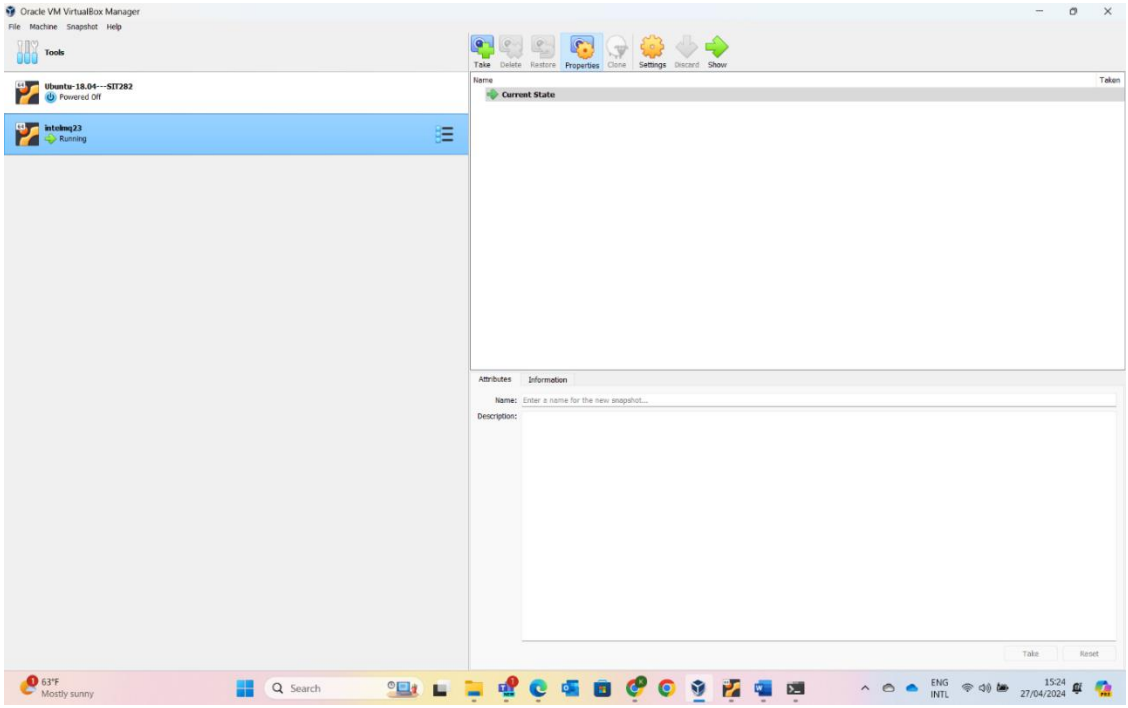
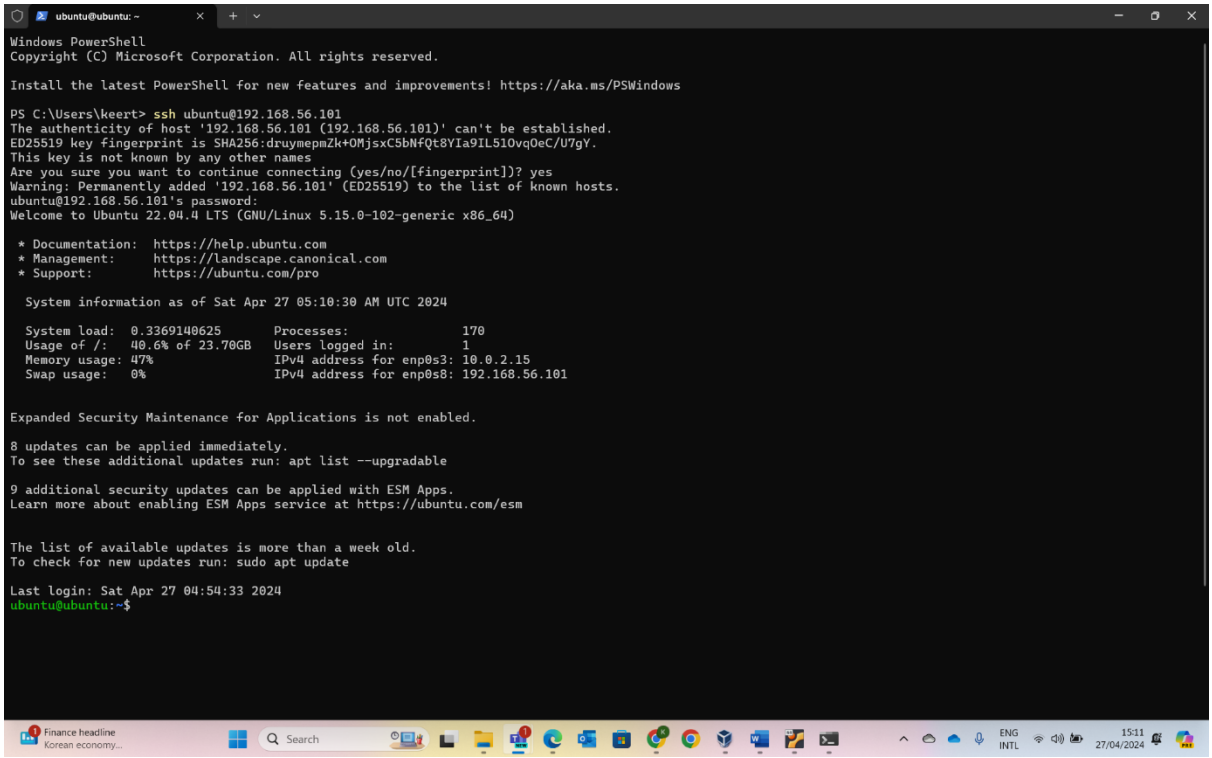
Integration of Intel MQ with an SQLite database.

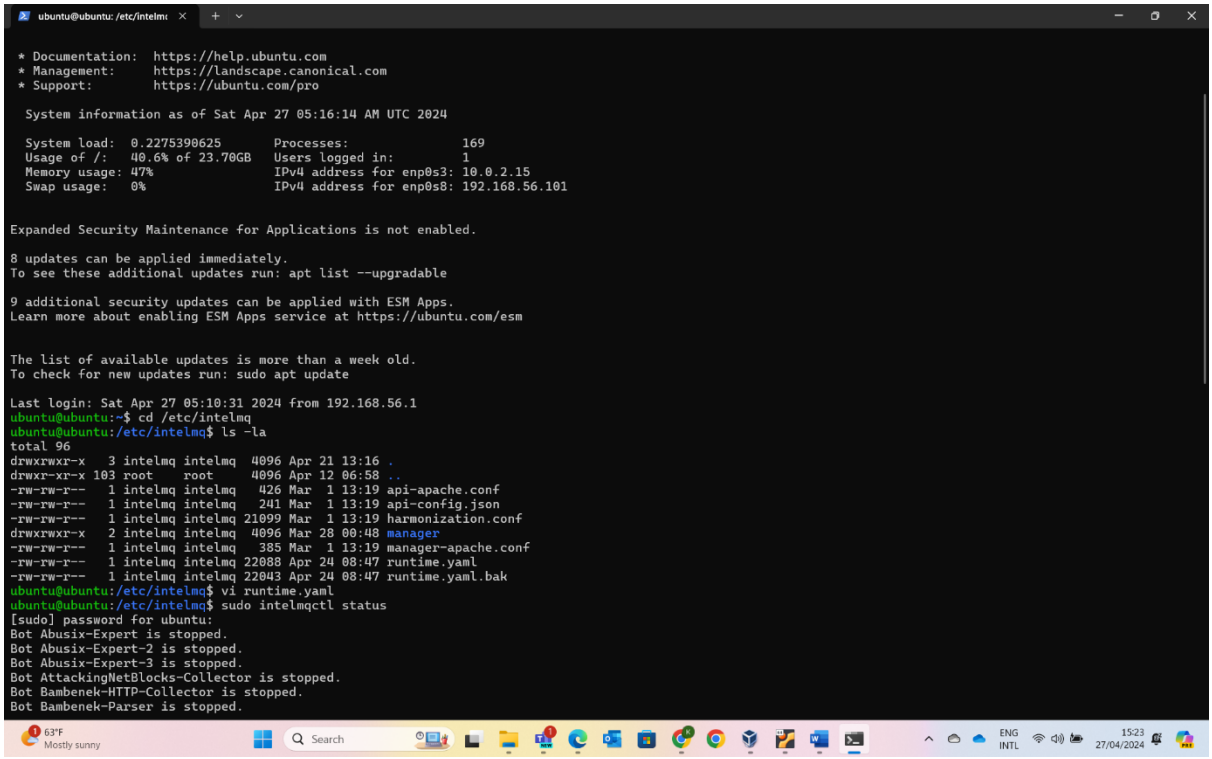
Intel MQ installation and configuration:

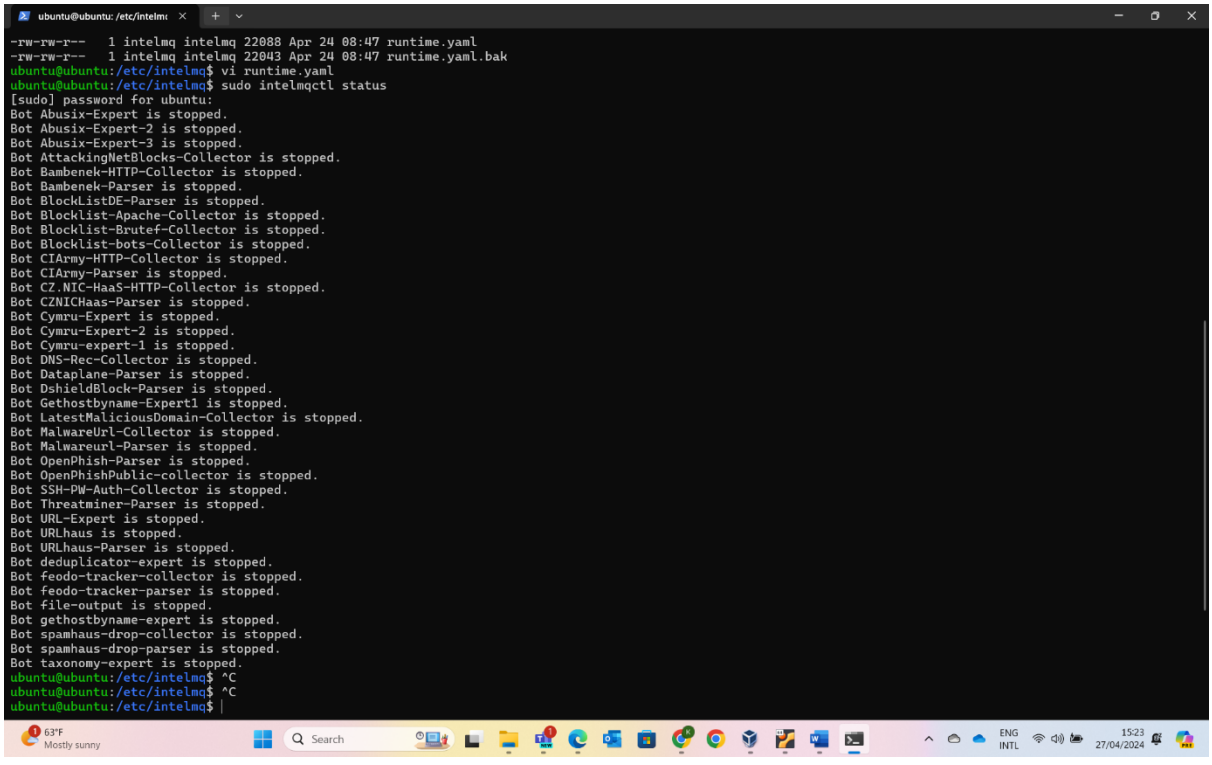
Using the correct login credentials from Rads (username: intelapi, password: intelapi), I successfully accessed the IntelMQ user interface. Subsequently, I configured and managed various bots for diverse data outputs.

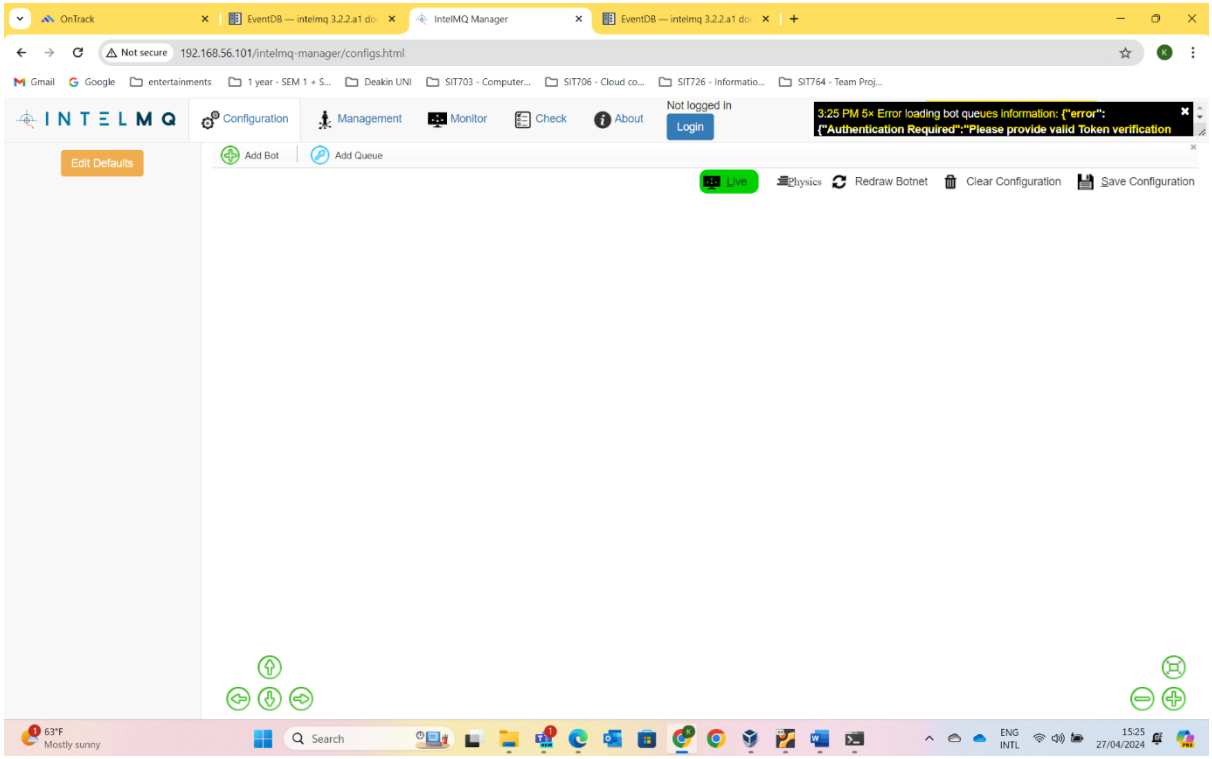


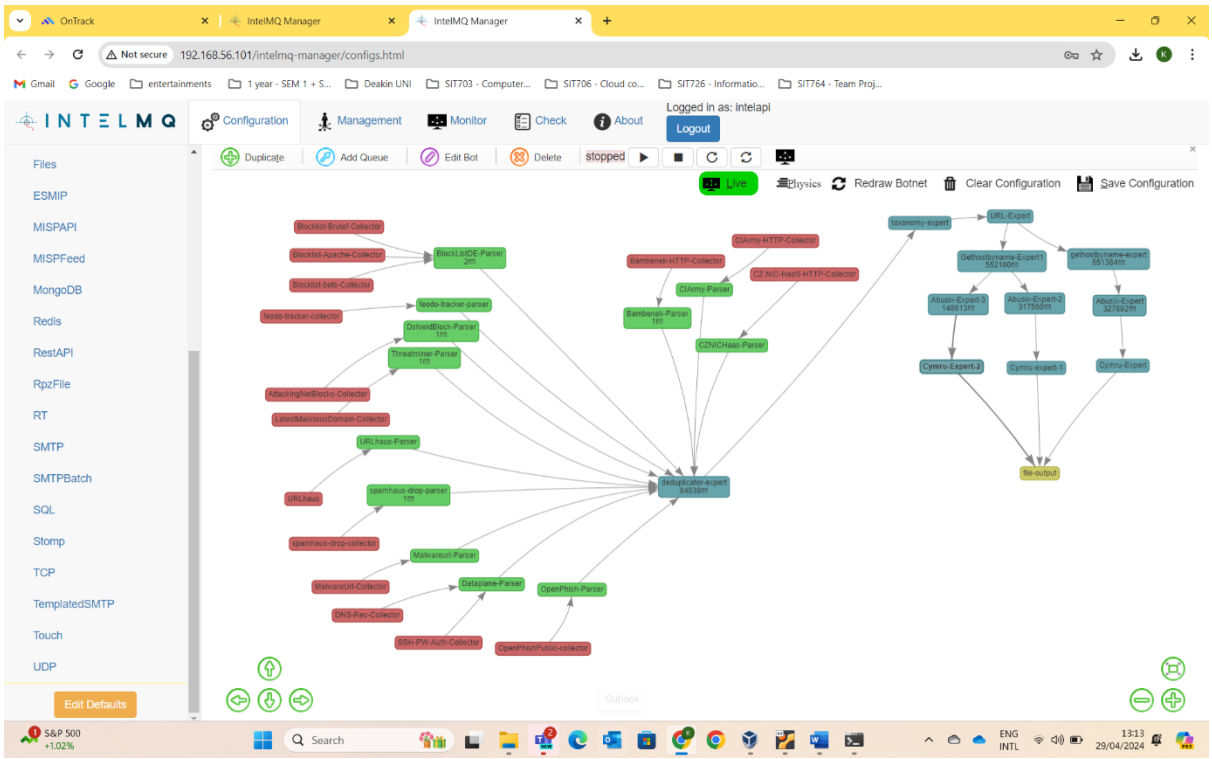
Access the server where IntelMQ is running. This can be done via SSH if you are working on a remote server.




ubuntu@ubuntu: /etc/intelmq
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Sat Apr 27 05:16:14 AM UTC 2024
System load: 0.2275390625 Processes: 169
Usage of /: 40.6% of 23.70GB Users logged in: 1
Memory usage: 47% IPv4 address for enp0s3: 10.0.2.15
Swap usage: 0% IPv4 address for enp0s8: 192.168.56.101
Expanded Security Maintenance for Applications is not enabled.
8 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Sat Apr 27 05:10:31 2024 from 192.168.56.1
ubuntu@ubuntu:~$ cd /etc/intelmq
ubuntu@ubuntu:/etc/intelmq$ ls -la
total 96
drwxrwxr-x 3 intelmq intelmq 4096 Apr 21 13:16 .
drwxr-xr-x 103 root root 4096 Apr 12 06:58 ..
-rw-rw-r-- 1 intelmq intelmq 426 Mar 1 13:19 api-apache.conf
-rw-rw-r-- 1 intelmq intelmq 241 Mar 1 13:19 api-config.json
-rw-rw-r-- 1 intelmq intelmq 21099 Mar 1 13:19 harmonization.conf
drwxrwxr-x 2 intelmq intelmq 4096 Mar 28 00:48 manager
-rw-rw-r-- 1 intelmq intelmq 385 Mar 1 13:19 manager-apache.conf
-rw-rw-r-- 1 intelmq intelmq 22088 Apr 24 08:47 runtime.yaml
-rw-rw-r-- 1 intelmq intelmq 22043 Apr 24 08:47 runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ vi runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ sudo intelmqctl status
[sudo] password for ubuntu:
Bot Abusix-Expert is stopped.
Bot Abusix-Expert-2 is stopped.
Bot Abusix-Expert-3 is stopped.
Bot AttackingNetBlocks-Collector is stopped.
Bot Bambenek-HTTP-Collector is stopped.
Bot Bambenek-Parser is stopped.
63°F
Mostly sunny
Search
ENG
INTL
15:23
27/04/2024

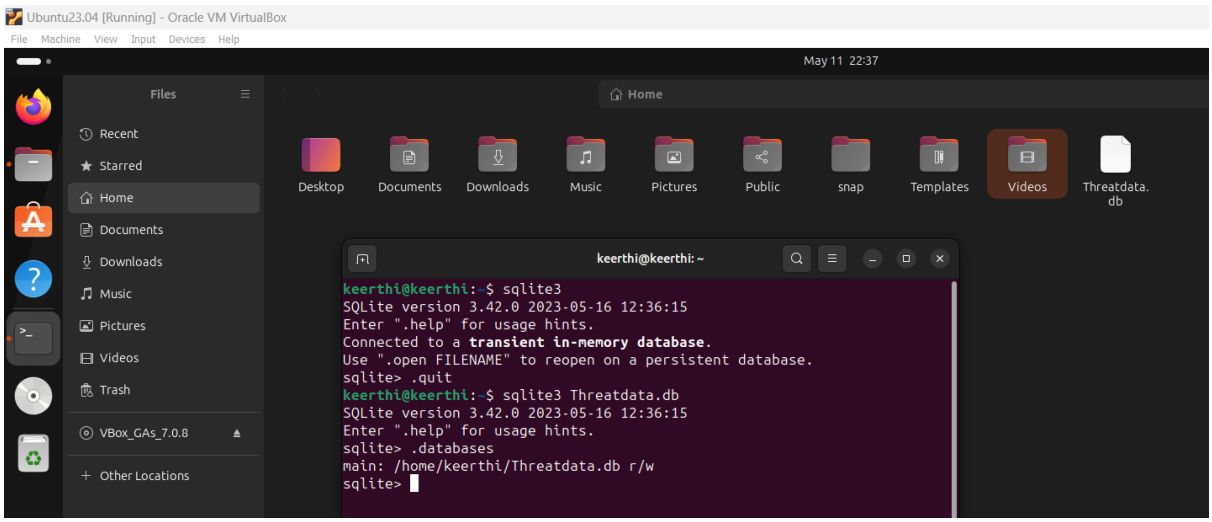

ubuntu@ubuntu: /etc/intelmq
-rw-rw-r-- 1 intelmq intelmq 22088 Apr 24 08:47 runtime.yaml
-rw-rw-r-- 1 intelmq intelmq 22043 Apr 24 08:47 runtime.yaml.bak
ubuntu@ubuntu:/etc/intelmq$ vi runtime.yaml
ubuntu@ubuntu:/etc/intelmq$ sudo intelmqctl status
[sudo] password for ubuntu:
Bot Abusix-Expert is stopped.
Bot Abusix-Expert-2 is stopped.
Bot Abusix-Expert-3 is stopped.
Bot AttackingNetBlocks-Collector is stopped.
Bot Bambenek-HTTP-Collector is stopped.
Bot Bambenek-Parser is stopped.
Bot BlockListDE-Parser is stopped.
Bot Blocklist-Apache-Collector is stopped.
Bot Blocklist-Brutef-Collector is stopped.
Bot Blocklist-bots-Collector is stopped.
Bot CIArmy-HTTP-Collector is stopped.
Bot CIArmy-Parser is stopped.
Bot CZ.NIC-HaaS-HTTP-Collector is stopped.
Bot CZNICHaas-Parser is stopped.
Bot Cymru-Expert is stopped.
Bot Cymru-Expert-2 is stopped.
Bot Cymru-expert-1 is stopped.
Bot DNS-Rec-Collector is stopped.
Bot Dataplane-Parser is stopped.
Bot DshieldBlock-Parser is stopped.
Bot Gethostbyname-Expert1 is stopped.
Bot LatestMaliciousDomain-Collector is stopped.
Bot MalwareUrl-Collector is stopped.
Bot Malwareurl-Parser is stopped.
Bot OpenPhish-Parser is stopped.
Bot OpenPhishPublic-collector is stopped.
Bot SSH-PW-Auth-Collector is stopped.
Bot Threatminer-Parser is stopped.
Bot URL-Expert is stopped.
Bot URLhaus is stopped.
Bot URLhaus-Parser is stopped.
Bot deduplicator-expert is stopped.
Bot feodo-tracker-collector is stopped.
Bot feodo-tracker-parser is stopped.
Bot file-output is stopped.
Bot gethostbyname-expert is stopped.
Bot spamhaus-drop-collector is stopped.
Bot spamhaus-drop-parser is stopped.
Bot taxonomy-expert is stopped.
ubuntu@ubuntu:/etc/intelmq$ ^C
ubuntu@ubuntu:/etc/intelmq$ ^C
ubuntu@ubuntu:/etc/intelmq$
63°F
Mostly sunny
Search
ENG
INTL
15:23
27/04/2024


OnTrack
EventDB — intelmq 3.2.2.a1 dor
IntelMQ Manager
Not secure
192.168.56.101/intelmq-manager/configs.html
INTELMQ
Configuration
Management
Monitor
Check
About
Not logged in
Login
3:25 PM 5× Error loading bot queues information: {"error":
{"Authentication Required":"Please provide valid Token verification
Edit Defaults
Add Bot
Add Queue
Live
Physics
Redraw Botnet
Clear Configuration
Save Configuration
63°F
Mostly sunny
Search
ENG
INTL
15:25
27/04/2024

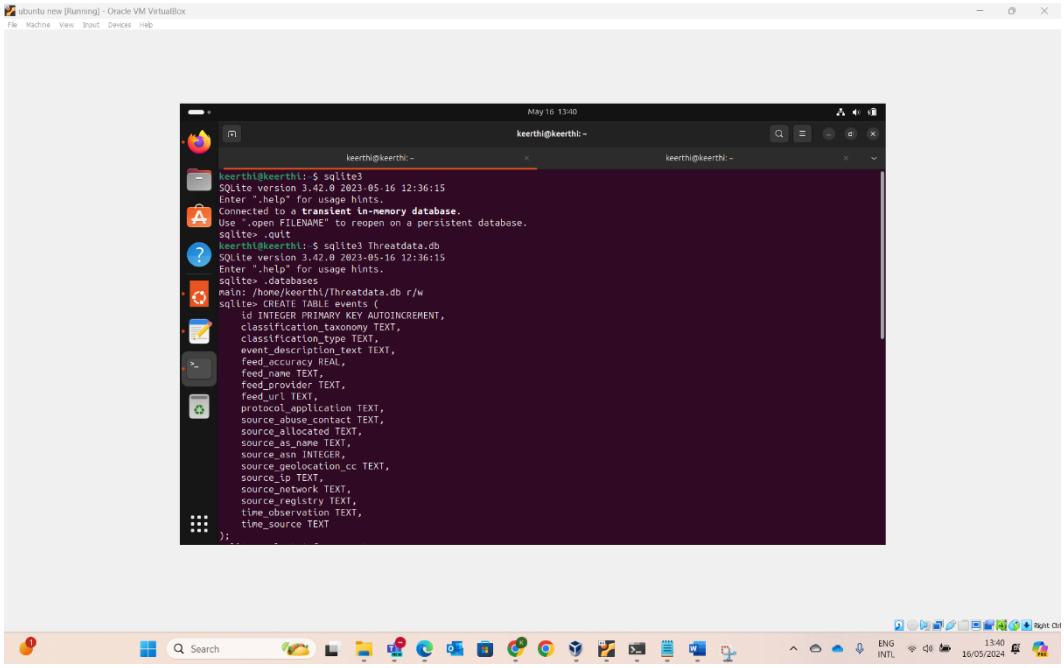

OnTrack
IntelMQ Manager
IntelMQ Manager
Not secure
192.168.56.101/intelmq-manager/configs.html
INTELMQ
Configuration
Management
Monitor
Check
About
Logged in as: intelapi
Logout
Files
ESMIP
MISPAPI
MISPFeed
MongoDB
Redis
RestAPI
RpzFile
RT
SMTP
SMTPBatch
SQL
Stomp
TCP
TemplatedSMTP
Touch
UDP
Edit Defaults
Duplicate
Add Queue
Edit Bot
Delete
stopped
Live
Physics
Redraw Botnet
Clear Configuration
Save Configuration
Blocklist-Brutef-Collector
Blocklist-Apache-Collector
Blocklist-bots-Collector
BlockListDE-Parser
feodo-tracker-collector
feodo-tracker-parser
DshieldBlock-Parser
ThreatminerParser
AttackingNetBlocks-Collector
LatestMaliciousDomain-Collector
URLhaus-Parser
URLhaus
spamhaus-drop-parser
spamhaus-drop-collector
MalwareUrl-Parser
MalwareUrl-Collector
Dataplane-Parser
DNS-Rec-Collector
SSH-PW-Auth-Collector
OpenPhish-Parser
OpenPhishPublic-collector
CIArmy-HTTP-Collector
Bambenek-HTTP-Collector
CZ.NIC-HaaS-HTTP-Collector
CIArmy-Parser
BambenekParser
CZNICHaas-Parser
deduplicator-expert
taxonomy-expert
URL-Expert
file-output
S&P 500
+1.02%
Search
ENG
INTL
13:13
29/04/2024

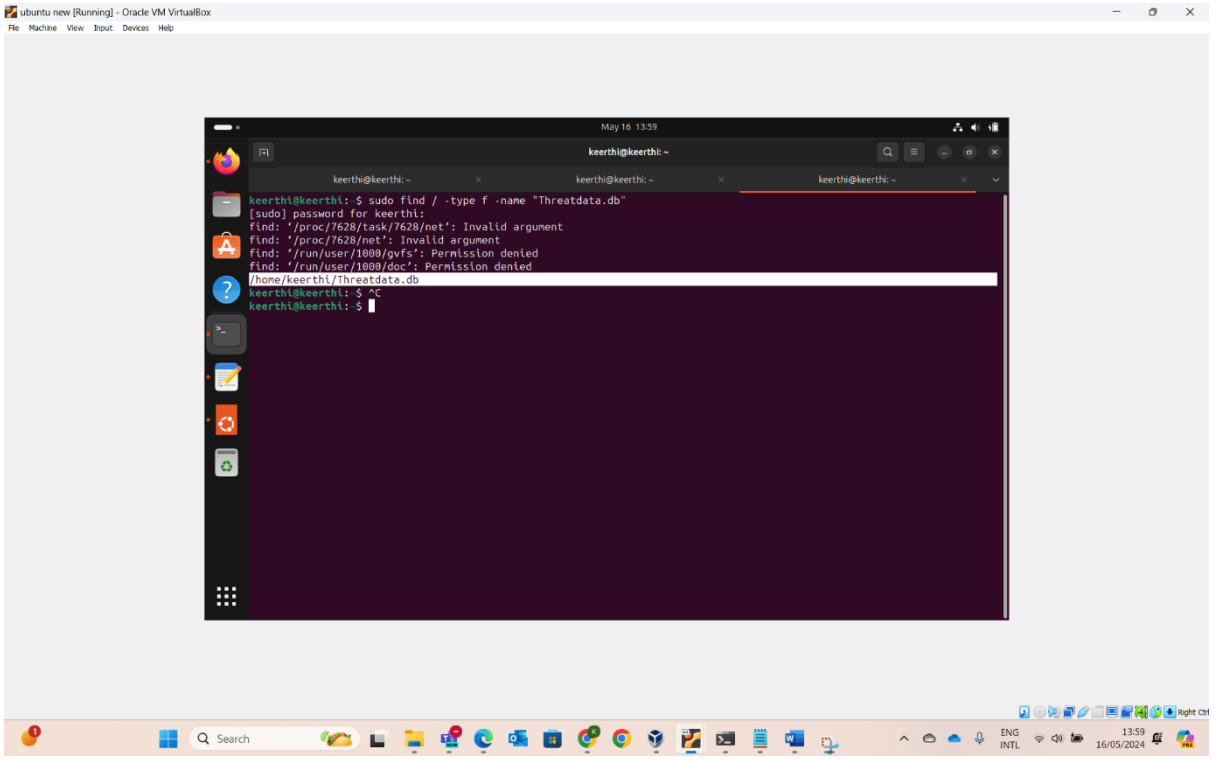
To facilitate data storage and management, I set up a dedicated Ubuntu virtual machine to host the SQLite3 database. Following the instructions outlined in the DigitalOcean tutorial:

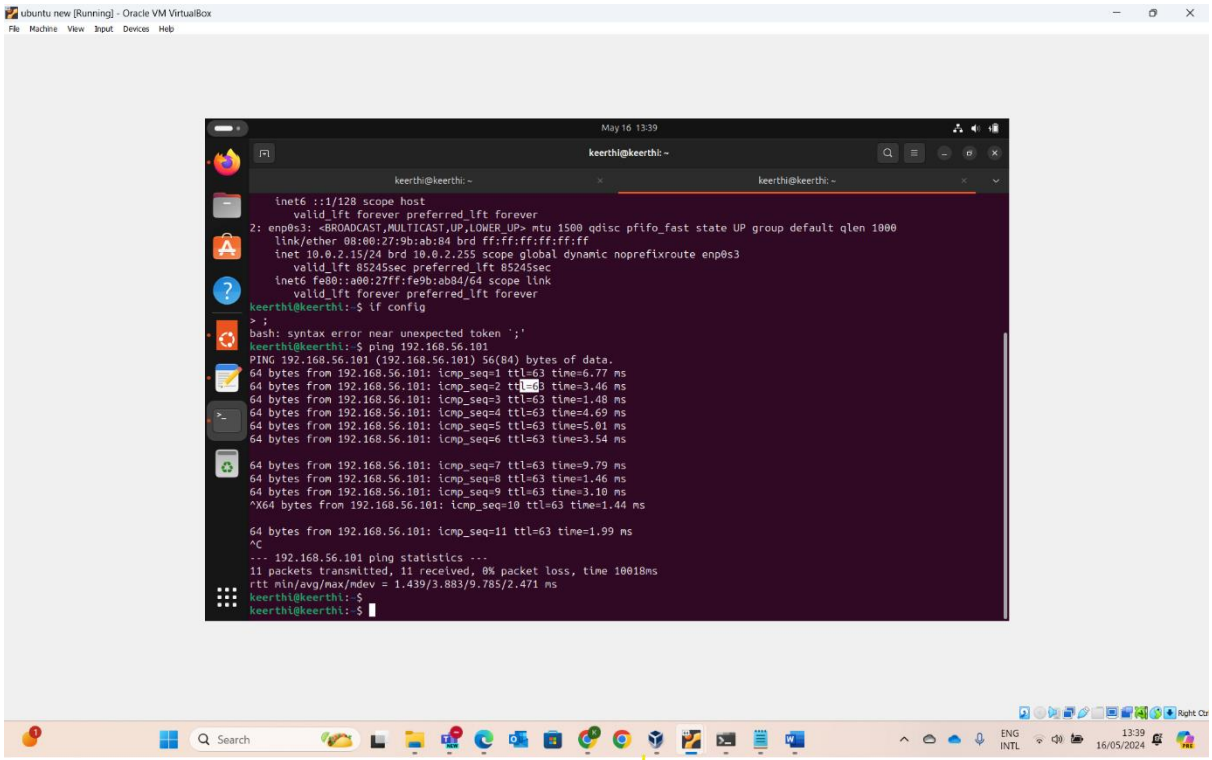
https://www.digitalocean.com/community/tutorials/how-to-install-and-use-sqlite-on-ubuntu-20-04, I installed the SQLite3.

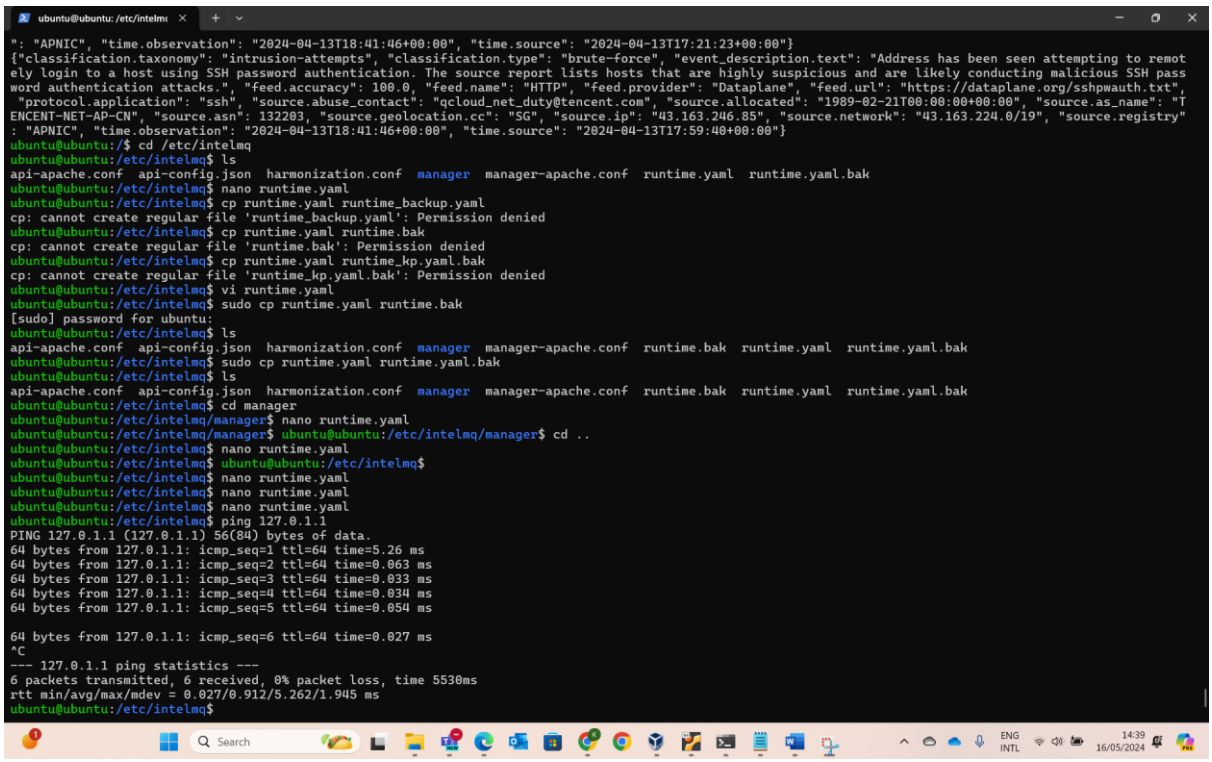


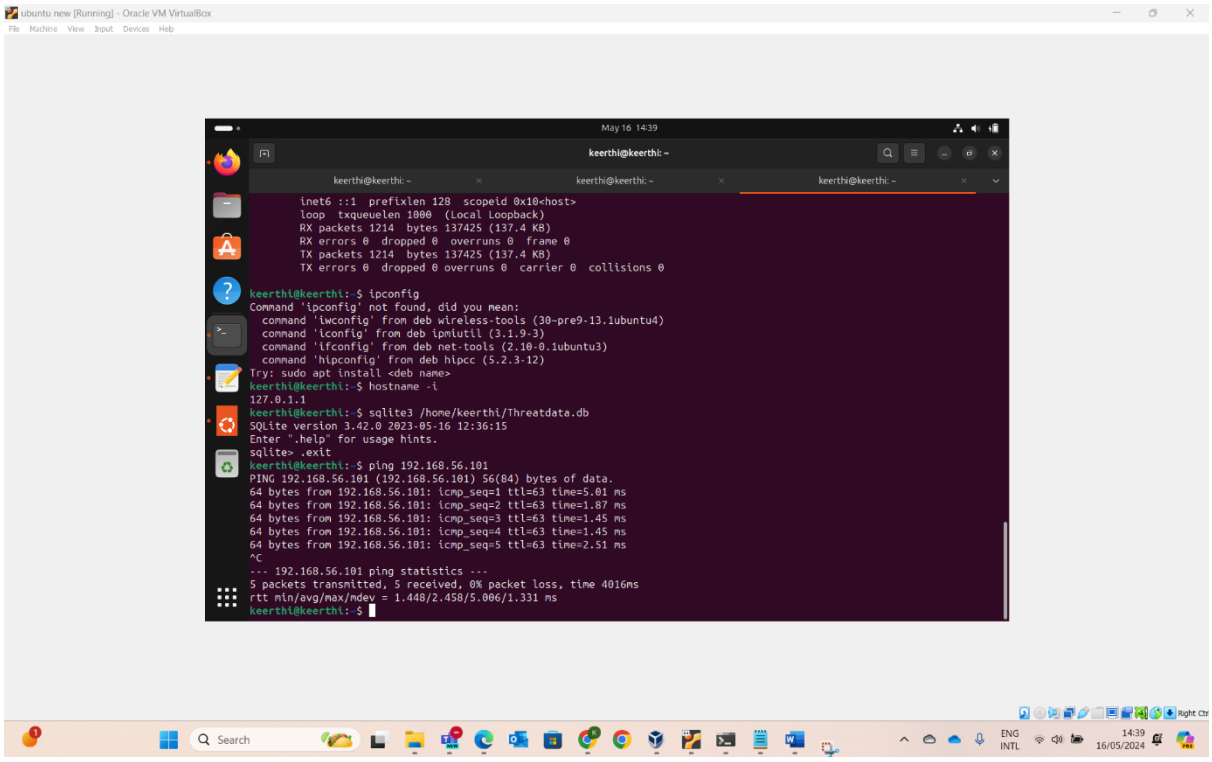
After completing the SQLite3 installation, I created a test database named Threatdata.db. Additionally, I created a new table called 'events' within the Threatdata.db database store the data. Testing connectivity between the IntelMQ instance and the Ubuntu VM hosting the database was successful, as confirmed by successful ping responses from both ends.




ubuntu new [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
May 16 13:59
keerthi@keerthi: ~
keerthi@keerthi: ~
keerthi@keerthi: ~
keerthi@keerthi: ~
keerthi@keerthi:~$ sudo find / -type f -name "Threatdata.db"
[sudo] password for keerthi:
find: '/proc/7628/task/7628/net': Invalid argument
find: '/proc/7628/net': Invalid argument
find: '/run/user/1000/gvfs': Permission denied
find: '/run/user/1000/doc': Permission denied
/home/keerthi/Threatdata.db
keerthi@keerthi:~$ ^C
keerthi@keerthi:~$
Search
ENG
INTL
13:59
16/05/2024


ubuntu new [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
May 16 13:39
keerthi@keerthi: ~
keerthi@keerthi: ~
keerthi@keerthi: ~
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:9b:ab:84 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
valid_lft 85245sec preferred_lft 85245sec
inet6 fe80::a00:27ff:fe9b:ab84/64 scope link
valid_lft forever preferred_lft forever
keerthi@keerthi:~$ if config
> ;
bash: syntax error near unexpected token `;'
keerthi@keerthi:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=63 time=6.77 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=63 time=3.46 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=63 time=1.48 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=63 time=4.69 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=63 time=5.01 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=63 time=3.54 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=63 time=9.79 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=63 time=1.46 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=63 time=3.10 ms
^X64 bytes from 192.168.56.101: icmp_seq=10 ttl=63 time=1.44 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=63 time=1.99 ms
^C
--- 192.168.56.101 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10018ms
rtt min/avg/max/mdev = 1.439/3.883/9.785/2.471 ms
keerthi@keerthi:~$
keerthi@keerthi:~$
Search
ENG
INTL
13:39
16/05/2024

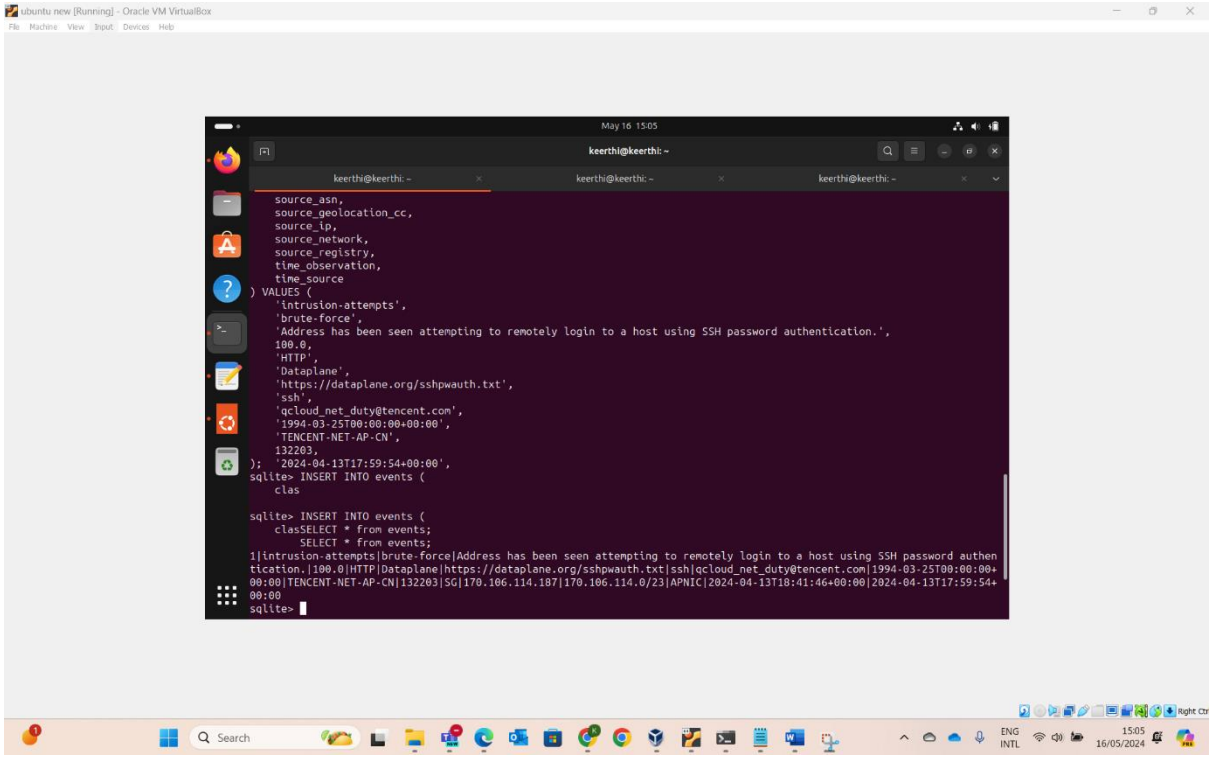


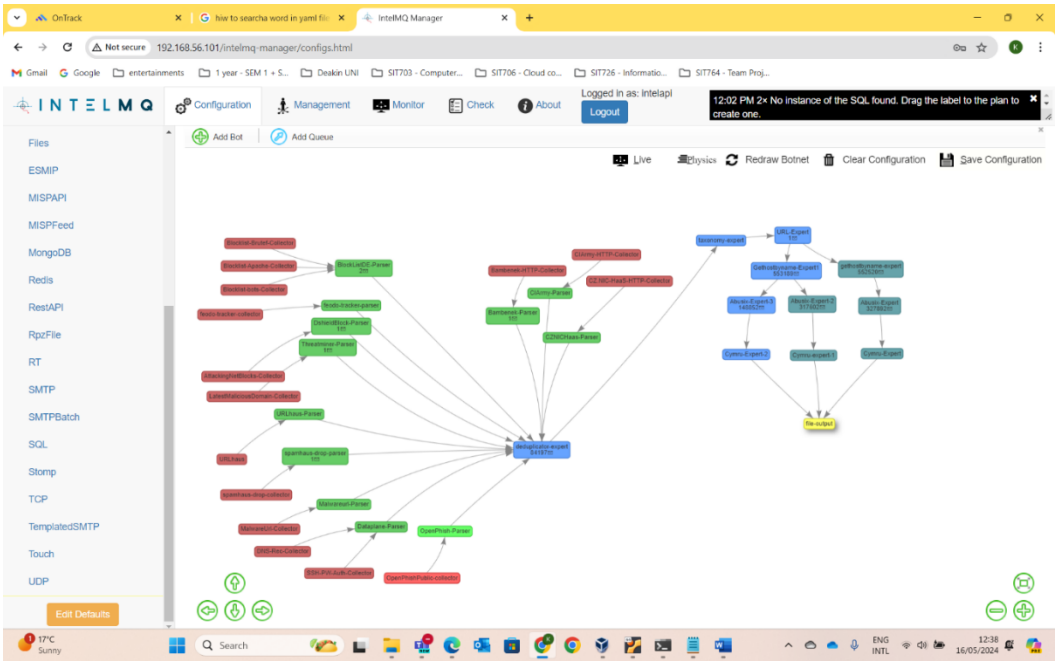


Inserted dummy data into the events table I have created in the SQLite database Threatdata.db. This INSERT statement inserts one row of data into the events table with the specified values. we can modify the values as needed or execute this statement multiple times to insert multiple rows of dummy data. After inserting the data, we can query the events table to verify that the data has been successfully inserted using below command:

SELECT * FROM events;

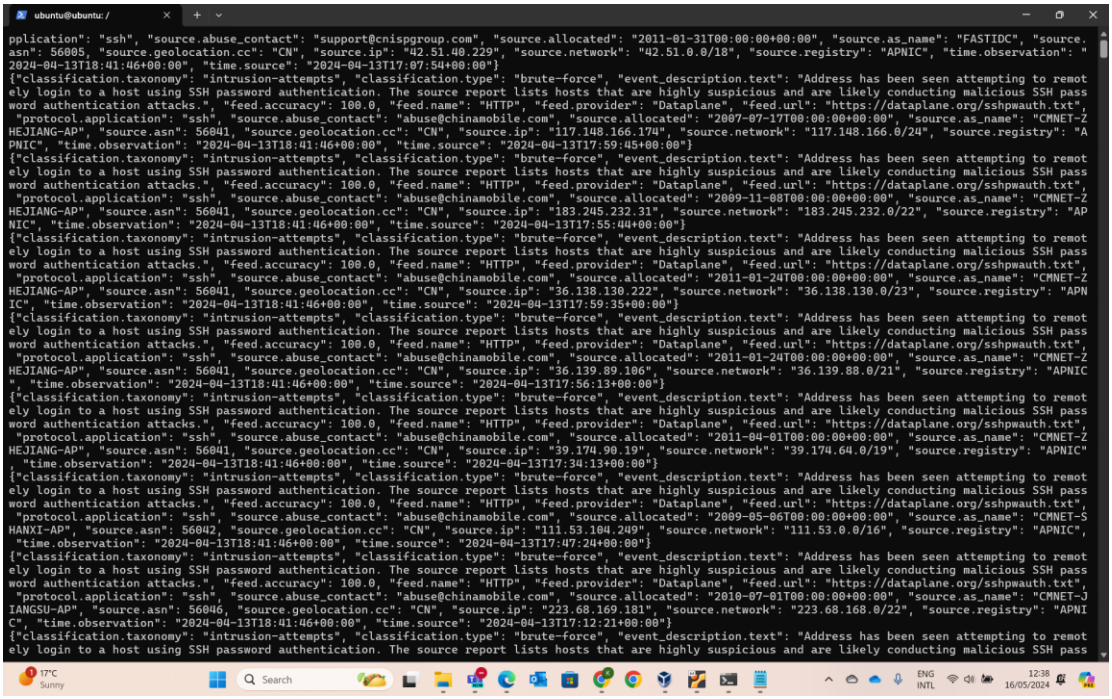
This query will retrieve all rows from the events table, allowing us to view the inserted dummy data.



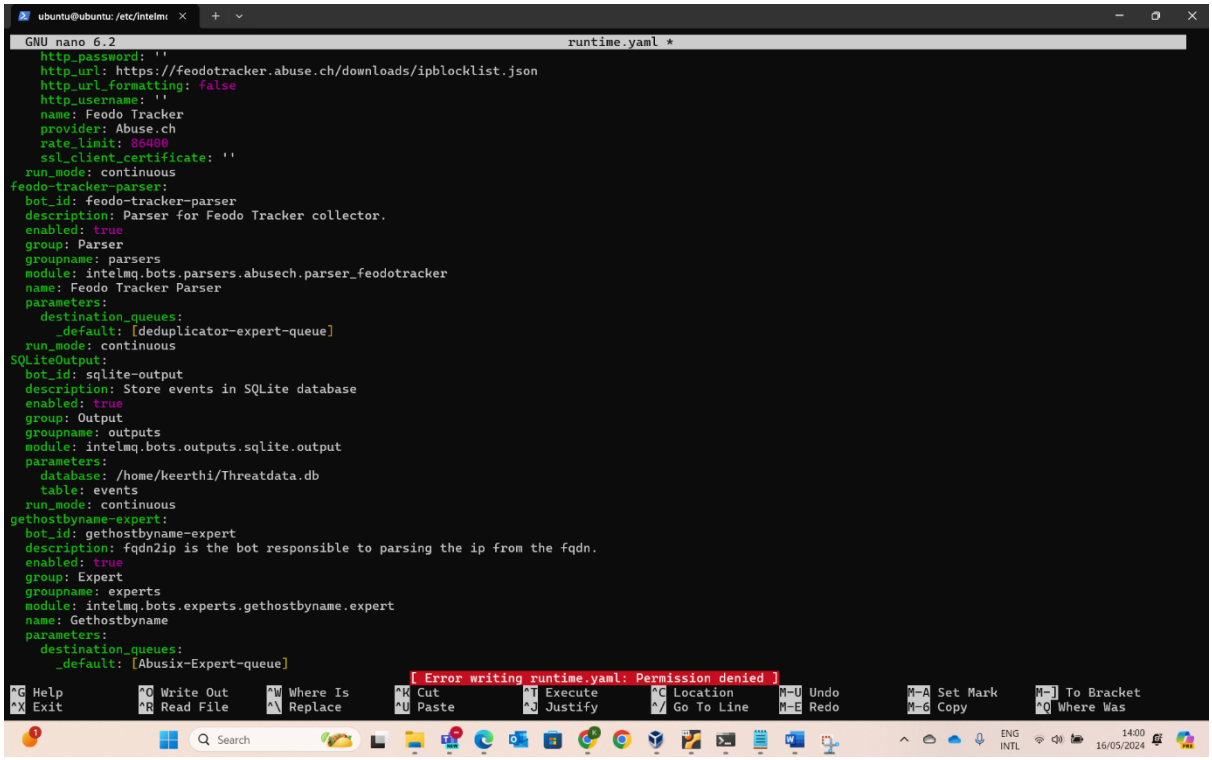


Use a command-line text viewer or editor to read the content of the events.txt file.

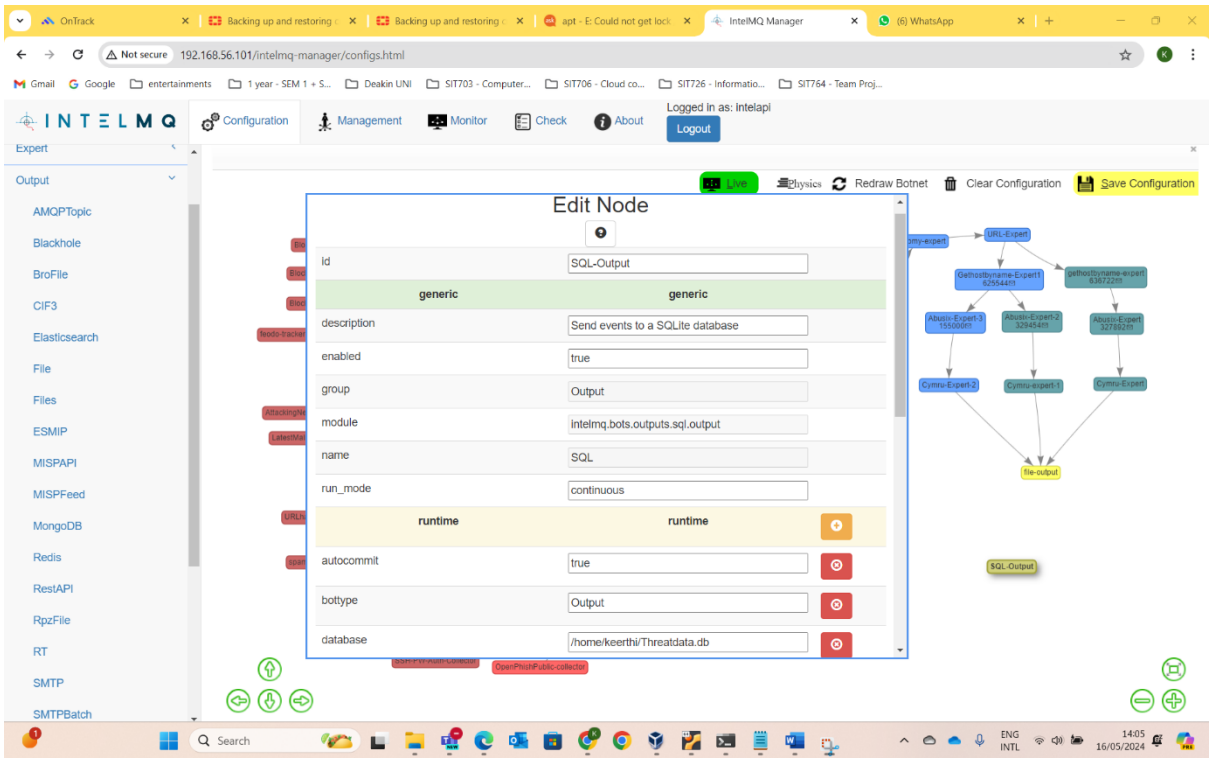
Using cat: This command will display the entire content of the file. I have used below command to open the contents of the file - cat /var/lib/intelmq/bots/file-output/events.txt.

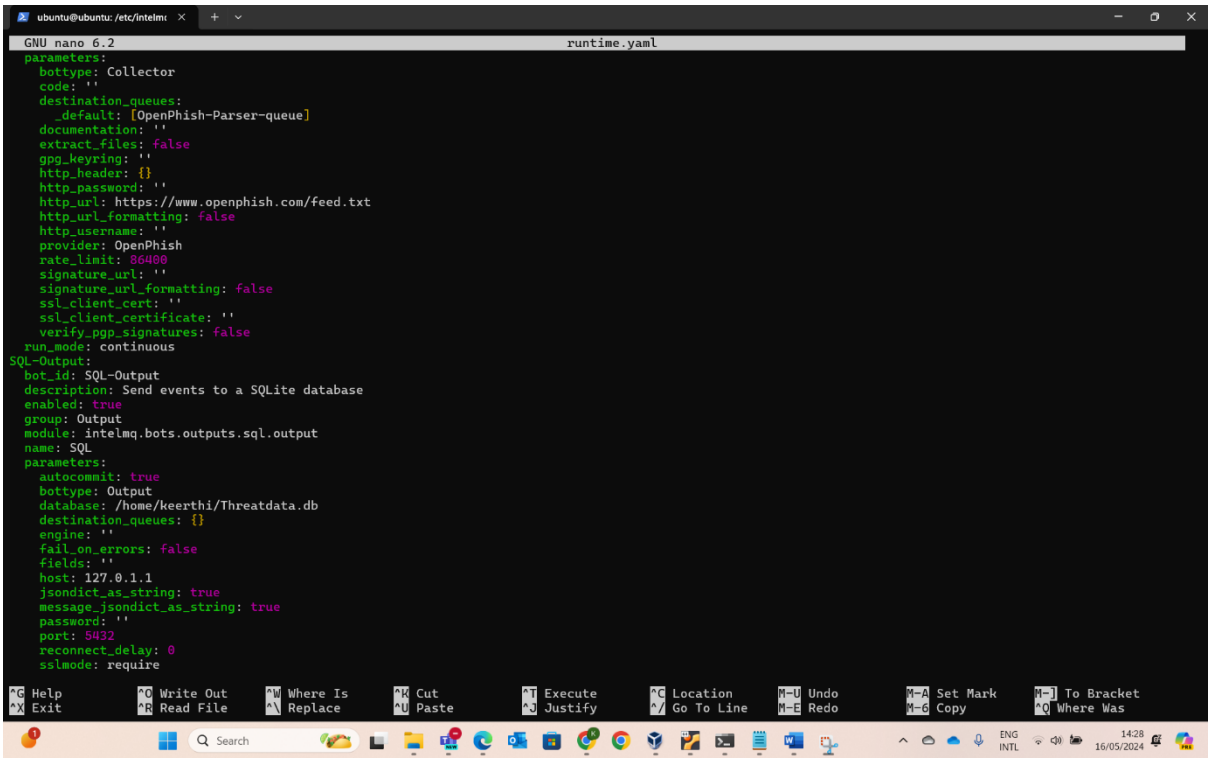


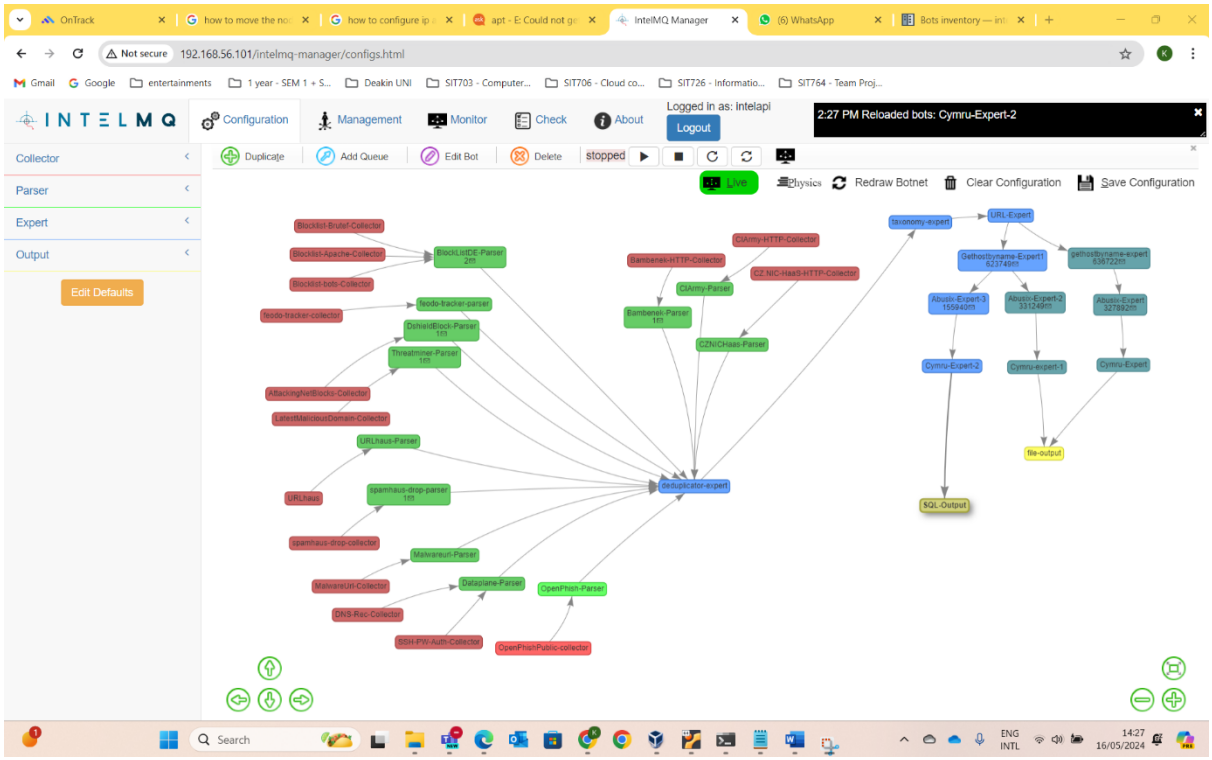
In the IntelMQ configuration file located at /etc/intelmq/runtime.yaml, I attempted to define an output section for the SQL output bot named SQLiteOutput. However, a permission denied error was encountered due to insufficient write permissions for the file.



To circumvent the permission issue, I configured the SQL-Output bot through the IntelMQ user interface in Intelmq-Manager. I integrated the bot into the workflow by dragging it and attaching it downstream of the parser component. Subsequently, I configured the necessary parameters such as description, database path(/home/keerthi/Threatdata.db), host (set to 127.0.1.1), table name, and user credentials.







Upon initiating the execution of the configured bots to process the data flow, the expected output was not generated as anticipated. Further investigation and troubleshooting are required to identify and address the underlying cause of this discrepancy. I did some trouble shooting to find the issue:

Checking Configuration: I double-checked the configuration I set up in the UI to ensure that the database path, host, table name, user, and all other relevant settings were correctly entered.

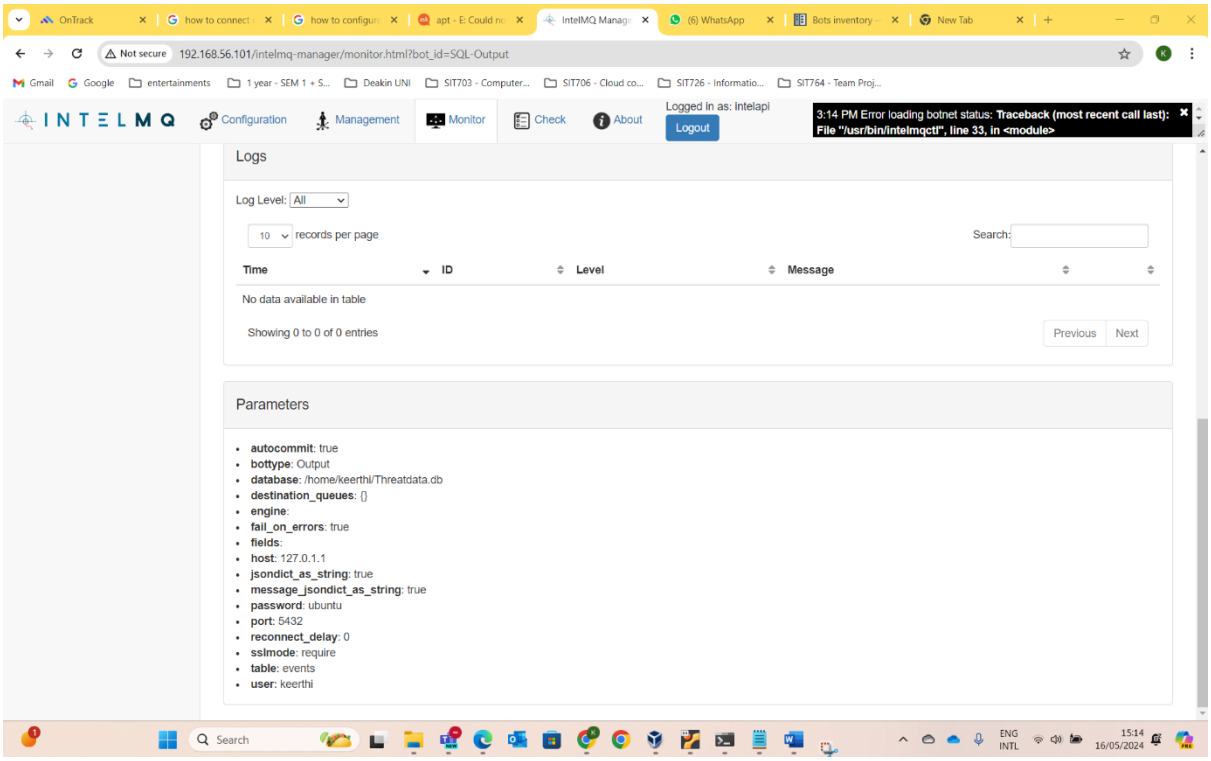
Database Connection: I verified that the SQLite database is accessible from the host where IntelMQ is running. I ensured there were no firewall rules or other network issues blocking the connection.

Bot Logs: Unfortunately, I couldn't find any logs for the SQL-Output bot. Checking the logs of the bot for any errors or warnings could provide valuable insight into what might be going wrong.

Data Flow: Due to being new to IntelMQ, I faced challenges in checking the data flow. It's essential to ensure that the data is being processed and passed to the SQL-Output bot correctly from preceding stages like parsers. Any issues upstream could prevent data from reaching the output bot.

Permissions: I observed that when I configured the output bot in IntelMQ Manager, the runtime.yaml file created the SQL-output bot with all the parameters I provided. Ensuring that the user running IntelMQ has the necessary permissions to write to the SQLite database file and access the specified table is crucial.

Restarting IntelMQ: I attempted to restart IntelMQ, as sometimes changes made in the UI may require a restart for them to take effect. Ensuring that I restarted IntelMQ after making the configuration changes was part of my trouble shooting process.



I was not able to see any log information and there is no output generated even after all that troubleshooting I was not able to fix the issue by myself.

Findings from the Intel MQ and SQL Database Integration task:

Successes:

Access to Intel MQ Interface: Successfully accessed the Intel MQ user interface using provided credentials.

Bot Configuration: Configured and managed various bots for data outputs within the Intel MQ environment.

SQLite Installation: Installed SQLite3 on a dedicated Ubuntu virtual machine to serve as the database backend.

Database Setup: Created a test database named Threatdata.db and initialized a table named 'events' within it for data storage.

Connectivity Establishment: Successfully established ping connectivity between the Intel MQ instance and the dedicated Ubuntu VM.

Bot Integration: Configured the SQL-Output bot through the Intel MQ user interface, specifying necessary parameters such as description, database path, host, table name, and user credentials.

Challenges:

Permission Error: Encountered a permission denied error while attempting to define the output section for the SQL-Output bot in the runtime.yaml file, indicating insufficient write permissions.

Output Discrepancy: Despite configuring the bots, initiating their execution did not generate the expected output as anticipated.

Troubleshooting Steps:

Configuration Verification: Confirmed the accuracy of configuration settings including database path, host, table name, and user credentials.

Accessibility Check: Ensured accessibility of the SQLite database from the Intel MQ host by ruling out firewall or network issues.

Log Examination: Attempted to retrieve logs from the SQL-Output bot for insights, unfortunately, logs were not available.

Data Flow Inspection: Investigated the data flow to confirm data transmission to the output bot.

Permissions Review: Reviewed user permissions for the Intel MQ process to access and write to the database file.

System Restart: Restarted IntelMQ to enforce configuration changes.

Unresolved Issue: Despite diligent troubleshooting efforts, the expected output from the SQL-Output bot remains elusive. The absence of logs from the bot complicates further investigation.

Next Steps:

Thorough Investigation: Need thorough investigation to pinpoint the root cause of why the SQL-Output bot fails to generate output with seniors/experts to gain insights and perspectives on resolving the issue efficiently.

References:

[1] DigitalOcean, "How To Install and Use SQLite on Ubuntu 20.04," DigitalOcean, 23 July 2020. [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-install-and-use-sqlite-on-ubuntu-20-04. [Accessed: 17-May-2024].

[2] IntelMQ Team, "EventDB — IntelMQ 3.0.0 documentation," IntelMQ, 2024. [Online]. Available: https://intelmq.readthedocs.io/en/develop/user/eventdb.html. [Accessed: 17-May-2024].

[3] IntelMQ Team, "IntelMQ Tutorial: Lesson 3," GitHub, 2024. [Online]. Available: https://github.com/certtools/intelmq-tutorial/blob/master/lesson-3.md. [Accessed: 17-May-2024].

[4] IntelMQ Team, "intelmq/bots/outputs at develop," GitHub, 2024. [Online]. Available: https://github.com/certtools/intelmq/tree/develop/intelmq/bots/outputs. [Accessed: 17-May-2024].

[5] A. Kaplan, "IntelMQ: A Framework for CERTs for Collecting and Processing Security Feeds," FIRST, 2020. [Online]. Available: https://www.first.org/resources/papers/malaga20/PUBLIC-Aaron-Kaplan-IntelMQ-malaga-20200131.pdf. [Accessed: 17-May-2024].