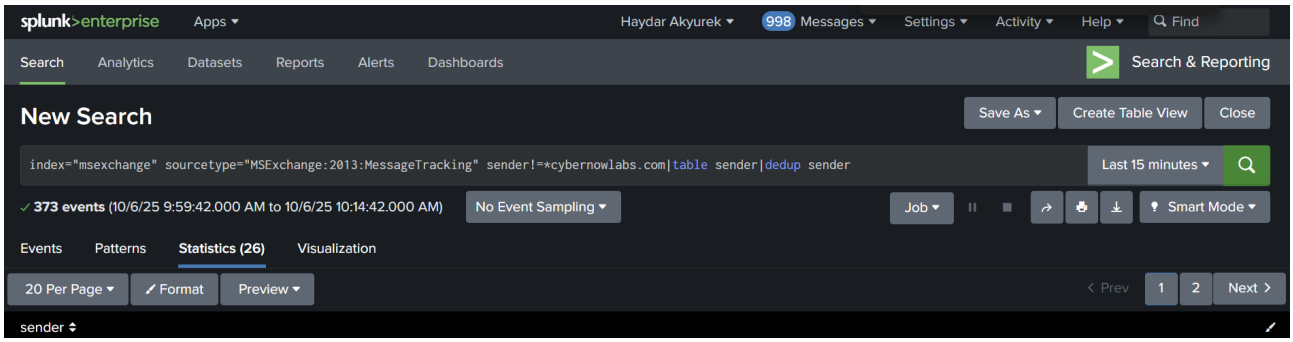
Email LOGS

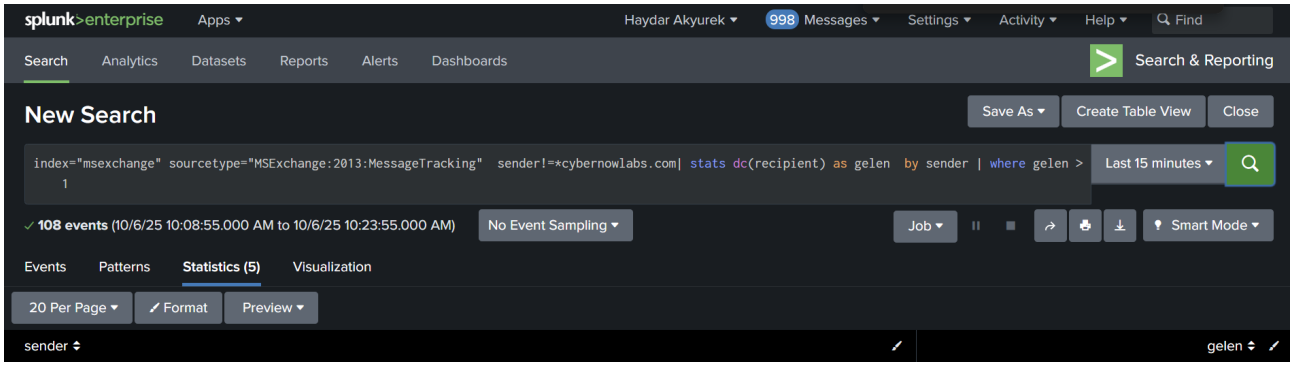
1.Identify external email addresses that have sent emails to CNL users in the last 15 minutes.

index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender! =*company_email* | table sender | dedup sender



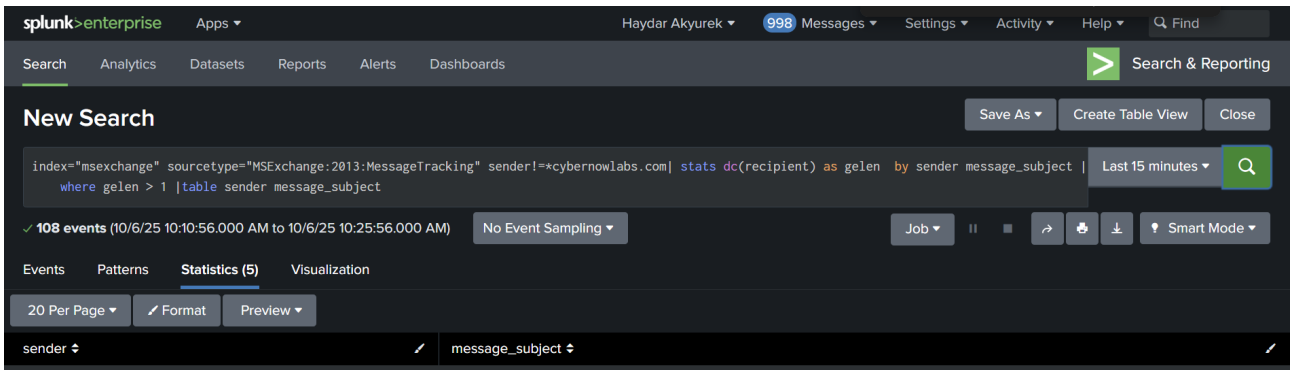
2. Identify external email addresses that have sent emails to more than one CNL user in the last 15 minutes.

index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender! =*cybernowlabs.com| stats dc(recipient) as gelen by sender | where gelen > 1



3. Identify external email addresses and email subjects that have sent emails to more than one CNL user in the last 15 minutes.

index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender! =*cybernowlabs.com| stats dc(recipient) as gelen by sender message_subject | where gelen > 1 |table sender message_subject


splunk>enterprise
Apps
Haydar Akyurek
998 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="msexchange" sourcetype="MSExchange:2013:MessageTracking" sender!=*cybernowlabs.com| stats dc(recipient) as gelen by sender message_subject | where gelen > 1 |table sender message_subject
Last 15 minutes
108 events (10/6/25 10:10:56.000 AM to 10/6/25 10:25:56.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (5)
Visualization
20 Per Page
Format
Preview
sender
message_subject