Practice search #1: Source and Destination Port Analysis

Objective: I want to identify the most frequently used source ports and the relationships between source and destination ports. This helps me understand potential security issues or usage trends.

Query:

index=botsv3 sourcetype=*

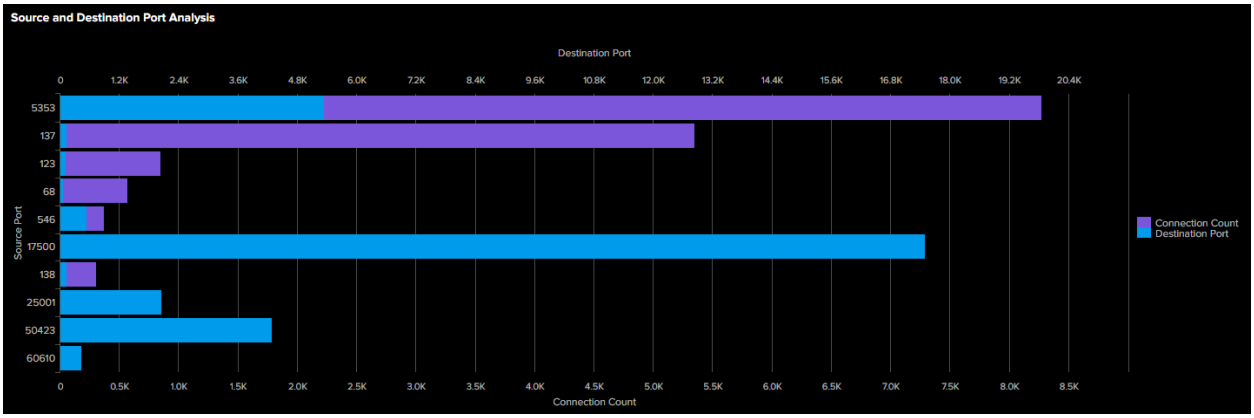
| stats count by src_port, dest_port

| sort - count

| head 10

| rename src_port as "Source Port", dest_port as "Destination Port", count as "Connection Count"

| table "Source Port", "Destination Port", "Connection Count"Dashboard Result:



Visualization reasoning:

I chose a Stacked Bar Chart because it allows me to compare the most used source ports while also showing how they connect to different destination ports. This makes it easy to see port relationships and spot trends.

Practice search #2: Visualization of Audit Failures (1 Day Timeframe)

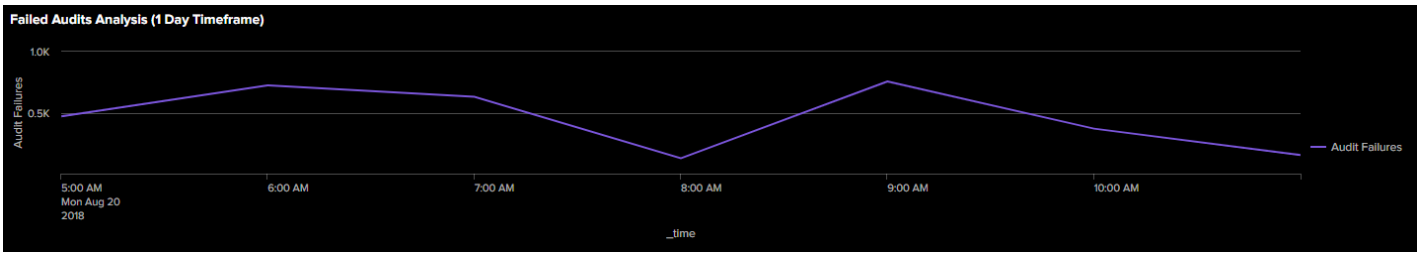
Objective: I want to track occurrences of audit failures on a specific day to identify potential security or configuration issues in the system.

Query:

index=botsv3 sourcetype=* "Audit Failure"

| stats count by _time

| timechart span=1h count as "Audit Failures"



Visualization Reasoning:
I picked a Line Chart to track changes in audit failures over time, allowing me to visualize trends and spikes in the data. This visualization makes it easier to identify when problems occur, detect patterns, and understand the frequency and severity of audit failures.

Practice search #3: Top 15 Bandwidth Consumers (Bytes Transferred)

Objective: I want to identify which source IPs are responsible for the highest data consumption by measuring the total bytes transferred. This helps identify abnormal data transfers which can be a sign of a potential security concern.

Query:

index=botsv3 sourcetype=*

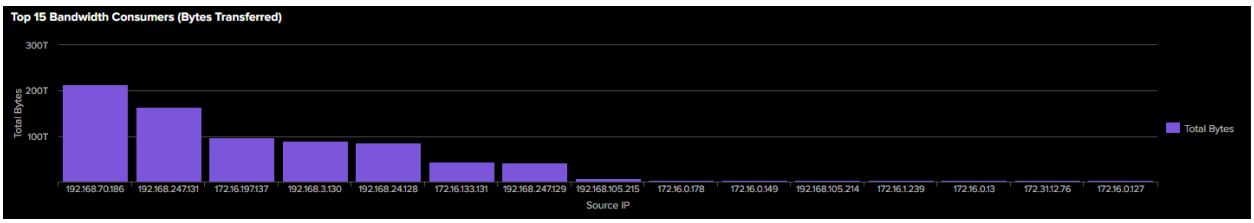
| stats sum(bytes) as total_bytes by src_ip

| sort - total_bytes

| head 15

| rename src_ip as "Source IP", total_bytes as "Total Bytes"

| table "Source IP", "Total Bytes"

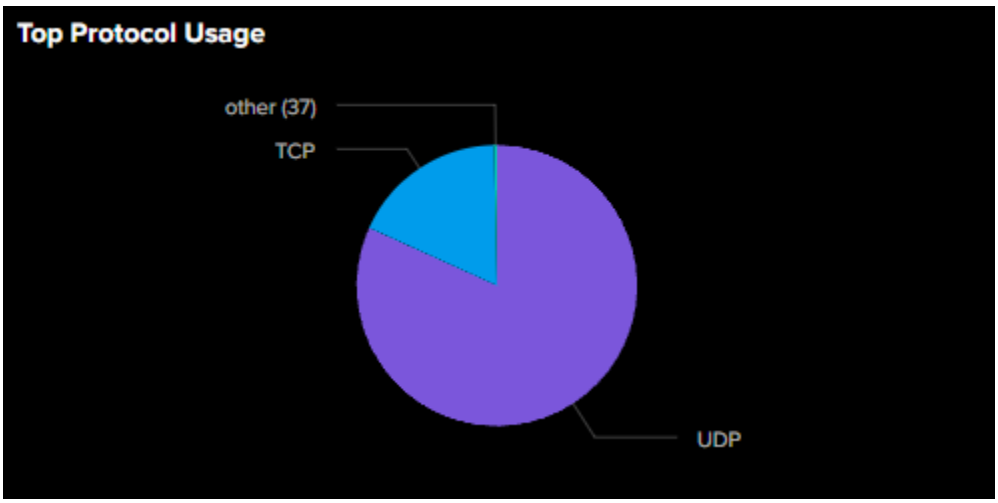


Visualization Reasoning:

I chose a column chart because it allows me to easily compare bandwidth usage across different source IPs. Sorting the chart in descending order makes it clear which IPs are consuming the most data, and the visual format is perfect for highlighting these differences at a glance.

Practice search #4: Top Protocol Usage

Objective: I want to understand the relative frequency of different network protocols in use (e.g., UDP, TCP) to identify which protocols are being utilized most frequently in the network. This can help determine the type of traffic dominating the network, which is important for performance monitoring and security.



Visualization Reasoning:

I chose a pie chart to visualize protocol usage because it effectively shows the percentage distribution of each protocol, giving a clear overview of how the network traffic is divided. This emphasizes how dominant UDP and TCP traffic is at a glance.