(\_sourceCategory="mjolnir/hunt")

**1. Create a pie chart based on the event\_type [panel1]**

(\_sourceCategory="mjolnir/hunt")

| count by event\_type

2. (\_sourceCategory="mjolnir/hunt")

| where event\_type = "alert"

| count by event\_type

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

| 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 = "Public" AND dest\_ip\_type = "Public" AND event\_type = "alert"

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

| topk(10, \_count)

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

| lookup latitude, longitude from geo://location on ip = src\_ip

| where src\_ip\_type = "Public" AND dest\_ip\_type = "Public" AND event\_type = "alert"

| count by src\_ip, dest\_ip, src\_ip\_type, dest\_ip\_type, event\_type, latitude, longitude

| topk(10, \_count)

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

| 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 AND event\_type = "alert"

| 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

6. (\_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="Public"

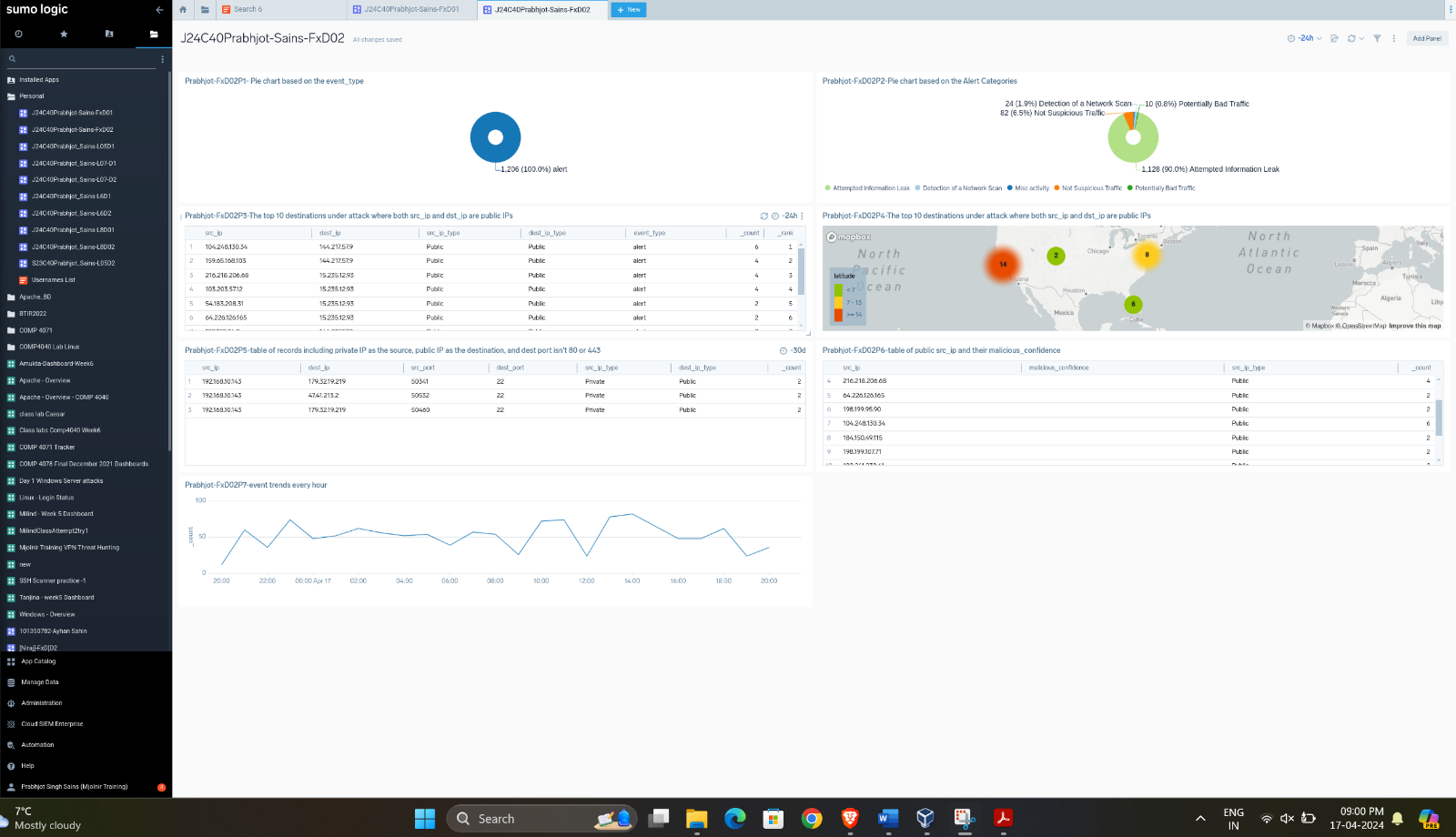
| fields src\_ip, malicious\_confidence, src\_ip\_type

| count by src\_ip,malicious\_confidence, src\_ip\_type

7. (\_sourceCategory="mjolnir/hunt")

| timeslice 60m

| count by \_timeslice



Panel 1 - Pie Chart based on Event Type:

Analysis: This panel provides a visual representation of the distribution of different event types within the "mjolnir/hunt" log source over the past 24 hours. By presenting the data in a pie chart format, it allows for easy identification of the proportion of each event type. Analysis of this chart can help in understanding the nature and prevalence of different types of events within the log data, aiding in incident detection and response prioritization.

Panel 2 - Pie Chart based on Alert Categories Count:

Analysis: This panel focuses specifically on events categorized as "alert" within the past 24 hours. By presenting a pie chart illustrating the distribution of different alert categories, it helps identify the most common types of alerts triggered within the observed time frame. Analysis of this chart can provide insights into potential security threats or issues, guiding further investigation and remediation efforts.

Panel 3 - Table for Top 10 Destinations under Attack:

Analysis: This panel lists the top 10 destinations under attack where both the source and destination IP addresses are public IPs. It helps identify frequently targeted destinations by attackers within the observed time frame, providing insights into potential high-value targets or recurring attack patterns. Analysis of this table can inform targeted security measures to mitigate ongoing threats.

Panel 4 - Map Visualization of Attack Source:

Analysis: This panel visualizes the geographic locations of attackers identified in Panel 3, plotting the source IP addresses on a map. By mapping the source IPs of attacks, it provides insights into the geographical distribution of attack sources, helping identify regions with high concentrations of malicious activity. Analysis of this map can inform geographically targeted security measures or threat intelligence efforts.

Panel 5 - Table of Records with Private Source IP and Public Destination IP:

Analysis: This panel presents a table of records where the source IP is private, the destination IP is public, and the destination port is neither 80 nor 443. It helps identify potentially suspicious network traffic patterns, such as private-to-public communication on non-standard ports. Analysis of this table can uncover indicators of compromise or potential security incidents, guiding further investigation and response efforts.

Panel 6 - Table of Public Source IPs and Their Malicious Confidence:

Analysis: This panel presents a table of public source IPs and their associated malicious confidence scores for "alert" records. It helps prioritize security actions based on the perceived severity or likelihood of malicious activity associated with each source IP. Analysis of this table can guide proactive security measures or response efforts targeted at higher-risk IP addresses.

Panel 7 - Graph of Event Trends Every Hour:

Analysis: This panel visualizes trends in event occurrence over time, aggregated by hour, for the past 7 days. It helps identify patterns, anomalies, or recurring trends in activity that may indicate security incidents or operational issues. Analysis of this graph can inform proactive security measures, operational adjustments, or investigations into unusual activity patterns.