

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.

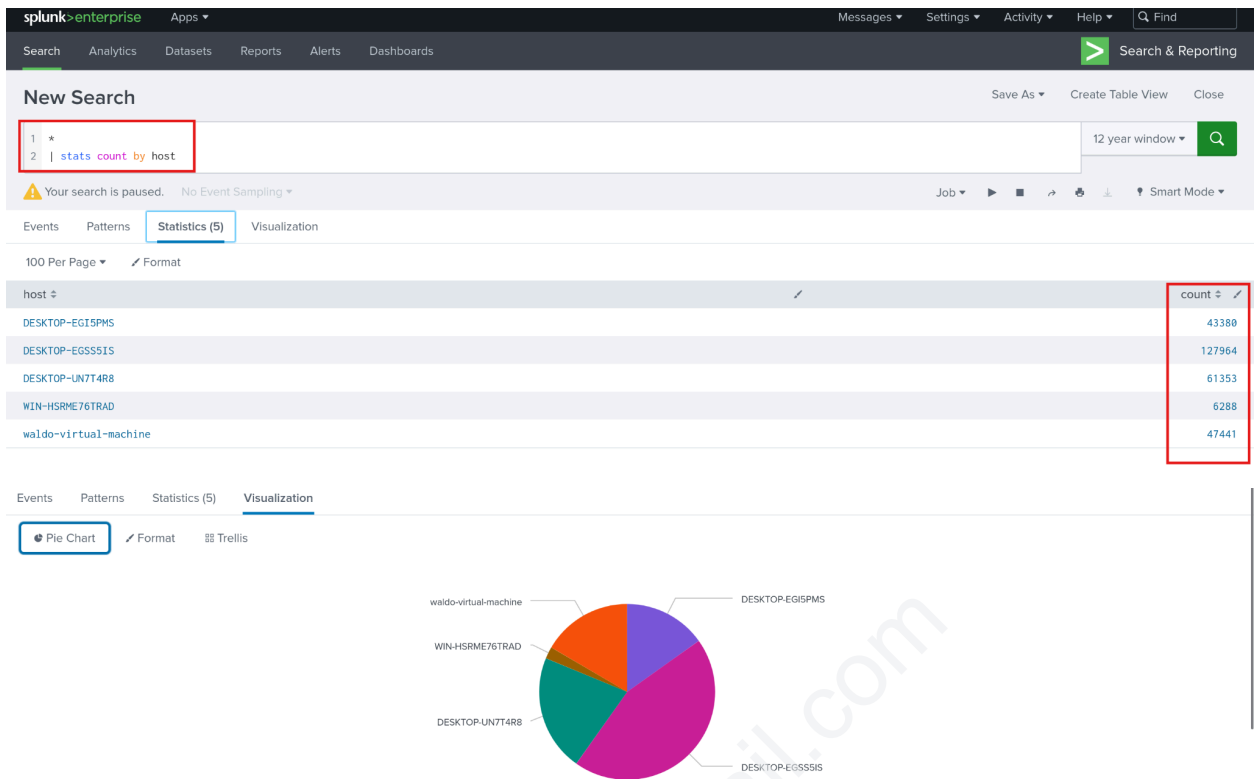
EventCode - 4768 (Kerberos authentication ticket requests)

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=* EventCode=4768`, `| stats count by Account_Name`, and `| sort - count`. The search is paused. The results table shows the following data:

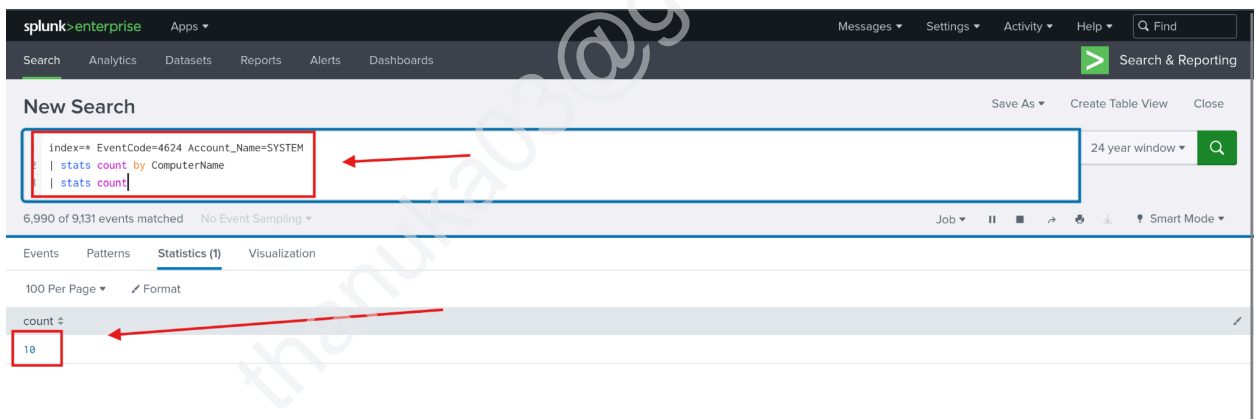
Account_Name	count
waldo	12
WIN-HSRME76TRAD\$	9
DESKTOP-UN7T4R8\$	8
DESKTOP-EGSS51S\$	7
Administrator	6
DESKTOP-EGISPM\$	6

ANSWER - waldo - 12

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

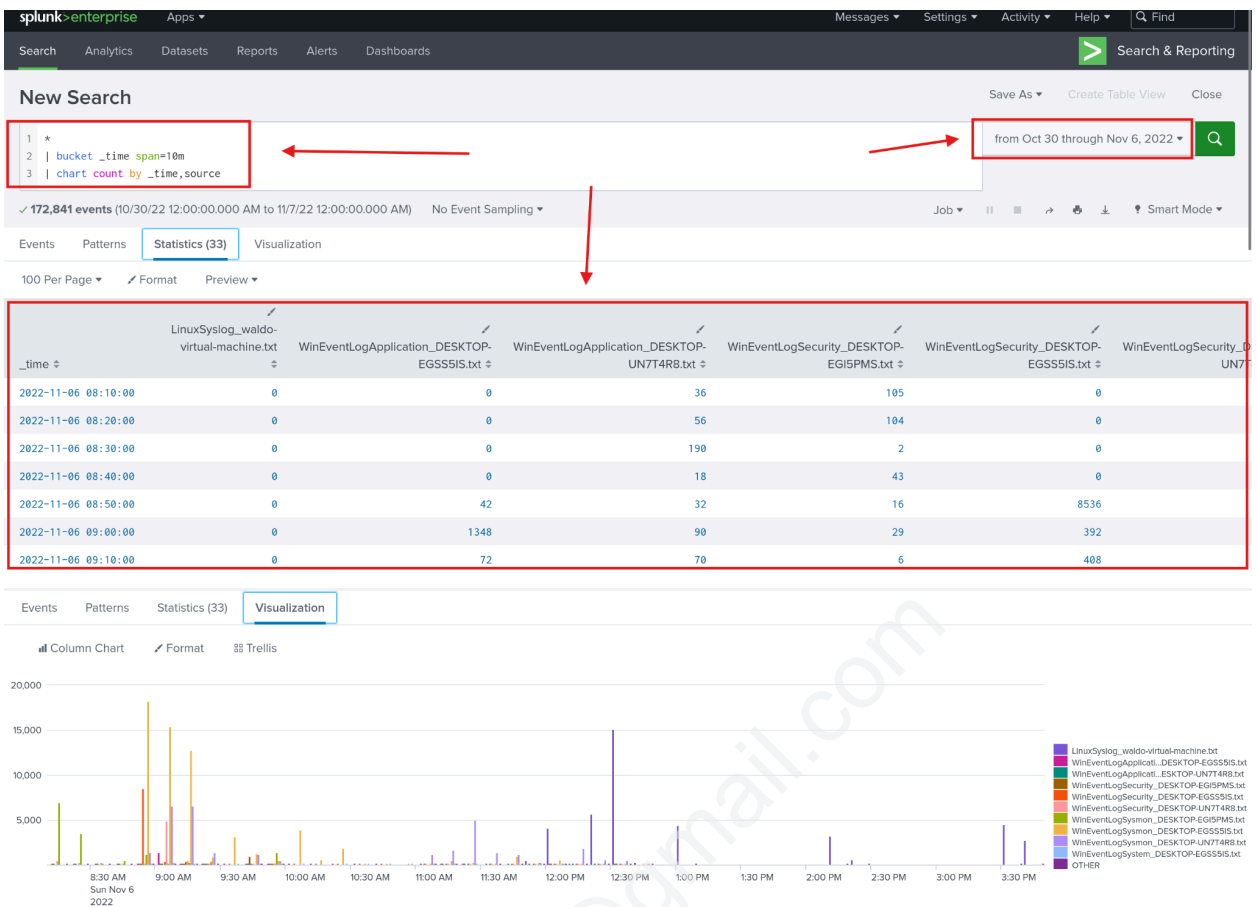


3. SPL search against all 4624 events the count of distinct computers accessed by the account name SYSTEM

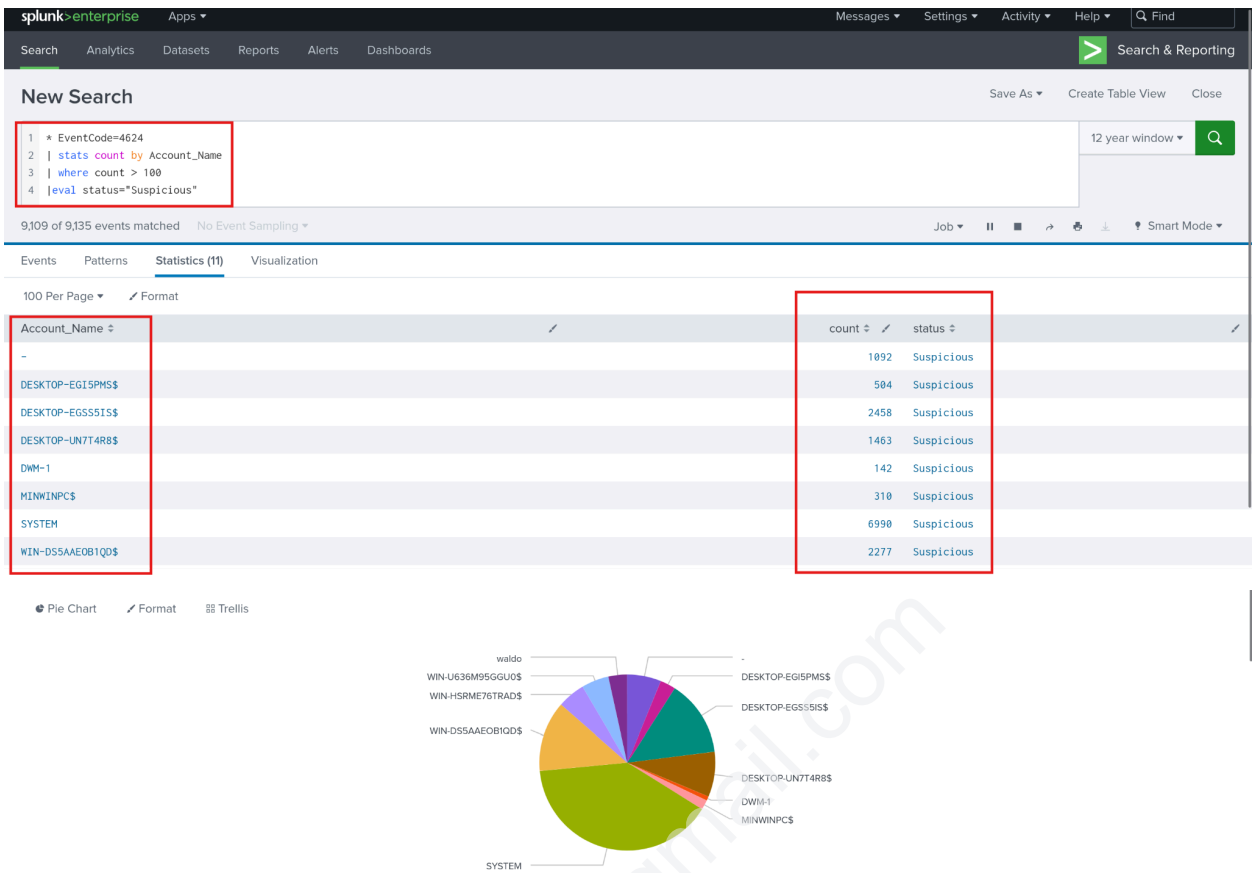


ANSWER - 10

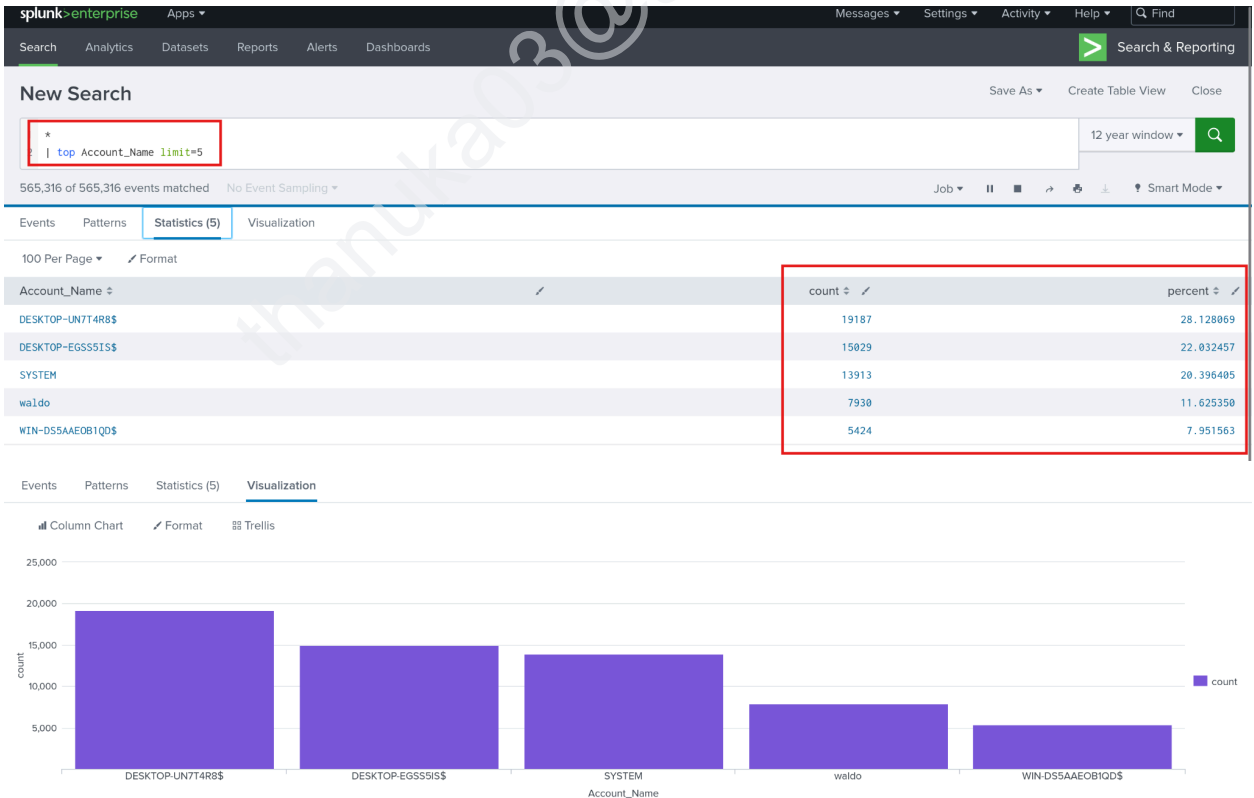
4. Create a time-based chart that shows the number of events from each source, grouped into 10-minute intervals. From Oct 30 - Nov 6 /2022



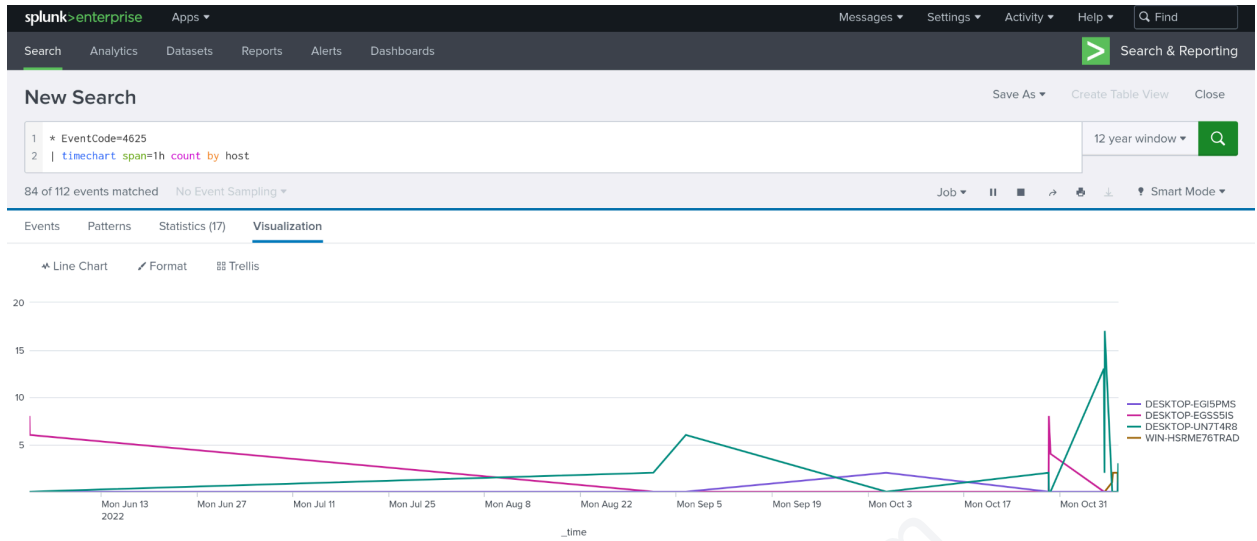
- SPL query to find users who made more than 100 login attempts (EventCode 4624) and label them as "Suspicious"



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



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



E N D