

# 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:

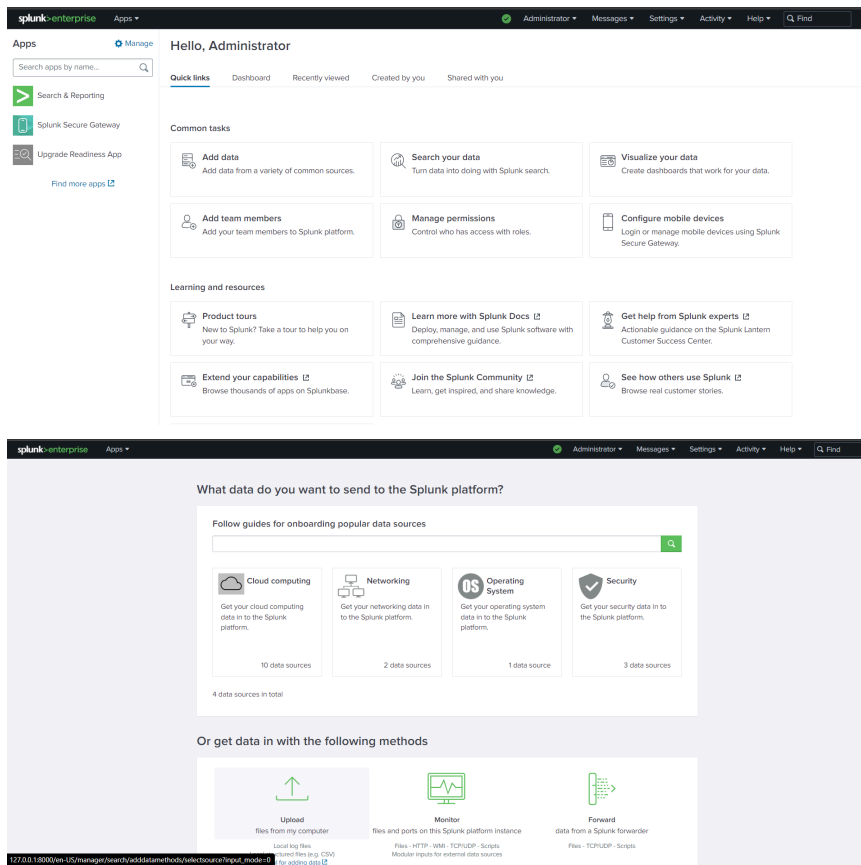
The dataset is a simulated firewall log file (firewall\_log\_example.txt), which contains entries for both normal and potentially malicious traffic, including:

- 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:

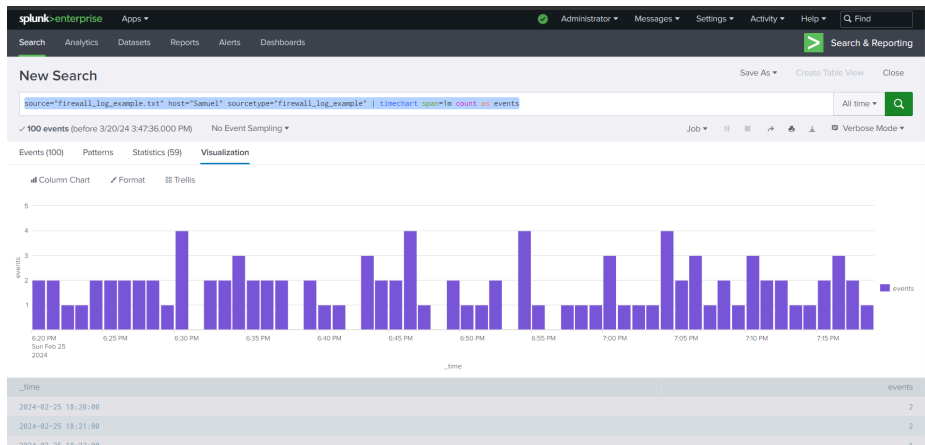
- This step involved ingesting the firewall log file that is to be analyzed.



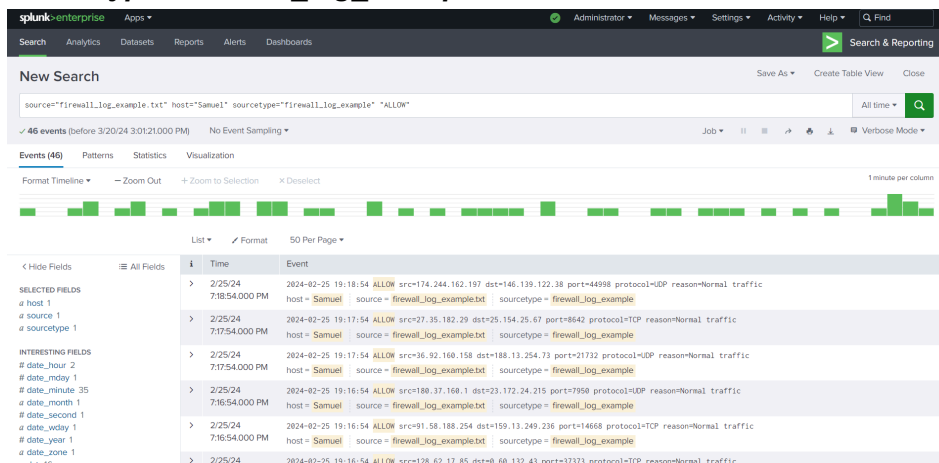
Add Data
Select Source
**Select Source Type**
Input Settings
Review
Done
< Back
**Next >**

Source type: default	Save As	List	Format	20 Per Page	<a href="#">← Prev</a> <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">Next →</a>
<ul style="list-style-type: none"> <li>Event Breaks</li> <li>Timestamp</li> <li>Advanced</li> </ul>		Time	Event		
	1	2/25/24 7:05:54.000 PM	2024-02-25 19:58:54 ALLOW src=148.216.221.4 dst=181.119.6 port=3883 protocol=TCP reason=Normal traffic		
	2	2/25/24 6:05:4.000 PM	2024-02-25 18:40:54 ALLOW src=122.253.168.114 dst=181.211.65.42 port=32 protocol=TCP reason=Normal traffic		
	3	2/25/24 7:06:54.000 PM	2024-02-25 19:16:54 ALLOW src=87.51.228.228 dst=97.155.38.98 port=3389 protocol=UDP reason=Normal traffic		
	4	2/25/24 6:33:54.000 PM	2024-02-25 18:33:54 ALLOW src=79.57.120.98 dst=206.38.189 port=443 protocol=TCP reason=Normal traffic		
	5	2/25/24 6:35:54.000 PM	2024-02-25 18:35:54 BLOCK src=58.237.211.286 dst=56.234.128.18 port=25462 protocol=TCP reason=Intrusion detection system alert		
	6	2/25/24 7:04:54.000 PM	2024-02-25 19:04:54 ALLOW src=166.148.174.27 dst=18.79.79.74 port=8 protocol=TCP reason=Normal traffic		
	7	2/25/24 6:54:54.000 PM	2024-02-25 18:54:54 BLOCK src=90.32.186.48 dst=140.269.219.95 port=58924 protocol=TCP reason=Intrusion detection system alert		
	8	2/25/24 6:30:54.000 PM	2024-02-25 18:30:54 BLOCK src=133.39.237.47 dst=216.162.75.98 port=22719 protocol=TCP reason=Intrusion detection system alert		
	9	2/25/24 7:05:54.000 PM	2024-02-25 19:07:54 BLOCK src=128.23.75.94 dst=252.246.77.67 port=20882 protocol=UDP reason=Intrusion detection system alert		

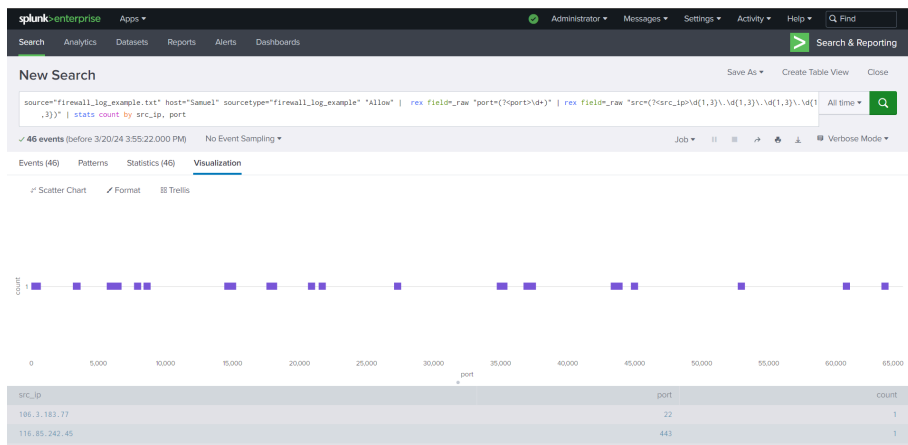
- The events that are logged are between time frame 6:20 pm - 7:20 pm on 25th Feb, 2024. Below is the visualized data:
- Search query used: ***source="firewall\_log\_example.txt" host="Samuel" sourcetype="firewall log example" | timechart span=1m count as events***



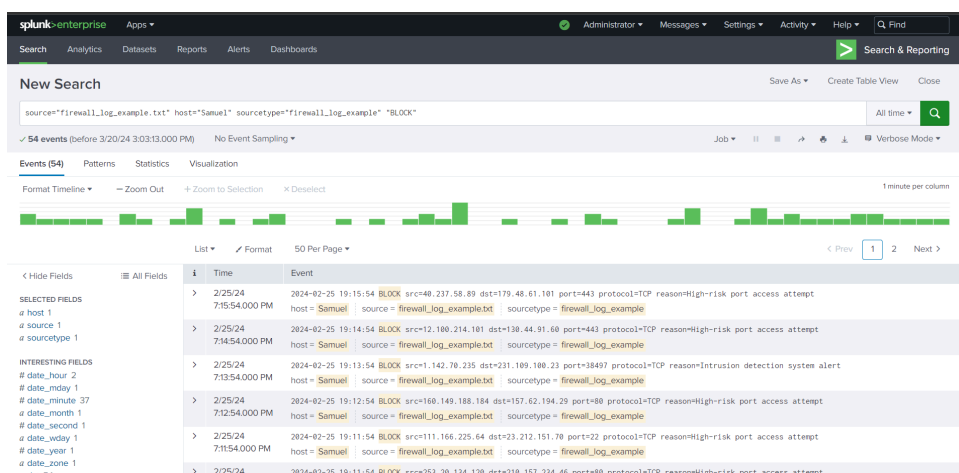
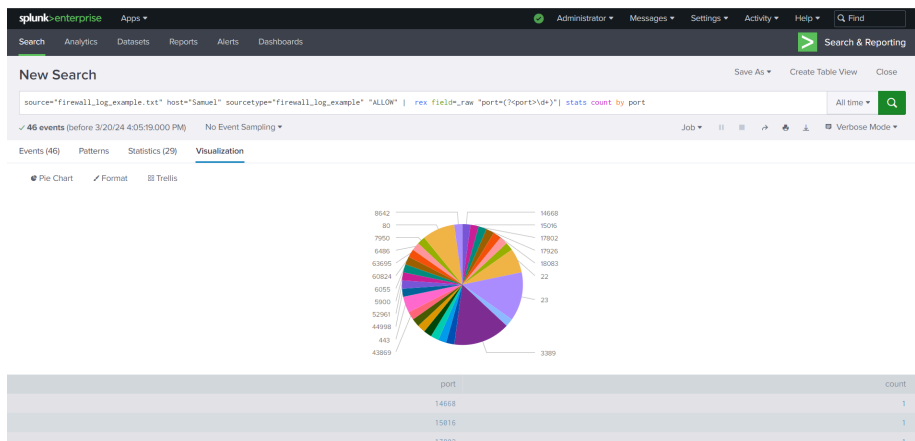
- The log file consists of 100 different events, where 46 events are 'Allow Events' and 54 are 'Block Events'
- The firewall allowed a total Allowed 46 different IP addresses to access a significant port.
- Search Query used: **source="firewall\_log\_example.txt" host="Samuel" sourcetype="firewall\_log\_example"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

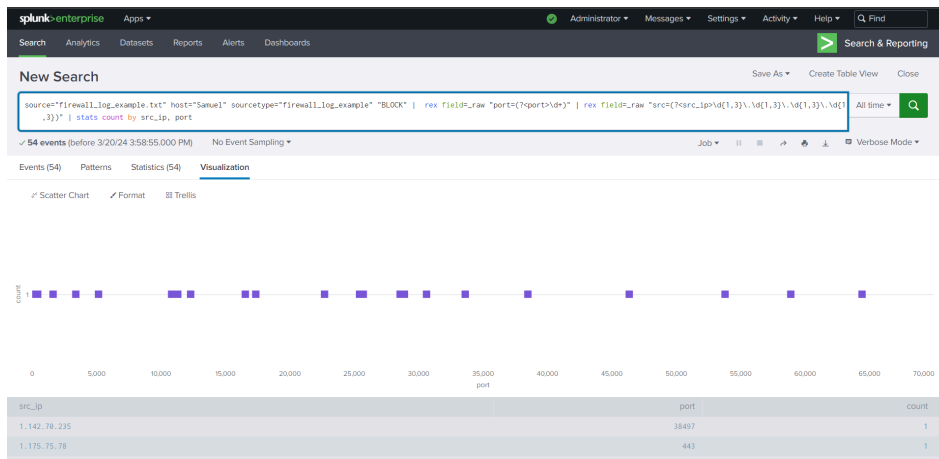


- Piechart based on Port numbers for all events that were allowed
- Search query: **source="firewall\_log\_example.txt" host="Samuel" sourcetype="firewall\_log\_example" "ALLOW" | rex field=\_raw "port=(?<port>\d+)" | stats count by port**

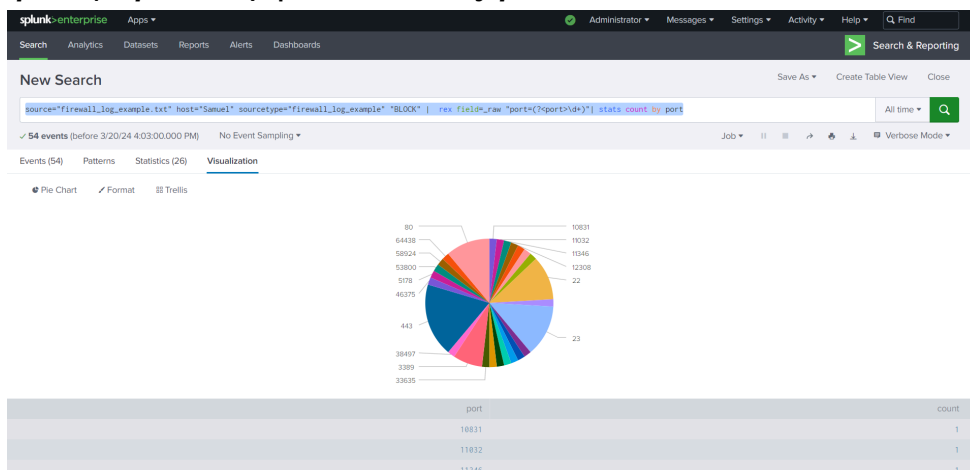


- Using search query: **source="firewall\_log\_example.txt" host="Samuel" sourcetype="firewall\_log\_example" "BLOCK"**
- Scatter Plot for all the blocked events based on Source IP address and Port number
- Search query used: **source="firewall\_log\_example.txt" host="Samuel" sourcetype="firewall\_log\_example" "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**



The screenshot shows a Splunk search interface with the following query: `source="firewall_log_example.txt" host="Samuel" sourcetype="firewall_log_example" | rex field=_raw "dst=(?<dst>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | stats count by dst | sort - count`. The results are displayed in a table with columns for `dst` and `count`.

dst	count
0.60.132.43	1
182.182.201.11	1
183.211.65.42	1
183.87.180.12	1
184.252.247.201	1
185.167.59.96	1
187.75.58.183	1
112.105.124.258	1
114.195.162.137	1
115.8.54.24	1
116.168.52.59	1
118.81.119.6	1
119.228.88.168	1

- 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>ld{1,3}\.ld\.ld\.ld)" | stats count by dst | sort - count***

src	count
1.142.70.235	1
1.175.75.78	1
103.151.179.59	1
106.3.183.77	1
106.88.145.186	1
11.177.131.252	1
111.166.225.64	1
111.219.216.199	1
116.85.242.45	1
12.108.214.101	1
120.45.73.37	1
122.184.145.48	1
122.253.168.114	1

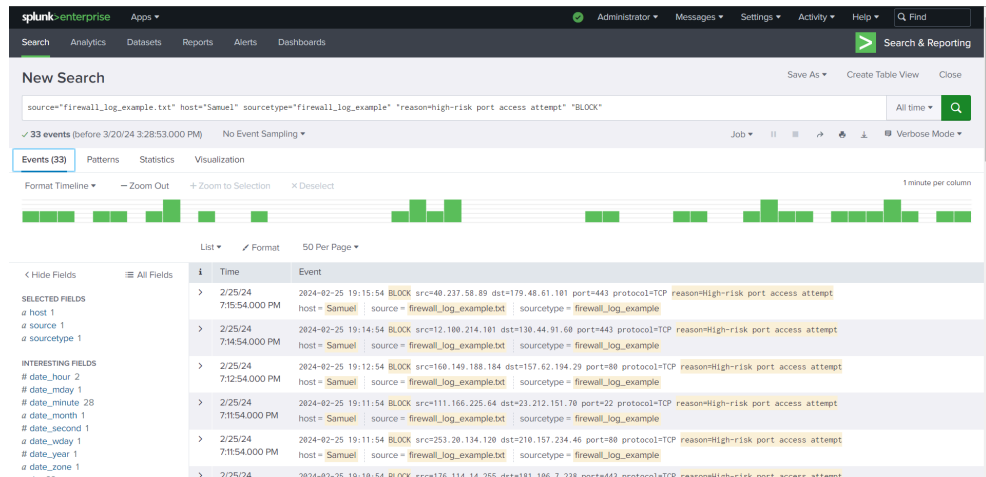
- Discovered 100 different src IP addresses using a search query  
***source="firewall\_log\_example.txt" host="Samuel"***  
***sourcetype="firewall\_log\_example" | rex field=\_raw***  
***"src=(?<src>ld{1,3}\.ld\.ld\.ld)" | stats count by src | sort - count***

### 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'

Time	Event
2/25/24 6:49:54.000 PM	2024-02-25 16:49:54 BLOCK src=92.50.250.183 dst=62.218.90.1 port=1653 protocol=UDP reason=Repeated access attempts detected host = Samuel source = firewall_log_example.txt sourcetype = firewall_log_example
2/25/24 6:41:54.000 PM	2024-02-25 18:41:54 BLOCK src=72.120.228.230 dst=83.27.58.21 port=53800 protocol=TCP reason=Repeated access attempts detected host = Samuel source = firewall_log_example.txt sourcetype = firewall_log_example

- 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"**

