**LAB - 8 REPORT**

Course Code - Course Name: - COMP4040 – Introduction to SOC

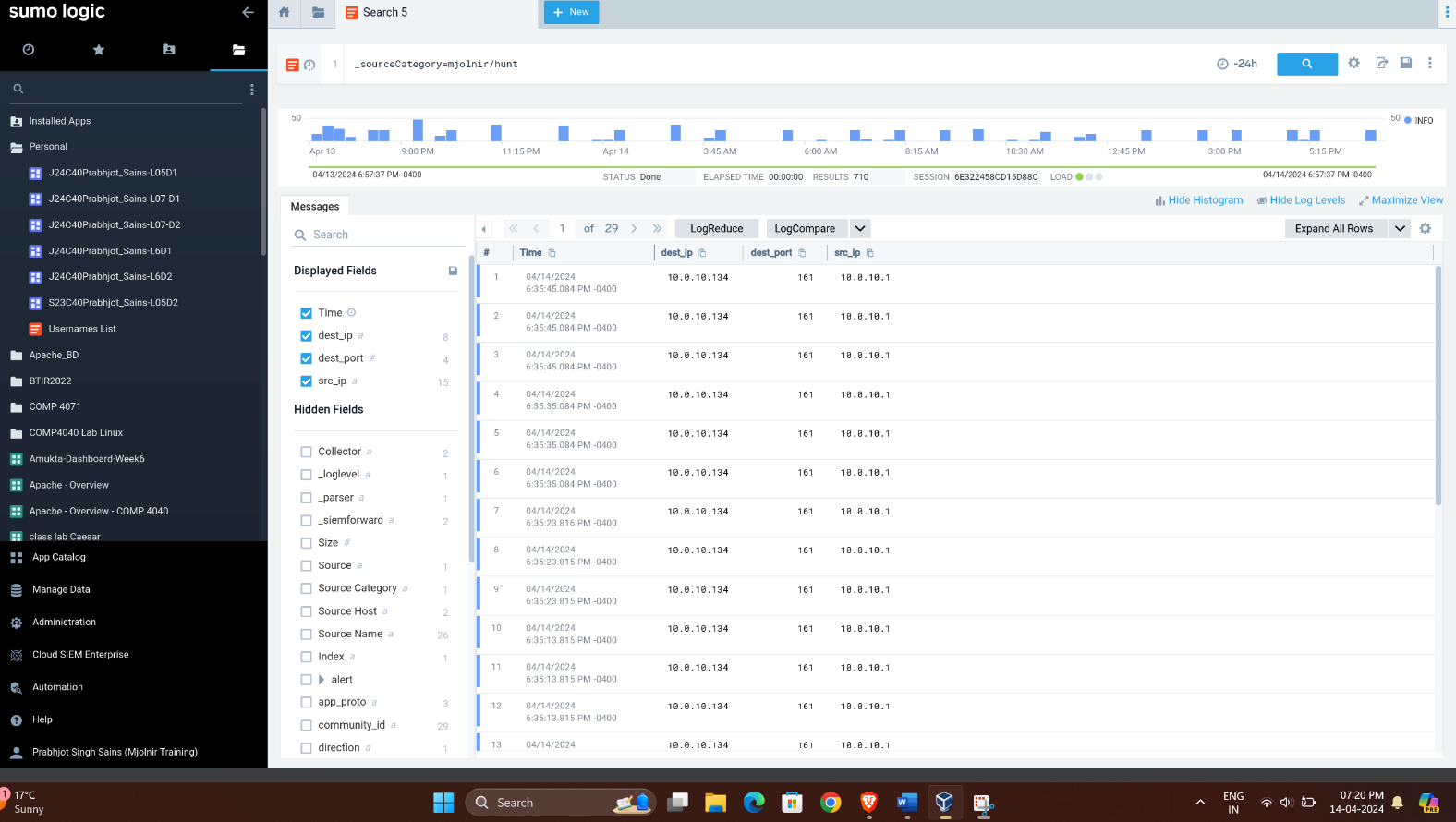
Program: T433 - Cybersecurity

Term: - Winter 2024

Student Names - ID:

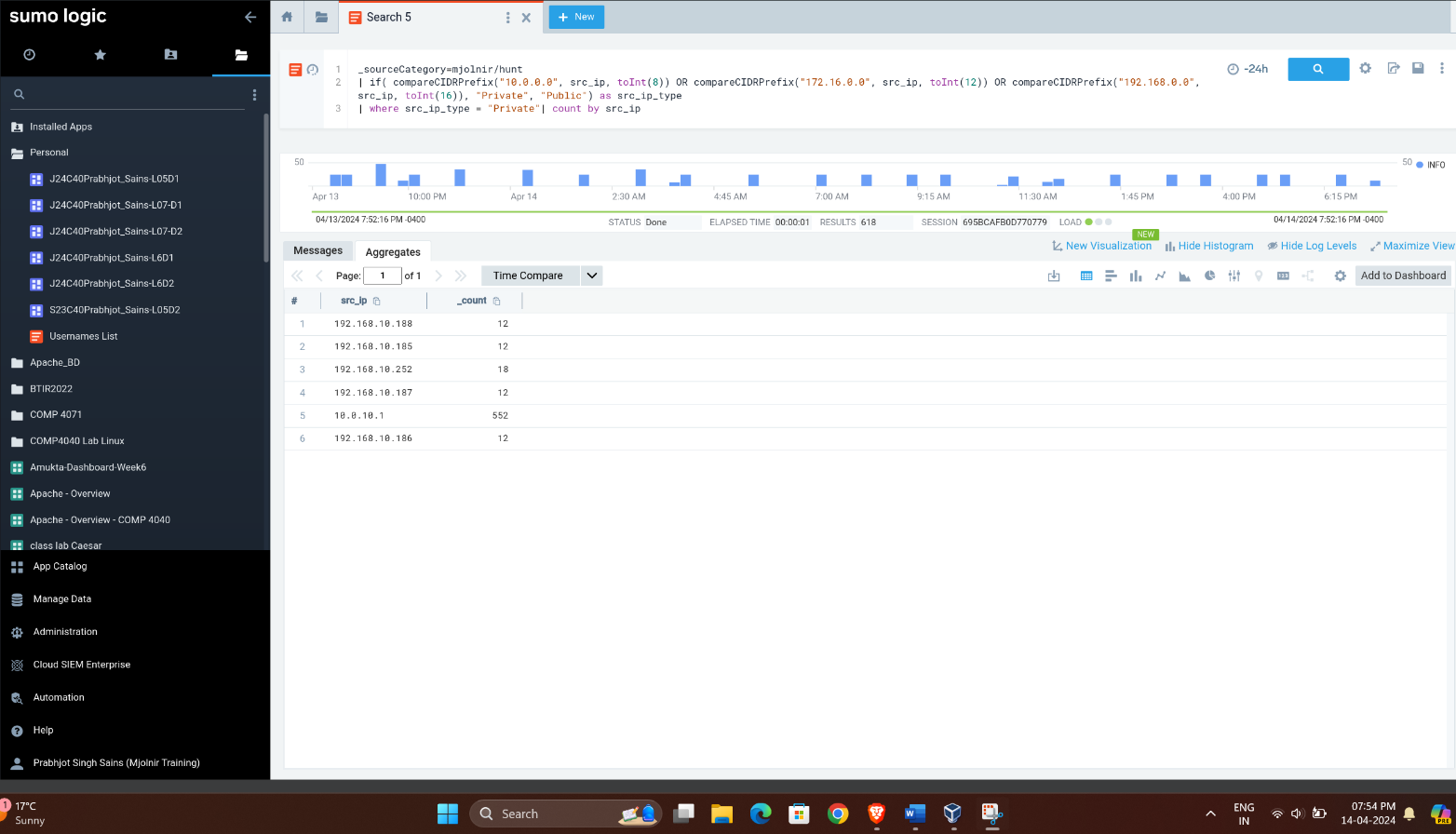
* Prabhjot Singh Sains – 101495218

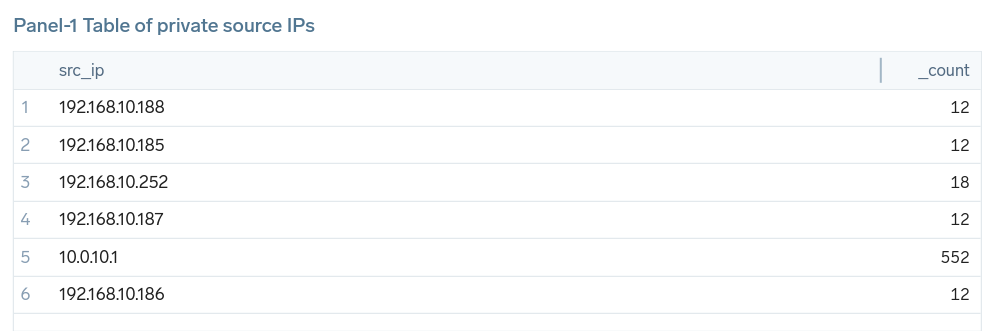
1. **Use \_sourceCategory=mjolnir/hunt**
   1. **Extract src\_ip, dest\_ip, and dest\_port:**



* 1. **Create a table of private source IPs Panel-1:**

\_sourceCategory=mjolnir/hunt | if( compareCIDRPrefix("10.0.0.0", src\_ip, toInt(8)) OR compareCIDRPrefix("172.16.0.0", src\_ip, toInt(12)) OR compareCIDRPrefix("192.168.0.0", src\_ip, toInt(16)), "Private", "Public") as src\_ip\_type | where src\_ip\_type = "Private"| count by src\_ip

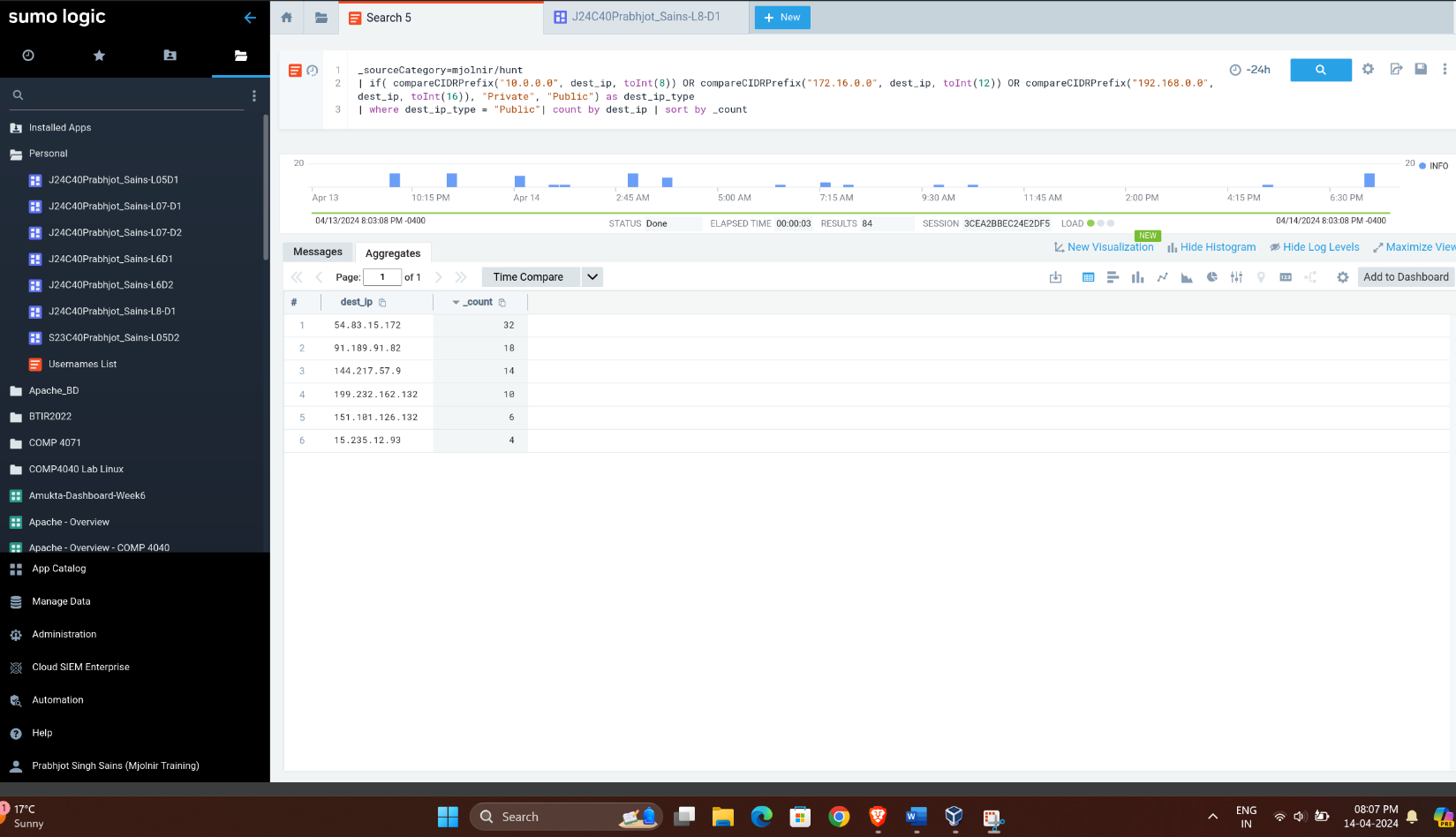




* 1. **Create a table of public destination IPs and sort it. Panel-2**

\_sourceCategory=mjolnir/hunt | if( compareCIDRPrefix("10.0.0.0", dest\_ip, toInt(8)) OR compareCIDRPrefix("172.16.0.0", dest\_ip, toInt(12)) OR compareCIDRPrefix("192.168.0.0", dest\_ip, toInt(16)), "Private", "Public") as dest\_ip\_type

| where dest\_ip\_type = "Public"| count by dest\_ip | sort by \_count

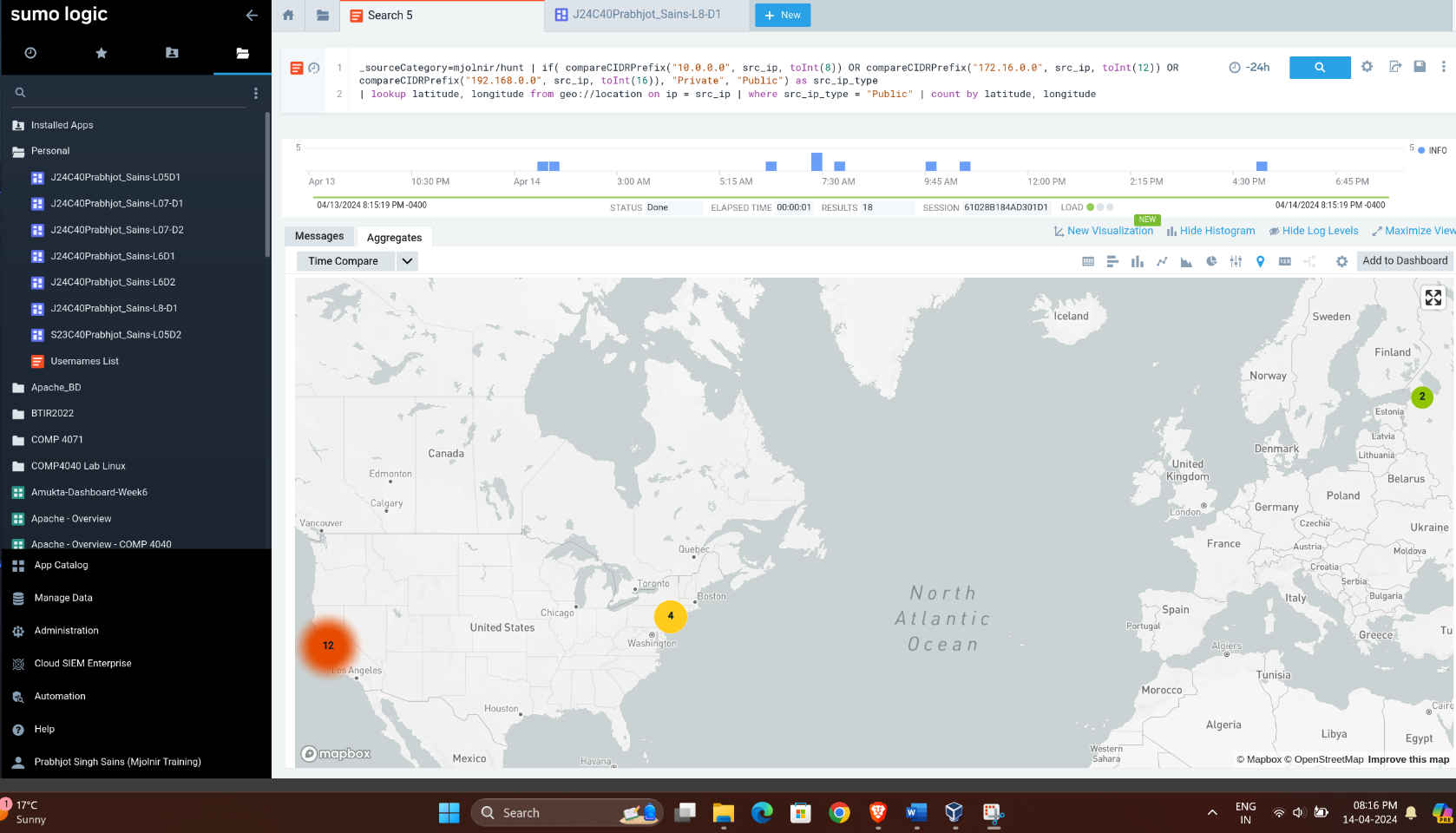


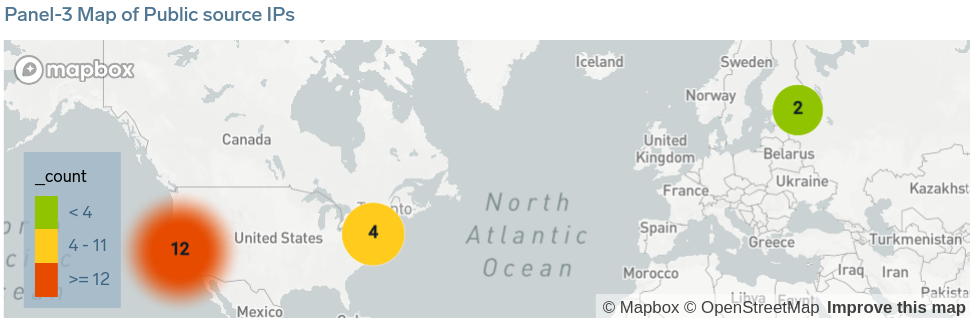


* 1. **Visualize Public source IPs on map Panel-3:**

\_sourceCategory=mjolnir/hunt | if( compareCIDRPrefix("10.0.0.0", src\_ip, toInt(8)) OR compareCIDRPrefix("172.16.0.0", src\_ip, toInt(12)) OR compareCIDRPrefix("192.168.0.0", src\_ip, toInt(16)), "Private", "Public") as src\_ip\_type

| lookup latitude, longitude from geo://location on ip = src\_ip | where src\_ip\_type = "Public" | count by latitude, longitude





* 1. **Create table of records including private IPs as the src, Public IP as the dest, and port isn’t 80 or 443 Panel-4:**

\_sourceCategory=mjolnir/hunt

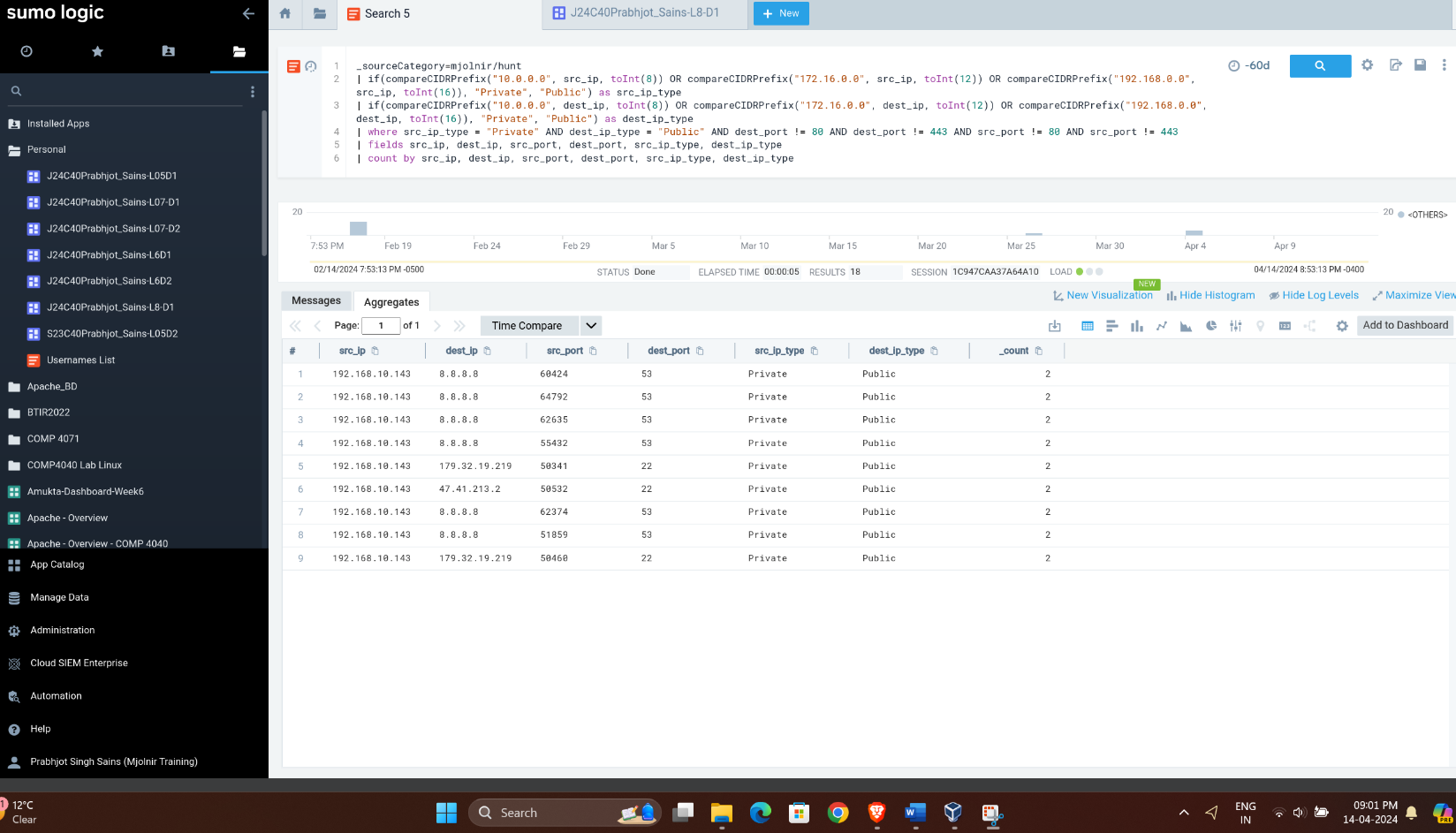
| if(compareCIDRPrefix("10.0.0.0", src\_ip, toInt(8)) OR compareCIDRPrefix("172.16.0.0", src\_ip, toInt(12)) OR compareCIDRPrefix("192.168.0.0", src\_ip, toInt(16)), "Private", "Public") as src\_ip\_type

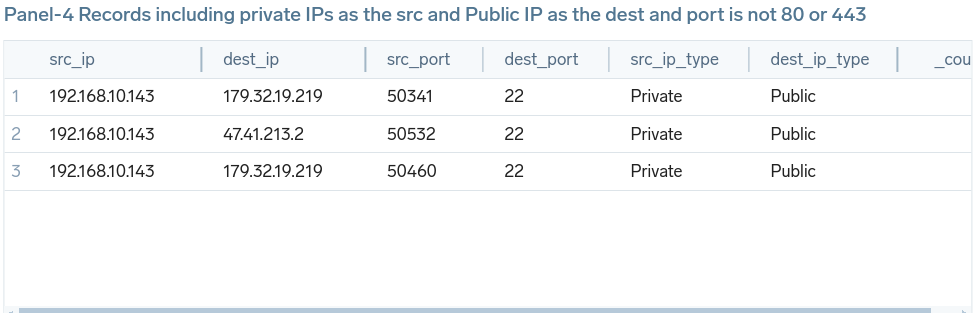
| if(compareCIDRPrefix("10.0.0.0", dest\_ip, toInt(8)) OR compareCIDRPrefix("172.16.0.0", dest\_ip, toInt(12)) OR compareCIDRPrefix("192.168.0.0", dest\_ip, toInt(16)), "Private", "Public") as dest\_ip\_type

| where src\_ip\_type = "Private" AND dest\_ip\_type = "Public" AND dest\_port != 80 AND dest\_port != 443 AND src\_port != 80 AND src\_port != 443

| fields src\_ip, dest\_ip, src\_port, dest\_port, src\_ip\_type, dest\_ip\_type

| count by src\_ip, dest\_ip, src\_port, dest\_port, src\_ip\_type, dest\_ip\_type





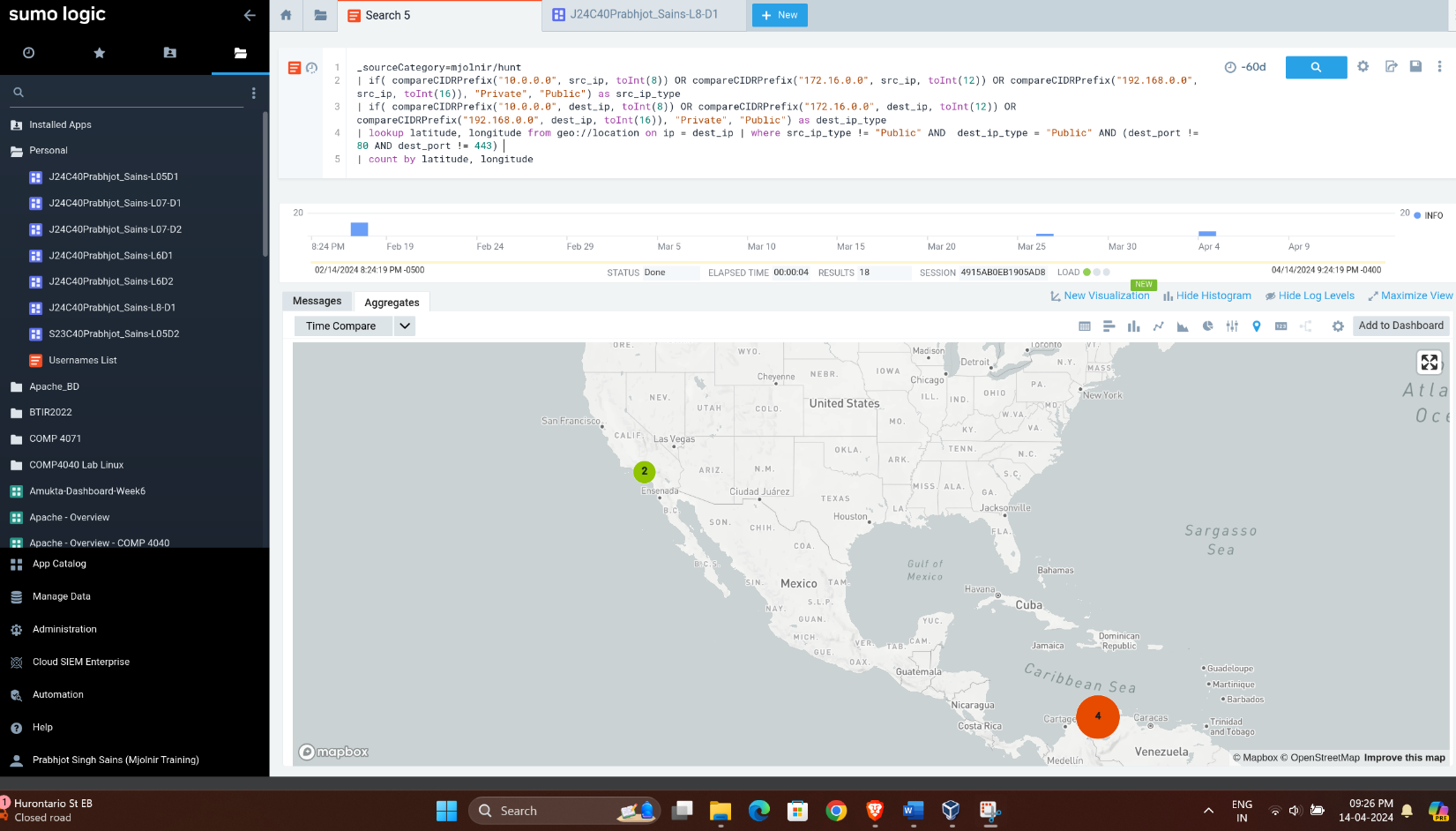
* 1. **Show the result of part “e” on a map Panel-5.**

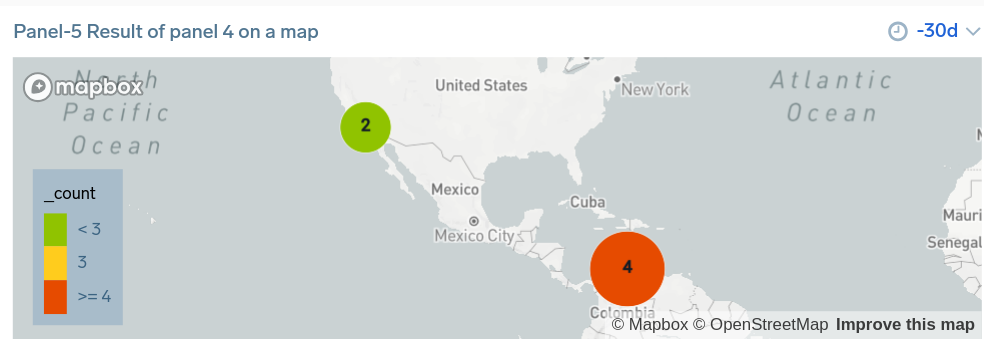
\_sourceCategory=mjolnir/hunt

| if( compareCIDRPrefix("10.0.0.0", src\_ip, toInt(8)) OR compareCIDRPrefix("172.16.0.0", src\_ip, toInt(12)) OR compareCIDRPrefix("192.168.0.0", src\_ip, toInt(16)), "Private", "Public") as src\_ip\_type

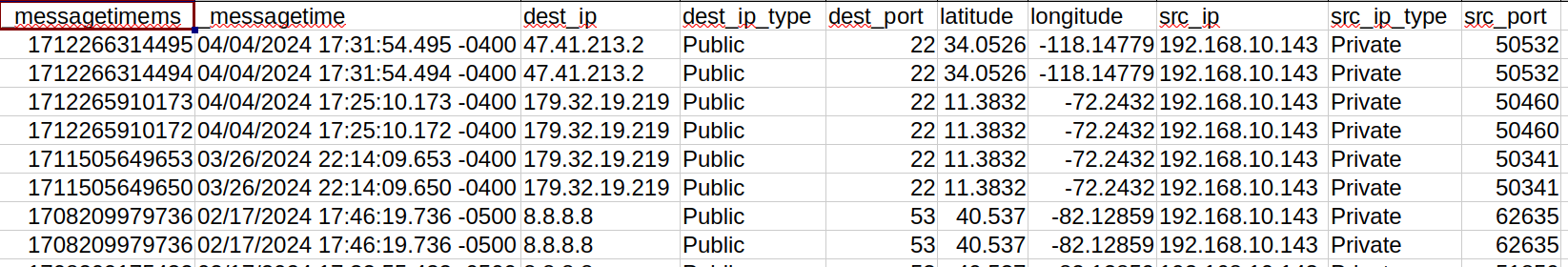
| if( compareCIDRPrefix("10.0.0.0", dest\_ip, toInt(8)) OR compareCIDRPrefix("172.16.0.0", dest\_ip, toInt(12)) OR compareCIDRPrefix("192.168.0.0", dest\_ip, toInt(16)), "Private", "Public") as dest\_ip\_type

| lookup latitude, longitude from geo://location on ip = dest\_ip | where src\_ip\_type != "Public" AND dest\_ip\_type = "Public" AND (dest\_port != 80 AND dest\_port != 443) | count by latitude, longitude



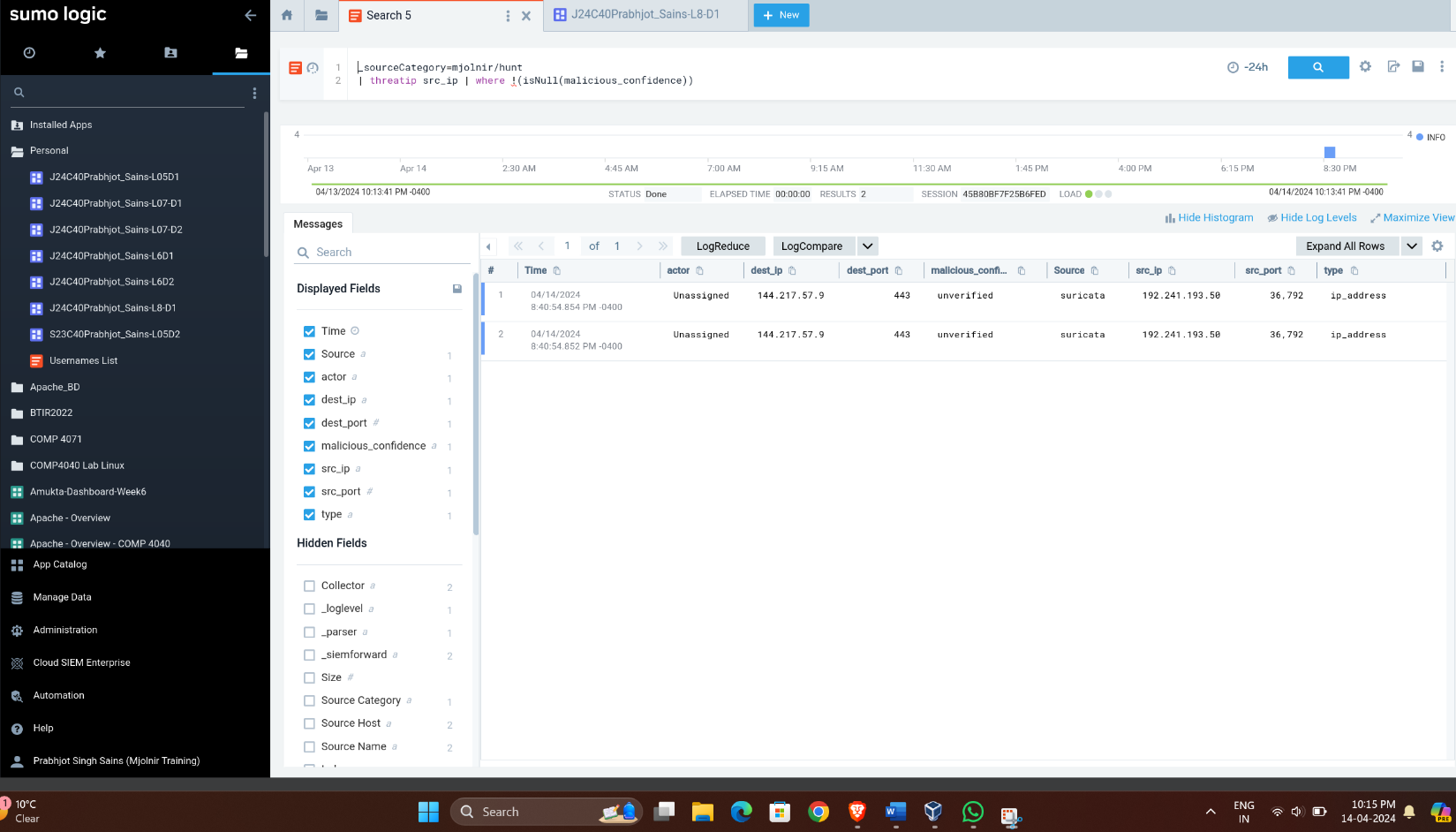


* 1. **Download the list of Attacker IPs:** Downloaded as a CSV file.

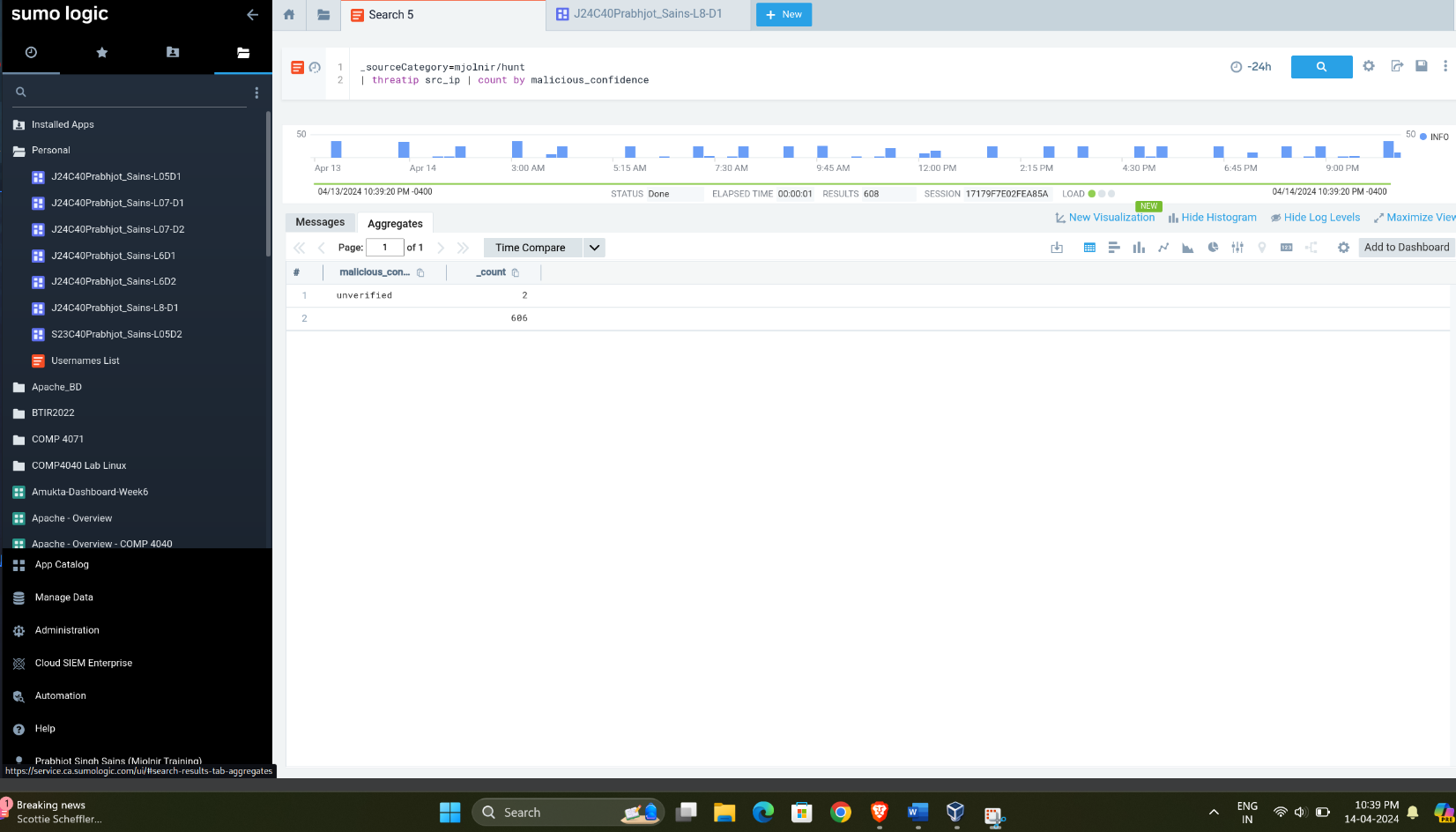


* 1. **Check malicious\_confidence of src\_ip :**

\_sourceCategory=mjolnir/hunt | threatip src\_ip | where !(isNull(malicious\_confidence))

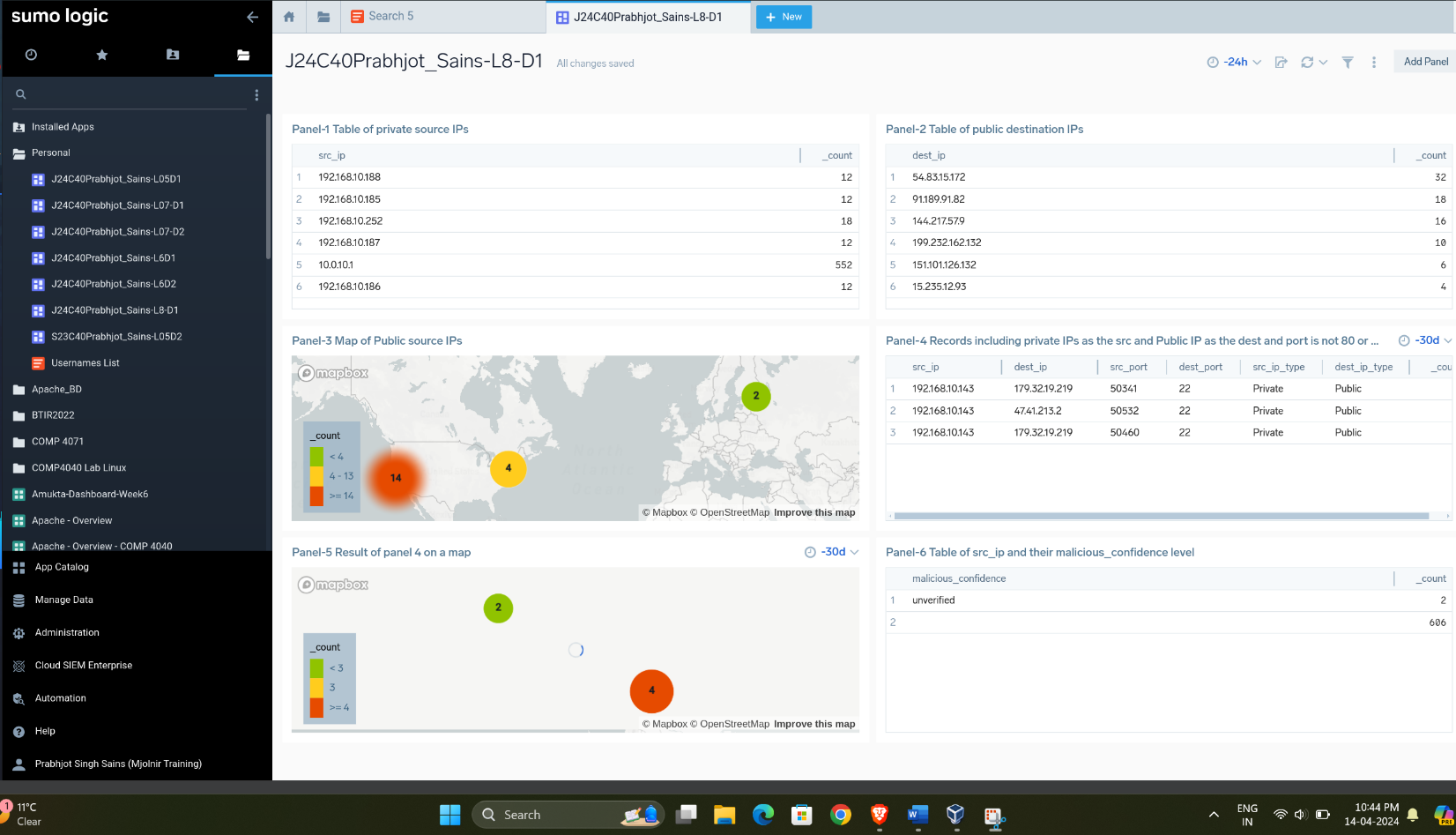


* 1. **Create a table of src\_ip and their malicious\_confidence level as Panel-6:**

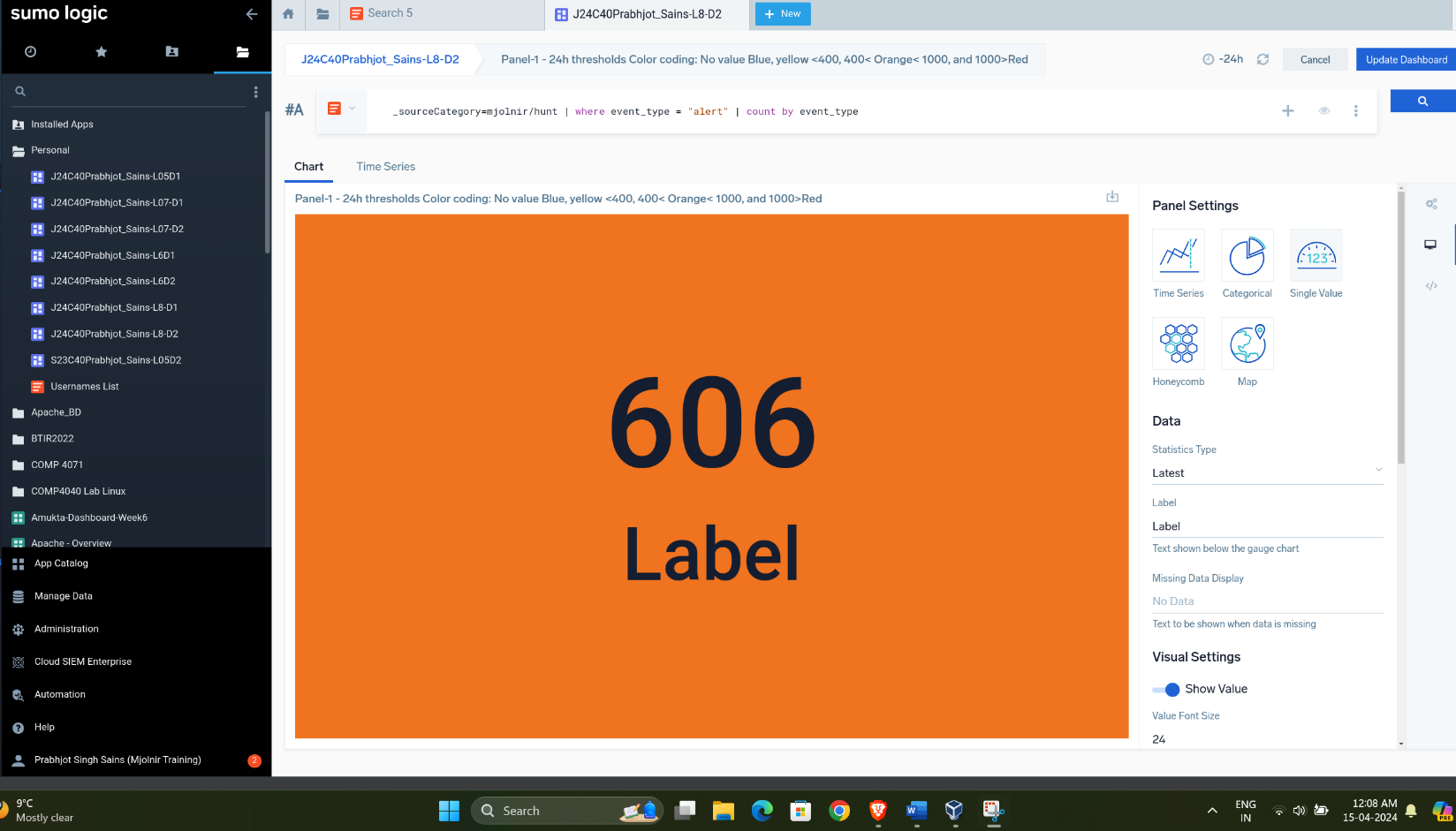




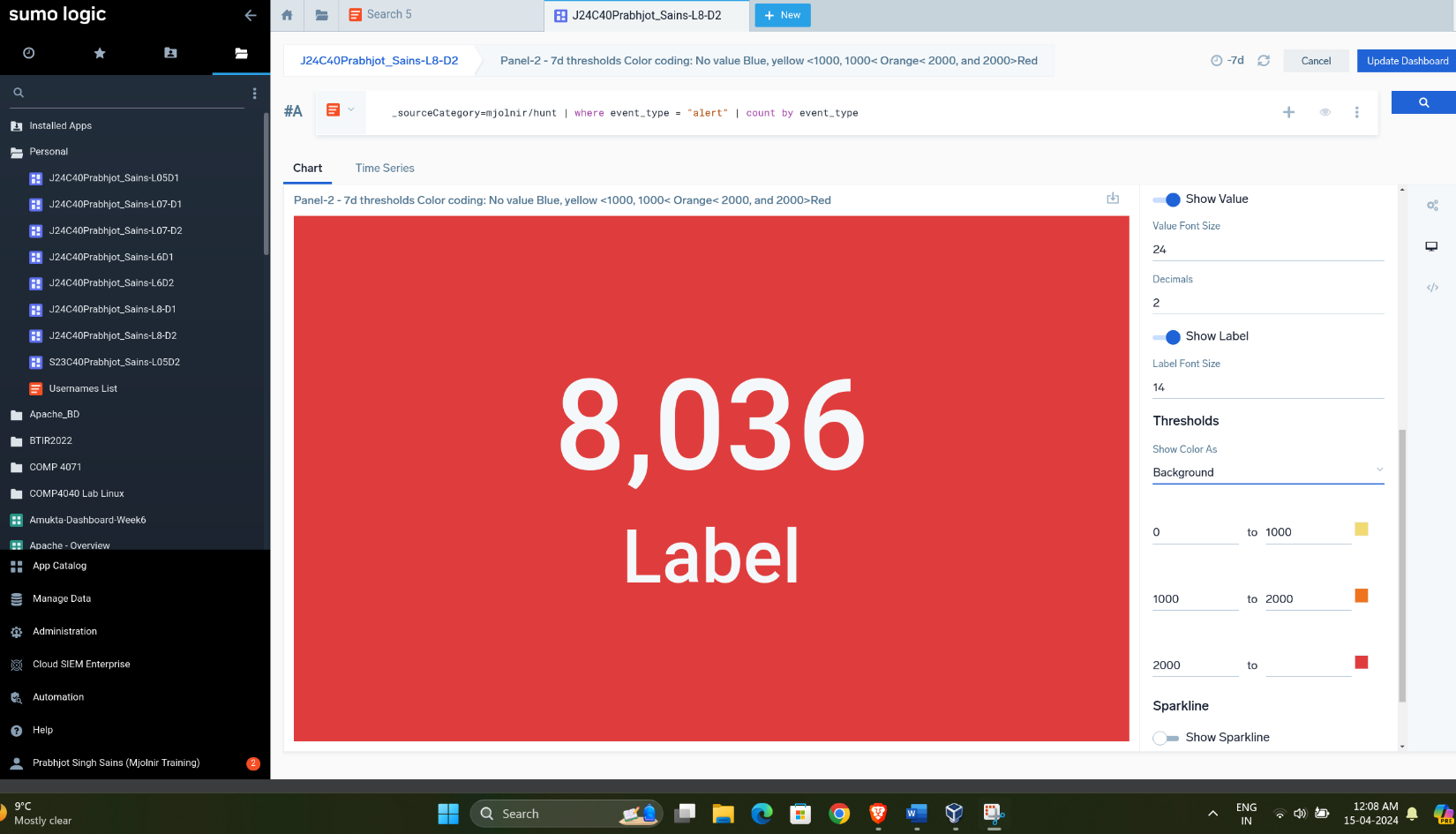
1. **Analyze what you can see in the panels:**
   * **Panel 1:** The table is used for monitoring network traffic, where the \_count represents the number of times each IP address has accessed a resource or triggered an event within a network. The high count for 10.0.10.1 suggests it’s a significant source of traffic or events. The other IPs have a count of 12, indicating less activity compared to 10.0.10.1.
   * **Panel 2:** The table is used for monitoring network traffic, where the \_count represents the number of times each IP address has accessed a resource or triggered an event within a network. It shows the frequency of public destination IPs.
   * **Panel 3:** It displays a world map with three regions highlighted, each marked with a colored circle representing the count of public source IPs in that area.
   * **Panel 4:** The table is used for monitoring network traffic, where the source IPs are within a private network and the destination IPs are public, with a focus on non-standard web ports (not 80 or 443). The consistent use of port 22 suggests SSH traffic.
   * **Panel 5:** It displays a world map with three regions highlighted, each marked with a colored circle representing IPs in that area. It is the graphical representation of panel 4.
   * **Panel 6:** This table is likely used in threat-hunting to track and analyze potentially malicious IP addresses. The high count of 606 suggests that one IP address has been flagged multiple times. The “unverified” status means that additional evidence is required to determine the nature of these IP addresses.
2. **Dashboard:**



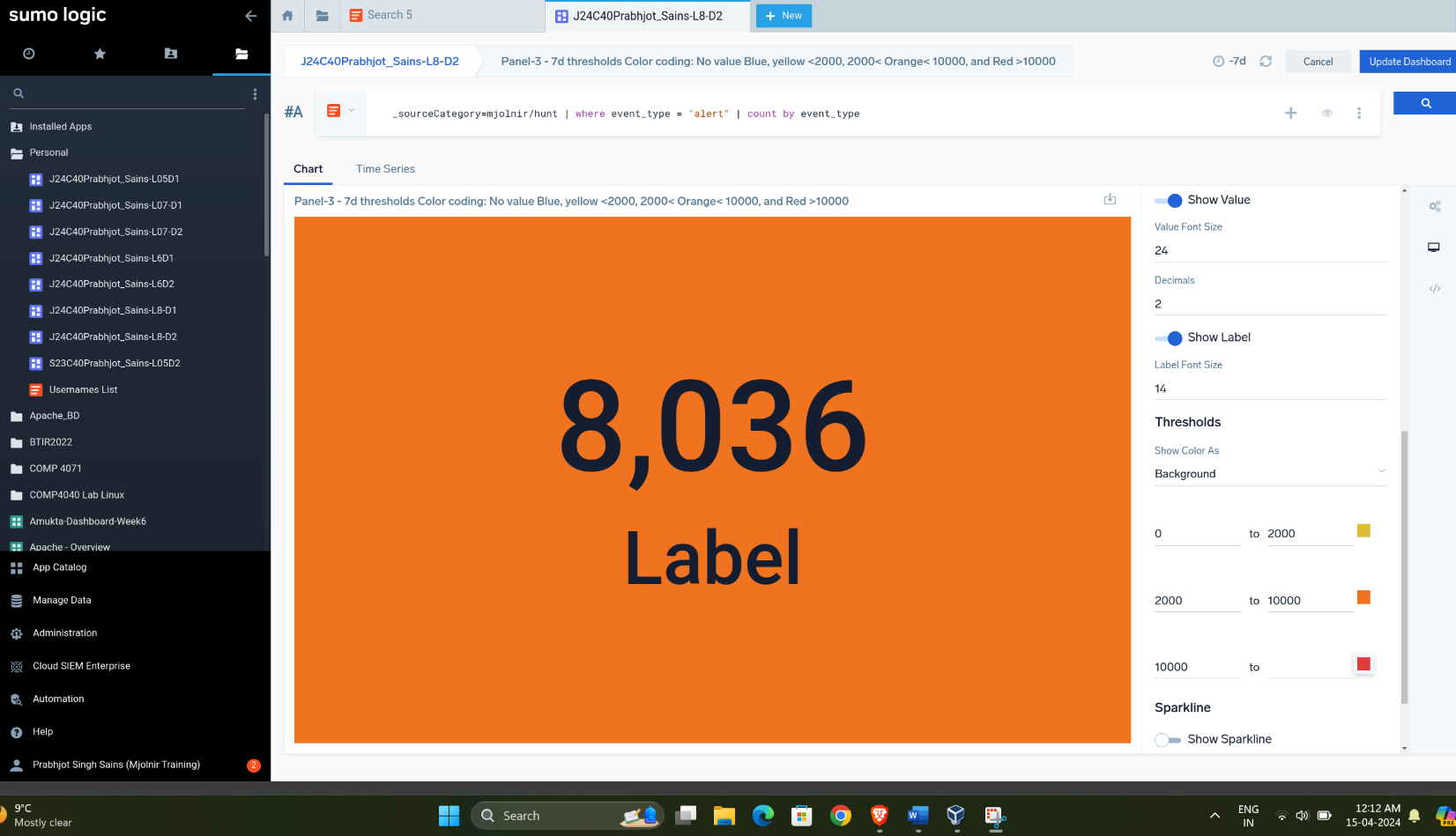
1. **Use \_sourceCategory=mjolnir/hunt and develop the below Dashboard**
   1. **Panel-1 for 24h thresholds Color coding: No value Blue, yellow <400, 400< Orange< 1000, and 1000>Red**



* 1. **Panel-2 for 7d thresholds Color coding: No value Blue, yellow <1000, 1000< Orange< 2000, and 2000>Red**

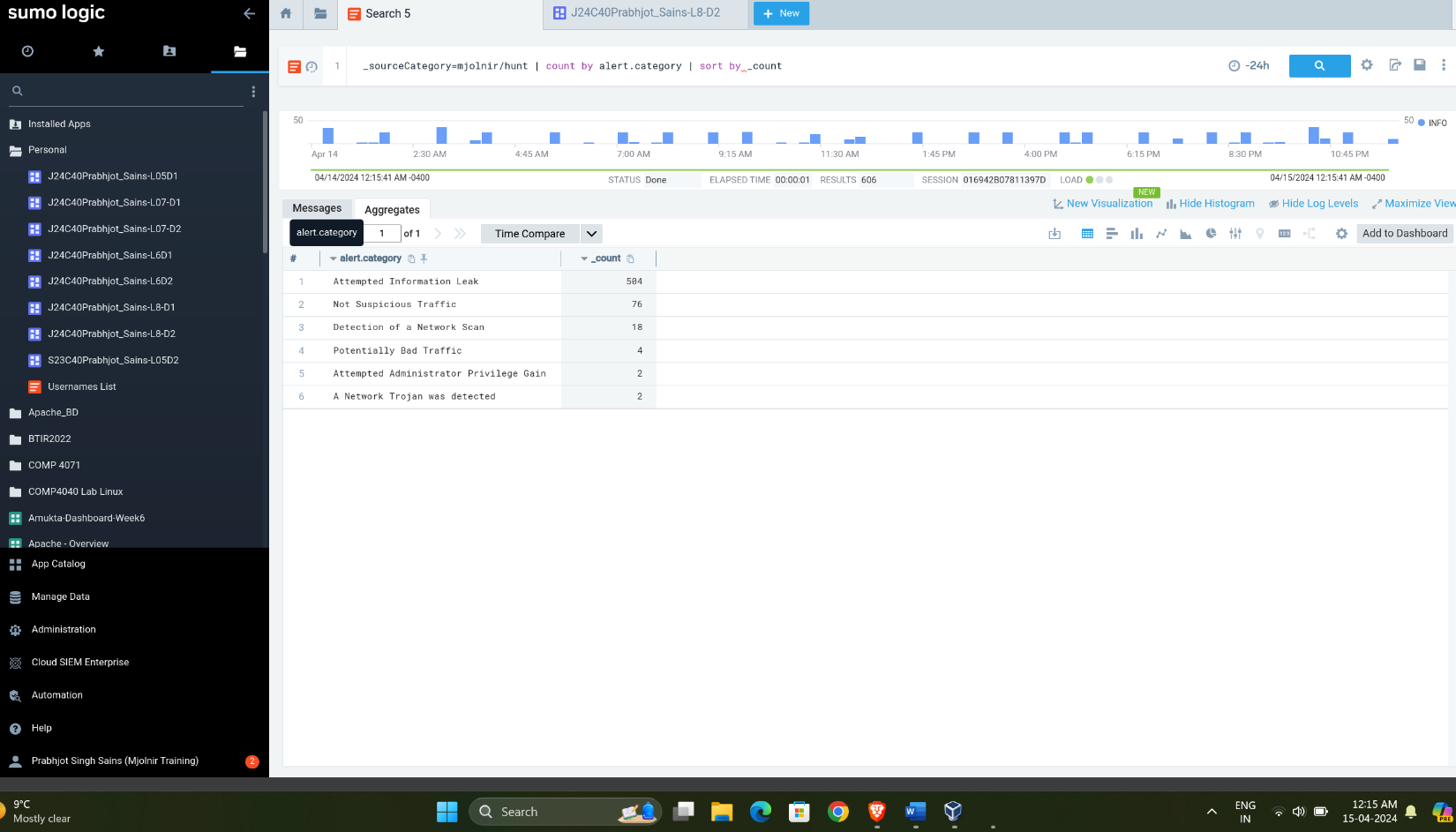
****

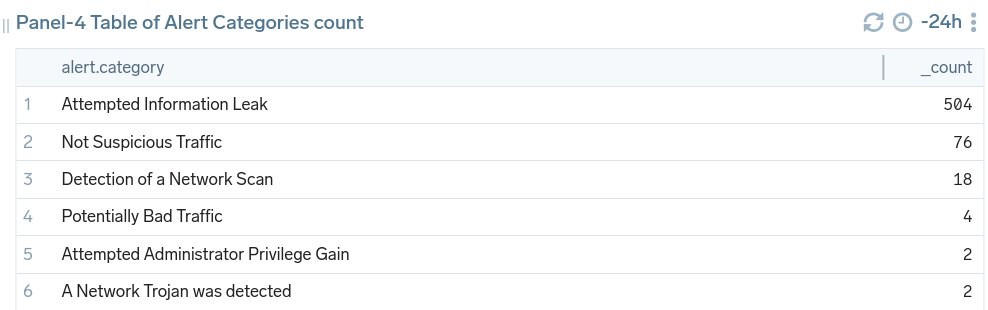
* 1. **Panel-3 for 7d thresholds Color coding: No value Blue, yellow <2000, 2000< Orange< 10000, and Red >10000**

****

* 1. **Panel-4 Table of Alert Categories count:**

\_sourceCategory=mjolnir/hunt | count by alert.category | sort by \_count



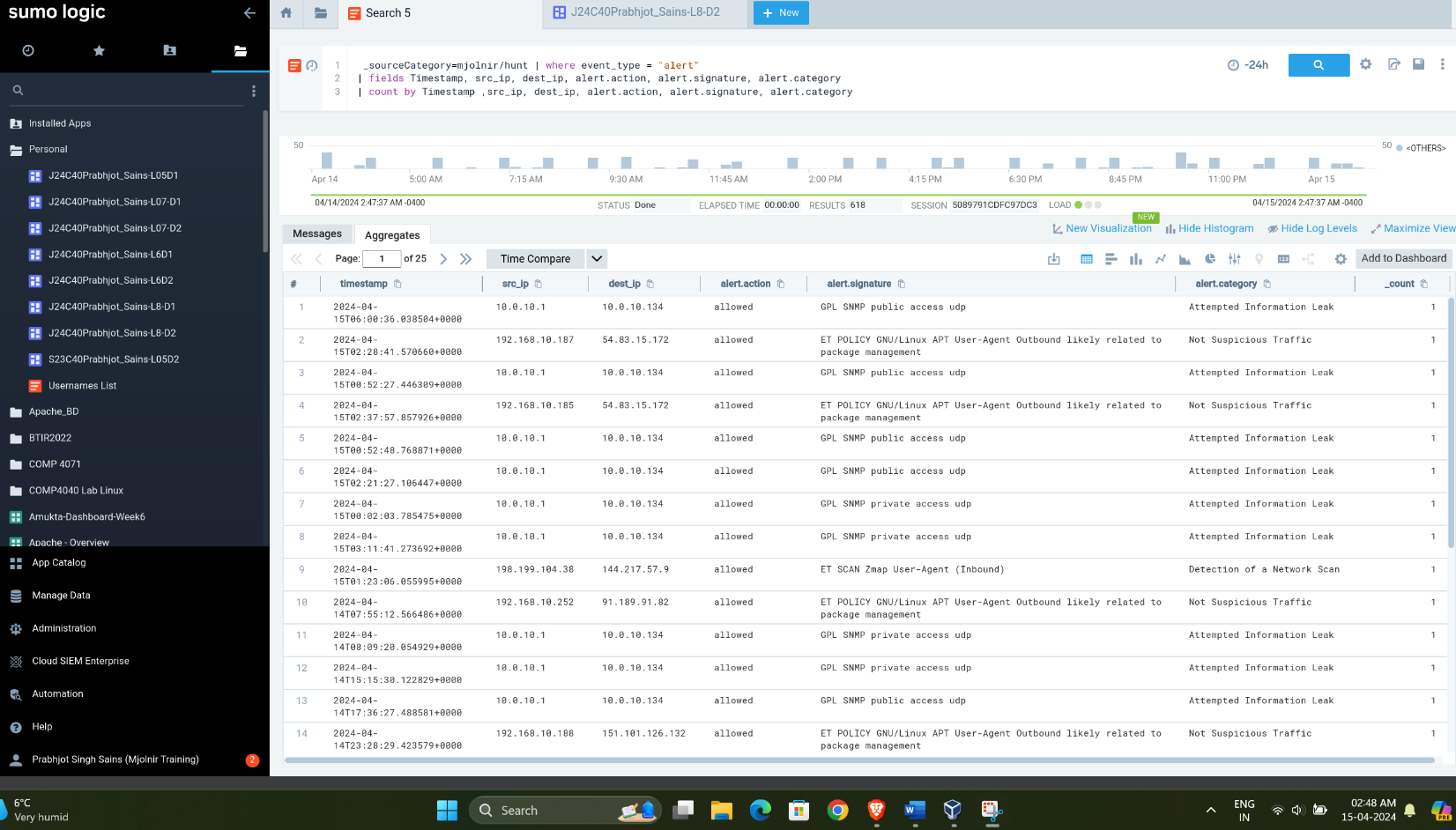


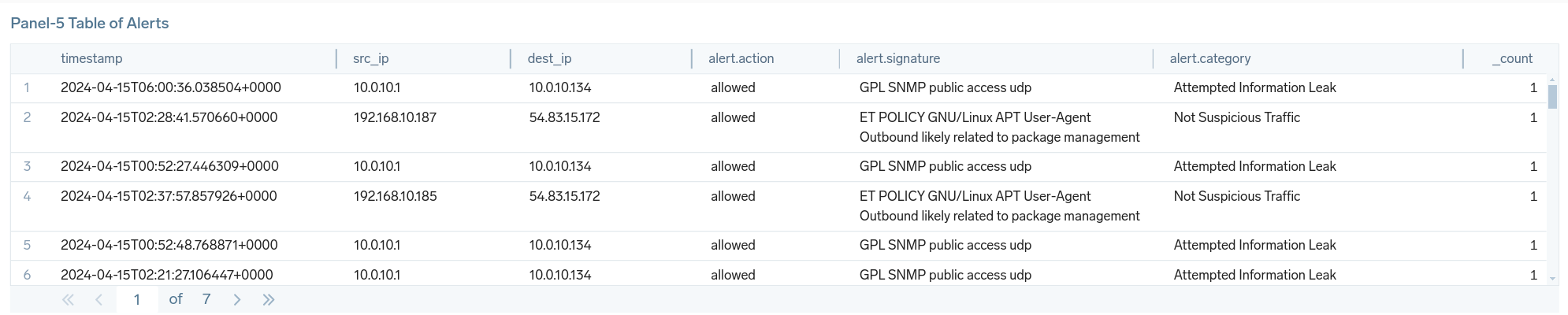
* 1. **Panel-5 Table of Alerts including below fields (time, src\_ip, dest\_ip, alert\_action, alert\_signature, alert\_category)**

\_sourceCategory=mjolnir/hunt | where event\_type = "alert"

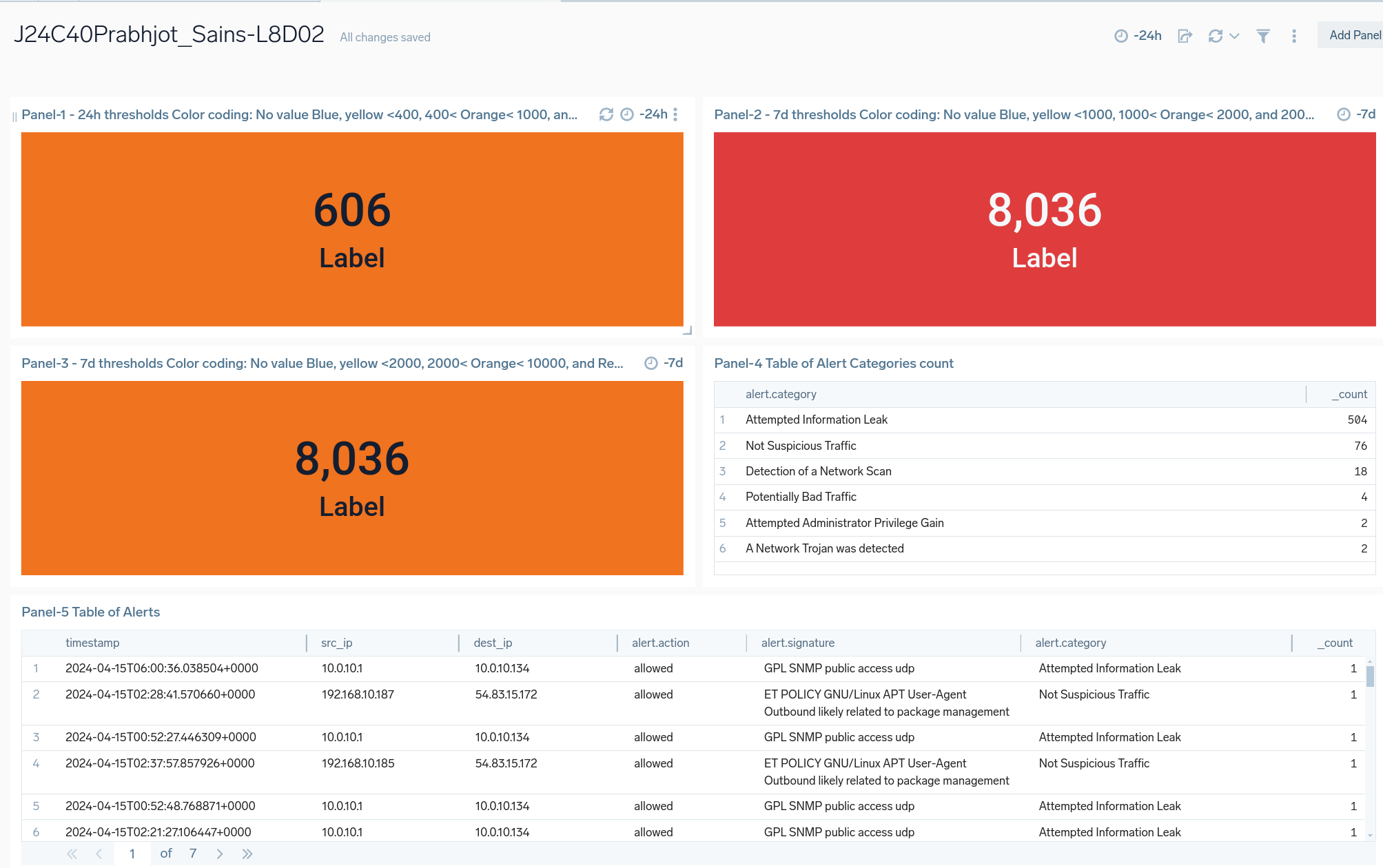
| fields Timestamp, src\_ip, dest\_ip, alert.action, alert.signature, alert.category

| count by Timestamp ,src\_ip, dest\_ip, alert.action, alert.signature, alert.category





* 1. **Dashboard:** Shared on Sumologic

****