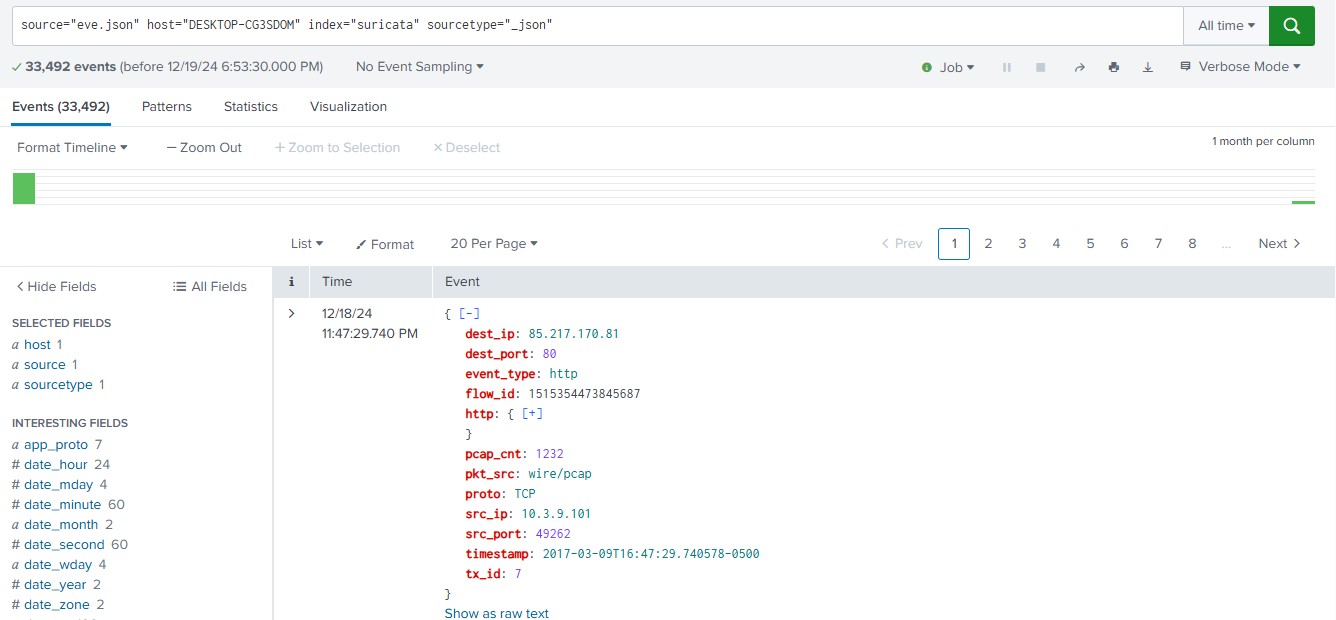
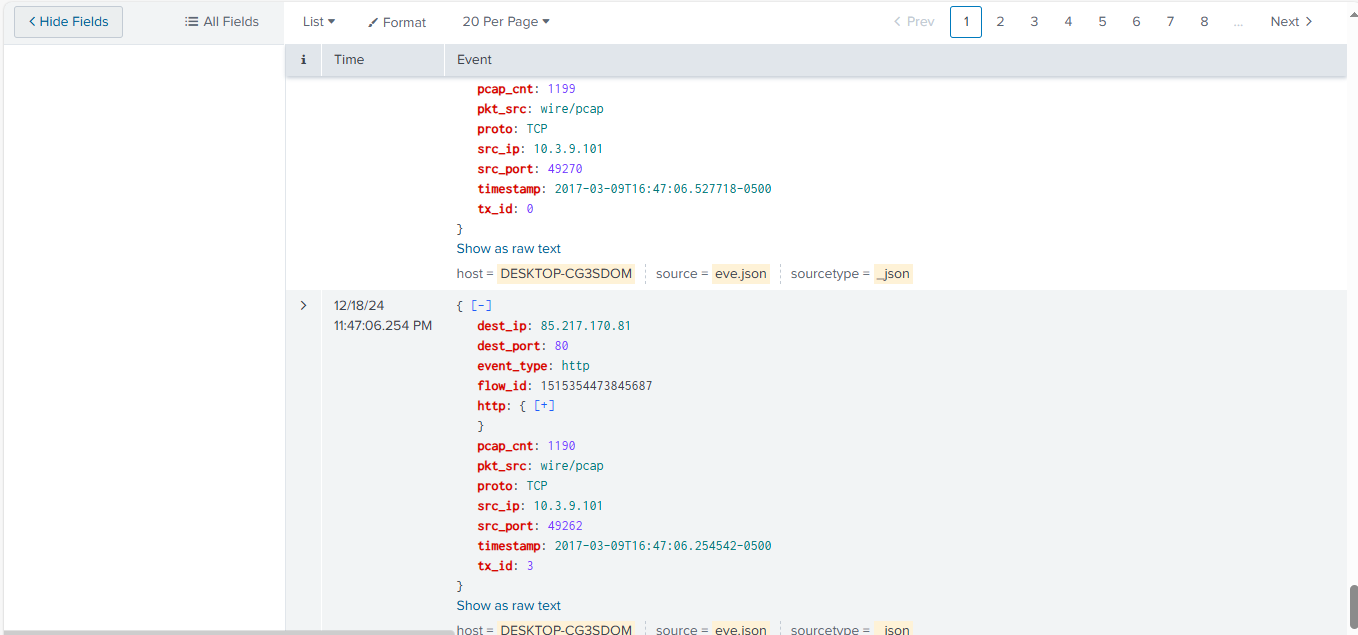
**Name: aya mohamed Abdelrahman**

**Id:20221380245**

**Proactive project**

1-



* This query retrieves events from the suricata index where the source file is eve.json, the host is DESKTOP-CG3SDOM, and the sourcetype is \_json.

**Results**:

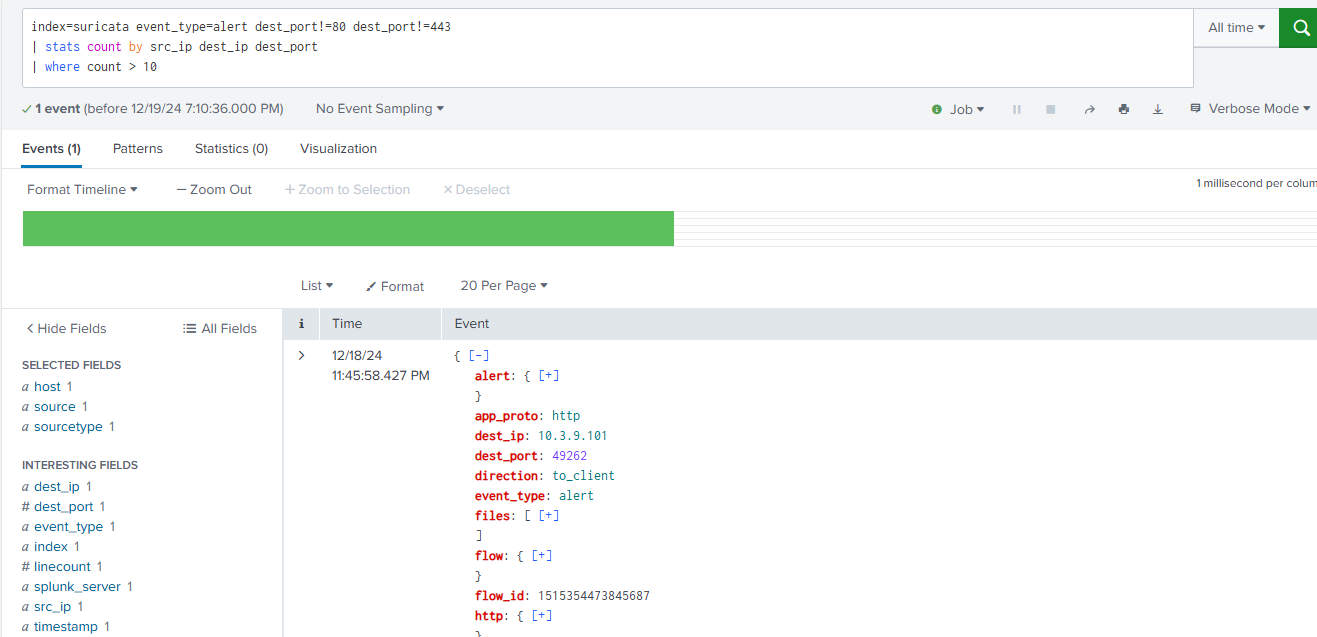
* **33,492 events** match the query.
* The results include parsed JSON objects generated by Suricata, a network intrusion detection system.

ach event includes structured fields that provide detailed information about network activity:

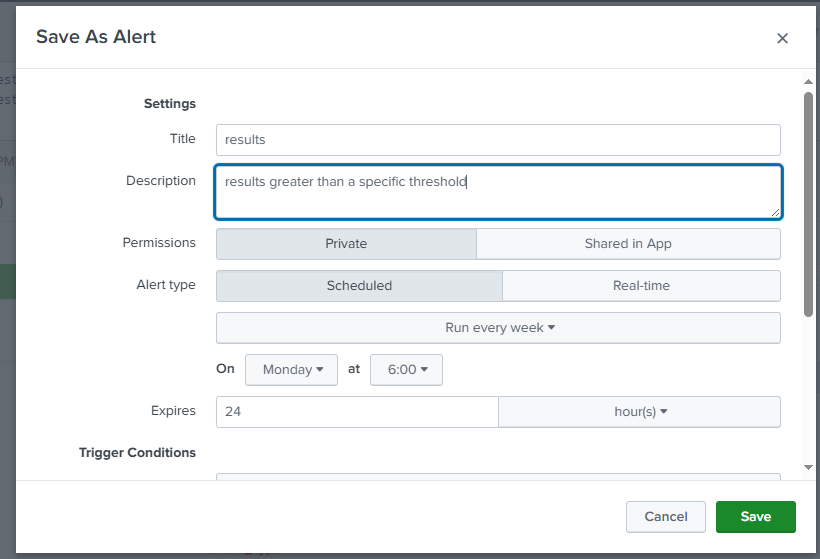
1. **Time**:
   * The timestamp (12/18/24 11:47:29.740 PM) indicates when the event was generated.
2. **Event Fields**:
   * **dest\_ip**: The destination IP address (85.217.170.81) targeted in the network communication.
   * **dest\_port**: The destination port (80), indicating the service (HTTP in this case).
   * **event\_type**: The type of the event (http), showing it relates to HTTP traffic.
   * **flow\_id**: A unique identifier (1515354473845687) for the network flow this event belongs to.
   * **http**: A nested field (clickable for details), likely containing HTTP-specific information like URL, headers, or method.
   * **pcap\_cnt**: The packet count (1232) related to this flow.
   * **pkt\_src**: The source of the packet capture (wire/pcap), indicating the origin of the data.
   * **proto**: The protocol (TCP), showing the transport layer protocol.
   * **src\_ip**: The source IP address (10.3.9.101) initiating the communication.
   * **src\_port**: The source port (49262), used by the initiating device.
   * **timestamp**: An additional timestamp (2017-03-09T16:47:29.740578-0500) for the event, possibly from the original log.

**Analysis for the Report**

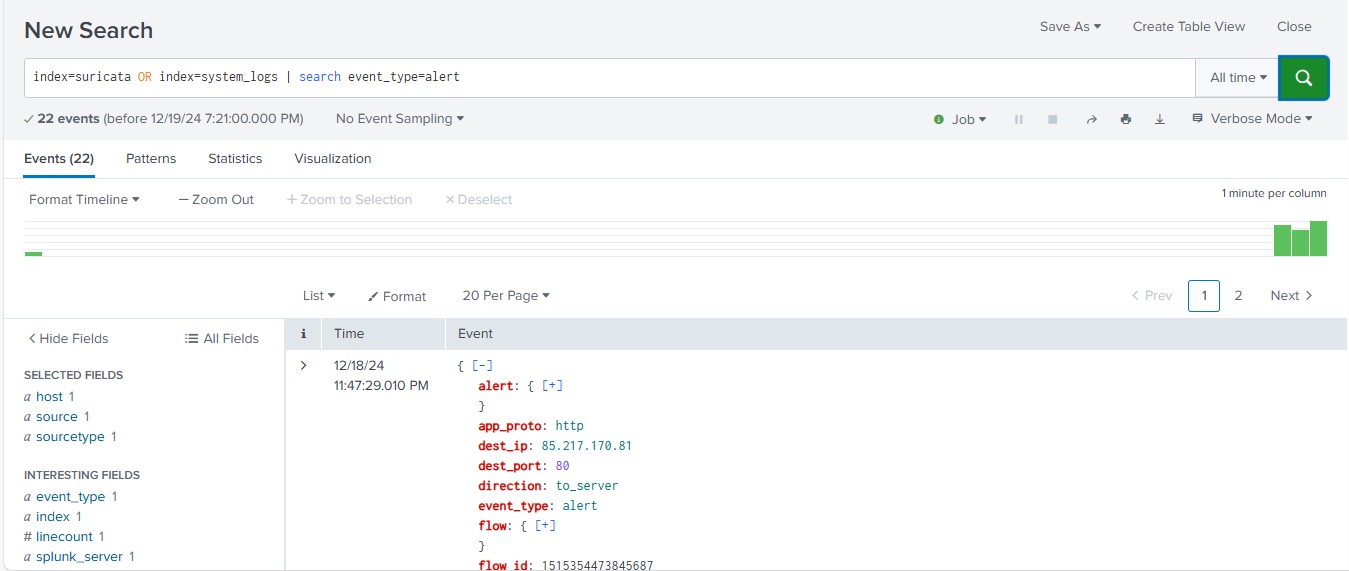
1. **Event Source**:  
   These logs are generated by Suricata, monitoring network traffic for suspicious or notable activity.
2. **HTTP Traffic**:  
   The event type (http) and the destination port (80) indicate that this is HTTP communication. The source and destination IPs provide insight into the parties involved.
3. **Packet Count**:  
   The packet count (1232) shows the volume of traffic associated with this flow. High packet counts could indicate prolonged or significant interactions.
4. **Flow Identification**:  
   The flow\_id uniquely identifies the session, which can be helpful for correlating related events.
5. **JSON Parsing**:  
   The structured format of the logs (JSON) allows Splunk to extract fields like event\_type, proto, and IP addresses for easier analysis.

2-

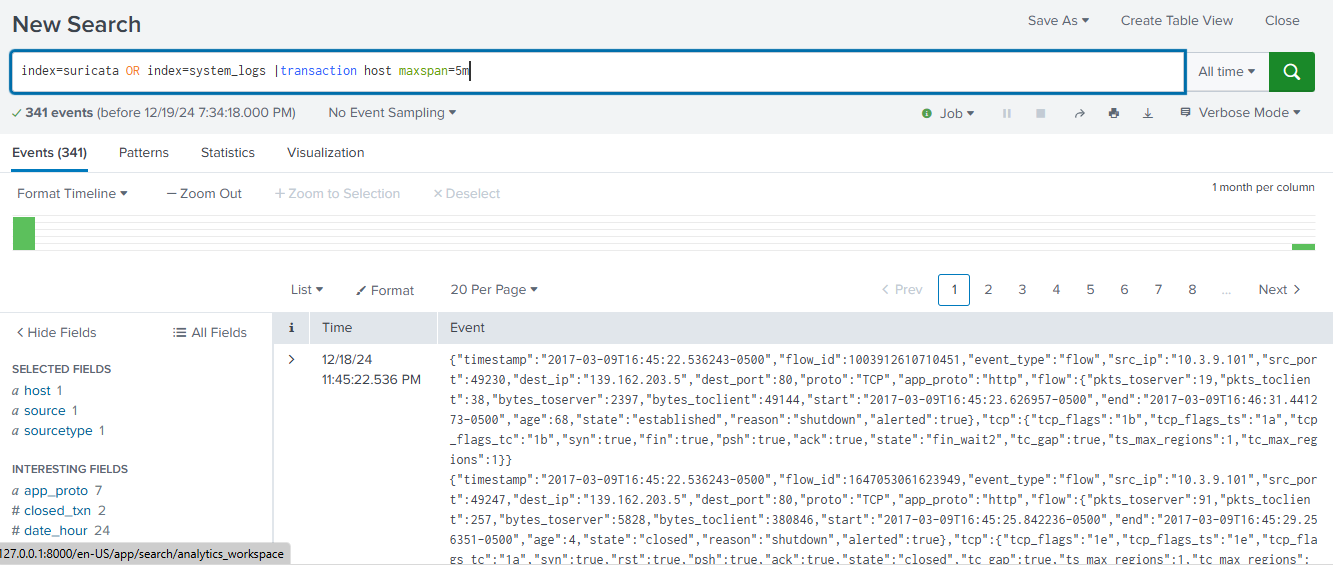
A Splunk search was conducted on Suricata alert logs to identify potentially suspicious network activity. The search focused on alerts occurring on non-standard ports (excluding 80 and 443) and aggregated results to identify connections generating more than 10 alerts. The results revealed a single instance where HTTP traffic was observed on destination port 49262 towards host 10.3.9.181. This unusual activity warrants further investigation, as using HTTP on a non-standard port is often associated with malicious behavior attempting to bypass standard port-based filtering.

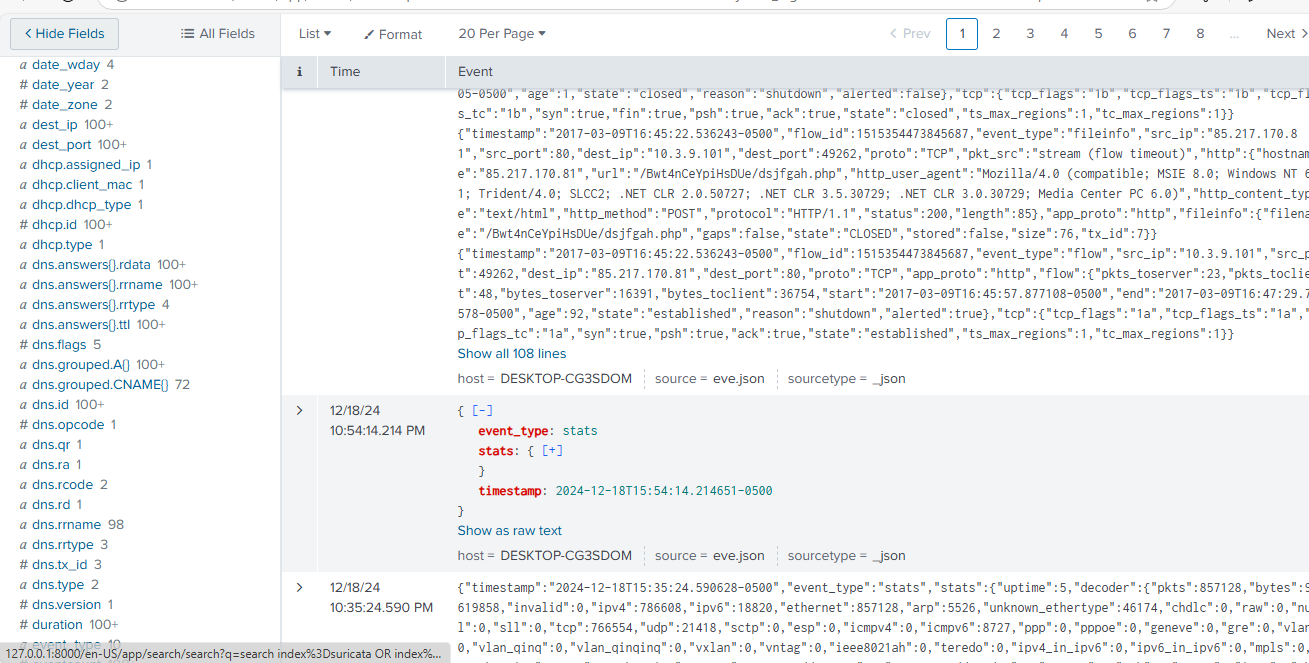
3-

To proactively monitor for suspicious network activity, a Splunk alert was configured. The alert was set to trigger based on the results of the Suricata alert search. The alert is configured with a descriptive title and description to clearly identify its purpose. The alert type is set to 'Scheduled' to run periodically (or 'Real-time' if immediate notification is needed). The trigger condition is set to activate if the search returns any results, indicating the presence of HTTP traffic on non-standard ports, which is a potential indicator of malicious activity. This automated alert mechanism allows for timely detection and response to potential security threats.

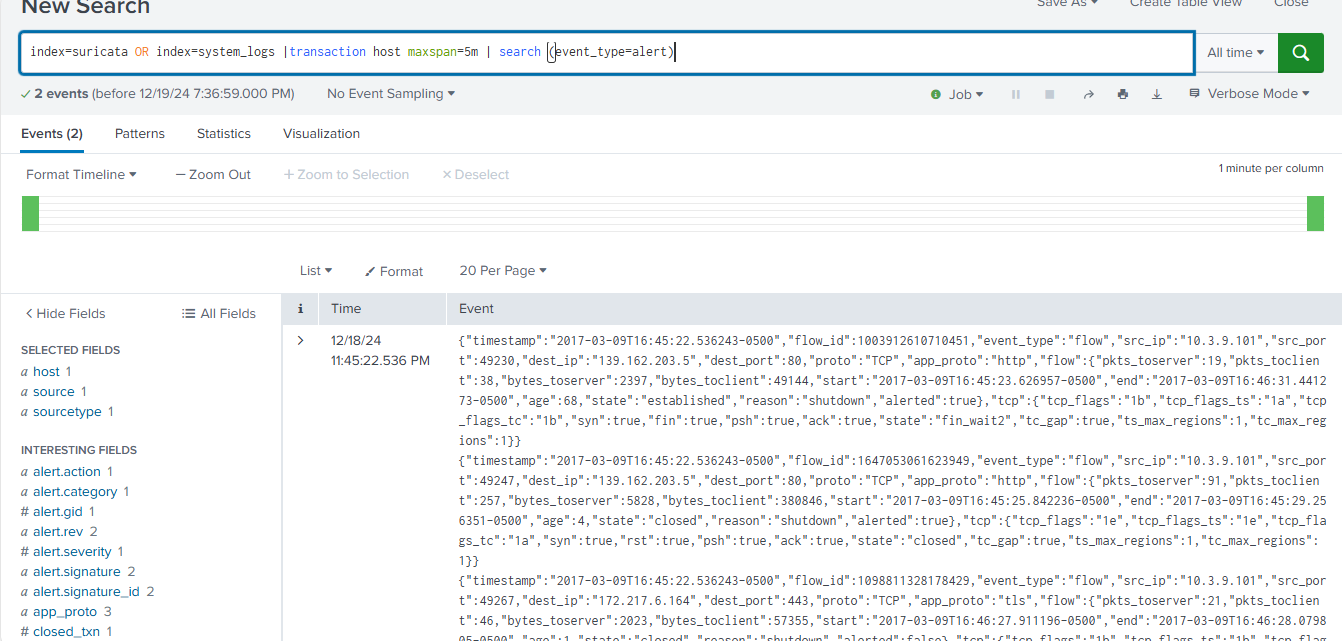
4-

A Splunk search was executed to identify security alerts from both Suricata (network intrusion detection) and system logs. The search queried the 'suricata' and 'system\_logs' indexes, filtering for events with the event\_type of 'alert'. The search returned 22 events before December 19, 2024, at 7:21 PM. An example event shows an HTTP connection (port 80) directed to the server at IP address 85.217.170.81. This indicates that some rule or signature in Suricata (or potentially a system log event) was triggered by this HTTP traffic. The flow\_id can be used to investigate other related network traffic.

5-



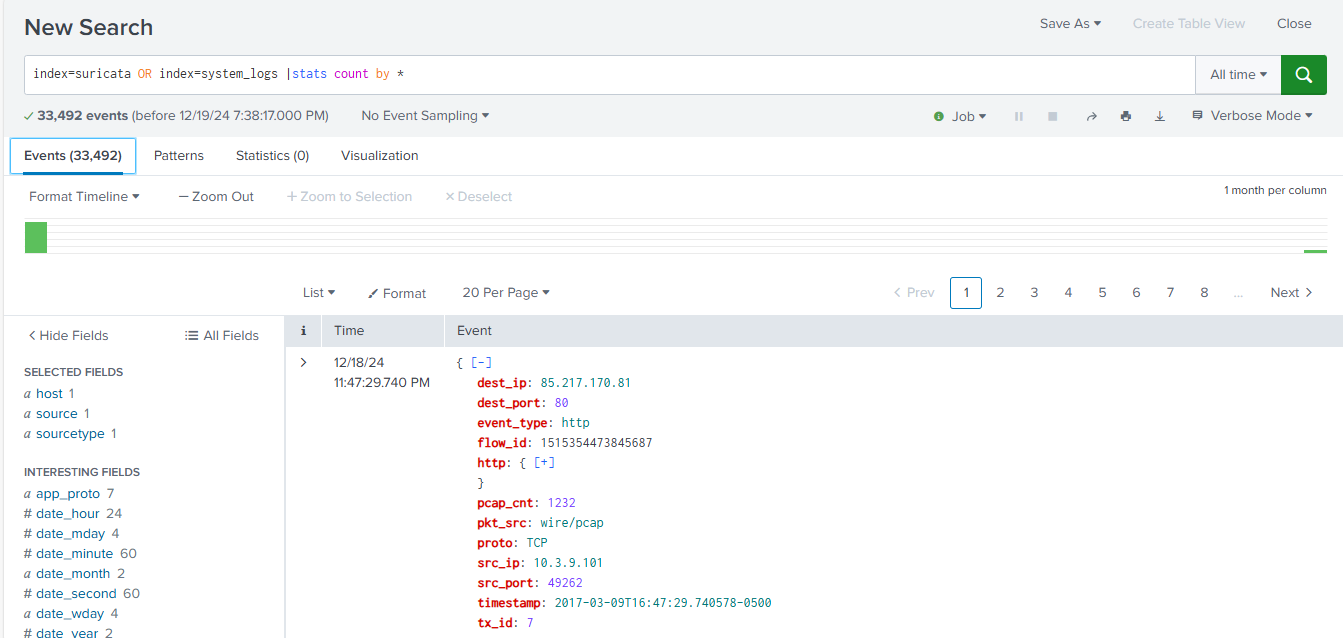
A Splunk search was conducted to analyze network transactions involving the host 'maxparan5'. The search queried the 'suricata' and 'system\_logs' indexes, using the 'transaction' command to group related events. The results show 341 events before December 19, 2024, at 7:34 PM. The example events shown are Suricata flow logs, indicating HTTP traffic (port 80) between host 10.3.9.101 (likely 'maxparan5') and the server at 139.162.203.5. The 'flow' field provides detailed information about the network connection, including packet and byte counts, start and end times, and the reason for connection termination. The 'alerted: true' flag indicates that these flows triggered an alert, warranting further investigation to determine the specific Suricata rule that was triggered and the nature of the potentially suspicious activity. The TCP flags provide further detail about the state of the TCP connection.

6-

A Splunk search was performed to analyze network transactions involving the host 'maxparan5', focusing on alerts. The search queried the 'suricata' and 'system\_logs' indexes, using the 'transaction' command with a 'span=5m' to group related events within 5-minute windows. This ensures that only closely related events are grouped together. The search further filtered for transactions containing alerts (event\_type=alert). The results showed two transactions before December 19, 2024, at 7:36 PM, each containing at least one alert.

The first transaction involves HTTP traffic (port 80) between 'maxparan5' (10.3.9.101) and 139.162.203.5. The second transaction involves TLS/HTTPS traffic (port 443) between 'maxparan5' and 172.217.6.164. Both transactions were flagged as alerts, as indicated by the 'alerted: true' flag. The 'flow' field provides detailed metrics for each network flow, including packet and byte counts, timing information, and connection state.

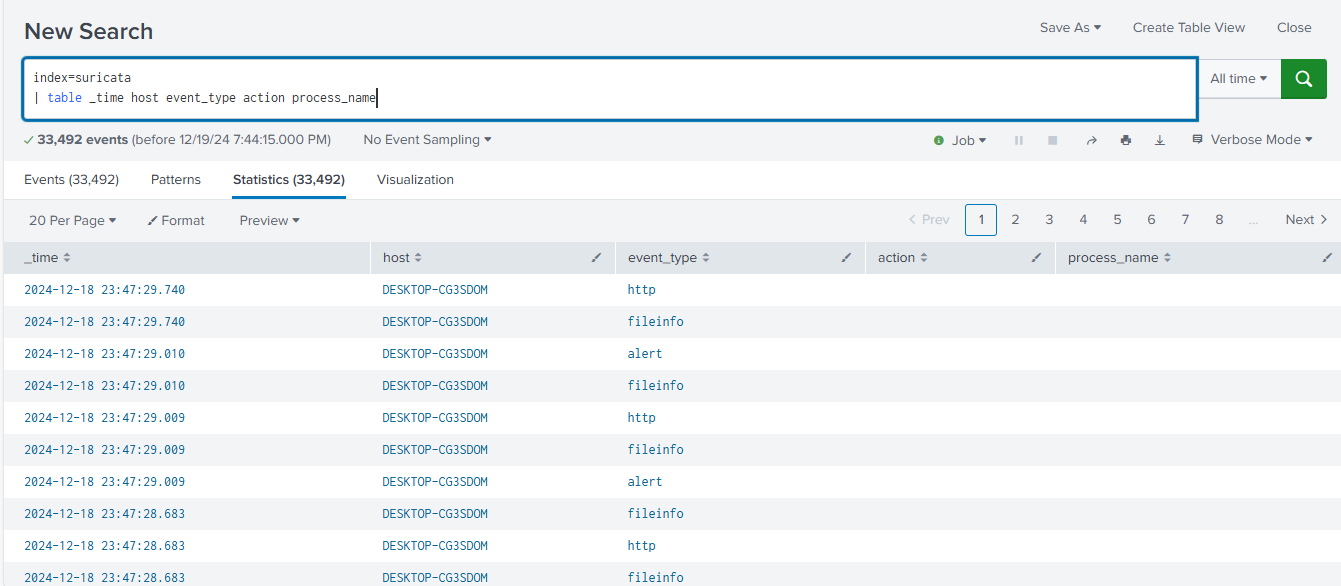
These alerts warrant further investigation to determine the specific Suricata rules triggered and the nature of the potentially suspicious activity. The use of the 'span=5m' option ensured that only relevant events within a short timeframe were grouped, providing a more accurate picture of the network activity associated with the alerts.

7-

A Splunk search was conducted to determine the total number of events present in the 'suricata' and 'system\_logs' indexes. The search used the stats count by \* command to count events grouped by all available fields. This resulted in a total of 33,492 events found before December 19, 2024, at 7:38 PM.

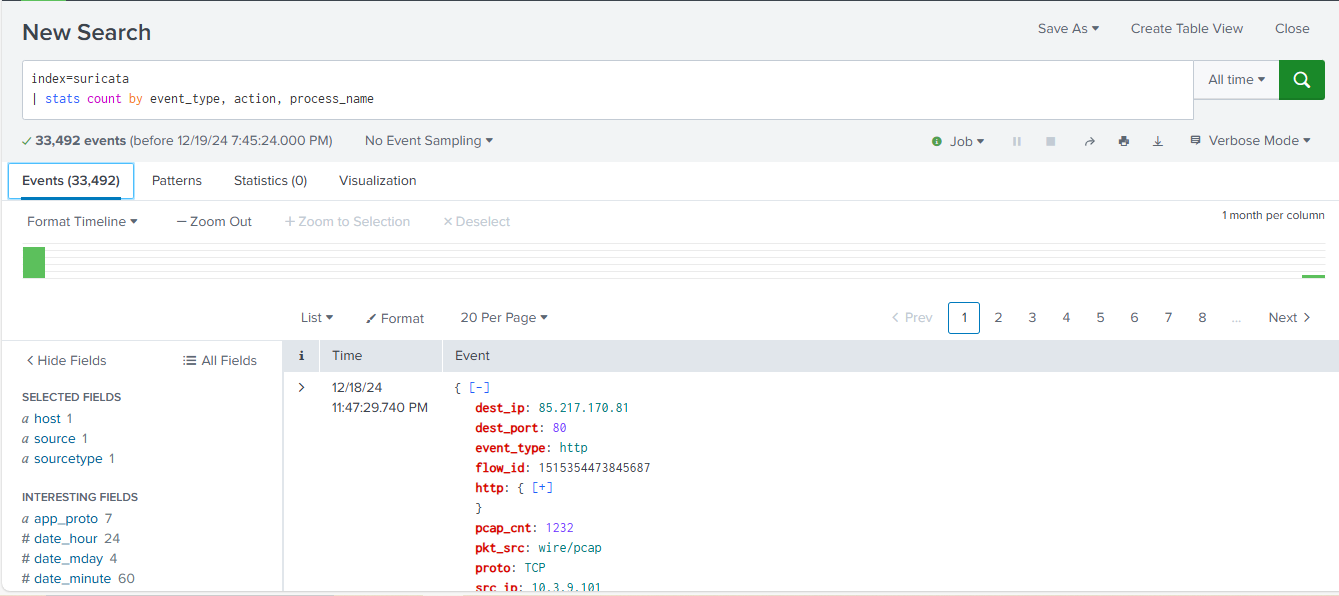
The screenshot displays an example of one of the events processed by the search. This particular event is related to HTTP traffic (port 80) between 10.3.9.101 and 85.217.170.81. It includes details such as the flow ID, packet count, source and destination IP addresses and ports, and a timestamp.

It is important to note that the stats count by \* command is generally not an efficient way to analyze data, as it creates a large number of groups. A more targeted approach, focusing on specific fields of interest, would typically be used for more meaningful analysis.

8-

A Splunk search was conducted on the 'suricata' index to examine network events. The search used the table command to display specific fields: \_time, host, event\_type, action, and process\_name. The search returned 33,492 events before December 19, 2024, at 7:44 PM.

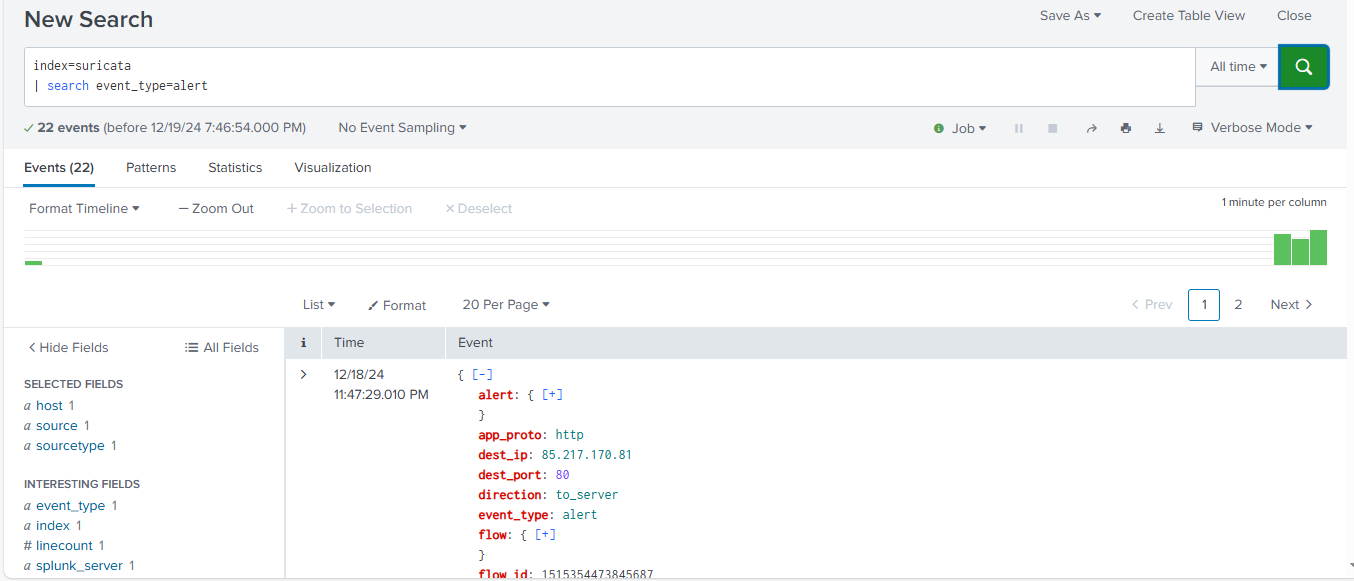
The results show a variety of event types occurring on the host 'DESKTOP-CG3SDOM', including 'http', 'fileinfo', and 'alert' events. The presence of 'alert' events indicates that Suricata detected potentially suspicious activity. The 'fileinfo' events suggest that Suricata was also logging information about file access or modifications. Further investigation is needed to analyze the details of the 'alert' events and understand the specific nature of the detected threats. The lack of data in the 'action' and 'process\_name' fields for these specific events suggests that those fields aren't populated for these particular event types in the Suricata logs.

9-

A Splunk search was performed on the 'suricata' index to analyze the distribution of events based on their type, associated action, and process name. The search used the stats count by event\_type, action, process\_name command to aggregate the events. The search found a total of 33,492 events before December 19, 2024, at 7:45 PM.

The results are presented in a table (partially shown), where each row represents a unique combination of event type, action, and process name, along with the number of times that combination occurred. The example event displayed in the screenshot is an HTTP event with details such as destination IP, port, and flow ID. This specific event contributed to the overall count of HTTP events (and potentially a specific action and process name combination in the full table).

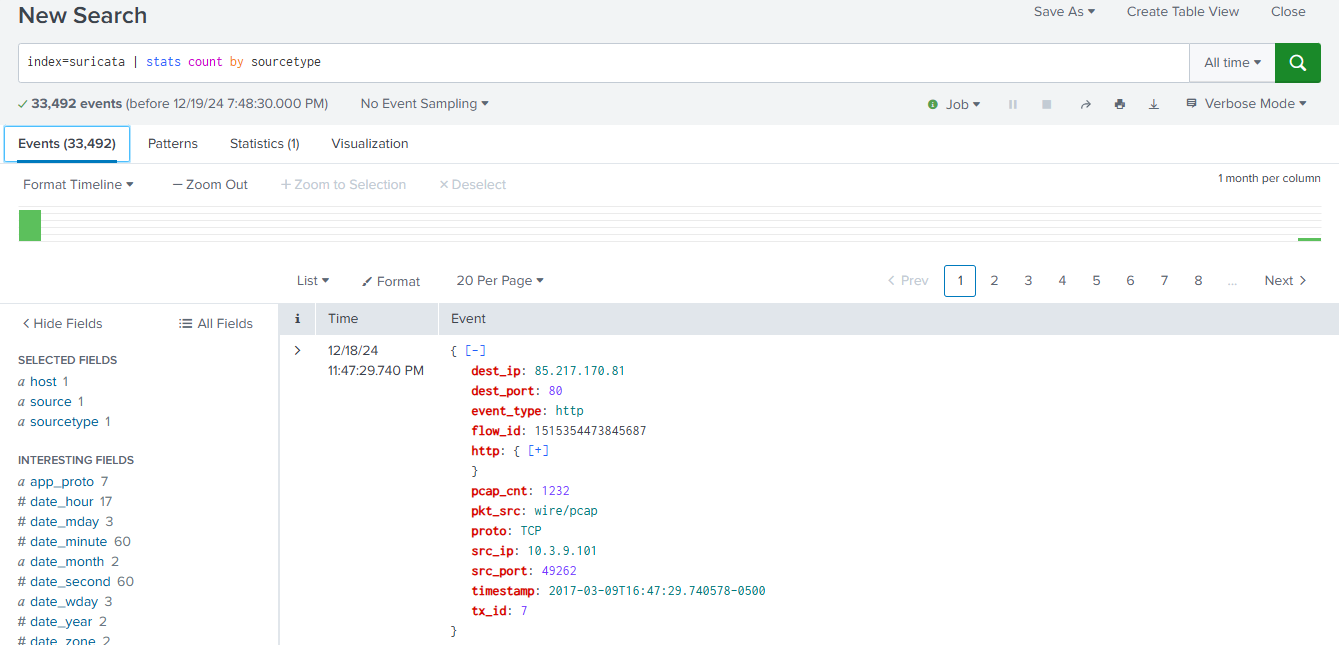
This analysis provides a high-level overview of the types of events being logged by Suricata and their distribution. Further analysis can then be performed by drilling down into specific event types or combinations of fields to investigate potential security issues.

10-

A Splunk search was conducted on the 'suricata' index to identify security alerts. The search specifically filtered for events where the event\_type field was 'alert'. The search returned 22 alerts before December 19, 2024, at 7:46 PM.

An example alert, occurring on December 18, 2024, at 11:47 PM, was triggered by HTTP traffic (port 80) directed to the server at IP address 85.217.170.81. The traffic was outbound from the monitored system ('to\_server'). The unique flow\_id (1515354473845687) allows for correlation with other network events related to this specific connection.

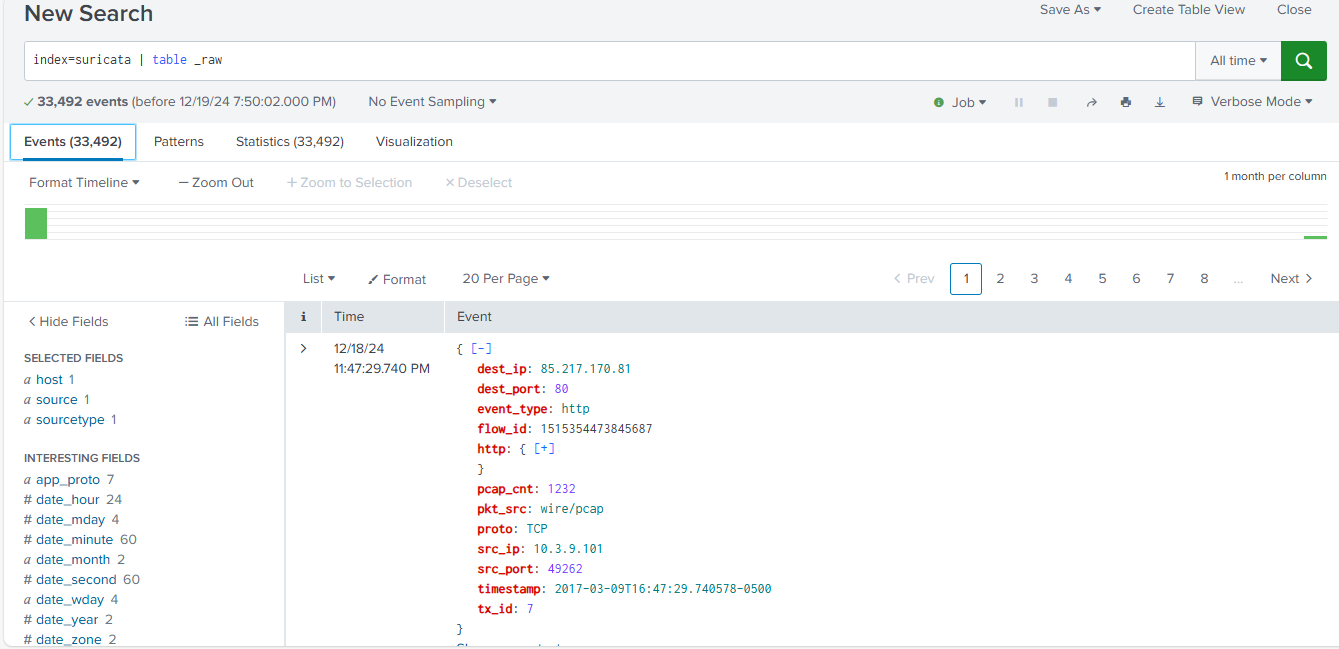
This alert indicates that Suricata detected potentially suspicious activity within the HTTP traffic to the specified server. Further investigation is required to determine the specific Suricata rule that was triggered and the nature of the potential threat.

11-

A Splunk search was performed on the 'suricata' index to analyze the distribution of events based on their source type. The search used the stats count by sourcetype command to aggregate the events. The search found a total of 33,492 events before December 19, 2024, at 7:48 PM.

The results are presented in a table (partially shown), where each row represents a unique sourcetype and the number of events belonging to that source type. The example event displayed in the screenshot is an HTTP event with details such as destination IP, port, and flow ID. This specific event contributed to the overall count for its corresponding sourcetype.

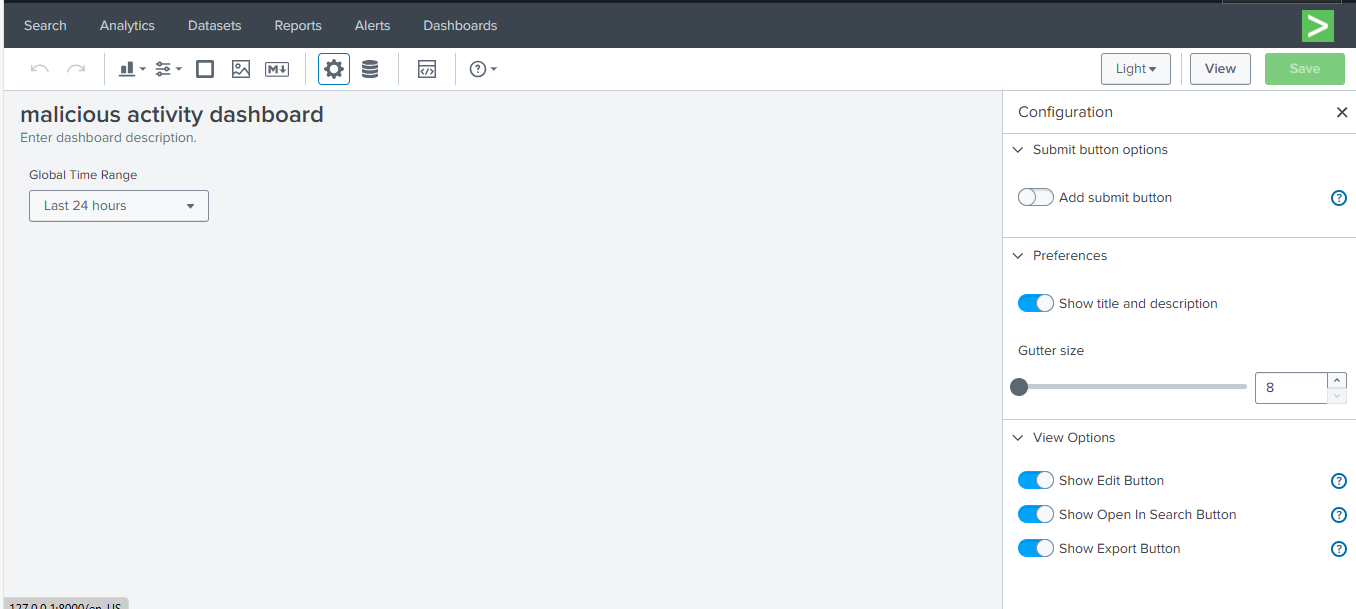
This analysis provides a high-level overview of the different types of logs being generated by Suricata. Further analysis can be performed by focusing on specific sourcetype values to investigate particular aspects of network activity or security events.

12-

A Splunk search was performed on the 'suricata' index to retrieve the raw event data. The search used the table \_raw command to display the complete, unprocessed log messages. The search returned 33,492 events before December 19, 2024, at 7:50 PM.

The screenshot displays an example of one of these raw events. The event is related to HTTP traffic (port 80) between 10.3.9.101 and 65.217.170.81. It contains various details about the network flow, including IP addresses, ports, protocol, packet count, and timestamps.

Retrieving the raw events is useful for detailed analysis and troubleshooting, as it provides the most complete information available. This raw data can then be further parsed and analyzed using other Splunk commands or external tools.

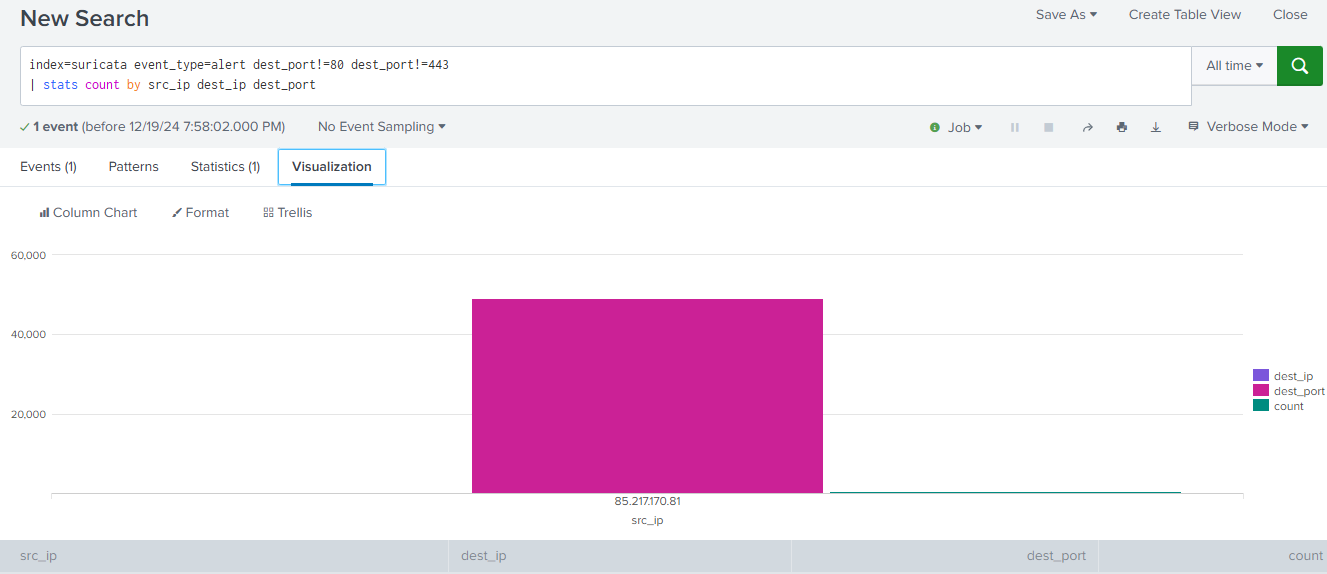
13-

A Splunk dashboard titled 'malicious activity dashboard' has been configured to monitor potential security threats. The dashboard's global time range is set to the 'Last 24 hours', displaying data from the past day.

The dashboard configuration includes the following settings:

* The title and description are set to be visible.
* The gutter size between panels is set to 8.
* Users have the ability to edit the dashboard, open the underlying searches in new search windows, and export the dashboard.

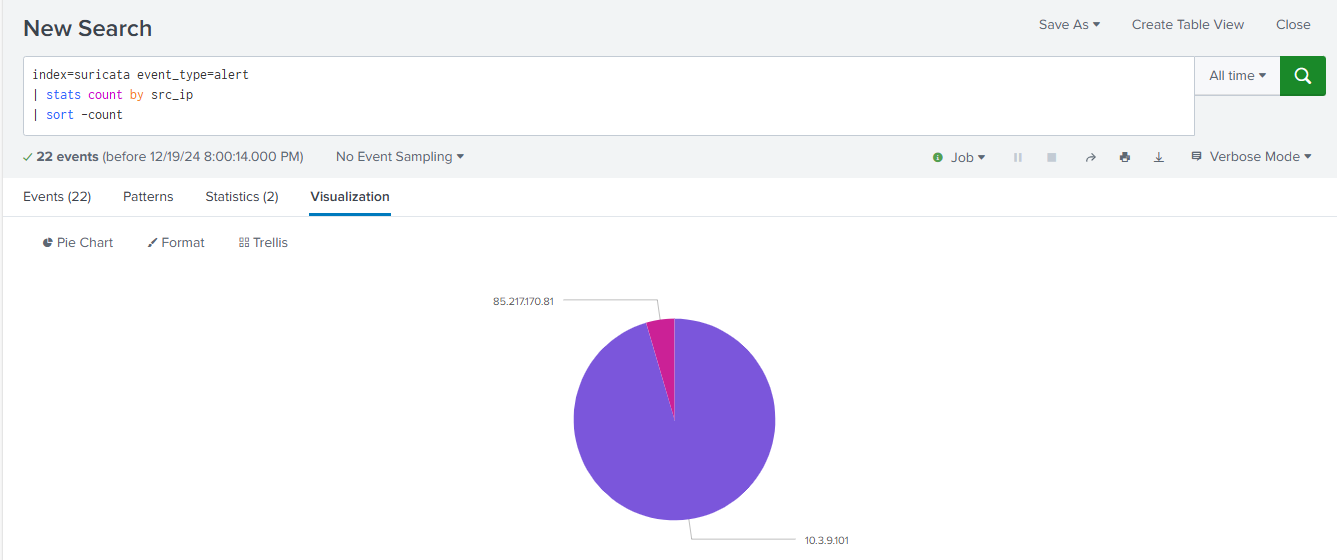
These configuration settings provide a clear and informative display of security-related data and allow users to interact with the dashboard for further analysis and investigation.

14-

A Splunk search was performed on the 'suricata' index to identify potentially suspicious network activity occurring on non-standard ports. The search filtered for alerts (event\_type=alert) excluding destination ports 80 (HTTP) and 443 (HTTPS) and then aggregated the results by source IP, destination IP, and destination port using the stats command.

The search identified one distinct combination of source IP, destination IP, and destination port that triggered alerts. The visualization (column chart) clearly shows this single instance. This result suggests that there was network traffic, possibly HTTP traffic (as seen in previous examples with the same flow ID), occurring on a non-standard port to the destination IP 85.217.170.81.

This activity warrants further investigation, as using HTTP on non-standard ports is often associated with malicious behavior attempting to evade detection. Further analysis should focus on the specific Suricata rules that were triggered and the details of the network traffic to determine the nature of the potential threat.

15-

A Splunk search was performed on the 'suricata' index to analyze the distribution of alerts based on source IP addresses. The search filtered for alerts (event\_type=alert) and then used the stats count by src\_ip command to count alerts per source IP. The results were then sorted in descending order of count using sort -count.

A total of 22 alerts were found before December 19, 2024, at 8:00 PM. The results were visualized using a pie chart to clearly show the distribution of alerts across different source IPs.

The pie chart reveals that the vast majority of alerts originated from the source IP address 10.3.9.101. A significantly smaller number of alerts originated from 85.217.170.81. This indicates that the host at 10.3.9.101 was the primary source of the detected suspicious activity. This host should be prioritized for further investigation to determine the nature of the alerts and whether any malicious activity occurred.