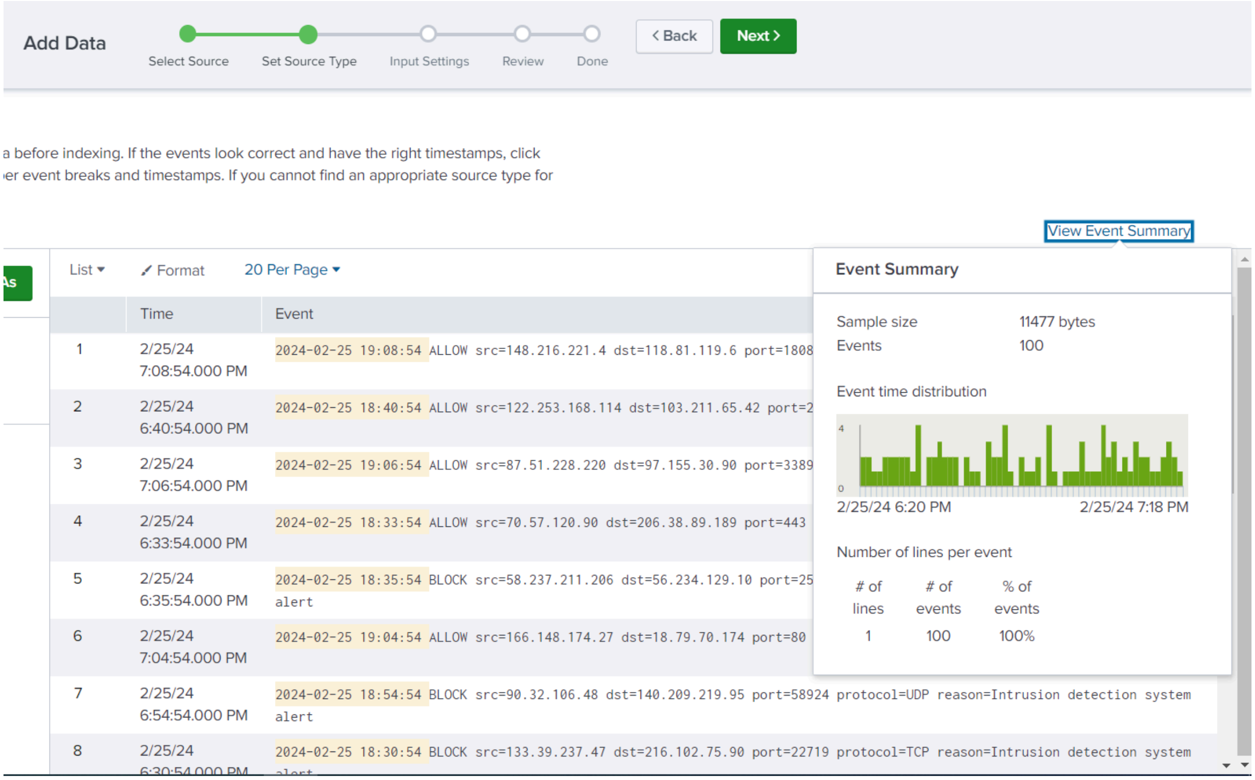
Case Study: Firewall Log Analysis with Splunk

After adding the given log file into splunk we can check the event summary at the start of the paper



a before indexing. If the events look correct and have the right timestamps, click
›er event breaks and timestamps. If you cannot find an appropriate source type for

	Time	Event
1	2/25/24 7:08:54.000 PM	2024-02-25 19:08:54 ALLOW src=148.216.221.4 dst=118.81.119.6 port=1808
2	2/25/24 6:40:54.000 PM	2024-02-25 18:40:54 ALLOW src=122.253.168.114 dst=103.211.65.42 port=2
3	2/25/24 7:06:54.000 PM	2024-02-25 19:06:54 ALLOW src=87.51.228.220 dst=97.155.30.90 port=3389
4	2/25/24 6:33:54.000 PM	2024-02-25 18:33:54 ALLOW src=70.57.120.90 dst=206.38.89.189 port=443
5	2/25/24 6:35:54.000 PM	2024-02-25 18:35:54 BLOCK src=58.237.211.206 dst=56.234.129.10 port=25 alert
6	2/25/24 7:04:54.000 PM	2024-02-25 19:04:54 ALLOW src=166.148.174.27 dst=18.79.70.174 port=80
7	2/25/24 6:54:54.000 PM	2024-02-25 18:54:54 BLOCK src=90.32.106.48 dst=140.209.219.95 port=58924 protocol=UDP 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=216.102.75.90 port=22719 protocol=TCP reason=Intrusion detection system alert

Event Summary

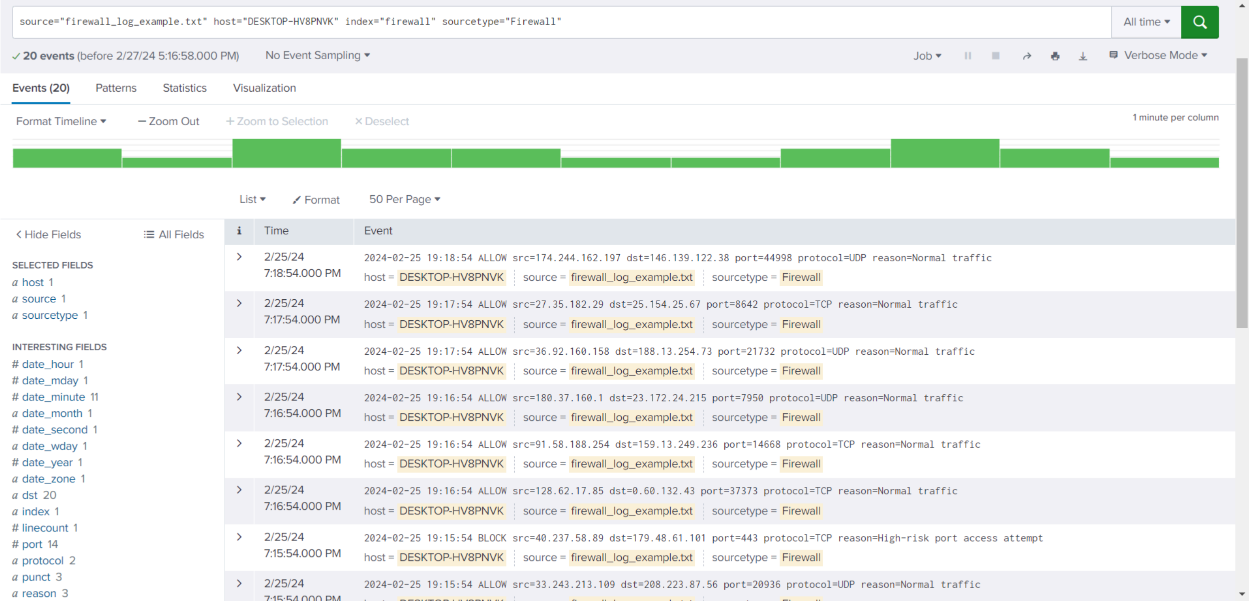
Sample size	11477 bytes
Events	100

Event time distribution

2/25/24 6:20 PM — 2/25/24 7:18 PM

Number of lines per event

# of lines	# of events	% of events
1	100	100%



```
source="firewall_log_example.txt" host="DESKTOP-HV8PNVK" index="firewall" sourcetype="Firewall"
```

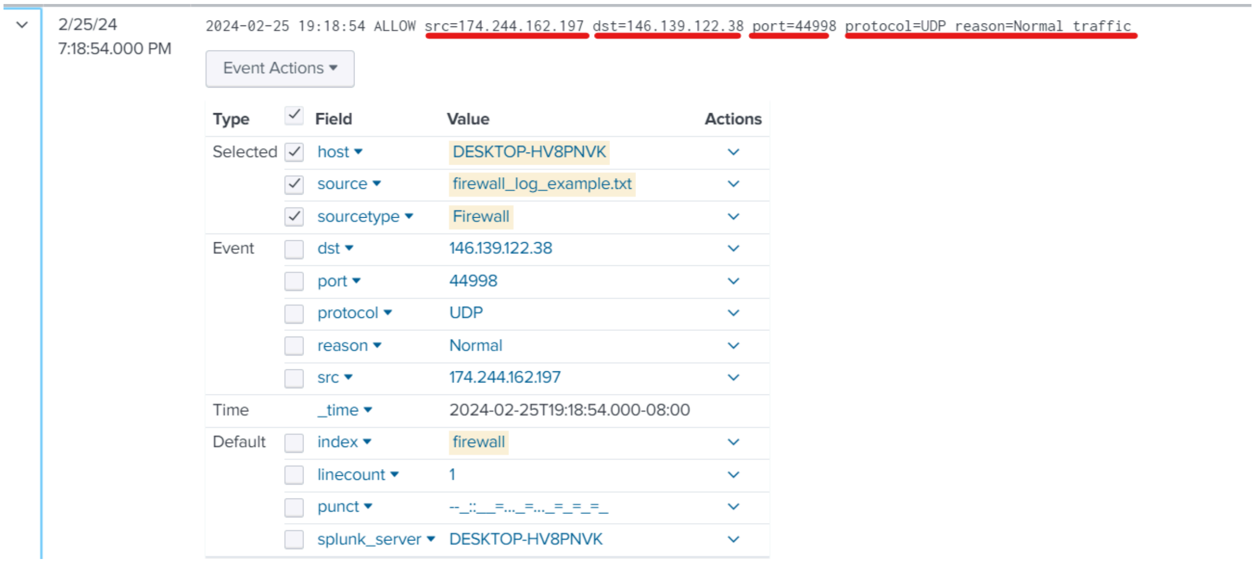
✓ **20 events** (before 2/27/24 5:16:58.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 11
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1
a dst 20
a index 1
# linecount 1
# port 14
a protocol 2
a punct 3
a reason 3

i	Time	Event
>	2/25/24 7:18:54.000 PM	2024-02-25 19:18:54 ALLOW src=174.244.162.197 dst=146.139.122.38 port=44998 protocol=UDP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
>	2/25/24 7:17:54.000 PM	2024-02-25 19:17:54 ALLOW src=27.35.182.29 dst=25.154.25.67 port=8642 protocol=TCP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
>	2/25/24 7:17:54.000 PM	2024-02-25 19:17:54 ALLOW src=36.92.160.158 dst=188.13.254.73 port=21732 protocol=UDP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
>	2/25/24 7:16:54.000 PM	2024-02-25 19:16:54 ALLOW src=180.37.160.1 dst=23.172.24.215 port=7950 protocol=UDP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
>	2/25/24 7:16:54.000 PM	2024-02-25 19:16:54 ALLOW src=91.58.188.254 dst=159.13.249.236 port=14668 protocol=TCP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
>	2/25/24 7:16:54.000 PM	2024-02-25 19:16:54 ALLOW src=128.62.17.85 dst=0.60.132.43 port=37373 protocol=TCP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
>	2/25/24 7:15:54.000 PM	2024-02-25 19:15:54 BLOCK src=40.237.58.89 dst=179.48.61.101 port=443 protocol=TCP reason=High-risk port access attempt host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
>	2/25/24 7:15:54.000 PM	2024-02-25 19:15:54 ALLOW src=33.243.213.109 dst=208.223.87.56 port=20936 protocol=UDP reason=Normal traffic

After carefully viewing the event we can find lot of information like src ip and dst ip, with what protocol being used and timestamp

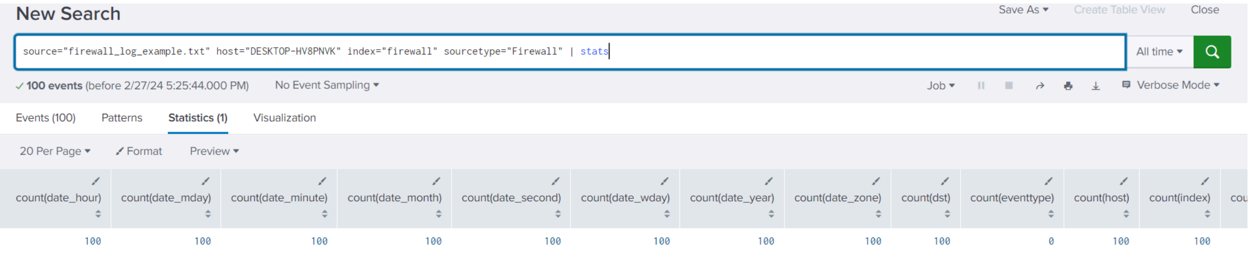


2/25/24
7:18:54.000 PM

```
2024-02-25 19:18:54 ALLOW src=174.244.162.197 dst=146.139.122.38 port=44998 protocol=UDP reason=Normal traffic
```

Type	☑ Field	Value	Actions
Selected	☑ host ▾	DESKTOP-HV8PNVK	⌄
	☑ source ▾	firewall_log_example.txt	⌄
	☑ sourcetype ▾	Firewall	⌄
Event	□ dst ▾	146.139.122.38	⌄
	□ port ▾	44998	⌄
	□ protocol ▾	UDP	⌄
	□ reason ▾	Normal	⌄
	□ src ▾	174.244.162.197	⌄
Time	_time ▾	2024-02-25T19:18:54.000-08:00	
Default	□ index ▾	firewall	⌄
	□ linecount ▾	1	⌄
	□ punct ▾	--_::__=..._=..._=_=_=_	⌄
	□ splunk_server ▾	DESKTOP-HV8PNVK	⌄

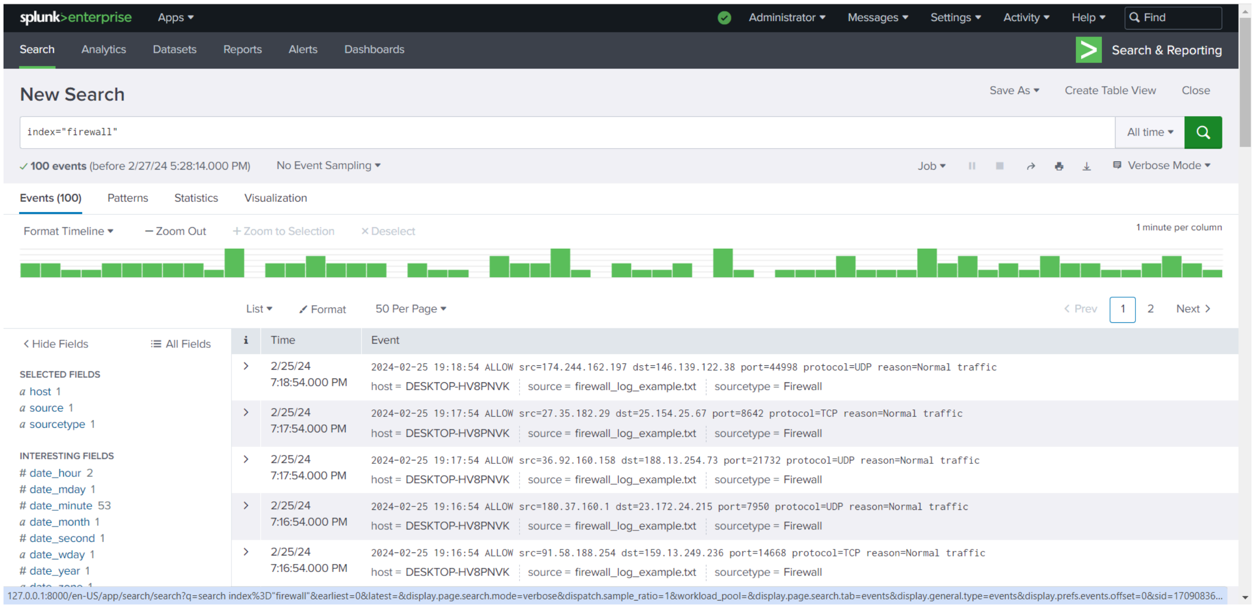
Checking stats of the event stats



```
source="firewall_log_example.txt" host="DESKTOP-HV8PNVK" index="firewall" sourcetype="Firewall" | stats
```

✓ 100 events (before 2/27/24 5:25:44.000 PM)

count(date_hour)	count(date_mday)	count(date_minute)	count(date_month)	count(date_second)	count(date_wday)	count(date_year)	count(date_zone)	count(dst)	count(eventtype)	count(host)	count(index)	cou
100	100	100	100	100	100	100	100	100	0	100	100	



```
index="firewall"
```

✓ 100 events (before 2/27/24 5:28:14.000 PM)

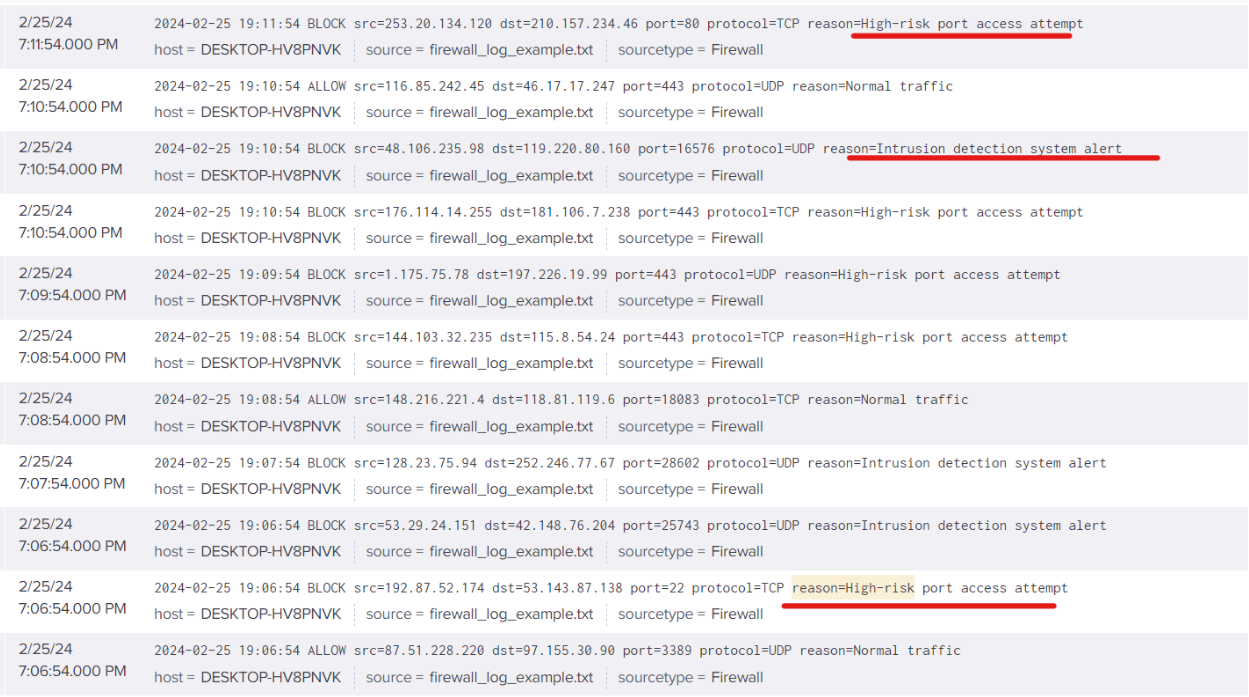
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 53
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1

i	Time	Event
›	2/25/24 7:18:54.000 PM	2024-02-25 19:18:54 ALLOW src=174.244.162.197 dst=146.139.122.38 port=44998 protocol=UDP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
›	2/25/24 7:17:54.000 PM	2024-02-25 19:17:54 ALLOW src=27.35.182.29 dst=25.154.25.67 port=8642 protocol=TCP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
›	2/25/24 7:17:54.000 PM	2024-02-25 19:17:54 ALLOW src=36.92.160.158 dst=188.13.254.73 port=21732 protocol=UDP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
›	2/25/24 7:16:54.000 PM	2024-02-25 19:16:54 ALLOW src=180.37.160.1 dst=23.172.24.215 port=7950 protocol=UDP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall
›	2/25/24 7:16:54.000 PM	2024-02-25 19:16:54 ALLOW src=91.58.188.254 dst=159.13.249.236 port=14668 protocol=TCP reason=Normal traffic host = DESKTOP-HV8PNVK source = firewall_log_example.txt sourcetype = Firewall

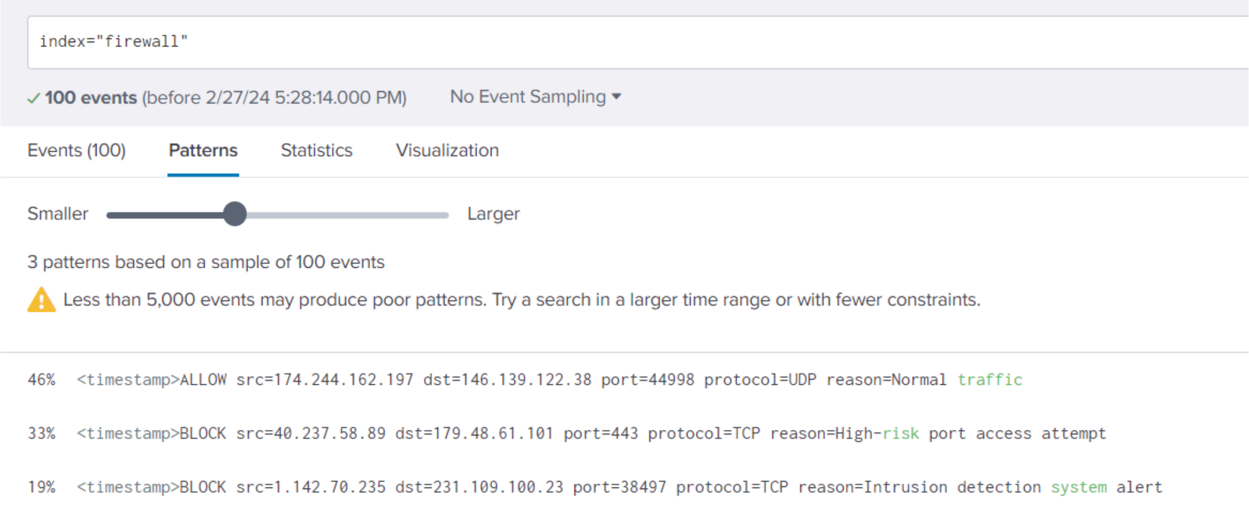
127.0.0.1:8000/en-US/app/search/search?q=search index%3D"firewall"&earliest=0&latest=&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&display.page.search.tab=events&display.general.type=events&display.prefs.events.offset=0&sid=17090836...

We can analyse the events with the reasons and identify what type of traffic is present



```
2/25/24            2024-02-25 19:11:54 BLOCK src=253.20.134.120 dst=210.157.234.46 port=80 protocol=TCP reason=High-risk port access attempt
7:11:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:10:54 ALLOW src=116.85.242.45 dst=46.17.17.247 port=443 protocol=UDP reason=Normal traffic
7:10:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:10:54 BLOCK src=48.106.235.98 dst=119.220.80.160 port=16576 protocol=UDP reason=Intrusion detection system alert
7:10:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:10:54 BLOCK src=176.114.14.255 dst=181.106.7.238 port=443 protocol=TCP reason=High-risk port access attempt
7:10:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:09:54 BLOCK src=1.175.75.78 dst=197.226.19.99 port=443 protocol=UDP reason=High-risk port access attempt
7:09:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:08:54 BLOCK src=144.103.32.235 dst=115.8.54.24 port=443 protocol=TCP reason=High-risk port access attempt
7:08:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:08:54 ALLOW src=148.216.221.4 dst=118.81.119.6 port=18083 protocol=TCP reason=Normal traffic
7:08:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:07:54 BLOCK src=128.23.75.94 dst=252.246.77.67 port=28602 protocol=UDP reason=Intrusion detection system alert
7:07:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:06:54 BLOCK src=53.29.24.151 dst=42.148.76.204 port=25743 protocol=UDP reason=Intrusion detection system alert
7:06:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:06:54 BLOCK src=192.87.52.174 dst=53.143.87.138 port=22 protocol=TCP reason=High-risk port access attempt
7:06:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall

2/25/24            2024-02-25 19:06:54 ALLOW src=87.51.228.220 dst=97.155.30.90 port=3389 protocol=UDP reason=Normal traffic
7:06:54.000 PM     host = DESKTOP-HV8PNVK | source = firewall_log_example.txt | sourcetype = Firewall
```

Here is the pattern



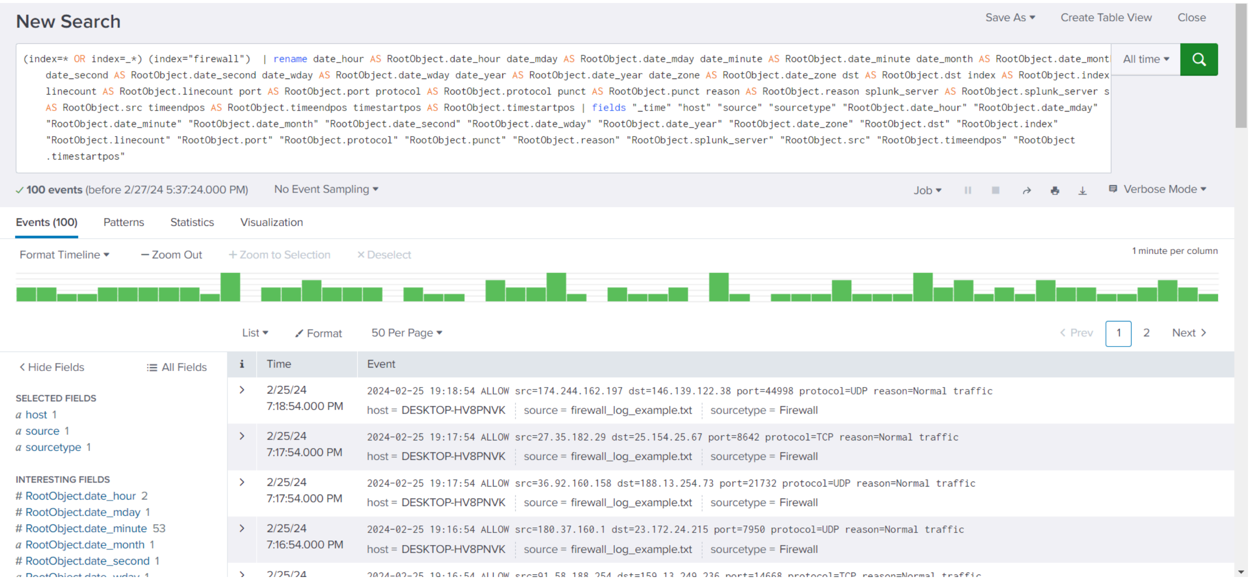
```
index="firewall"
```

✓ **100 events** (before 2/27/24 5:28:14.000 PM)

3 patterns based on a sample of 100 events

⚠ Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.

```
46%  <timestamp>ALLOW src=174.244.162.197 dst=146.139.122.38 port=44998 protocol=UDP reason=Normal traffic

33%  <timestamp>BLOCK src=40.237.58.89 dst=179.48.61.101 port=443 protocol=TCP reason=High-risk port access attempt

19%  <timestamp>BLOCK src=1.142.70.235 dst=231.109.100.23 port=38497 protocol=TCP reason=Intrusion detection system alert
```



```
(index=* OR index=_*) (index="firewall")  | rename date_hour AS RootObject.date_hour date_mday AS RootObject.date_mday date_minute AS RootObject.date_minute date_month AS RootObject.date_mont
    date_second AS RootObject.date_second date_wday AS RootObject.date_wday date_year AS RootObject.date_year date_zone AS RootObject.date_zone dst AS RootObject.dst index AS RootObject.index
    linecount AS RootObject.linecount port AS RootObject.port protocol AS RootObject.protocol punct AS RootObject.punct reason AS RootObject.reason splunk_server AS RootObject.splunk_server s
    AS RootObject.src timeendpos AS RootObject.timeendpos timestartpos AS RootObject.timestartpos | fields "_time" "host" "source" "sourcetype" "RootObject.date_hour" "RootObject.date_mday"
    "RootObject.date_minute" "RootObject.date_month" "RootObject.date_second" "RootObject.date_wday" "RootObject.date_year" "RootObject.date_zone" "RootObject.dst" "RootObject.index"
    "RootObject.linecount" "RootObject.port" "RootObject.protocol" "RootObject.punct" "RootObject.reason" "RootObject.splunk_server" "RootObject.src" "RootObject.timeendpos" "RootObject
    .timestartpos"
```

```
> 2/25/24 7:18:54.000 PM
2024-02-25 19:18:54 ALLOW src=174.244.162.197 dst=146.139.122.38 port=44998 protocol=UDP reason=Normal traffic
host = DESKTOP-HV8PNVK   source = firewall_log_example.txt   sourcetype = Firewall

> 2/25/24 7:17:54.000 PM
2024-02-25 19:17:54 ALLOW src=27.35.182.29 dst=25.154.25.67 port=8642 protocol=TCP reason=Normal traffic
host = DESKTOP-HV8PNVK   source = firewall_log_example.txt   sourcetype = Firewall

> 2/25/24 7:17:54.000 PM
2024-02-25 19:17:54 ALLOW src=36.92.160.158 dst=188.13.254.73 port=21732 protocol=UDP reason=Normal traffic
host = DESKTOP-HV8PNVK   source = firewall_log_example.txt   sourcetype = Firewall

> 2/25/24 7:16:54.000 PM
2024-02-25 19:16:54 ALLOW src=180.37.160.1 dst=23.172.24.215 port=7950 protocol=UDP reason=Normal traffic
host = DESKTOP-HV8PNVK   source = firewall_log_example.txt   sourcetype = Firewall

> 2/25/24
2024-02-25 19:16:54 ALLOW src=91.58.188.254 dst=159.13.249.236 port=14668 protocol=TCP reason=Normal traffic
```

What I learn from the assignment is that the assignment include the importance of understanding log data and proficiency in Splunk for effective analysis. Initial analysis aids in grasping traffic patterns, while identifying security threats requires recognizing patterns like repeated access attempts and high-volume traffic to risky ports. Advanced search capabilities and correlation techniques are vital for in-depth analysis. Reporting findings with specific examples and proposing actionable recommendations, such as adjusting firewall rules, are crucial for improving network security.