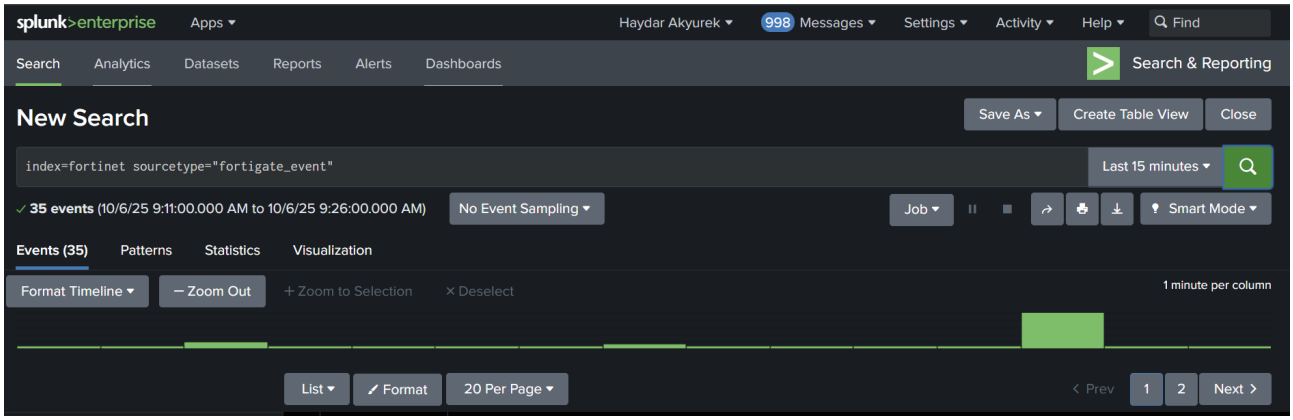
VPN LOGS

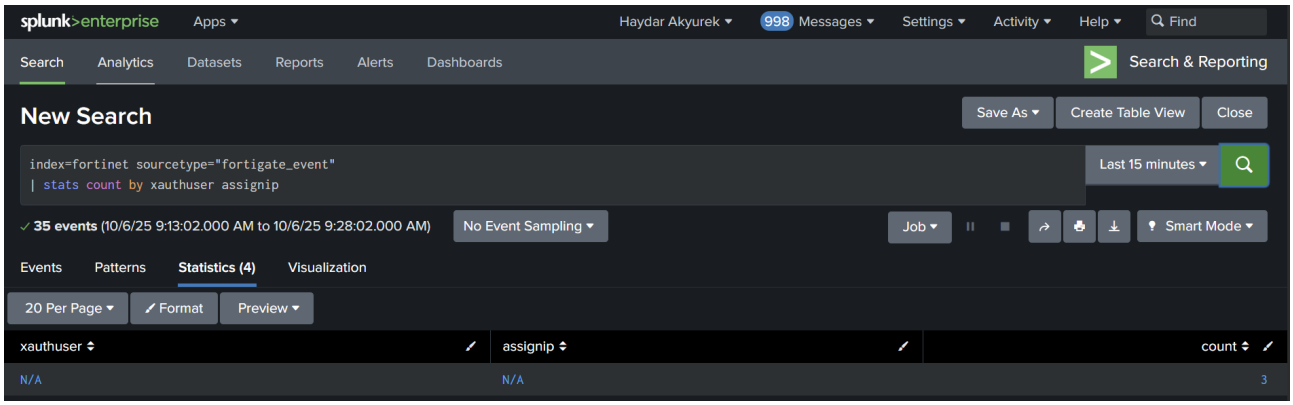
1. Filter Firewall Event logs.

index="fortinet" sourcetype="fortigate_event"



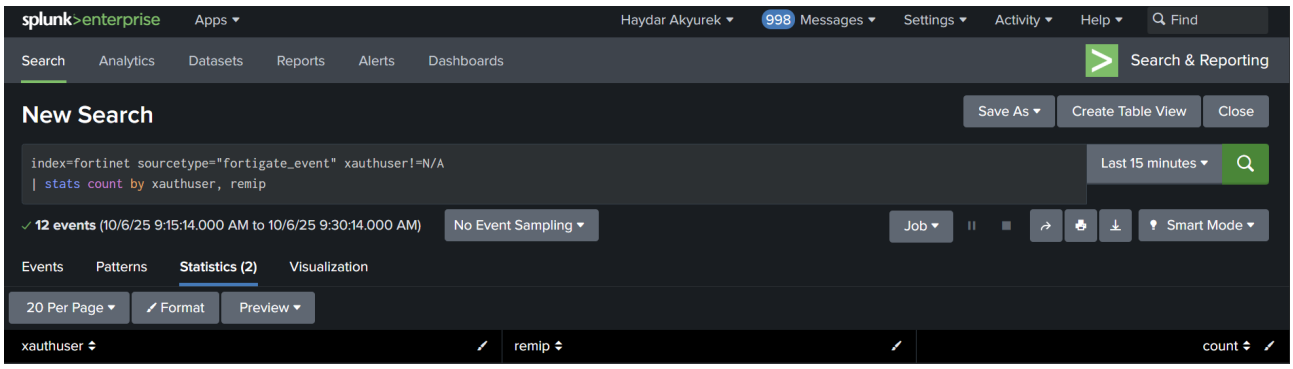
2. List VPN users and their assigned internal IP addresses in the last 15 minutes.

index=fortinet sourcetype="fortigate_event" | stats count by xauthuser assignip



3. List VPN users and their external IP addresses in the last 15 minutes.

index=fortinet sourcetype="fortigate_event" xauthuser!=N/A earliest=-1h latest=now | stats count by xauthuser, remip



4. List VPN users and their internal IP addresses that have failed login attempts in the last 24 hours.