Firewall Log Analysis Using Splunk

Introduction:

This report consists of analyzing firewall logs on Splunk, a Security Information and Event Management Tool. The analysis includes data ingestion, security threat identification, and analysis.

Dataset:

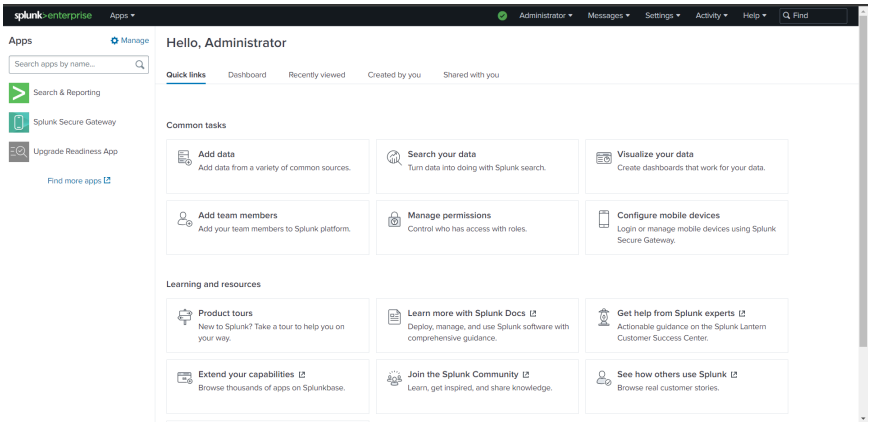
The dataset is a simulated firewall log file (firewall_log_example.txt), which contains entries for both normal and potentially malicious traffic, including:

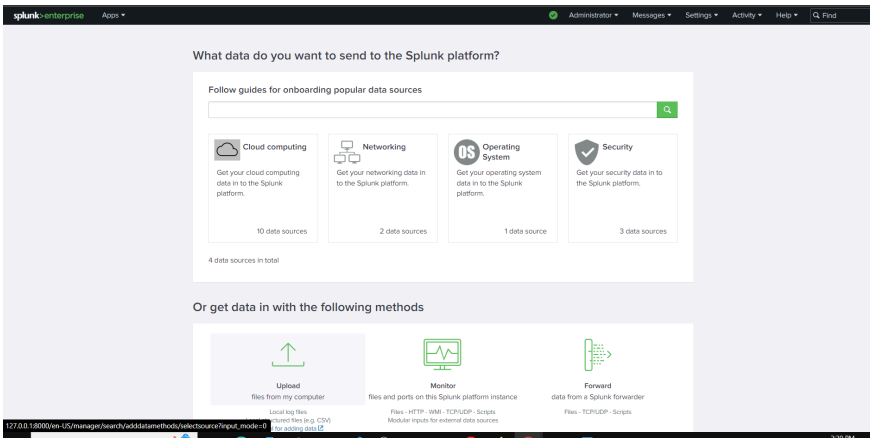
- Allowed and blocked traffic events.
- Access attempts to high-risk ports.
- Repeated access attempts from the same IP address.
- Intrusion detection system alerts.

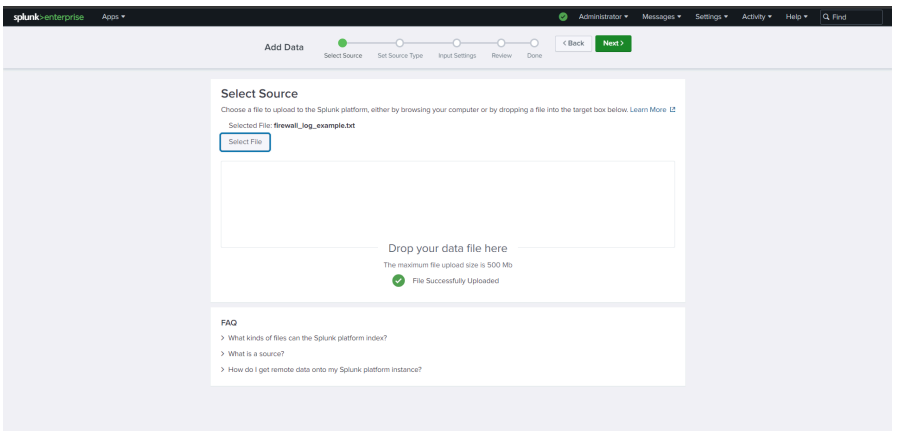
Tasks:

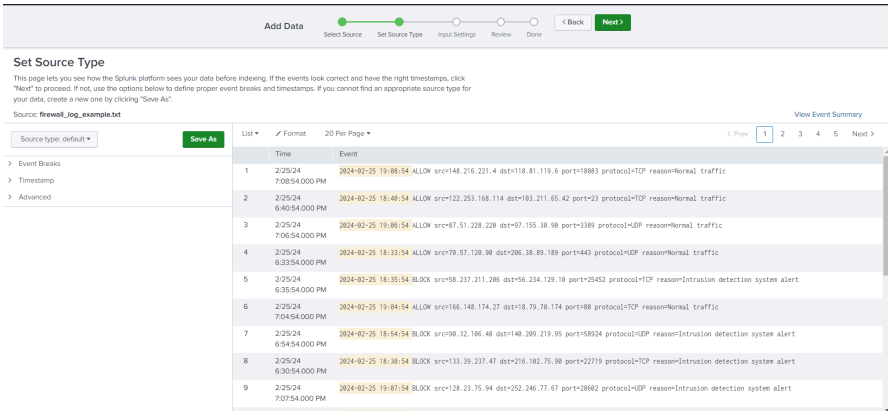
1. **Data Ingestion:**

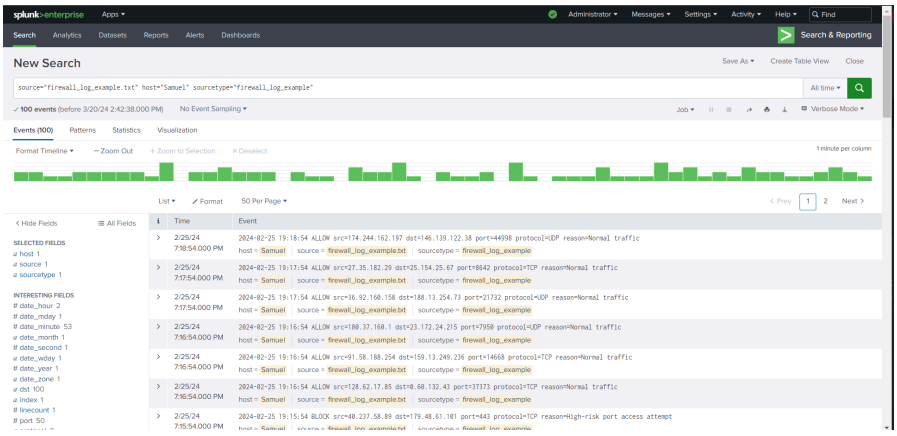
- This step involved ingesting the firewall log file that is to be analyzed.





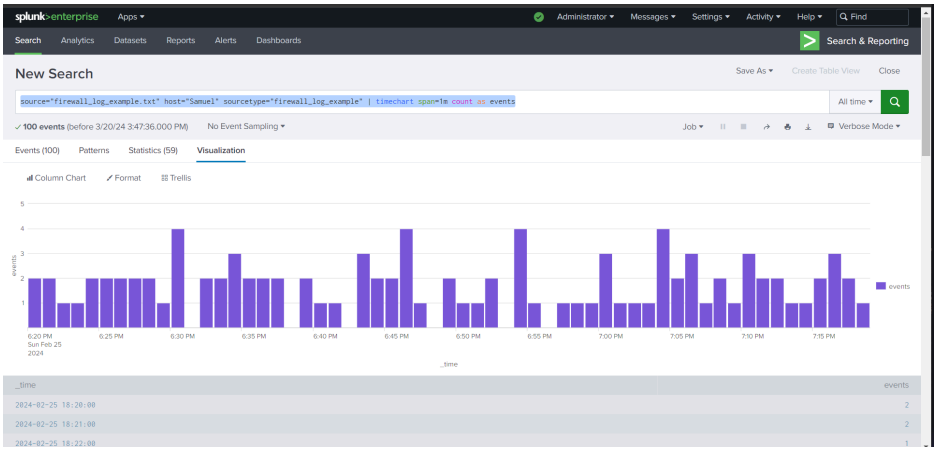


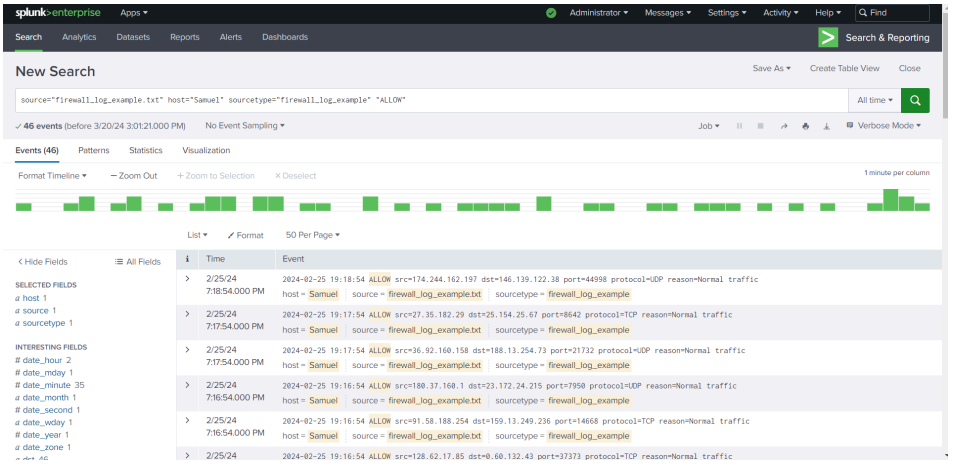




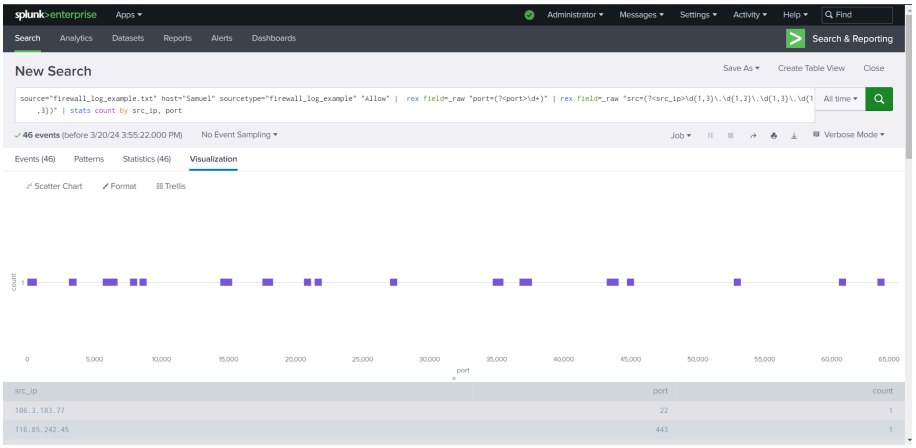
2. **Analysis:**

- The events that are logged are between time frame 6:20 pm - 7:20 pm on 25th Feb, 2024. Below is the visualized data:
- Search query used: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" | timechart span=1m count as events***

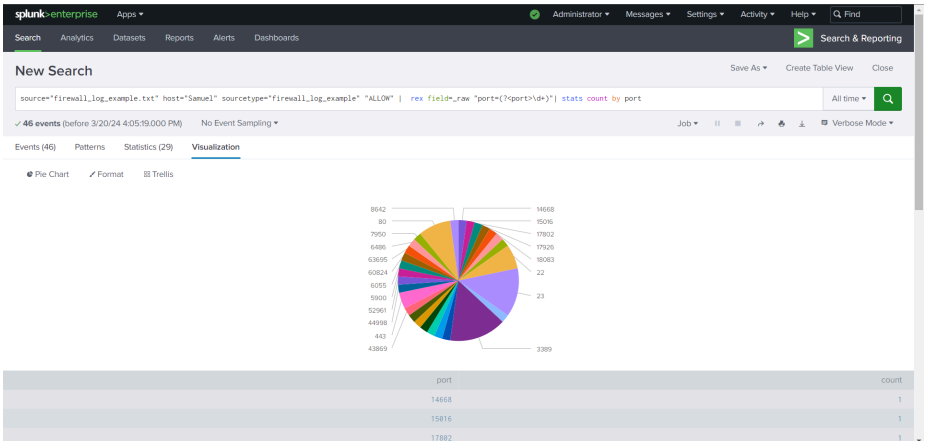
- 

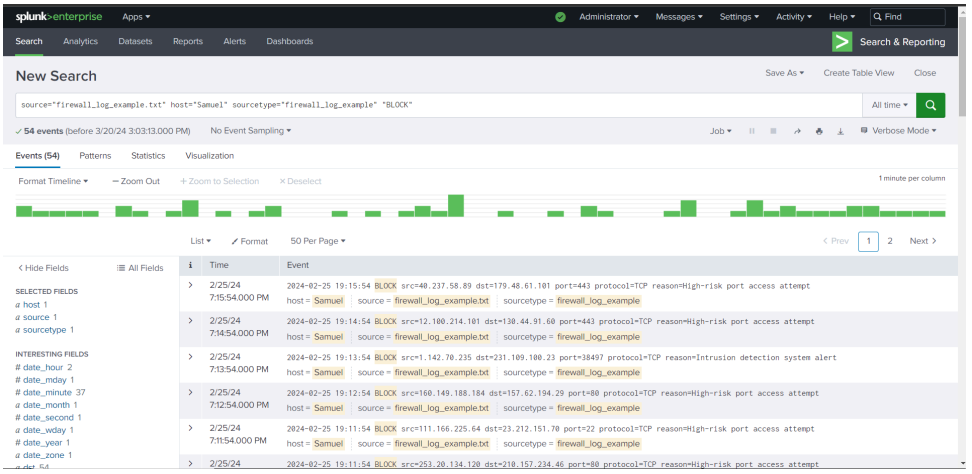
- The log file consists of 100 different events, where 46 events are ‘Allow Events’ and 54 are ‘Block Events’
- The firewall allowed a total Allowed 46 different IP addresses to access a significant port.
- Search Query used: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "ALLOW"***
- 

- Scatter Plot for all the allowed events:
- Search query used: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "BLOCK" | rex field=_raw "port=(?<port>\d+)" | rex field=_raw "src=(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | stats count by src_ip, port***

- 

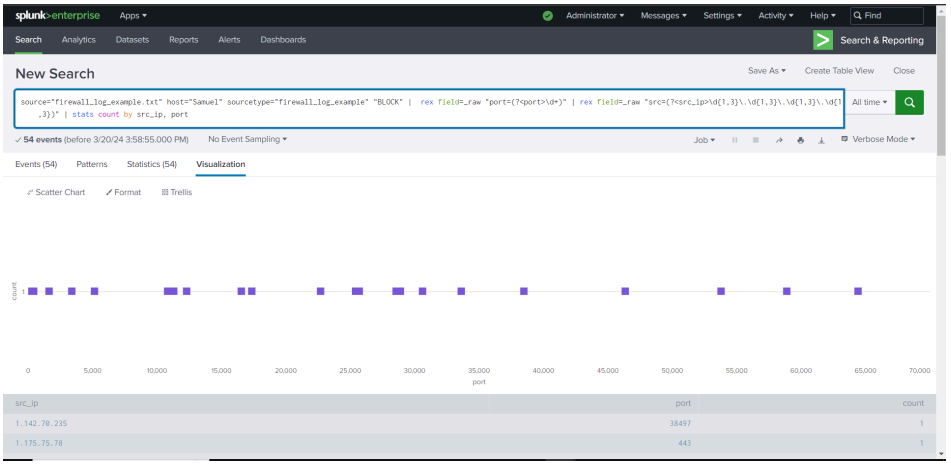
- Piechart based on Port numbers for all events that were allowed
- Search query: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "ALLOW" | rex field=_raw "port=(?<port>\d+)"| stats count by port***

- 

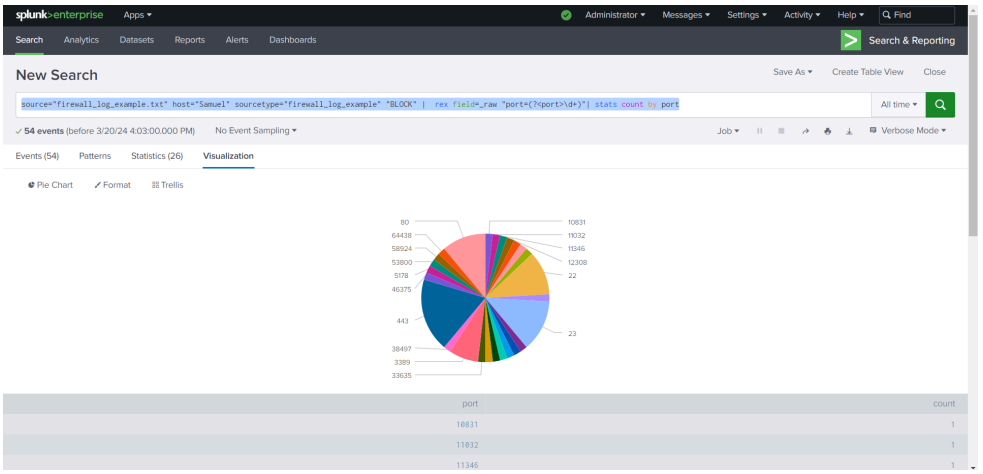
- 

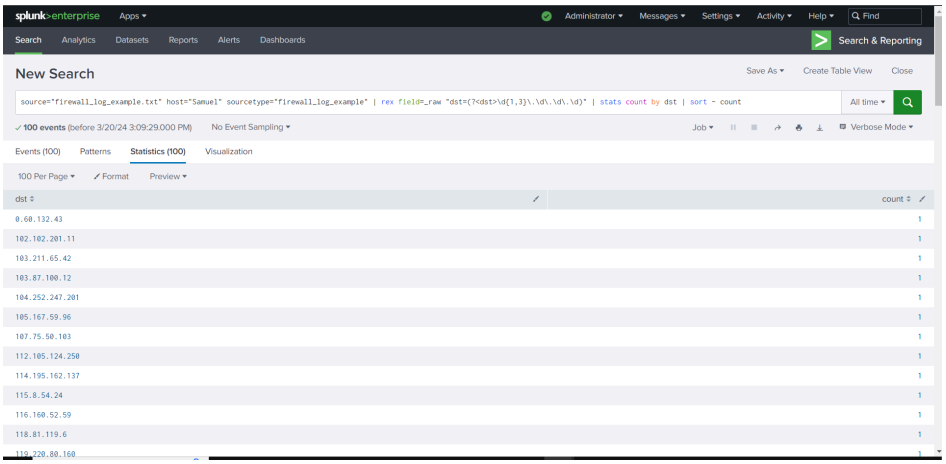
- Using search query: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "BLOCK"***
- Scatter Plot for all the blocked events based on Source IP address and Port number
- Search query used: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "BLOCK" | rex field=_raw***

"port=(?<port>\d+)" | rex field=_raw "src=(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | stats count by src_ip, port



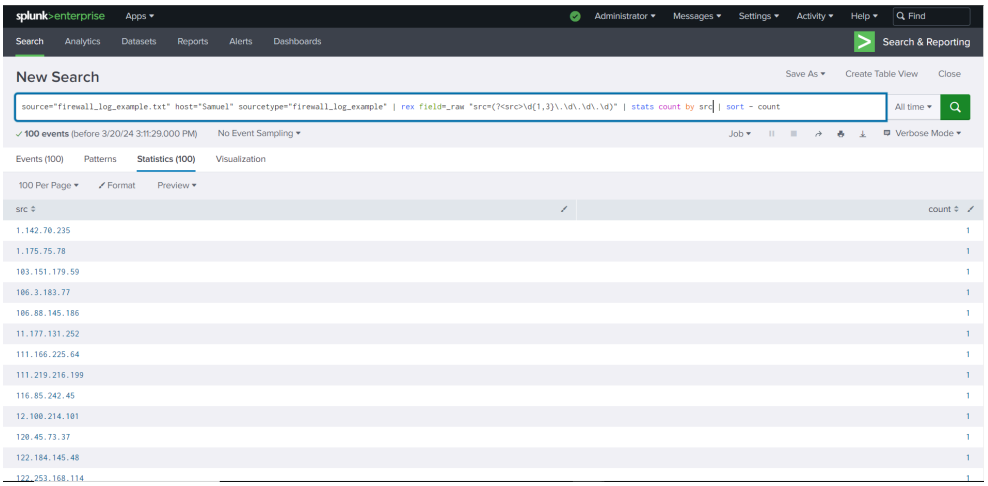
- Piechart based on Port numbers for all events that were blocked
- Search query: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "BLOCK" | rex field=_raw "port=(?<port>\d+)"| stats count by port***





- Discovered 100 different destination IP addresses using search query: ***source="firewall_log_example.txt" host="Samuel"***

sourcetype="firewall_log_example" | rex field=_raw "dst=(?<dst>\d{1,3}\.\d\.\d\.\d)" | stats count by dst | sort - count

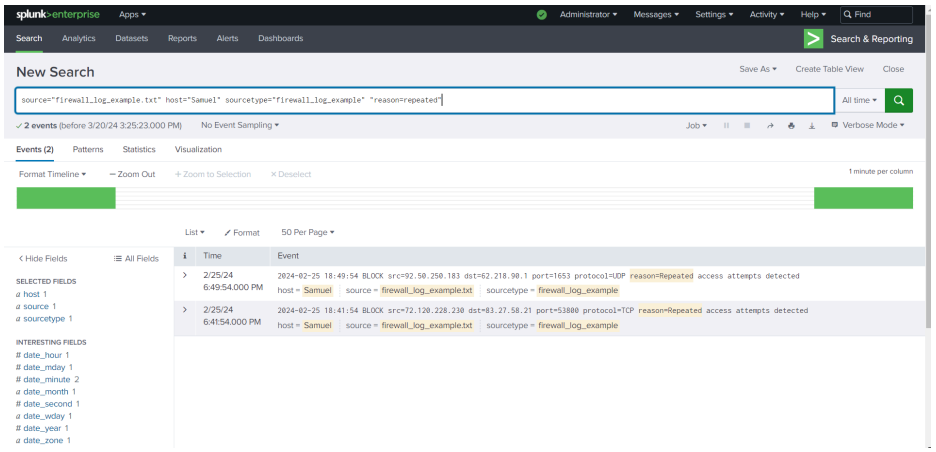


-

- Discovered 100 different src IP addresses using a search query ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" | rex field=_raw "src=(?<src>\d{1,3}\.\d\.\d\.\d)" | stats count by src | sort - count***

3. Security Threat Identification:

- Repeated Access Attempts: Below mentioned IP addresses were blocked from accessing specific ports of an IP address due to repeated access attempts
  - '`92.50.250.183`' was blocked from access port '`1653`' of '`62.218.90.1`'
  - '`72.120.228.230`' was blocked from accessing port '`53800`' of '`83.27.58.21`'

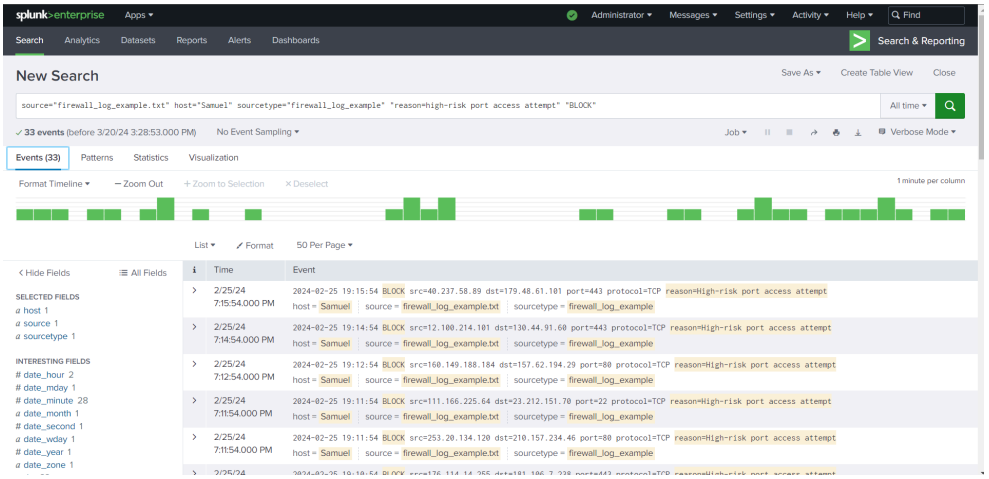


-

  - Search query used: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "reason=repeated"***

- High Volume Of Traffic On High-Risk Ports:
  - Discovered 33 events with a high risk of port access attempts which blocked different IP 33 addresses
  - Search query used: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "reason=high-risk port access attempt" "BLOCK"***

-



- Alert Generated By Intrusion Detection System:
  - Discovered 19 different events when the Intrusion detection system triggered an alert.
  - Search query used: ***source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" "reason=Intrusion detection system alert" "BLOCK"***

-