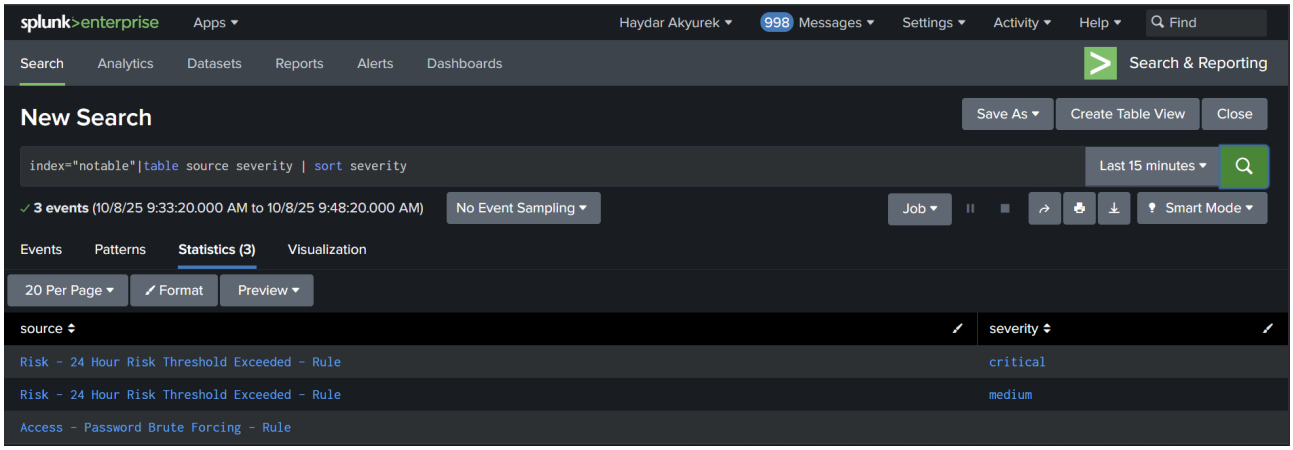
NOTABLE LOGS

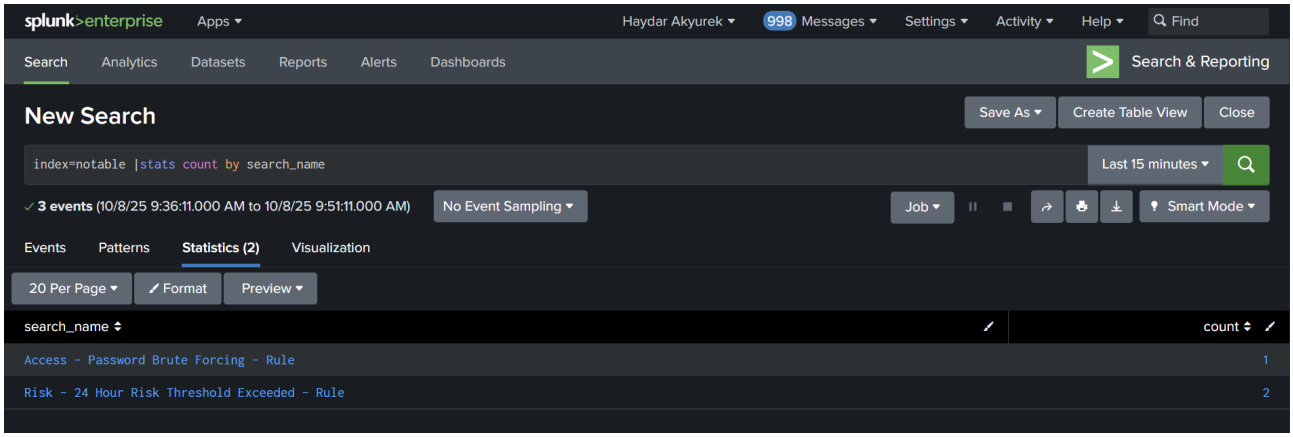
1) List notable events that occurred within 15 minutes.

index="notable"|table source severity | sort severity



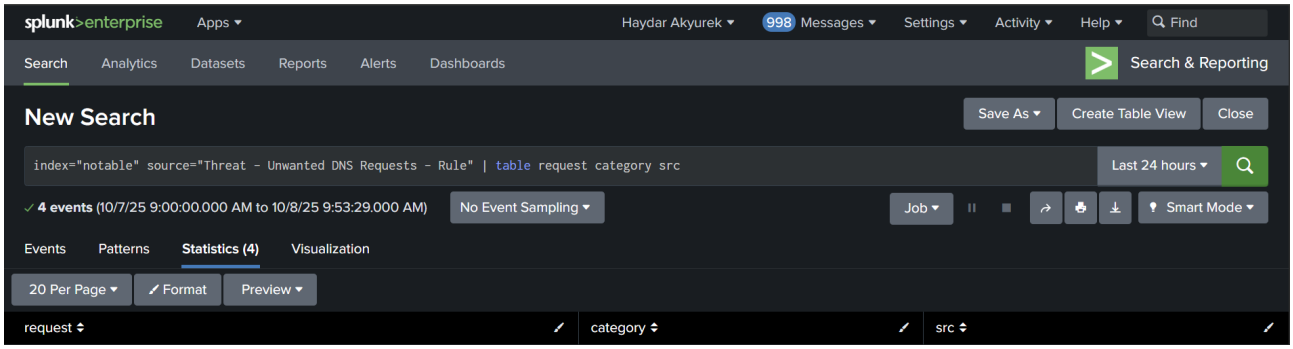
2) Identify notable events and their numbers within 15 minutes.

index=notable |stats count by search_name



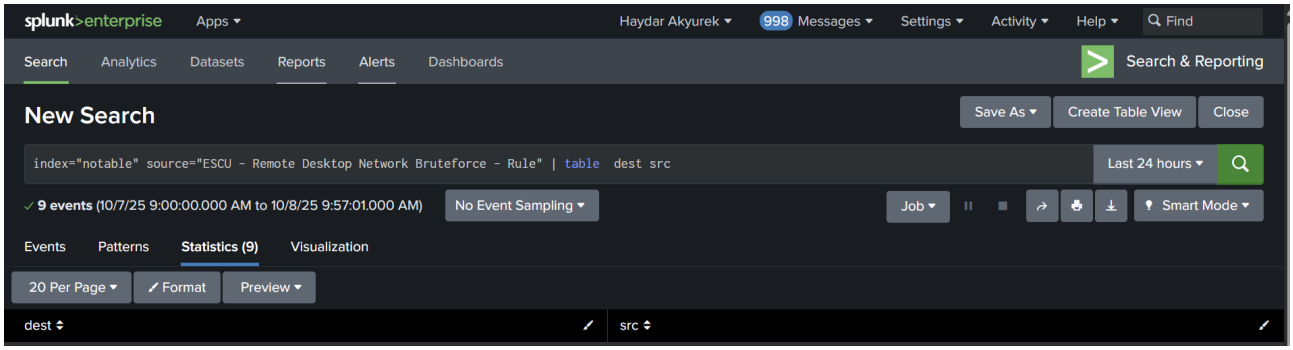
3) List the source IP addresses, categories, and requests involved in the "Unwanted DNS Request" event within 24 hours.

index="notable" source="Threat - Unwanted DNS Requests - Rule" | table request category src



4) List the source and destination IP addresses involved in the "Remote Desktop Network Bruteforce" incident within 24 hours.

index="notable" source="ESCU - Remote Desktop Network Bruteforce - Rule" | table dest src



5) Identify source external IP addresses involved in more than 1 incident in 24 hours.

index="notable" | stats dc(source) as olay values(source) as kurallar count by src_ip | where olay > 1