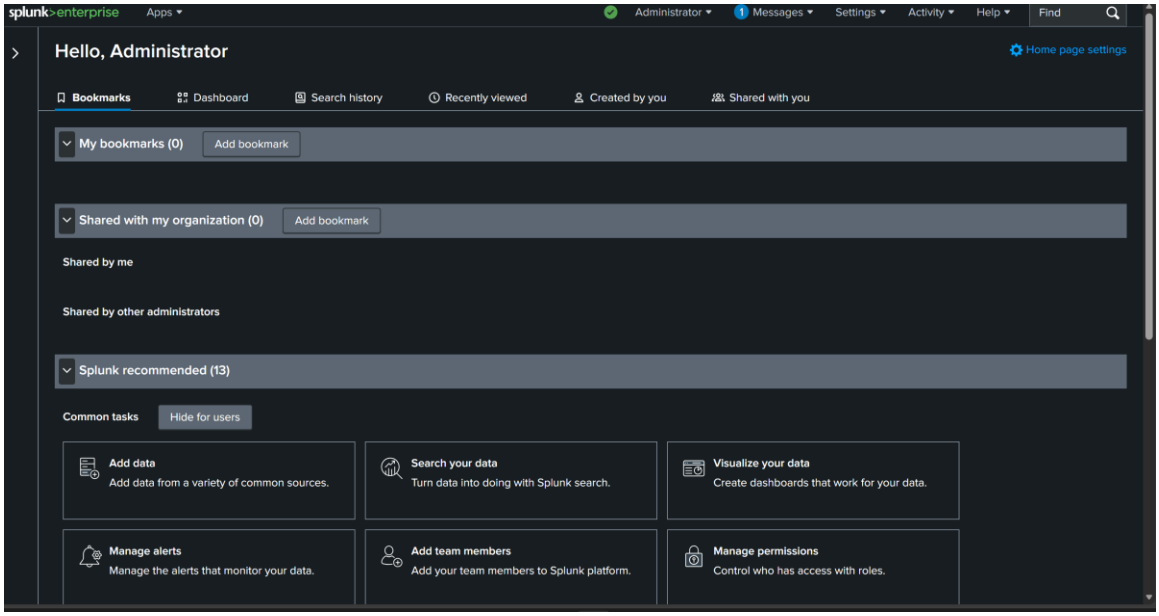
Hands-On Splunk Log Analysis Project

source="bns_practice.csv" host="OLALEKAN" sourcetype="csv"

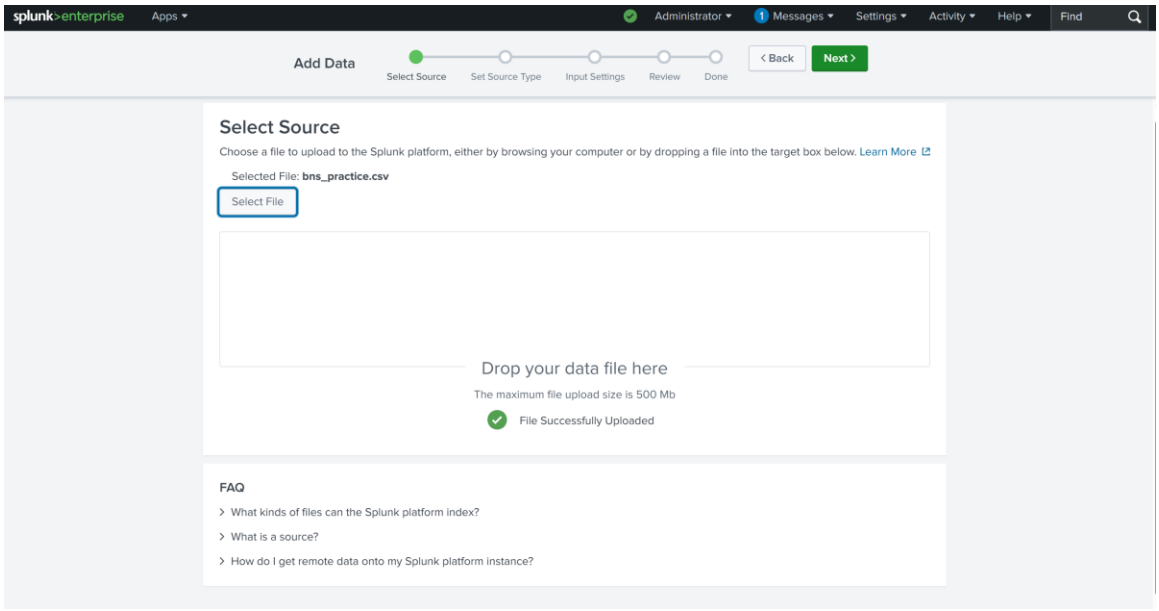
Step 1: Open Splunk

Open your Splunk instance.



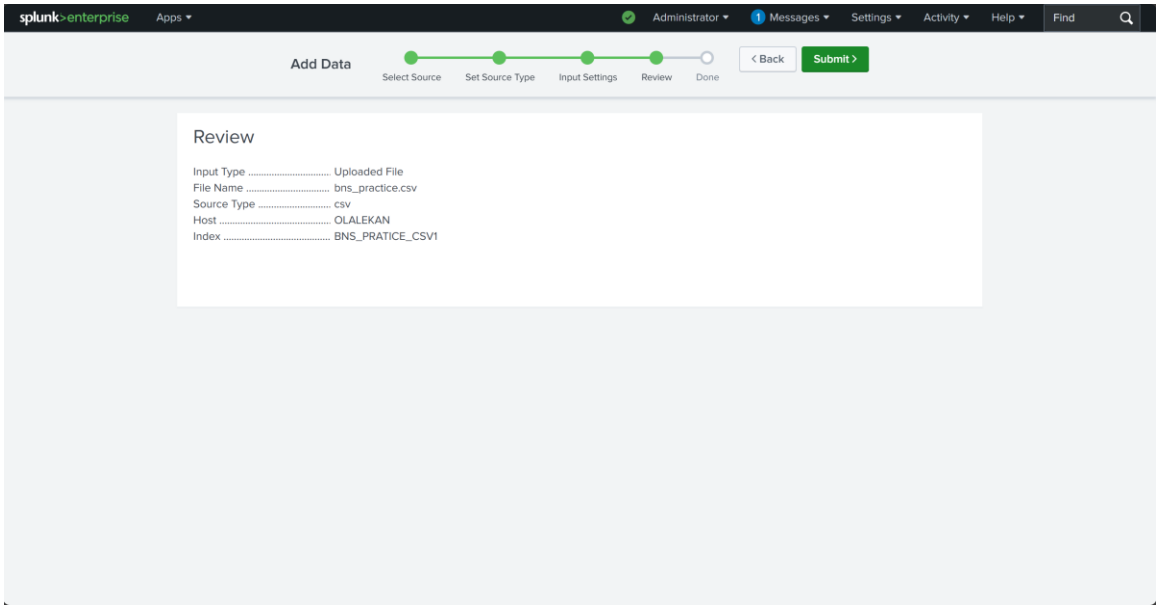
Step 2: Add Data

Navigate to Settings > Add Data.
Upload bns_practice.csv with source type set to CSV.



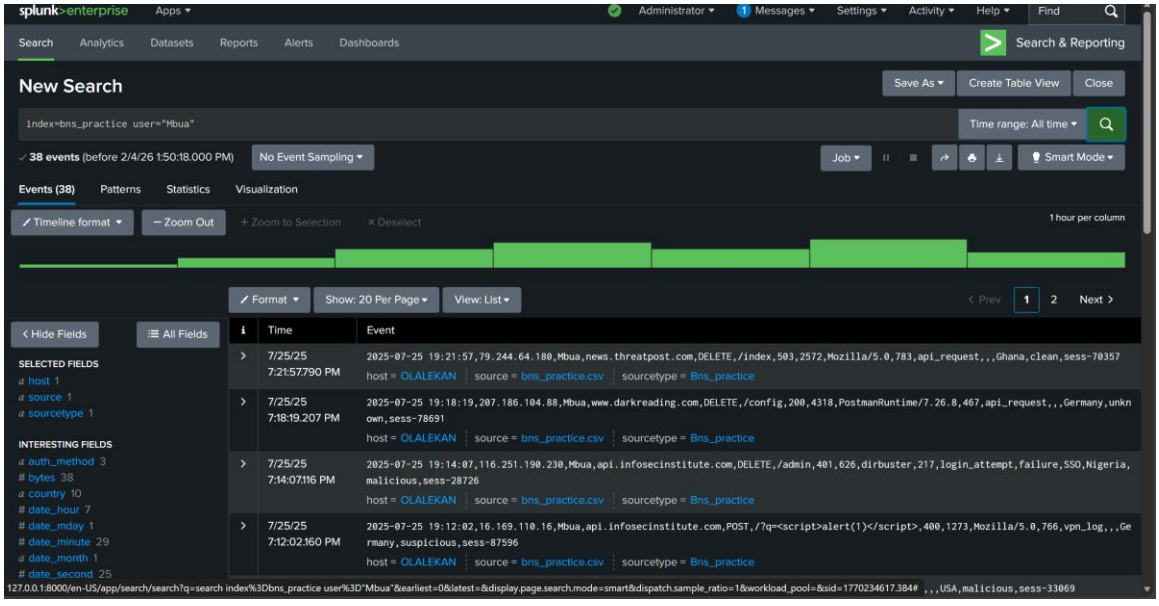
Step 3: Create Index

Index the data under a new index (e.g., bns_practice).



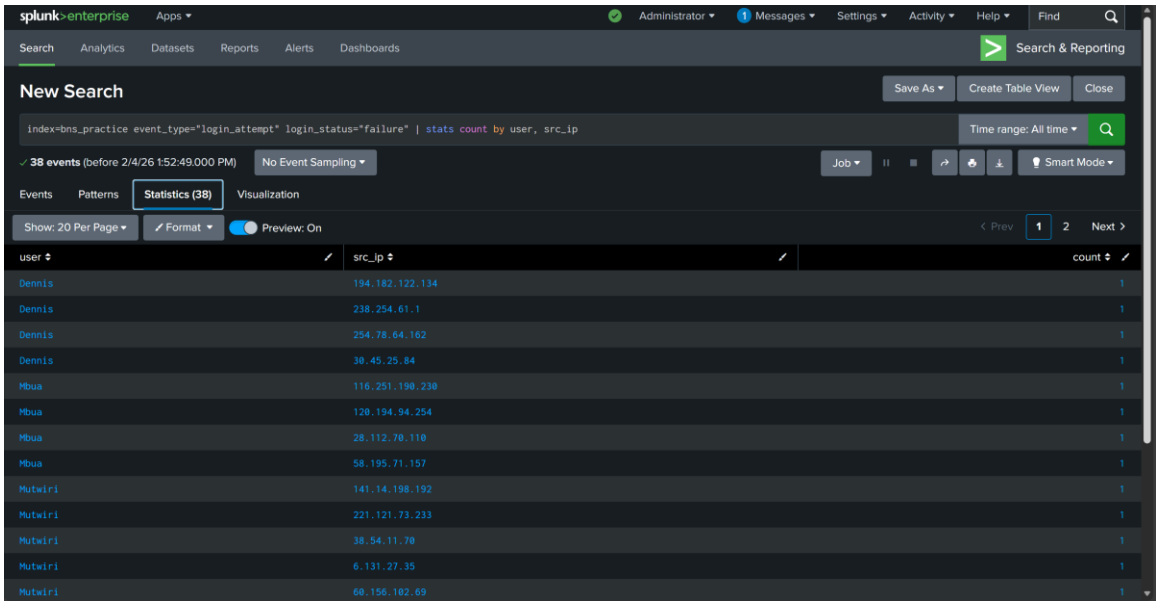
Step 4: Search Events by User

index=bns_practice user="Mbua"



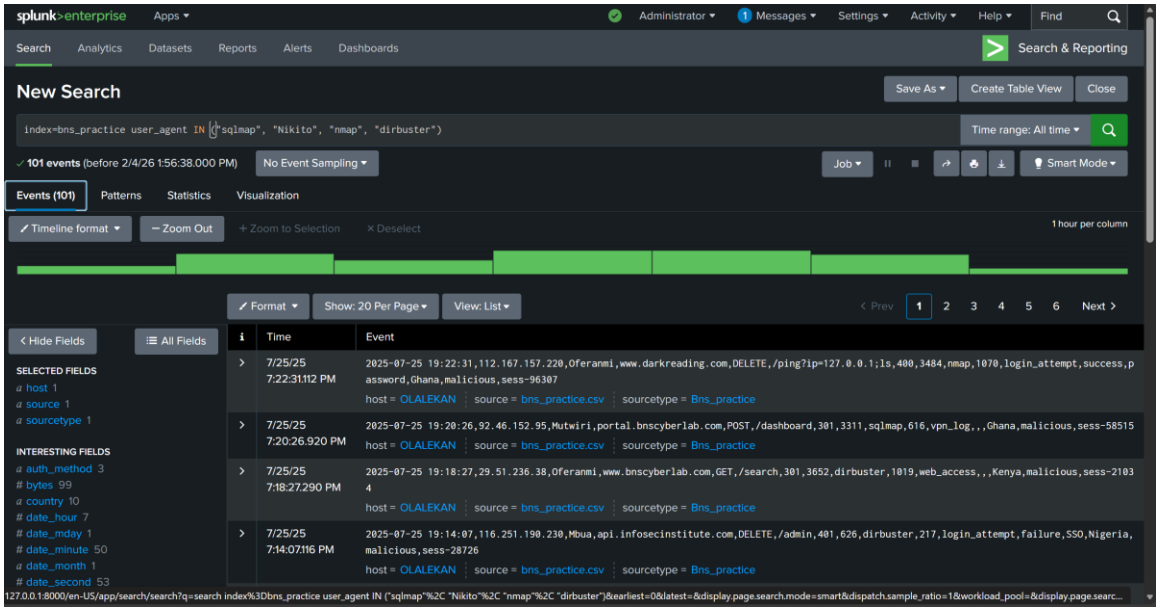
Step 5: Failed Logins per User

index=bns_practice event_type="login_attempt" login_status="failure" | stats count by user, src_ip



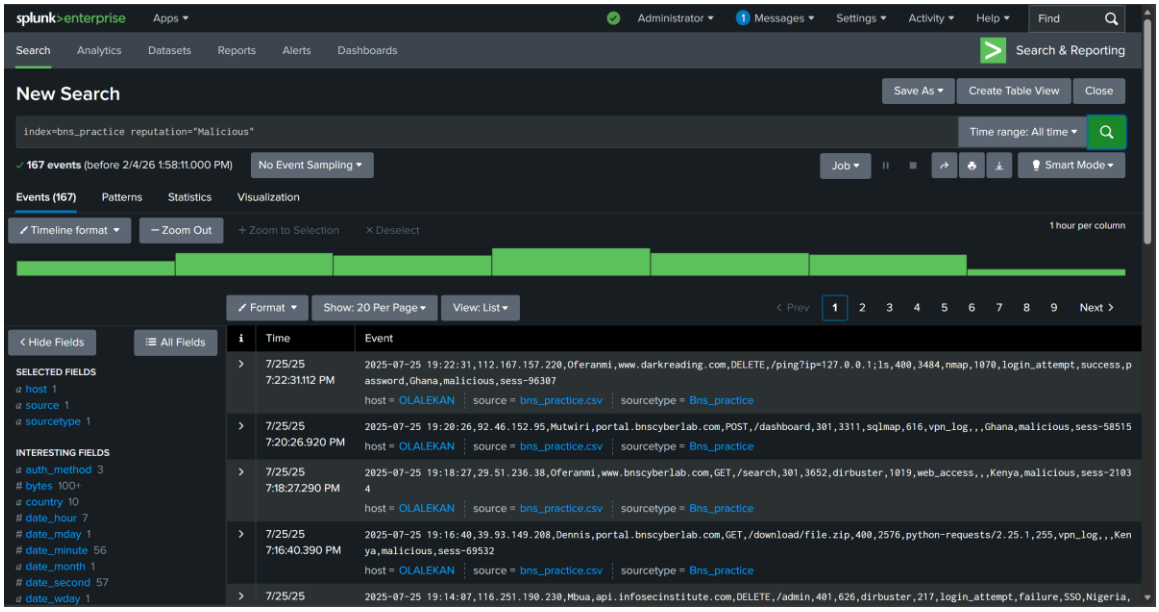
Step 6: Detect Known Bad Tools

index=bns_practice user_agent IN ("sqlmap", "Nikito", "nmap", "dirbuster")



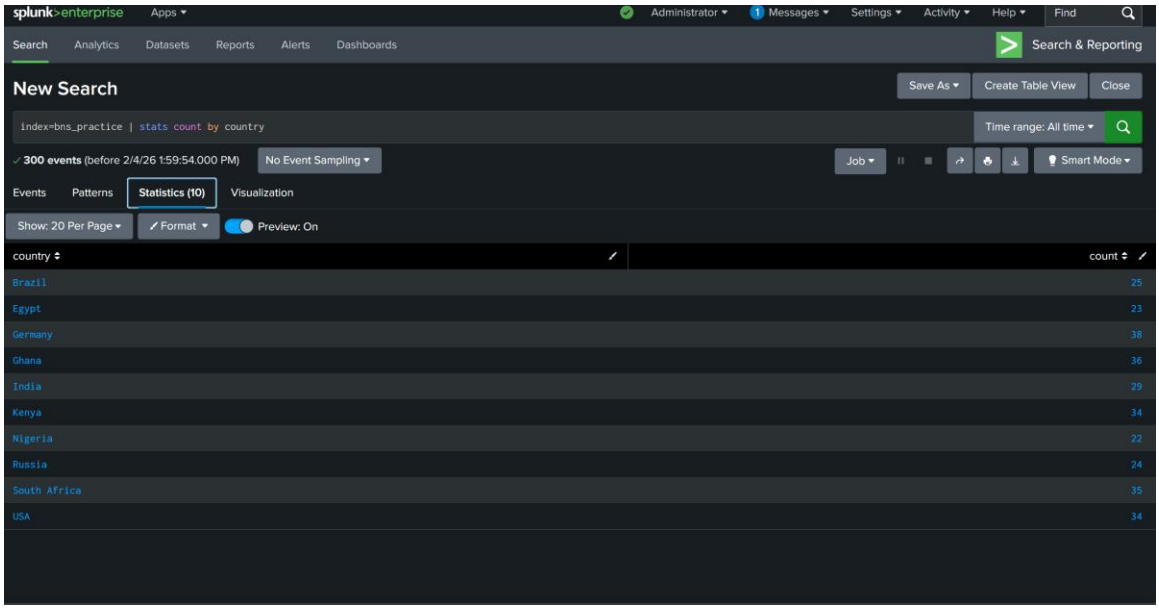
Step 7: Malicious Reputation Events

index=bns_practice reputation="Malicious"



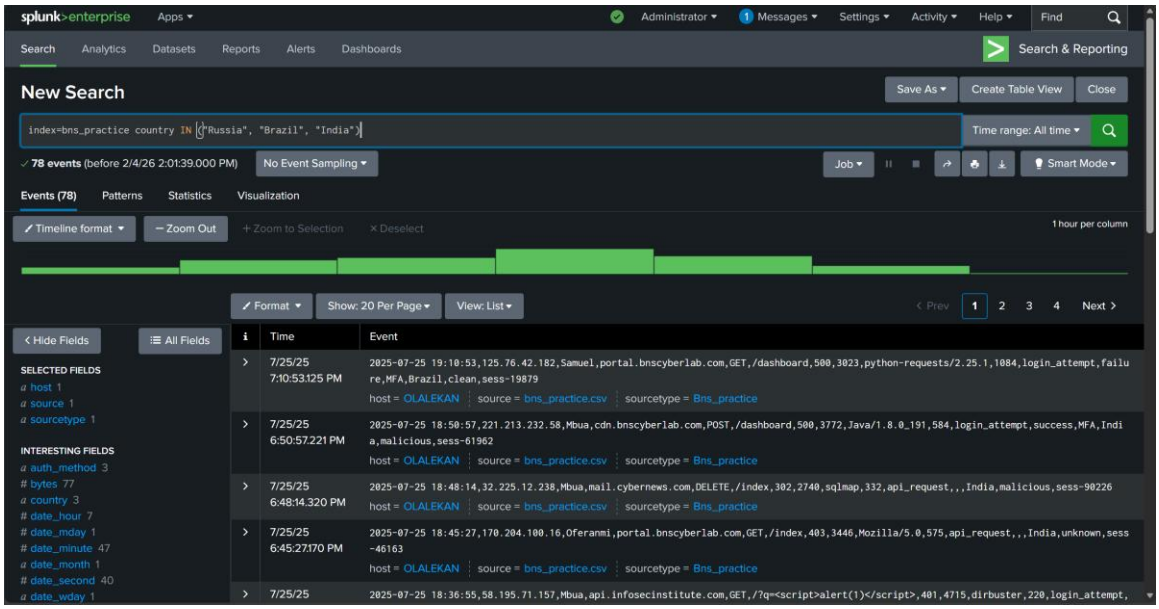
Step 8: Top Countries by Event Count

index=bns_practice | stats count by country



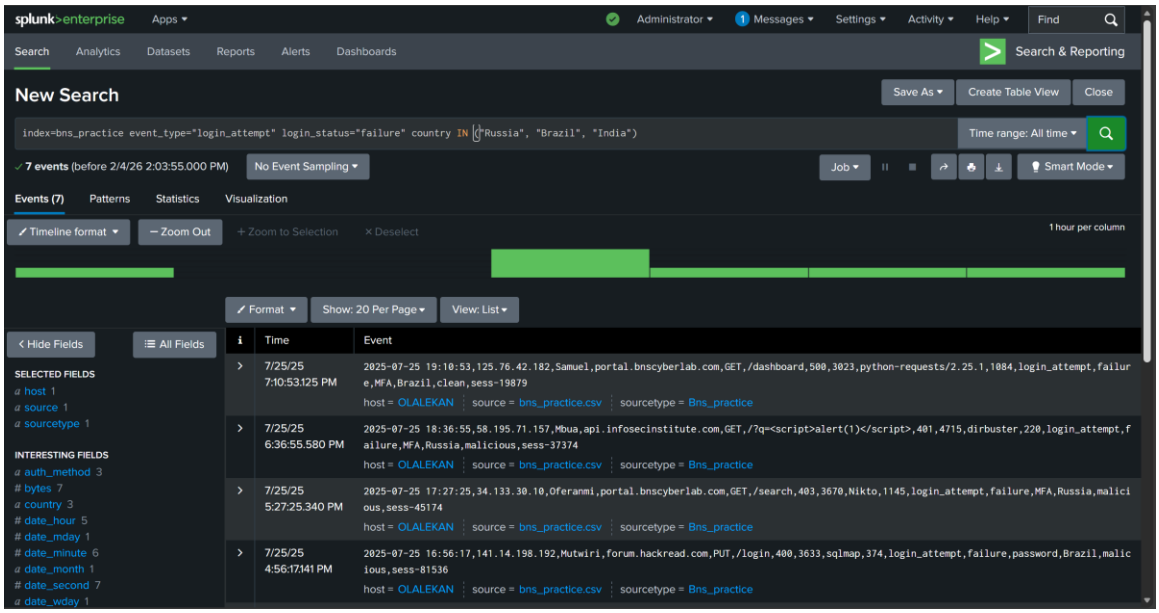
Step 9: Access from Unusual Countries

index=bns_practice country IN ("Russia", "Brazil", "India")



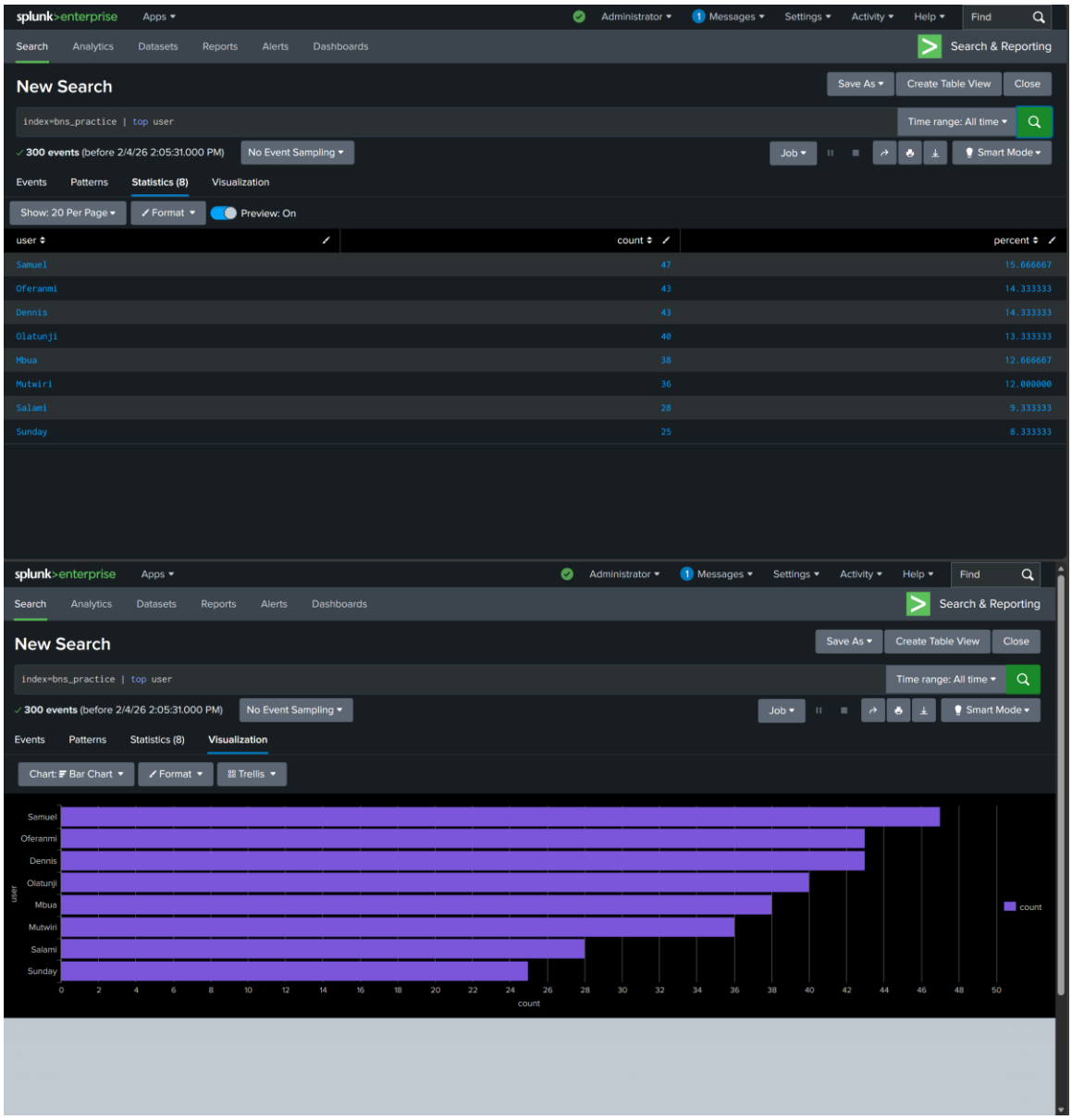
Step 10: Failed Logins from High-Risk Countries

index=bns_practice event_type="login_attempt" login_status="failure" country IN ("Russia", "Brazil", "India")



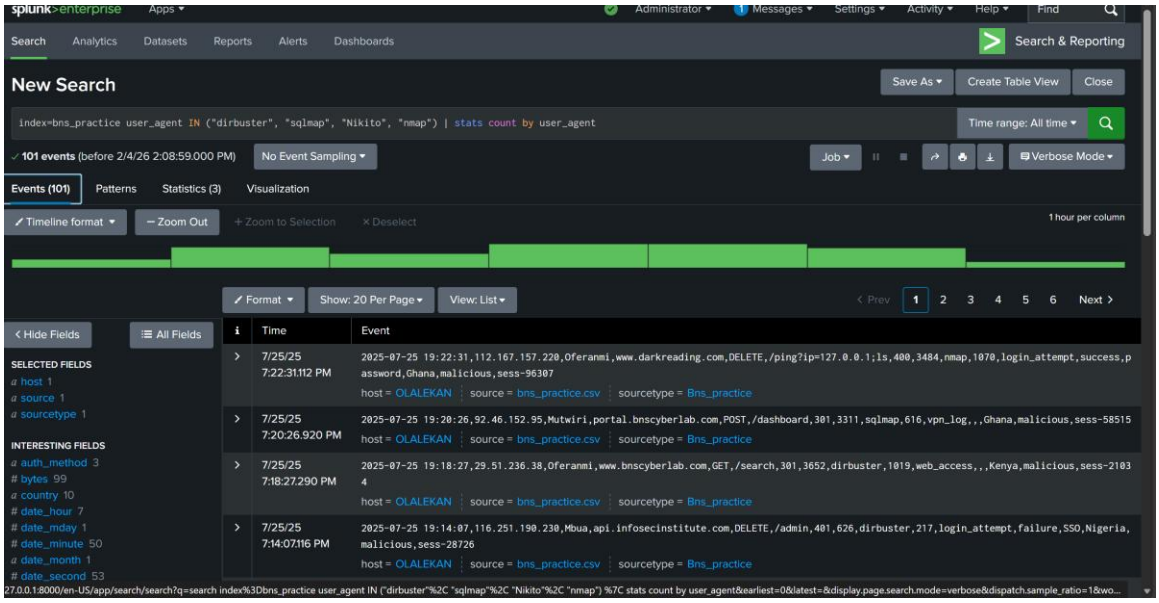
Step 11: Create User Activity Dashboard

index=bns_practice | top user
Click Visualization > Select Bar Chart.



Step 12: Visualize Automated Tool Activity

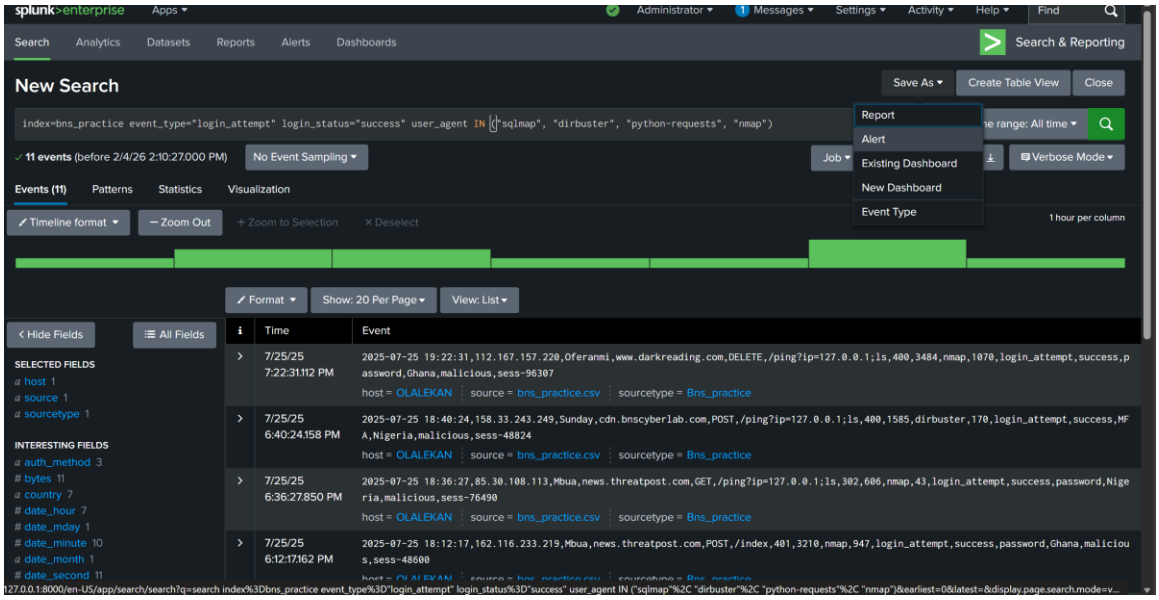
index=bns_practice user_agent IN ("dirbuster", "sqlmap", "Nikito", "nmap") | stats count by user_agent

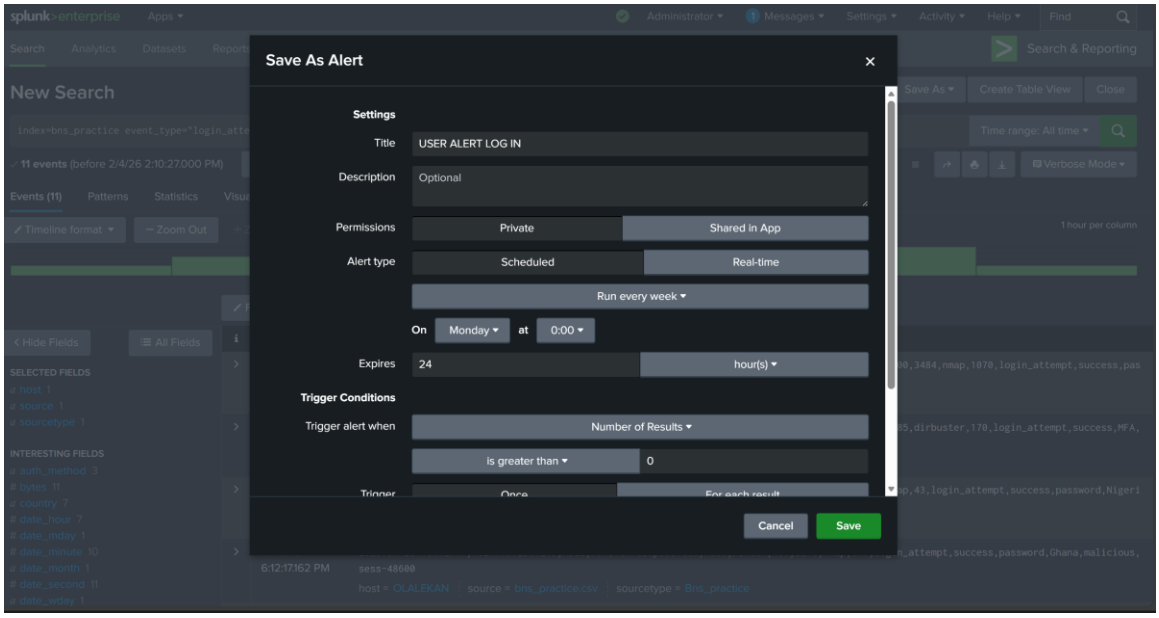


Step 13: Create Alert for Suspicious Successful Login

index=bns_practice event_type="login_attempt" login_status="success" user_agent IN ("sqlmap", "dirbuster", "python-requests", "nmap")

Click Save As > Alert > Configure alert action.





BY AFOLABI MUHYDEEN OLALEKAN
CYBERSECURITY ANALYST