 10:12:38,0001C100461,THREAT,virus,29,2010/06/16 10:12:32,99.92.130.173,208.88.80.22,0.0.0.0,0.0
```

Source IP	66.66.66.66	Destination IP	208.82.82.82
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	53074	Destination Port	80
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP	0.0.0.0	Post NAT Destination IP	0.0.0.0
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

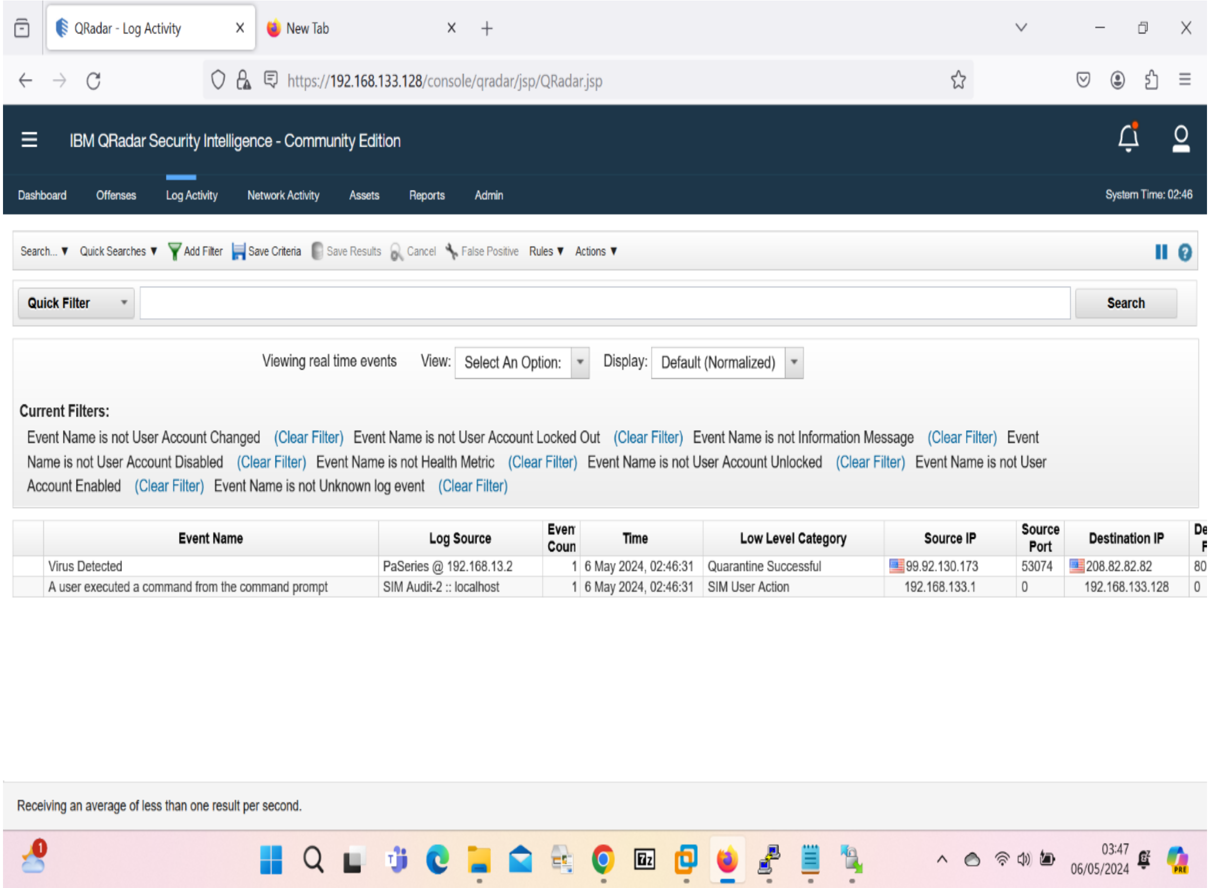
Payload Information

```
<182>May 06 01:59:20 192.168.10.10 <12>Jun 16 10:12:58 1,2010/06/16 10:12:38,0001C100461,THREAT,virus,29,2010/06/16
10:12:32,66.66.66.66,208.82.82.82,0.0.0.0,0.0.0.0,inbound-webtraffic,,,web-browsing,vsys1,untrust,trust,ethernet1/1,ethernet1/2,Q1Radar_log,2010/06/16
10:12:37,767321,1,53074,80,0,0,0x8000,tcp,deny,www.careerbuilder.com,Backdoor/Win32.poison.axwi(2024117),any,medium,client-to-server
```

Virus detection log

Rule Testing:

- Testing the custom rule to ensure it detects the simulated virus activity
- Verifying alerts and log entries in QRadar



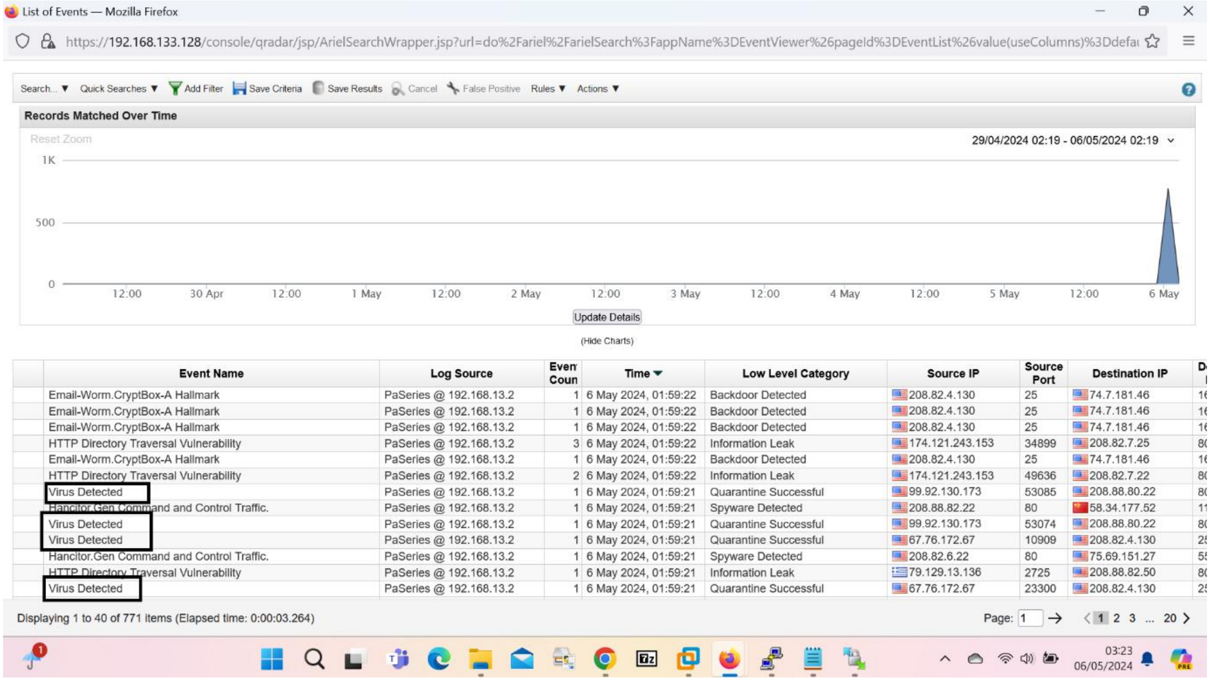
Viewing real time events View: Select An Option: Display: Default (Normalized)

Current Filters:

Event Name is not User Account Changed (Clear Filter) Event Name is not User Account Locked Out (Clear Filter) Event Name is not Information Message (Clear Filter) Event Name is not User Account Disabled (Clear Filter) Event Name is not Health Metric (Clear Filter) Event Name is not User Account Unlocked (Clear Filter) Event Name is not User Account Enabled (Clear Filter) Event Name is not Unknown log event (Clear Filter)

Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	De F
Virus Detected	PaSeries @ 192.168.13.2	1	6 May 2024, 02:46:31	Quarantine Successful	99.92.130.173	53074	208.82.82.82	80
A user executed a command from the command prompt	SIM Audit-2 :: localhost	1	6 May 2024, 02:46:31	SIM User Action	192.168.133.1	0	192.168.133.128	0

Receiving an average of less than one result per second.



Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	D
Email-Worm.CryptBox-A Hallmark	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:22	Backdoor Detected	208.82.4.130	25	74.7.181.46	16
Email-Worm.CryptBox-A Hallmark	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:22	Backdoor Detected	208.82.4.130	25	74.7.181.46	16
Email-Worm.CryptBox-A Hallmark	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:22	Backdoor Detected	208.82.4.130	25	74.7.181.46	16
HTTP Directory Traversal Vulnerability	PaSeries @ 192.168.13.2	3	6 May 2024, 01:59:22	Information Leak	174.121.243.153	34899	208.82.7.25	80
Email-Worm.CryptBox-A Hallmark	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:22	Backdoor Detected	208.82.4.130	25	74.7.181.46	16
HTTP Directory Traversal Vulnerability	PaSeries @ 192.168.13.2	2	6 May 2024, 01:59:22	Information Leak	174.121.243.153	49636	208.82.7.22	80
Virus Detected	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:21	Quarantine Successful	99.92.130.173	53085	208.88.80.22	80
Hancitor.Gen Command and Control Traffic.	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:21	Spyware Detected	208.88.82.22	80	58.34.177.52	11
Virus Detected	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:21	Quarantine Successful	99.92.130.173	53074	208.88.80.22	80
Virus Detected	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:21	Quarantine Successful	67.76.172.67	10909	208.82.4.130	25
Hancitor.Gen Command and Control Traffic.	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:21	Spyware Detected	208.82.6.22	80	75.69.151.27	55
HTTP Directory Traversal Vulnerability	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:21	Information Leak	79.129.13.136	2725	208.88.82.50	80
Virus Detected	PaSeries @ 192.168.13.2	1	6 May 2024, 01:59:21	Quarantine Successful	67.76.172.67	23300	208.82.4.130	25

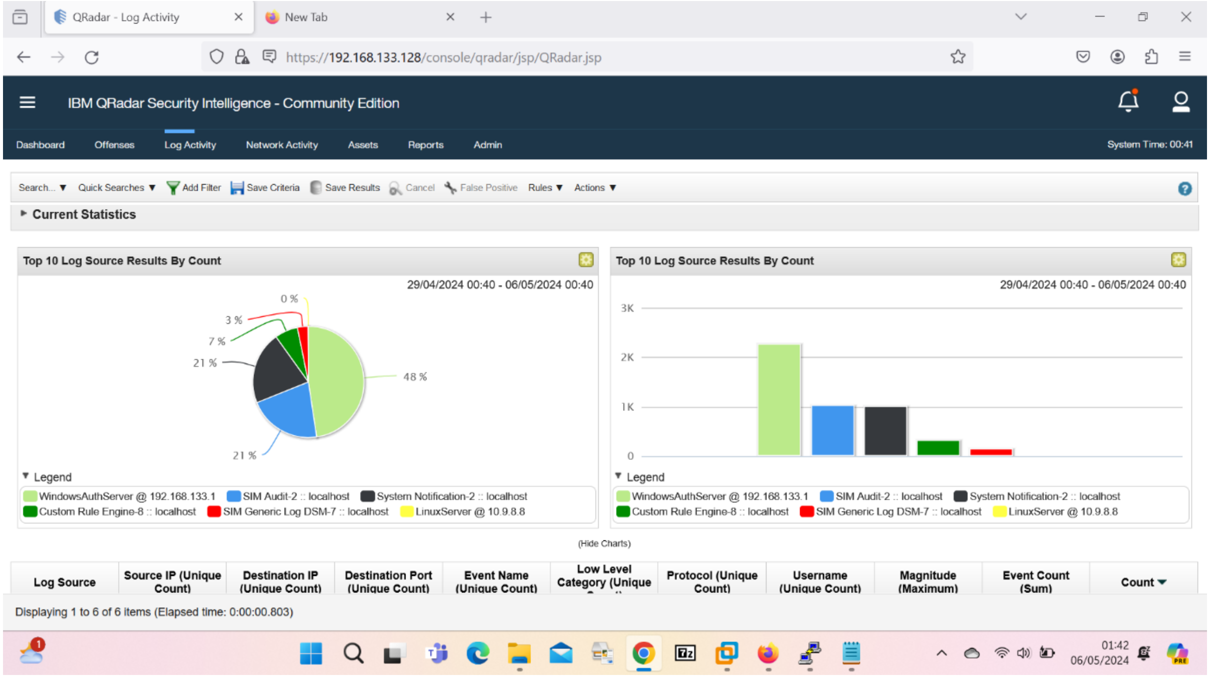
Displaying 1 to 40 of 771 items (Elapsed time: 0:00:03.264)

5-Dashboard:

Dashboards:

- Steps to create a custom dashboard in QRadar

- Adding relevant widgets (e.g., virus activity charts, alert summaries)



QRadar - Log Activity | New Tab

https://192.168.133.128/console/qradar/jsp/QRadar.jsp

IBM QRadar Security Intelligence - Community Edition

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin | System Time: 00:41

Search... ▼ | Quick Searches ▼ | Add Filter | Save Criteria | Save Results | Cancel | False Positive | Rules ▼ | Actions ▼

▸ Current Statistics

Top 10 Log Source Results By Count

29/04/2024 00:40 - 06/05/2024 00:40

▼ Legend

🟩 WindowsAuthServer @ 192.168.133.1 🟦 SIM Audit-2 :: localhost ⬛ System Notification-2 :: localhost
🟩 Custom Rule Engine-8 :: localhost 🟥 SIM Generic Log DSM-7 :: localhost 🟨 LinuxServer @ 10.9.8.8

Top 10 Log Source Results By Count

29/04/2024 00:40 - 06/05/2024 00:40

▼ Legend

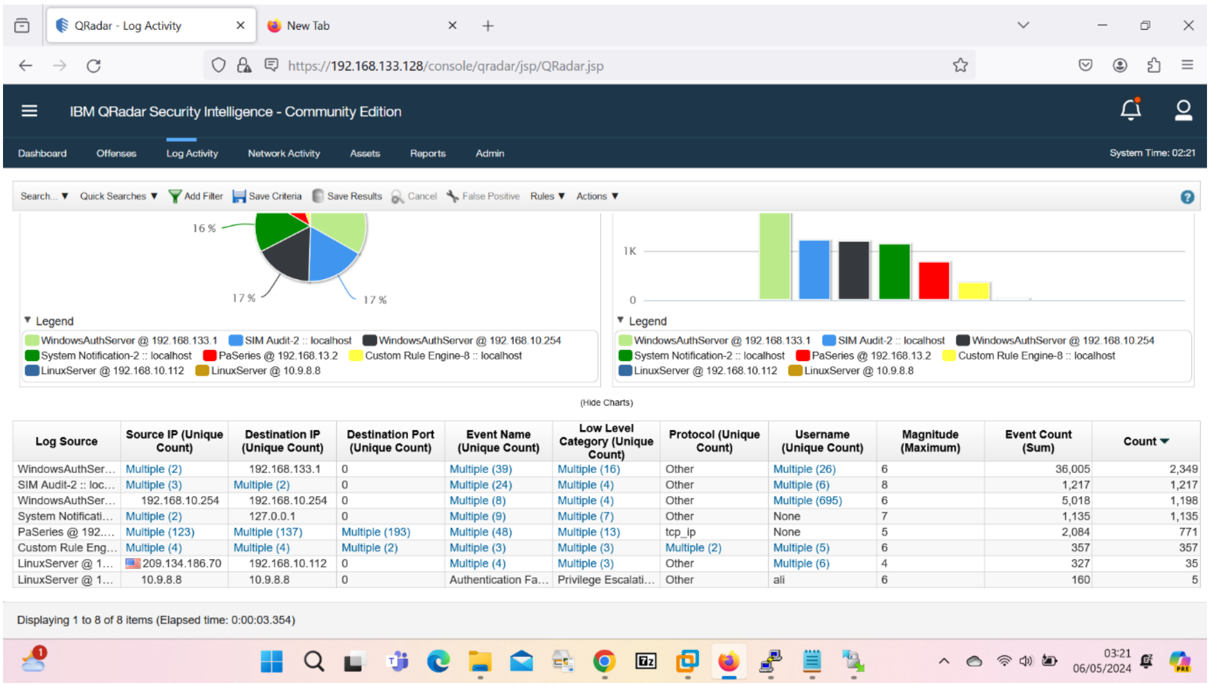
🟩 WindowsAuthServer @ 192.168.133.1 🟦 SIM Audit-2 :: localhost ⬛ System Notification-2 :: localhost
🟩 Custom Rule Engine-8 :: localhost 🟥 SIM Generic Log DSM-7 :: localhost 🟨 LinuxServer @ 10.9.8.8

(Hide Charts)

Log Source	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count ▼

Displaying 1 to 6 of 6 items (Elapsed time: 0:00:00.803)

01:42
06/05/2024



QRadar - Log Activity | New Tab

https://192.168.133.128/console/qradar/jsp/QRadar.jsp

IBM QRadar Security Intelligence - Community Edition

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin | System Time: 02:21

Search... ▼ | Quick Searches ▼ | Add Filter | Save Criteria | Save Results | Cancel | False Positive | Rules ▼ | Actions ▼

▼ Legend

🟩 WindowsAuthServer @ 192.168.133.1 🟦 SIM Audit-2 :: localhost ⬛ WindowsAuthServer @ 192.168.10.254
🟩 System Notification-2 :: localhost 🟥 PaSeries @ 192.168.13.2 🟨 Custom Rule Engine-8 :: localhost
🟦 LinuxServer @ 192.168.10.112 🟨 LinuxServer @ 10.9.8.8

▼ Legend

🟩 WindowsAuthServer @ 192.168.133.1 🟦 SIM Audit-2 :: localhost ⬛ WindowsAuthServer @ 192.168.10.254
🟩 System Notification-2 :: localhost 🟥 PaSeries @ 192.168.13.2 🟨 Custom Rule Engine-8 :: localhost
🟦 LinuxServer @ 192.168.10.112 🟨 LinuxServer @ 10.9.8.8

(Hide Charts)

Log Source	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count ▼
WindowsAuthSer...	Multiple (2)	192.168.133.1	0	Multiple (39)	Multiple (16)	Other	Multiple (26)	6	36,005	2,349
SIM Audit-2 :: loc...	Multiple (3)	Multiple (2)	0	Multiple (24)	Multiple (4)	Other	Multiple (6)	8	1,217	1,217
WindowsAuthSer...	192.168.10.254	192.168.10.254	0	Multiple (8)	Multiple (4)	Other	Multiple (695)	6	5,018	1,198
System Notificati...	Multiple (2)	127.0.0.1	0	Multiple (9)	Multiple (7)	Other	None	7	1,135	1,135
PaSeries @ 192....	Multiple (123)	Multiple (137)	Multiple (193)	Multiple (48)	Multiple (13)	tcp_ip	None	5	2,084	771
Custom Rule Eng...	Multiple (4)	Multiple (4)	Multiple (2)	Multiple (3)	Multiple (3)	Multiple (2)	Multiple (5)	6	357	357
LinuxServer @ 1...	209.134.186.70	192.168.10.112	0	Multiple (4)	Multiple (3)	Other	Multiple (6)	4	327	35
LinuxServer @ 1...	10.9.8.8	10.9.8.8	0	Authentication Fa...	Privilege Escalati...	Other	ali	6	160	5

Displaying 1 to 8 of 8 items (Elapsed time: 0:00:03.354)

03:21
06/05/2024

6-Conclusion

Summary of the project:

This project focuses on configuring IBM QRadar to detect virus activities using log data from a PA Series firewall. The project includes setting up QRadar, configuring log sources, developing detection rules, testing the system, and documenting the process. The goal is to demonstrate how QRadar can be effectively used to enhance network security by identifying and responding to virus threats.

Conclusion:

The successful completion of this project highlights the importance and effectiveness of using SIEM solutions like IBM QRadar in a cybersecurity framework. By configuring QRadar to detect virus activities, the project showcases how real-time log analysis and correlation can provide early warnings of potential threats, thereby enhancing an organization's ability to respond to security incidents promptly. This project serves as a valuable resource for security professionals looking to implement or improve their SIEM capabilities using IBM QRadar.