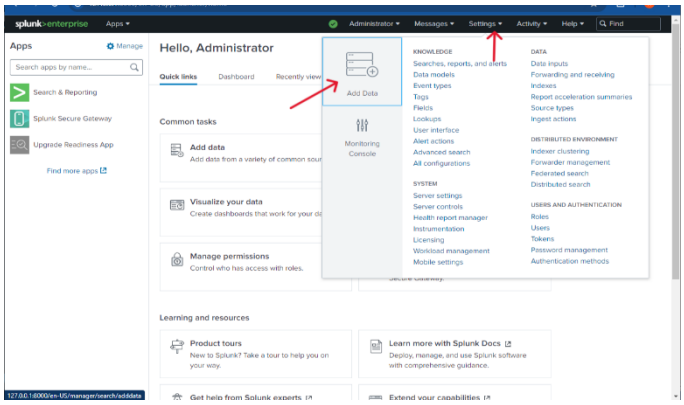
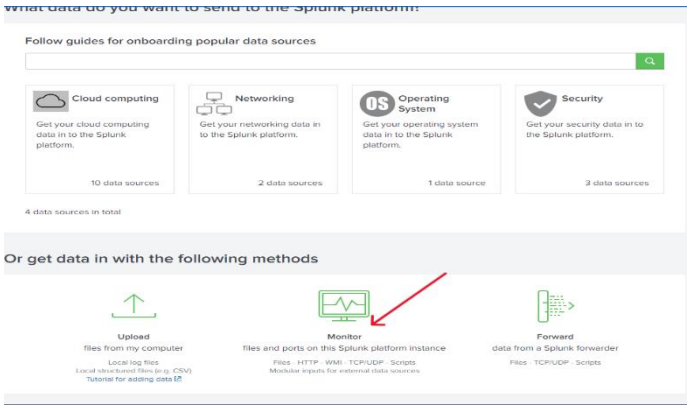
Instructions on log collection and basic searches:

To start monitoring local event logs in Splunk and utilize these search queries, follow these steps:

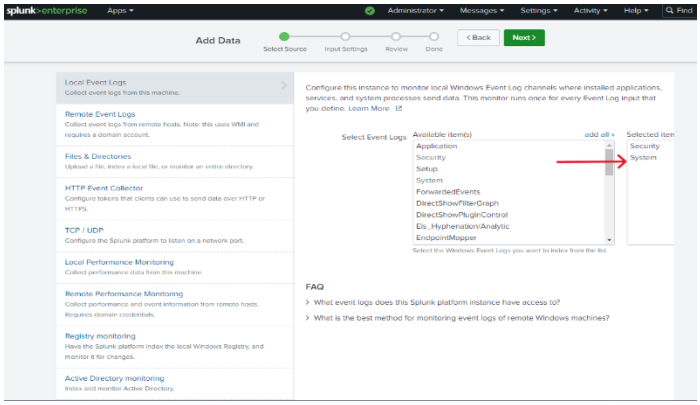
1. Go to the Settings tab and click "Add Data."



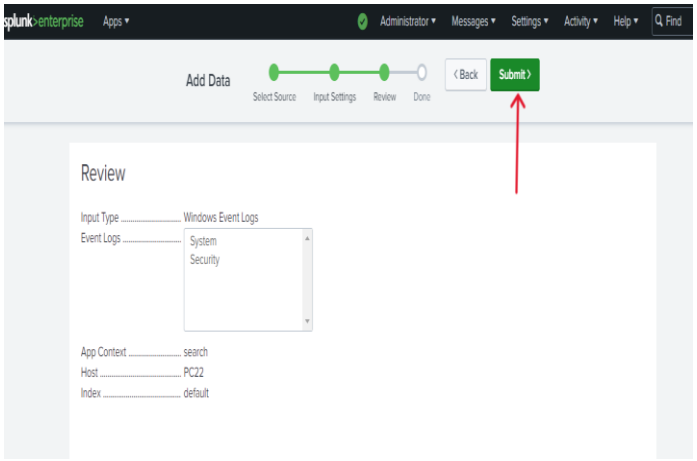
2. Select the monitor icon.



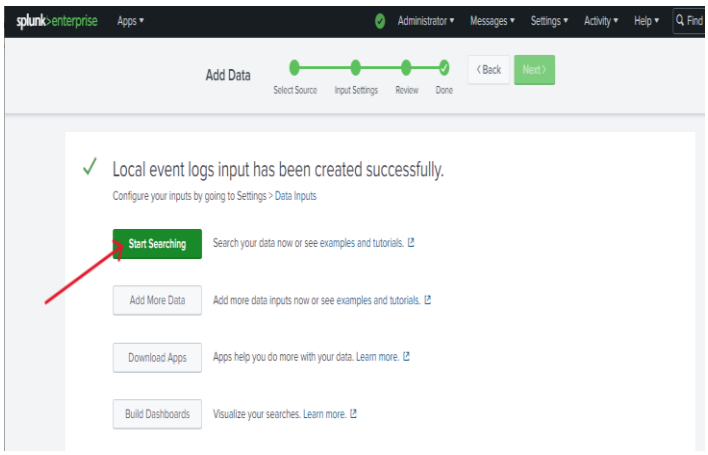
3. Choose to monitor local events logs and add security and system logs, then click "Next."



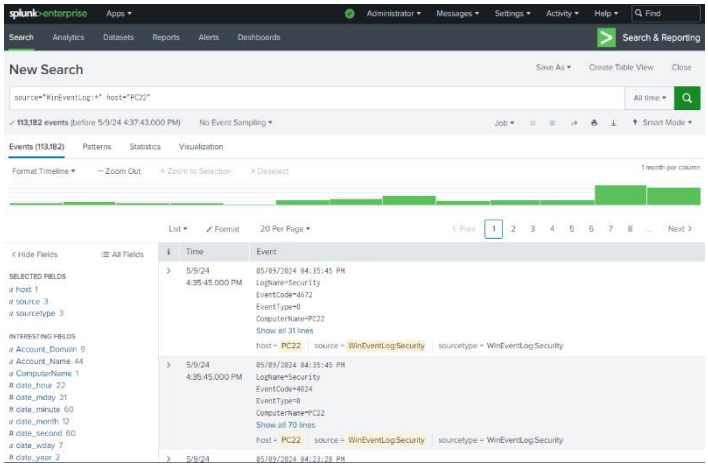
4. Review the settings and click "Submit."



5. Click on "Start searching your data" to begin analyzing the collected logs.



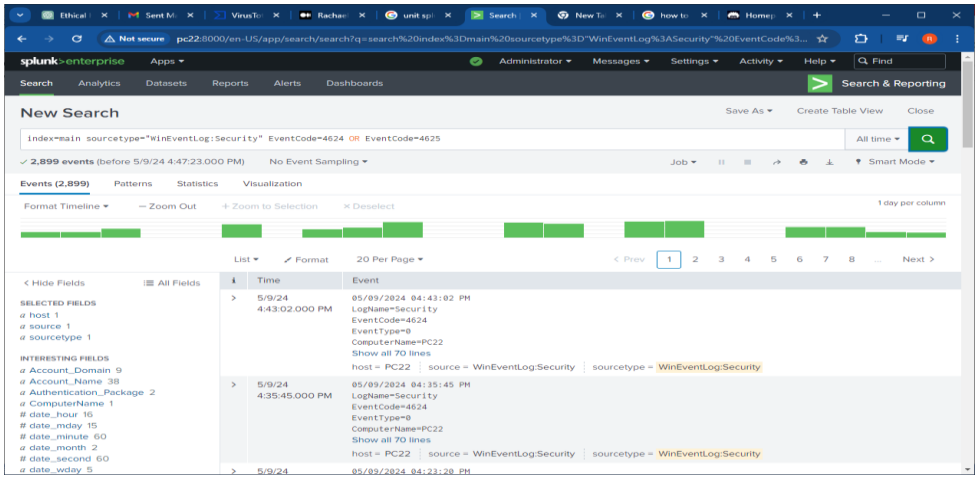
6. The results will be generated as per below. On the search bar you can generate more searches per the information you need.



7. 1. Search for Specific Event IDs :

This search will retrieve all security events with Event IDs 4624 (successful logins) and 4625 (failed logins).

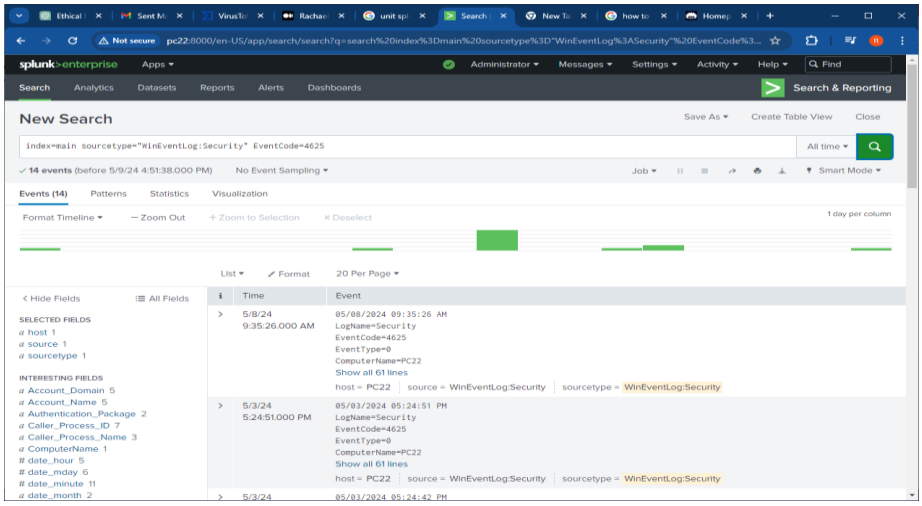
index=main sourcetype="WinEventLog:Security" EventCode=4624 OR EventCode=4625



8. Search for Failed Logins:

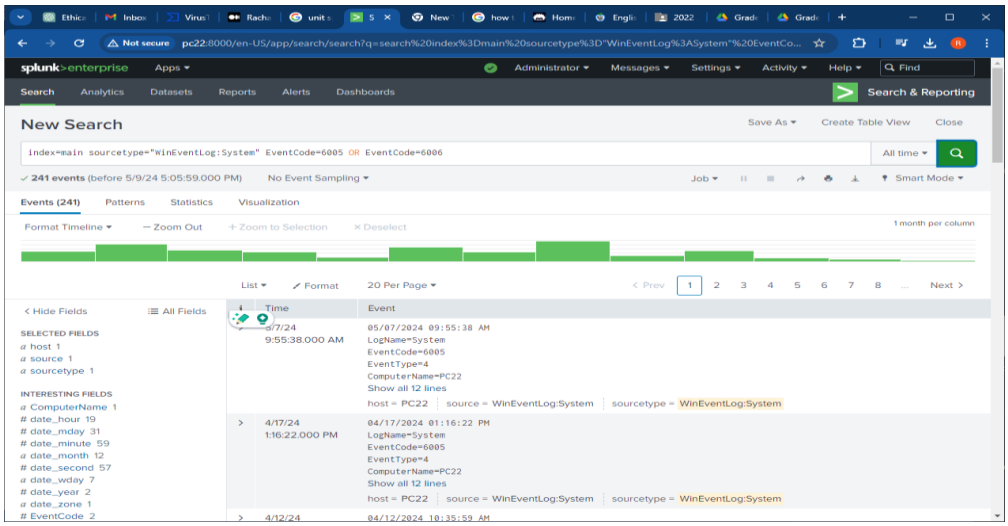
This search will retrieve all security events indicating failed login attempts.

index=main sourcetype="WinEventLog:Security" EventCode=4625



9. Search for System Startup and Shutdown Events:

index=main sourcetype="WinEventLog:System" EventCode=6005 OR EventCode=6006



10. Search for Logins by a Specific User. Replace "username" with the username you want to search for. This search will retrieve successful login events for the specified user.

index=main sourcetype="WinEventLog:Security" EventCode=4624 Account_Name="username"

11. 4. Search for Logins from Specific IP Addresses:

Replace "192.168.1.100" with the IP address you want to search for. This search will retrieve successful login events from the specified IP address.

```
index=main sourcetype="WinEventLog:Security" EventCode=4624
Source_Network_Address="192.168.1.100"
```

12. Search for Account Lockouts

```
index=main sourcetype="WinEventLog:Security" EventCode=4740
```

13. Search for Specific Error Codes

```
index=main sourcetype="WinEventLog:System" EventCode=100
```