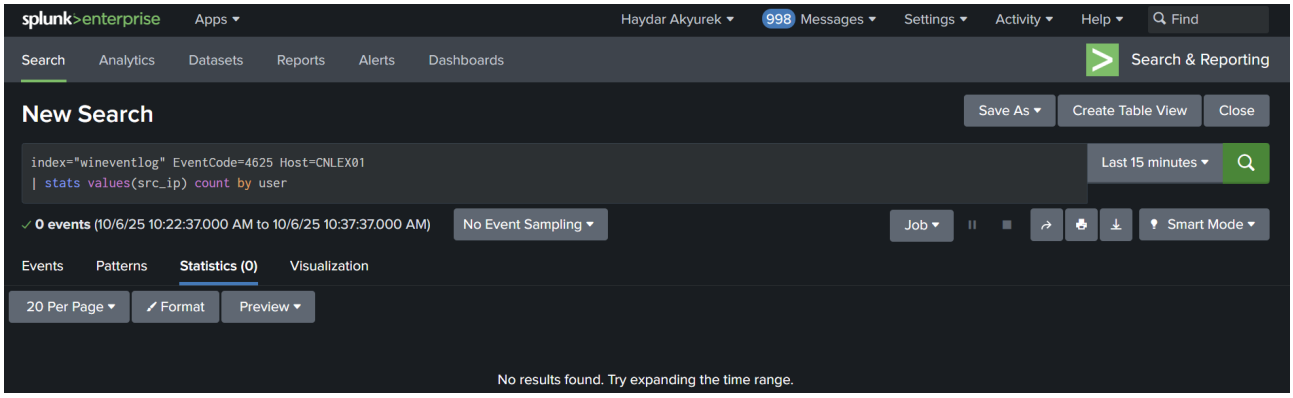
Windows LOGS

1. List the users and external IP addresses that have failed to log in to the Exchange machine security logs in the last 15 minutes.

index="wineventlog" EventCode=4625 Host=CNLEX01

| stats values(src_ip) count by user



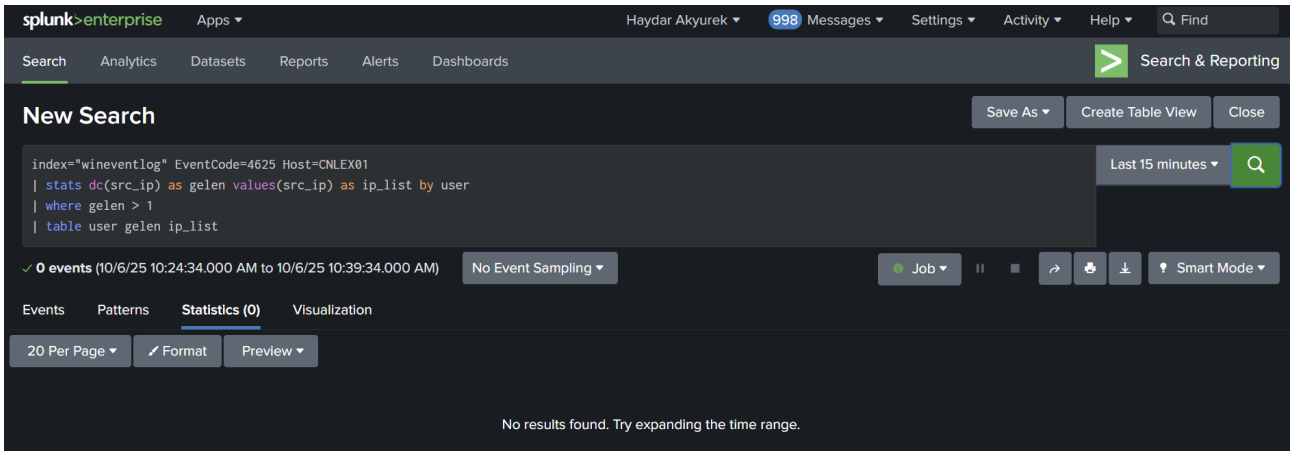
2. List users who have unsuccessfully logged in with more than one external IP address in the Exchange machine security logs in the last 15 minutes.

index="wineventlog" EventCode=4625 Host=CNLEX01

| stats dc(src_ip) as gelen values(src_ip) as ip_list by user

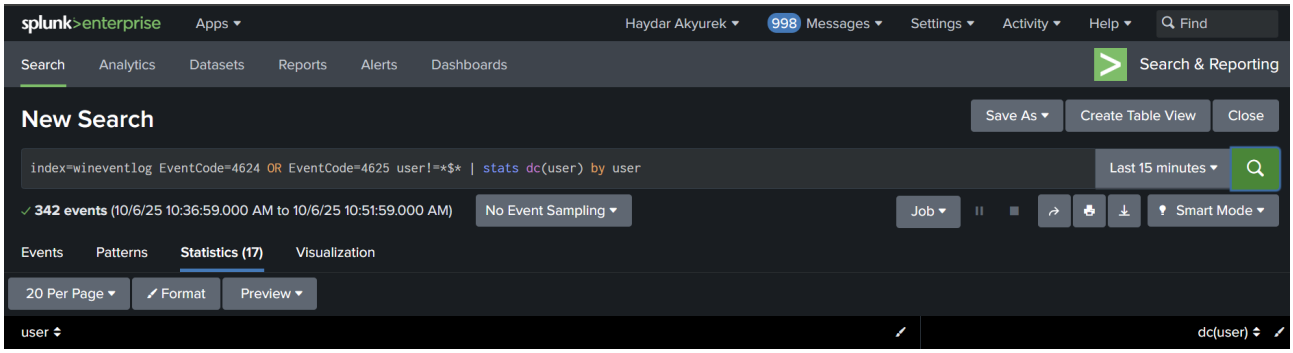
| where gelen > 1

| table user gelen ip_list



3. List successful and unsuccessful logins from the same user in the Windows security logs in the last 15 minutes.

index=wineventlog EventCode=4624 OR EventCode=4625 user!=*$* | stats dc(user) by user



4. List users whose accounts have been locked in the Windows security logs in the last 24 hours.

index="wineventlog" EventCode=4740 | table user| dedup user