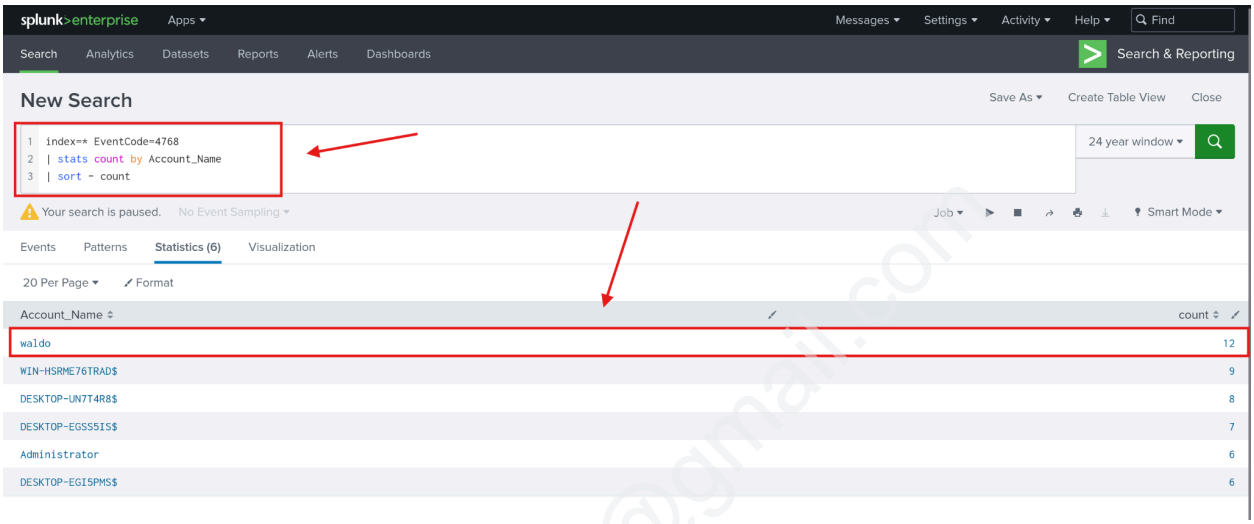
Splunk> Searching, Filtering, Transforming, and Visualizing Data using SPL.

---

1. SPL search against all data the account name with the highest amount of Kerberos authentication ticket requests.

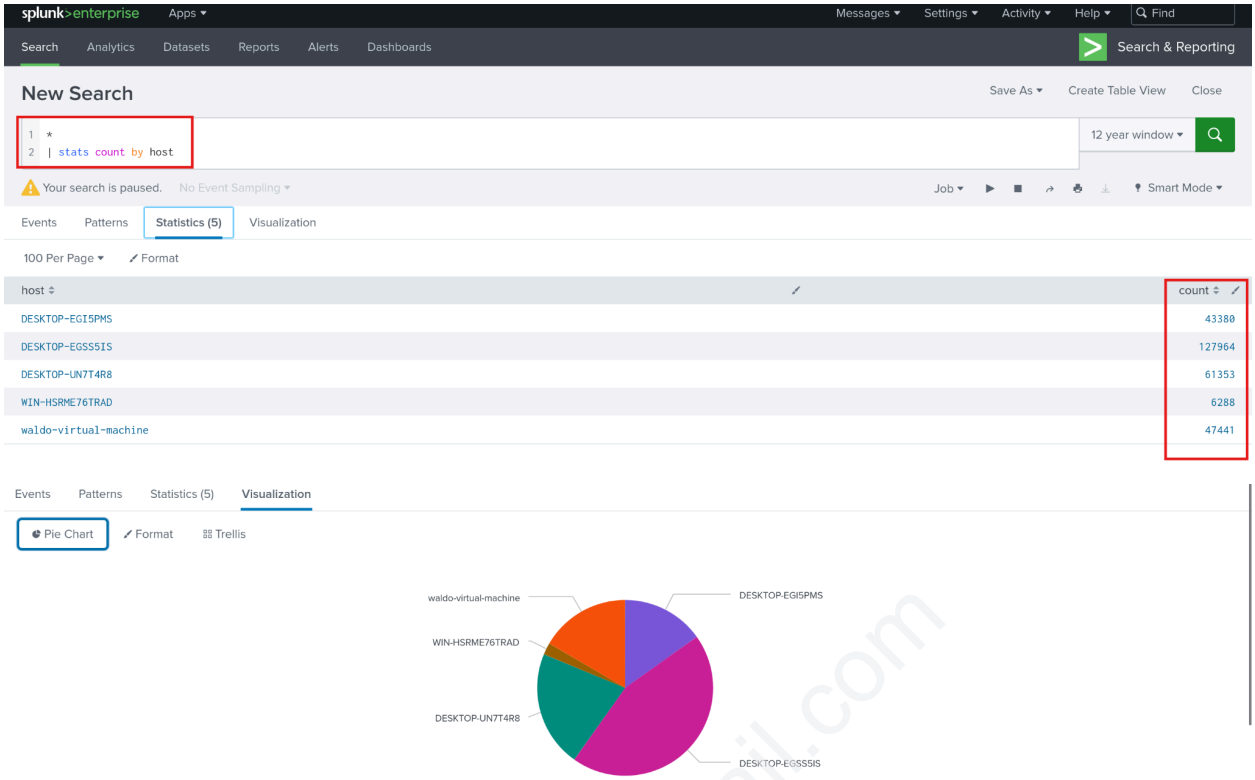
EventCode - 4768 (Kerberos authentication ticket requests)



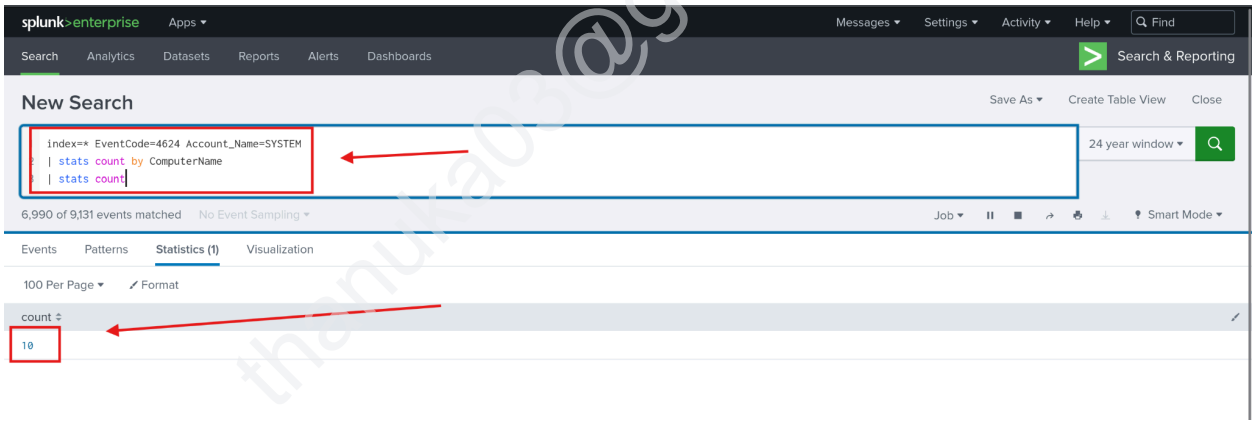
ANSWER - waldo - 12

2. SPL query to find the total number of events for each host.

thanuka03@gmail.com



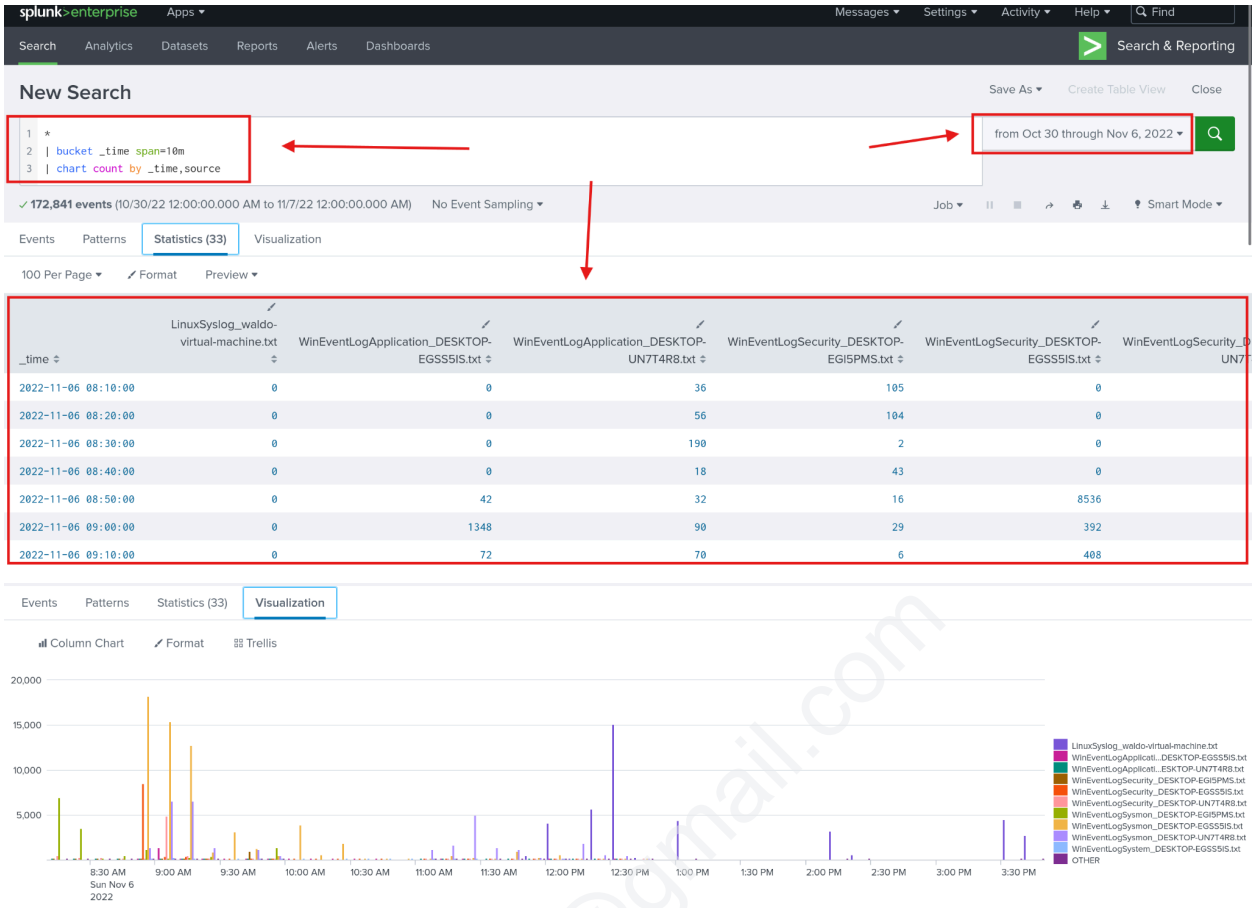
3. SPL search against all 4624 events the count of distinct computers accessed by the account name SYSTEM



ANSWER - 10

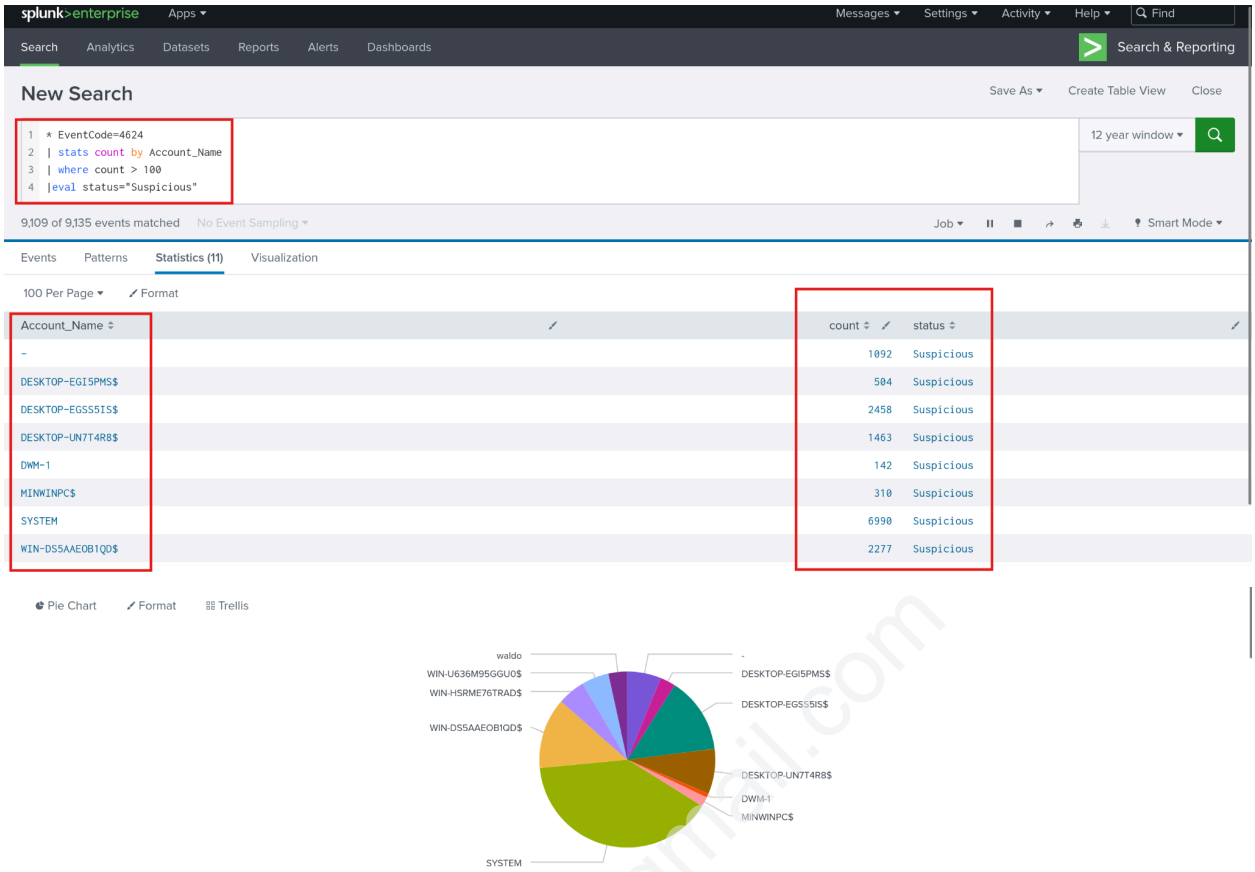
4. Create a time-based chart that shows the number of events from each source, grouped into 10-minute intervals. From Oct 30 - Nov 6 /2022

thanuka03@gmail.com

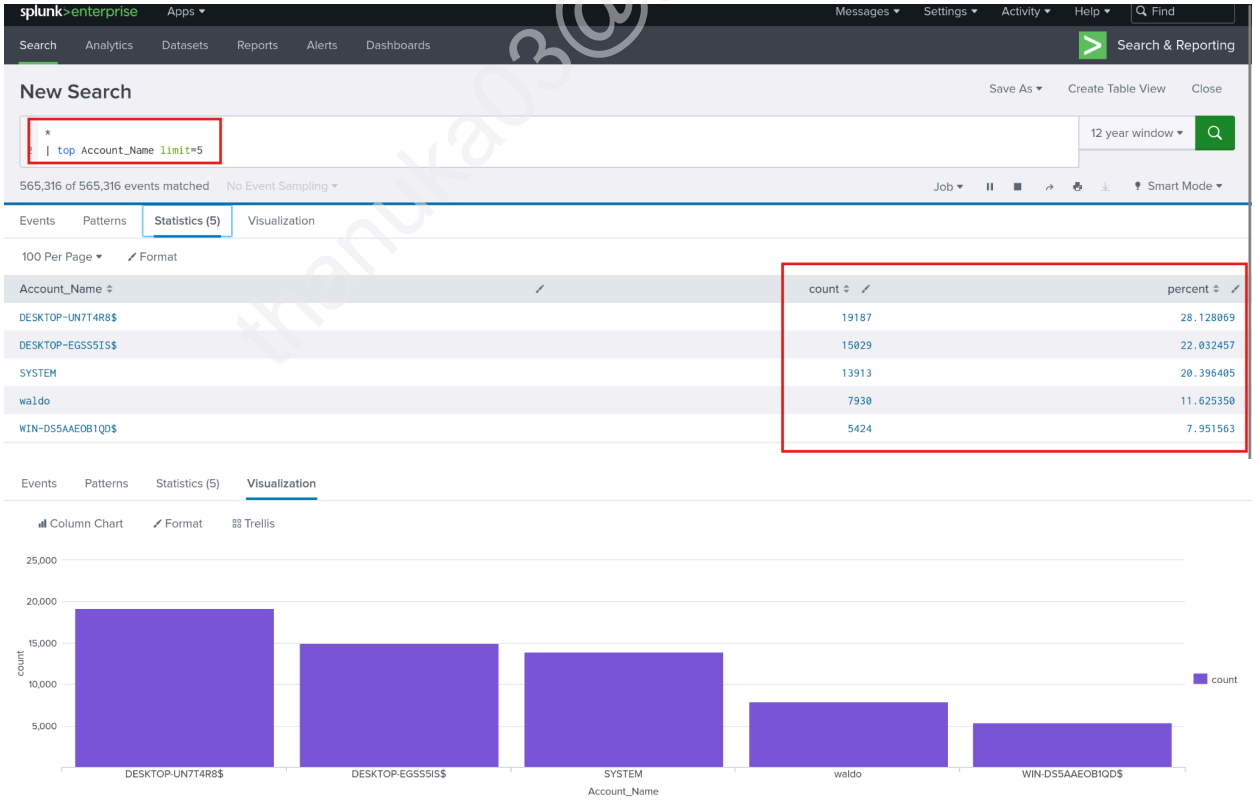


5. SPL query to find users who made more than 100 login attempts (EventCode 4624) and label them as "Suspicious"

thanuka03@gmail.com

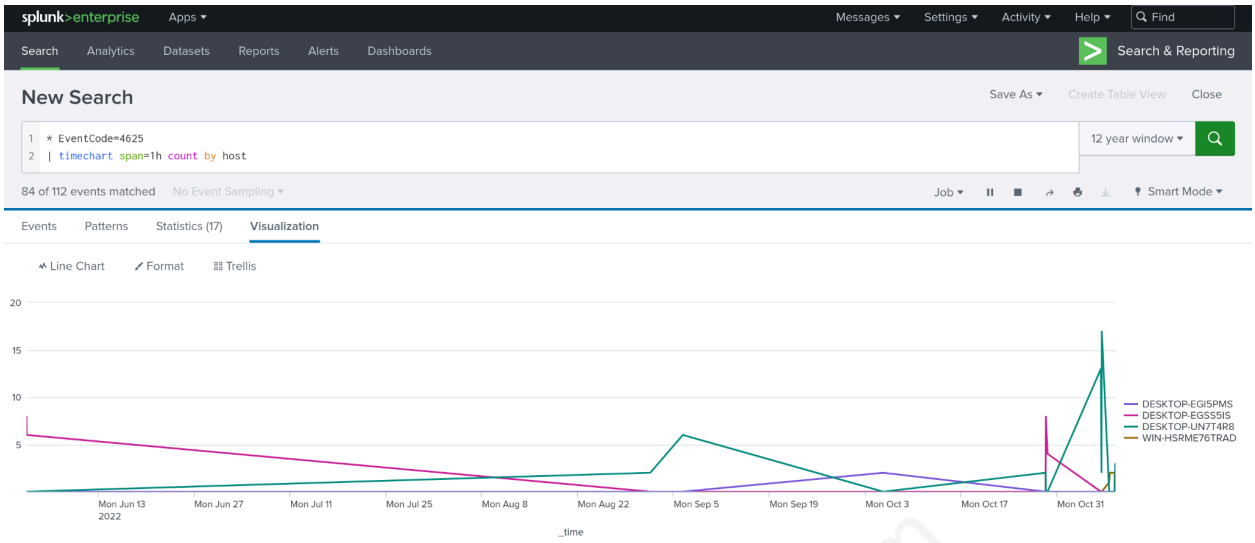


6. SPL query to find the top 5 most active users based on the number of events generated.



thanuka03@gmail.com

7. Create a time-based line chart showing the number of failed logins (EventCode 4625) per host over time.



E N D

thanuka03@gmail.com