Prepared by: Pelin Gülmez

Date: 16June 2025

# SIEM Project – Week 2 Report

## Table of Contents

## 1. Overview

This report summarizes the work done during Week 2 of the SIEM project. The main focus areas were:

- Log parsing techniques for SNORT and UFW logs using Elastic Stack 8.13.4.
- Creating visual dashboards for security monitoring.
- Parsing SNORT alerts and UFW firewall activity logs.

All tasks were performed on an Elastic Stack 8.13.4 instance with Filebeat configurations for IDS (SNORT) and Firewall (UFW) log sources.

## 2. Deliverable 1: Log Parsing Rules

### SNORT Log Parsing

Log Source: /var/log/snort/alert

Ingest Pipeline: parse-snort-pipeline

### Extracted Fields:

| Field | Description |
|---|---|
| alert_msg | SNORT alert message |
| priority | Alert priority level |
| gid | Generator ID |
| sid | Signature ID |
| rev | Rule revision |
| src_ip | Source IP address |
| dest_ip | Destination IP address |
| proto | Protocol (TCP/UDP/ICMP etc.) |
| time/month/day | Timestamp components |

### UFW Log Parsing

Log Source: /var/log/ufw.log

Ingest Pipeline: parse-ufw-pipeline

### Extracted Fields:

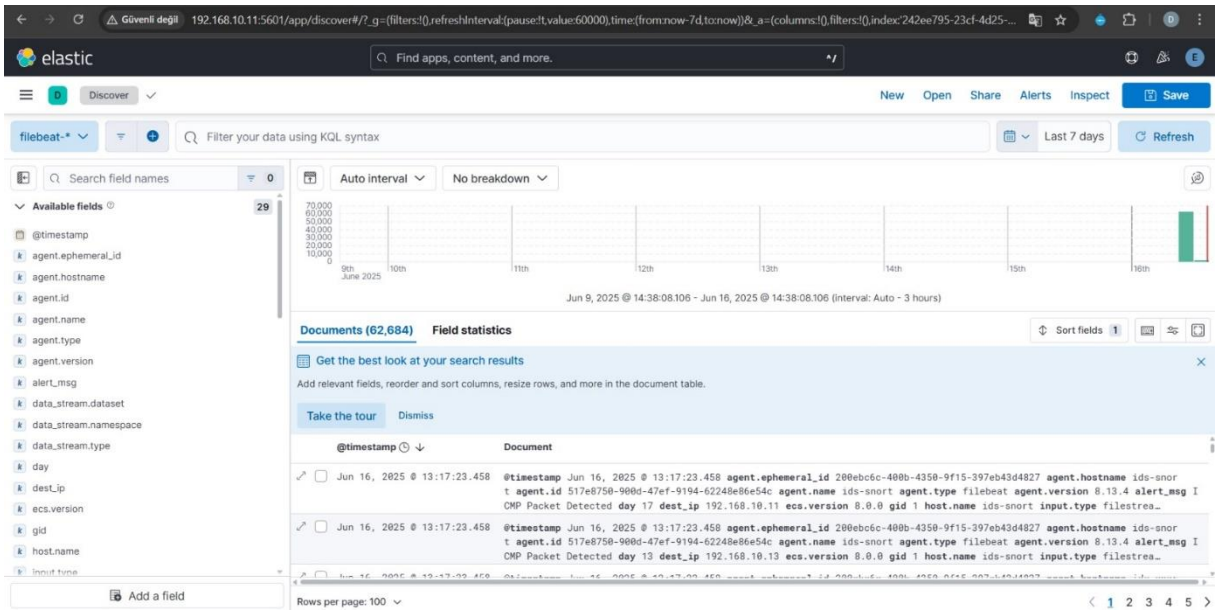
| Field | Description |
|---|---|
| src_ip | Source IP address |
| dest_ip | Destination IP address |
| proto | Protocol |
| src_port | Source port |
| dest_port | Destination port |
| action | ALLOW/DENY |
| length, ttl | Packet metrics |

## Tools Used:

- Grok Patterns
- Ingest Pipelines (via Kibana > Stack Management)

## 3. Deliverable 2: Dashboarding

A unified Kibana dashboard was created to visualize SNORT alert messages and firewall activities from UFW.

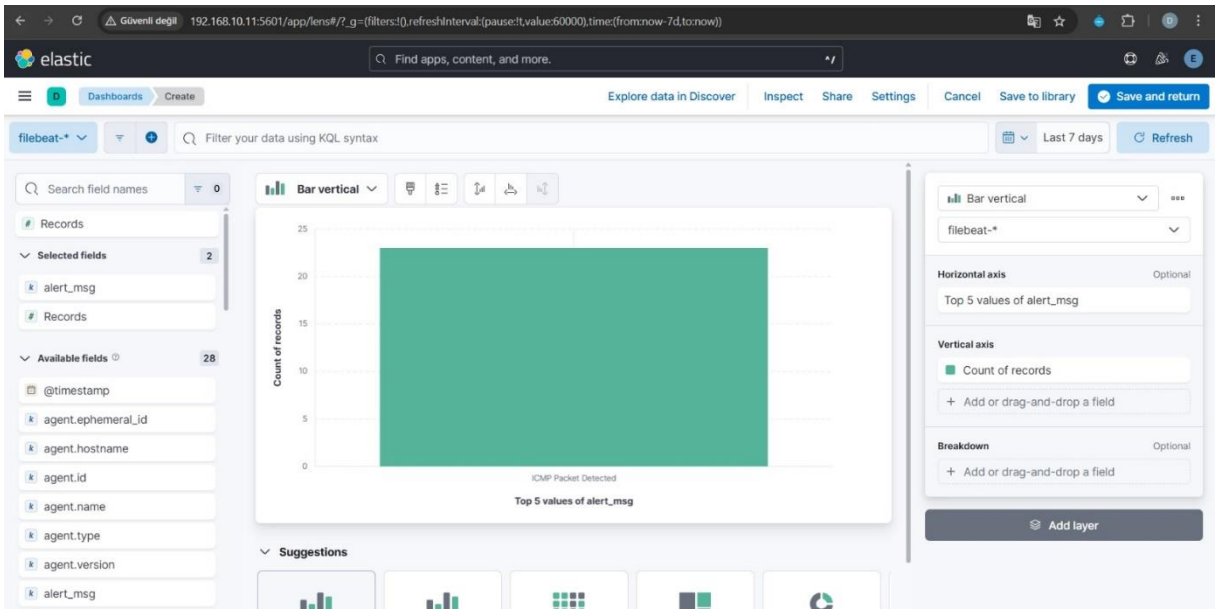


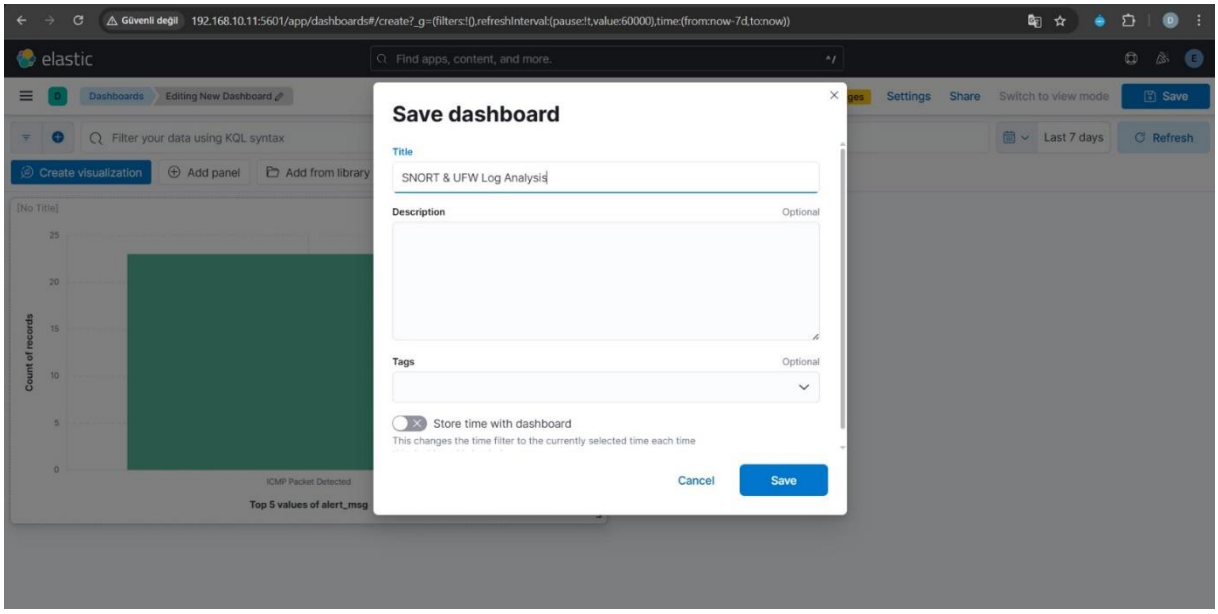
Visualizations:

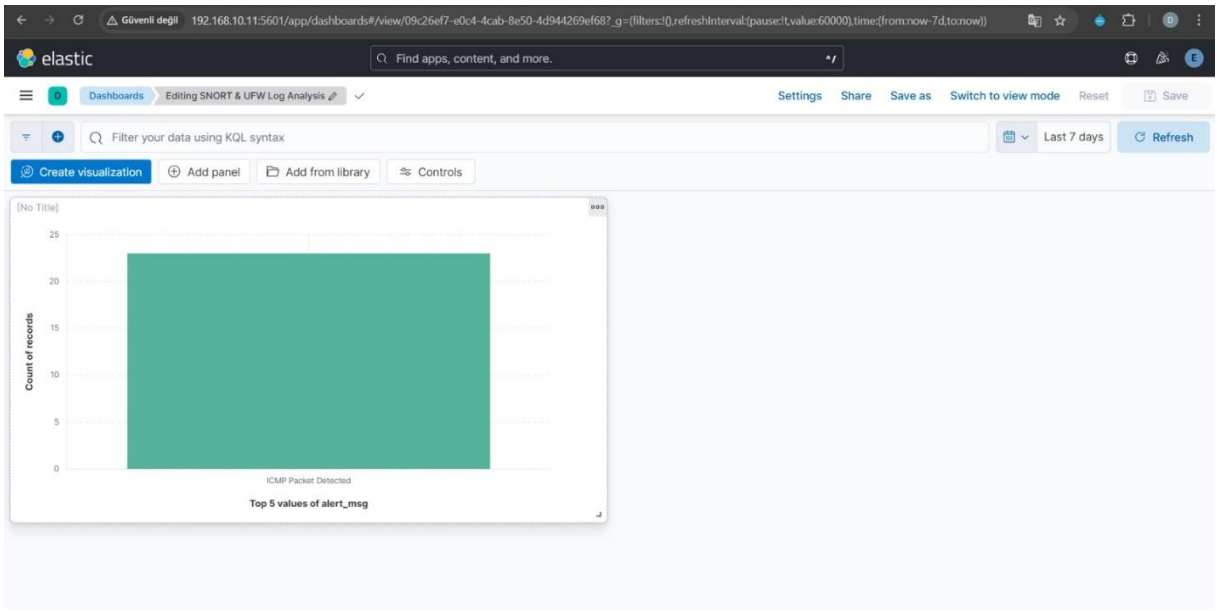
## 1. Top SNORT Alert Messages

Type: Pie Chart

Field: alert_msg



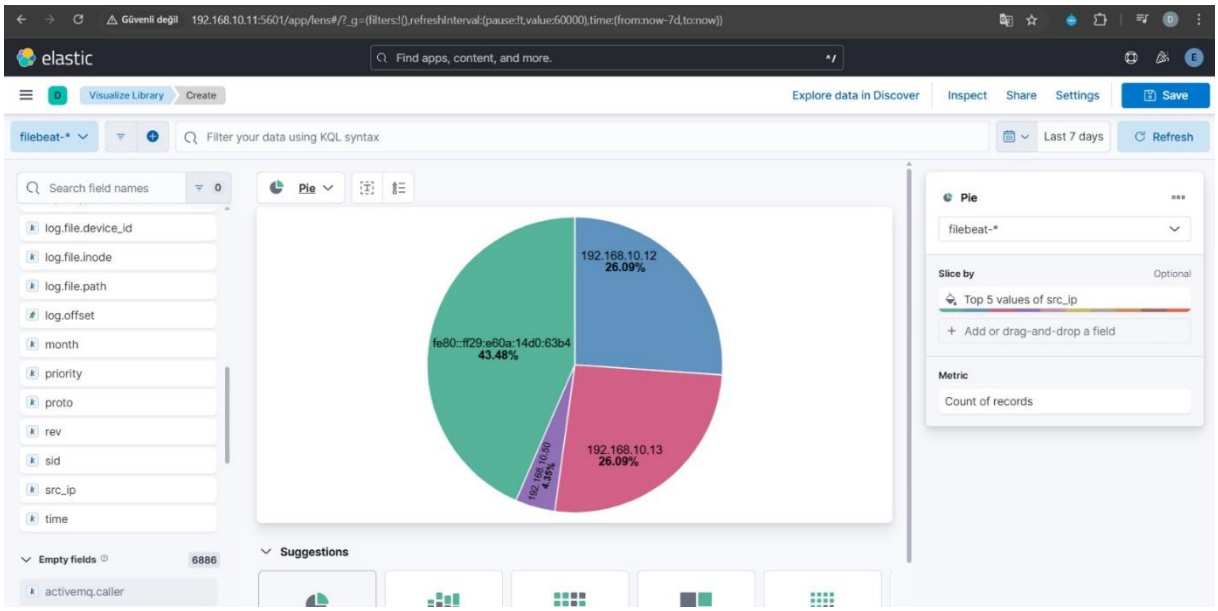



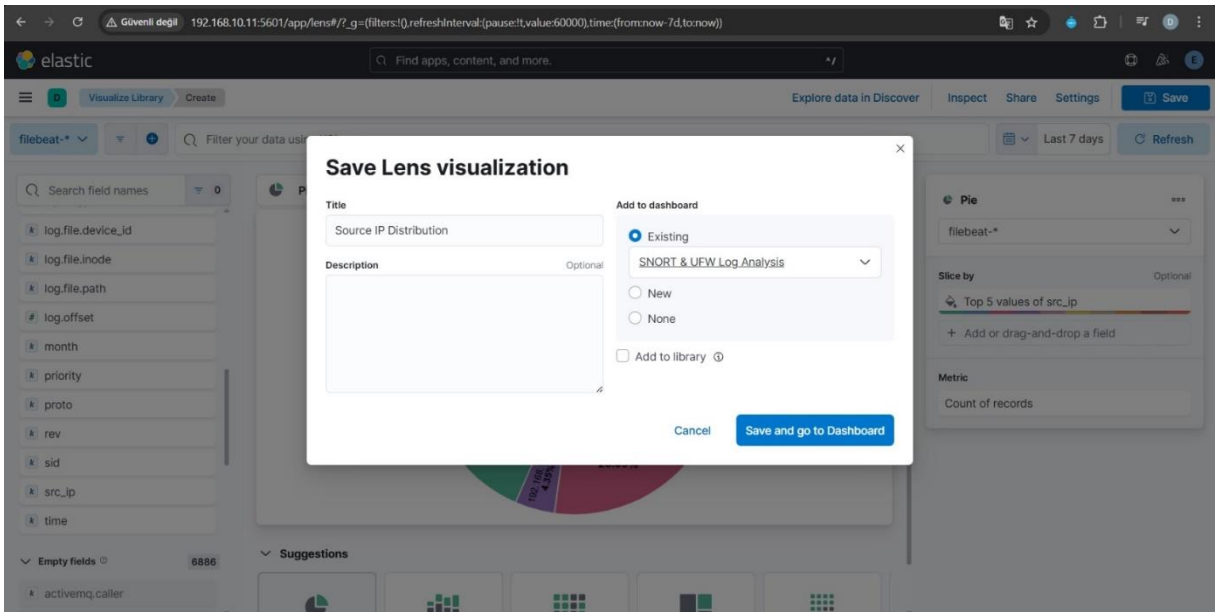


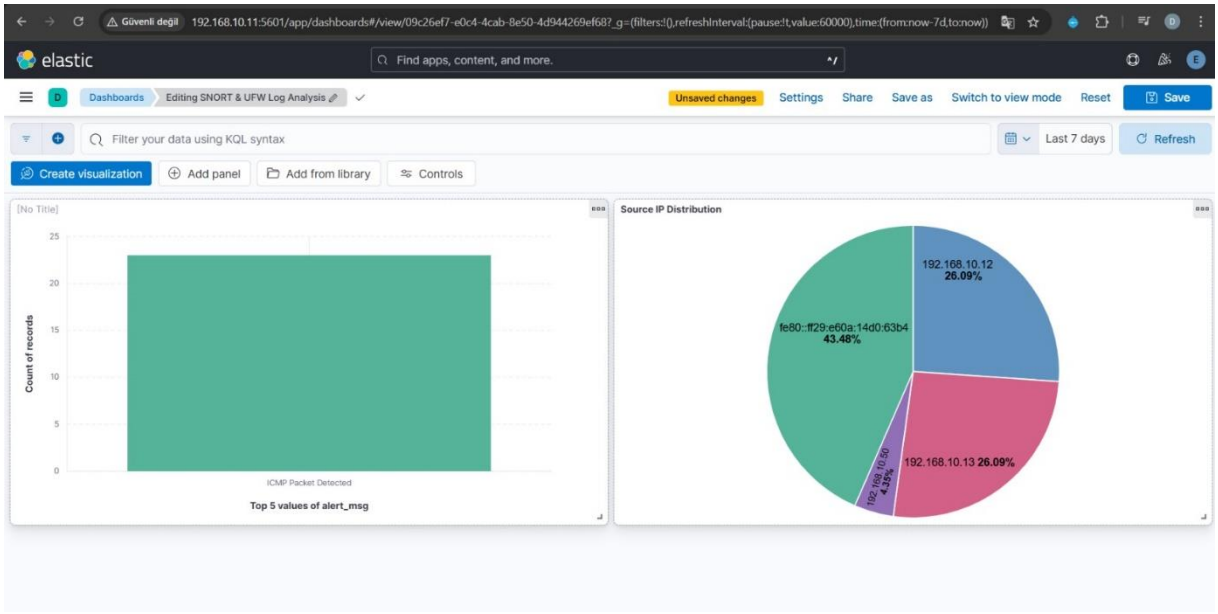

## 2. Source IP Distribution

Type: Pie Chart

Field: src_ip



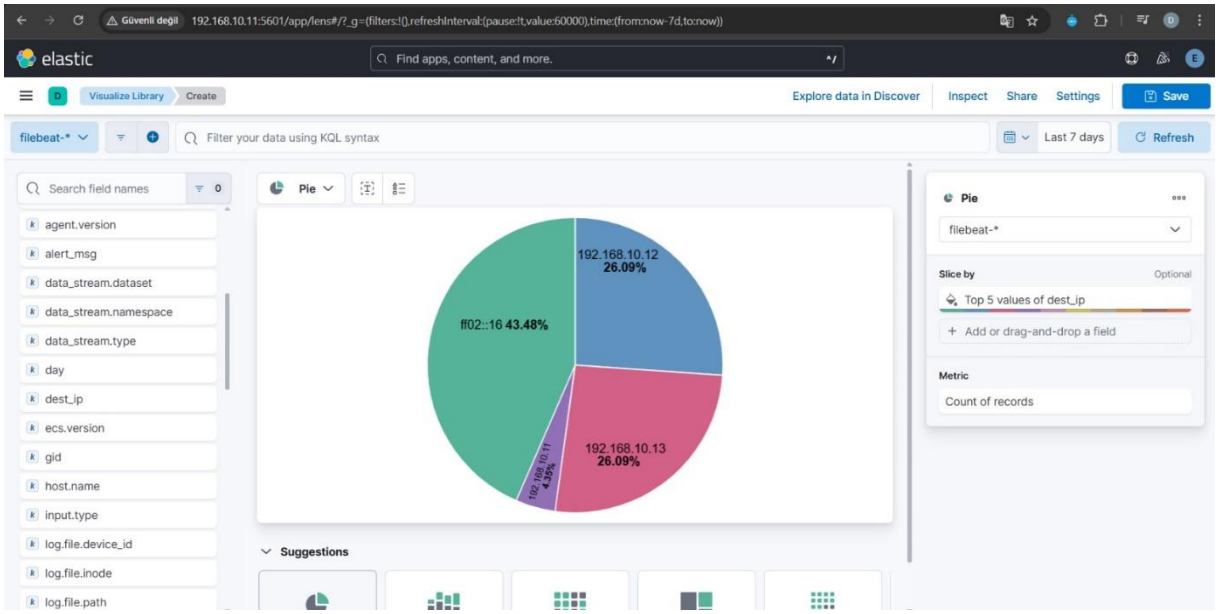

Güvenli değil
192.168.10.11:5601/app/lens#/?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-7d,to:now))
elastic
Find apps, content, and more.
Visualize Library
Create
Explore data in Discover
Inspect
Share
Settings
Save
filebeat-*
Filter your data using KQL syntax
Last 7 days
Refresh
Search field names
log.file.device_id
log.file.inode
log.file.path
log.offset
month
priority
proto
rev
sid
src_ip
time
Empty fields
6886
activemq.caller
Suggestions
Save Lens visualization
Title
Source IP Distribution
Description
Optional
Add to dashboard
Existing
SNORT & UFW Log Analysis
New
None
Add to library
Cancel
Save and go to Dashboard
Pie
filebeat-*
Slice by
Optional
Top 5 values of src_ip
Add or drag-and-drop a field
Metric
Count of records

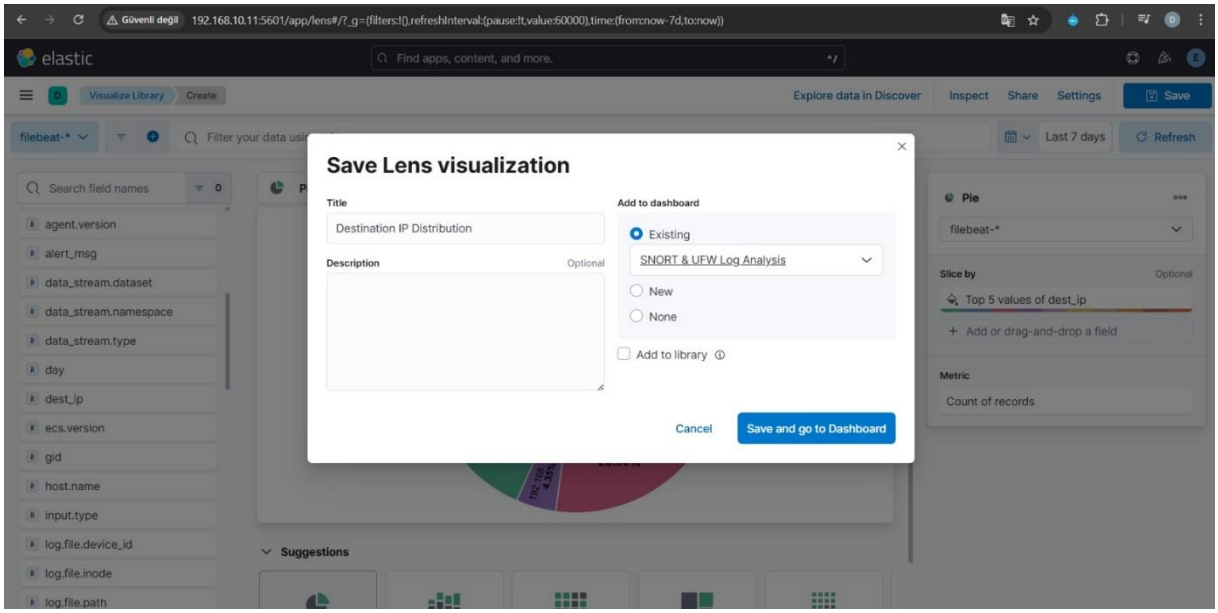

Güvenli değil
192.168.10.11:5601/app/dashboards#/view/09c26ef7-e0c4-4cab-8e50-4d944269ef68?_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:(from:now-7d,to:now))
elastic
Find apps, content, and more.
Dashboards
Editing SNORT & UFW Log Analysis
Unsaved changes
Settings
Share
Save as
Switch to view mode
Reset
Save
Filter your data using KQL syntax
Last 7 days
Refresh
Create visualization
Add panel
Add from library
Controls
[No Title]
Count of records
ICMP Packet Detected
Top 5 values of alert_msg
Source IP Distribution
192.168.10.12
26.09%
fe80::ff29:e60a:14d0:63b4
43.48%
192.168.10.13 26.09%

## 3. Destination IP Distribution

Type: Pie Chart

Field: dest_ip

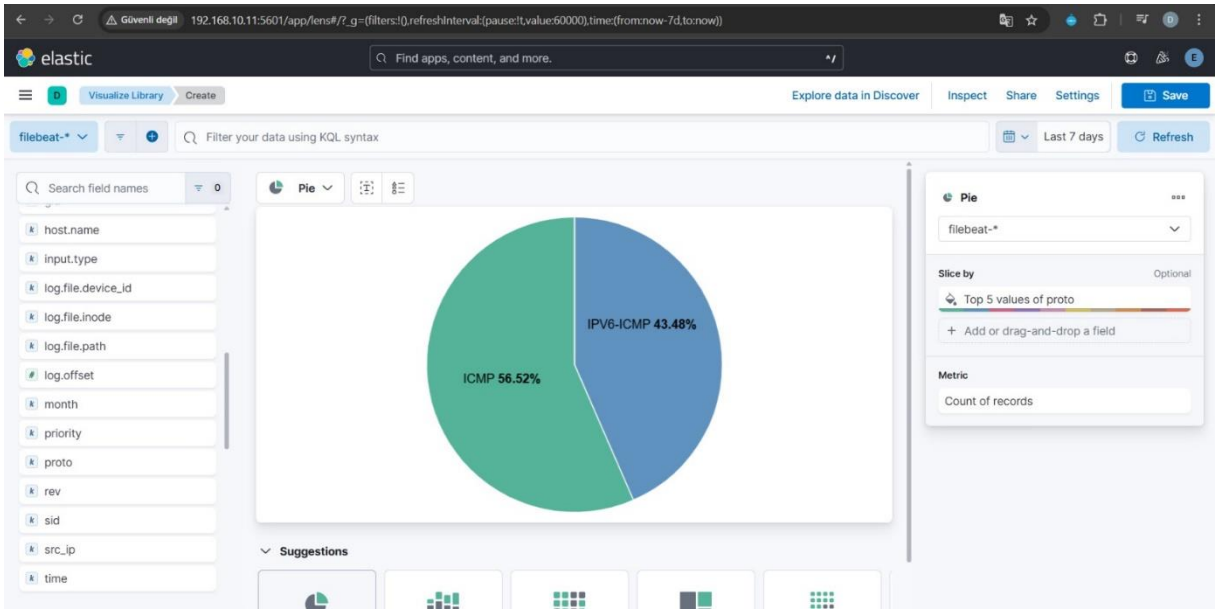


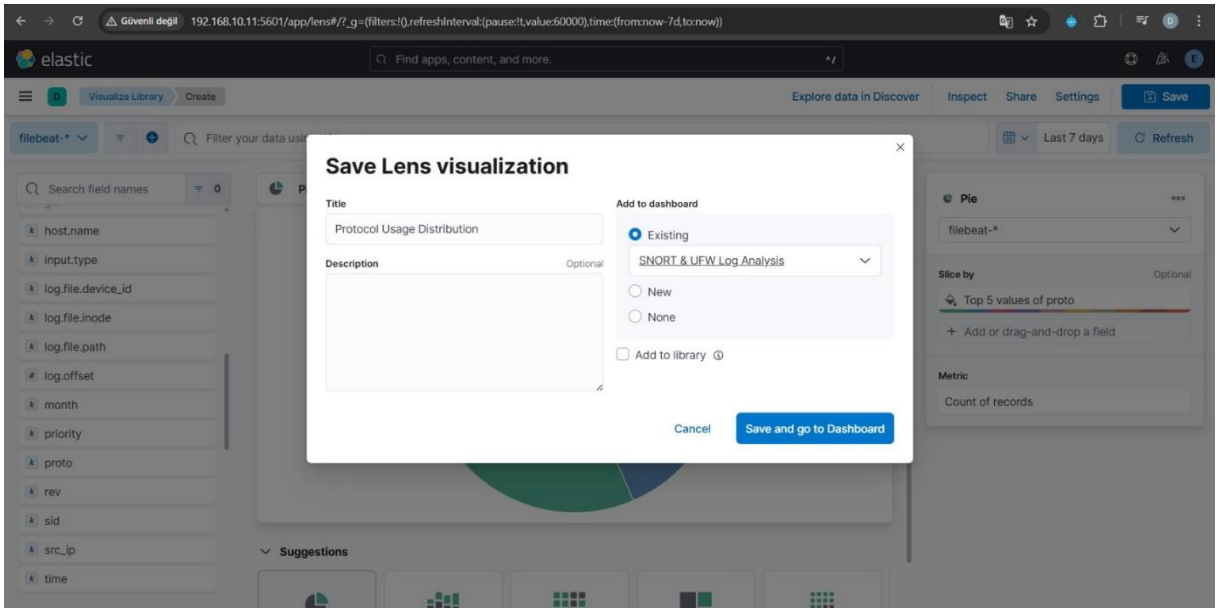



## 4. Protocol Usage Distribution

Type: Pie Chart

Field: proto

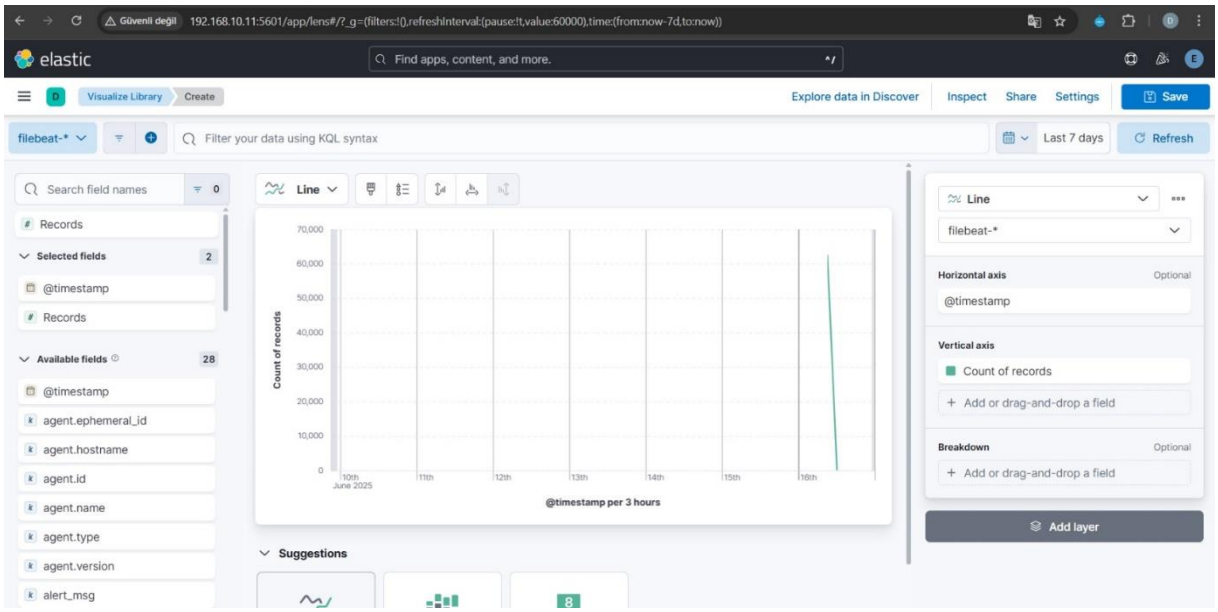


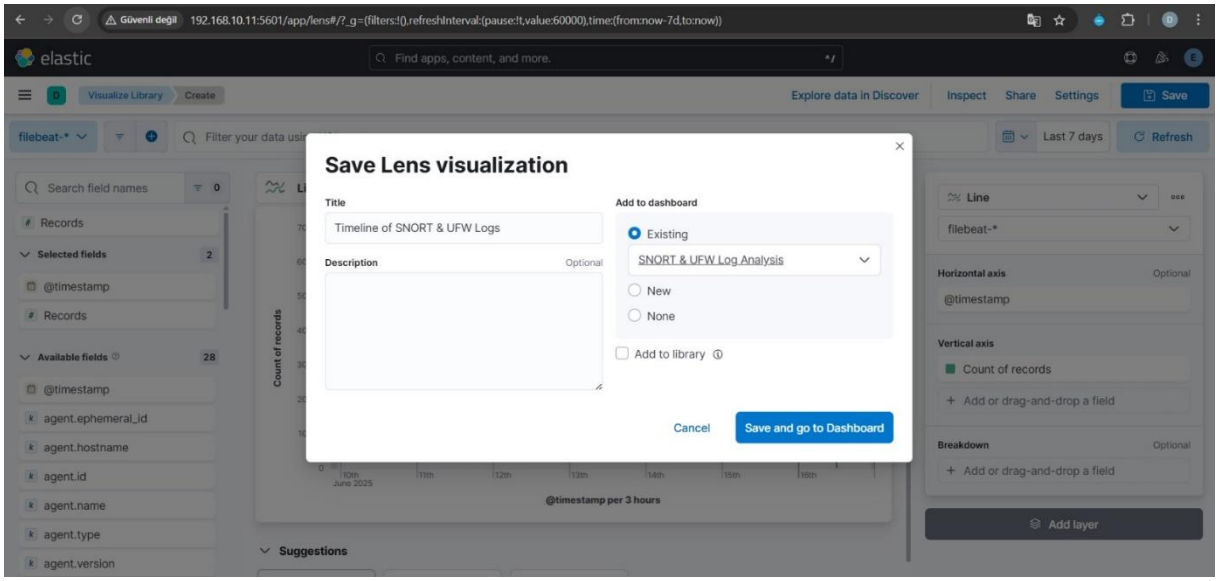



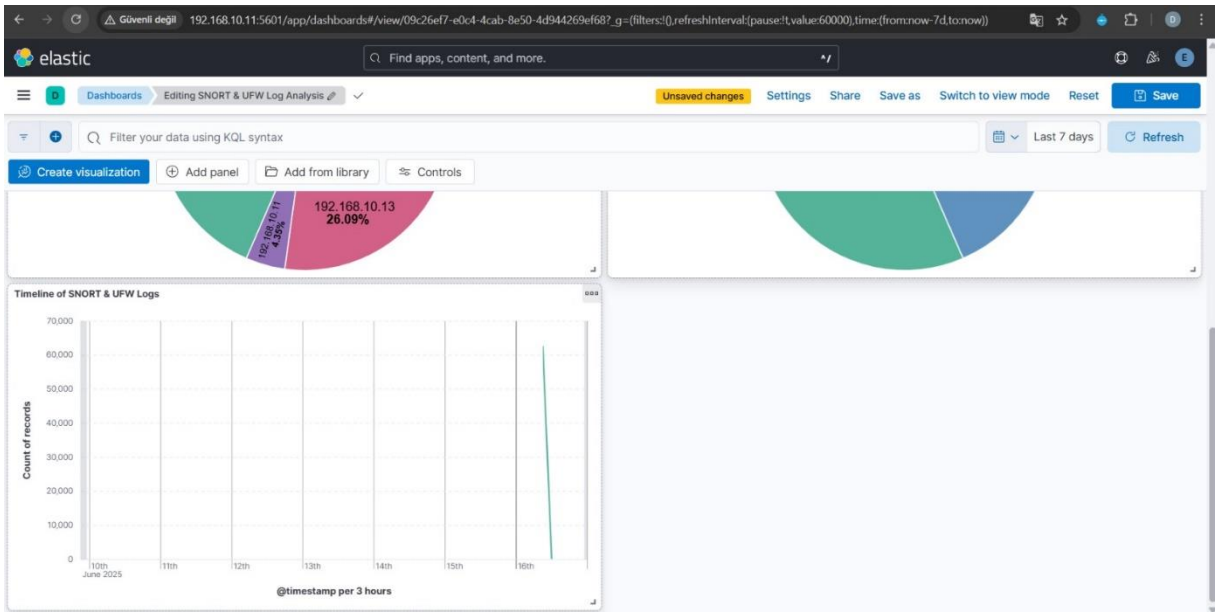
## 5. Security Events Timeline

Type: Line Chart

Field: @timestamp






## 4. Dashboard Summary Table

| Visualization | Source | Key Field | Description |
|---|---|---|---|
| Top SNORT Alerts | SNORT | alert_msg | Most triggered alert messages |
| Source IP Distribution | UFW | src_ip | Frequent source IPs |
| Destination IPs | Both | dest_ip | Targets of activity |
| Protocol Types | Both | proto | Protocol distribution |
| UFW Port Access | UFW | dest_port | Targeted ports |
| UFW Action | UFW | action | ALLOW vs DENY visualization |
| SNORT Timeline | SNORT | @timestamp | Alerts over time |
| UFW Timeline | UFW | @timestamp | UFW events over time |

## 5. Tools and Environment

| Component | Version / Info |
|---|---|
| Elastic Stack | 8.13.4 |
| Elasticsearch | 192.168.10.11:9200 |
| Kibana | 192.168.10.11:5601 |
| Filebeat | ids-snort, ufw-logger |
| Ingest Pipelines | Custom |
| Snort IDS | 2.9.20 |
| UFW Firewall | Default on Ubuntu |
| Parsing Tools | Grok Patterns |
| Data Visualization | Kibana Visualizations & Dashboards |

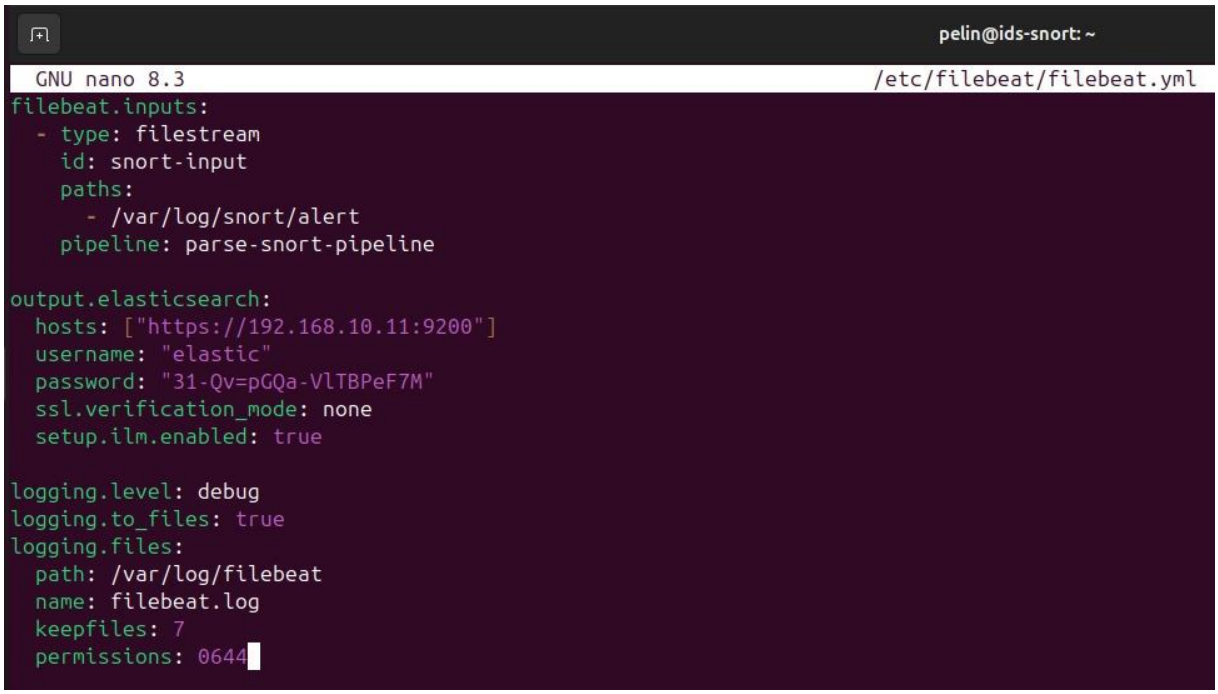
## 6. Conclusion

In this phase of the project, log parsing rules for both SNORT and UFW log sources were successfully developed and implemented through Filebeat ingest pipelines. The parsed logs were effectively visualized via customized Kibana dashboards, providing clear insights into key metrics such as top alerts, accessed ports, protocol distributions, and attack timelines. This foundation establishes a robust and scalable SIEM monitoring framework. In the future, the system can be flexibly enhanced.

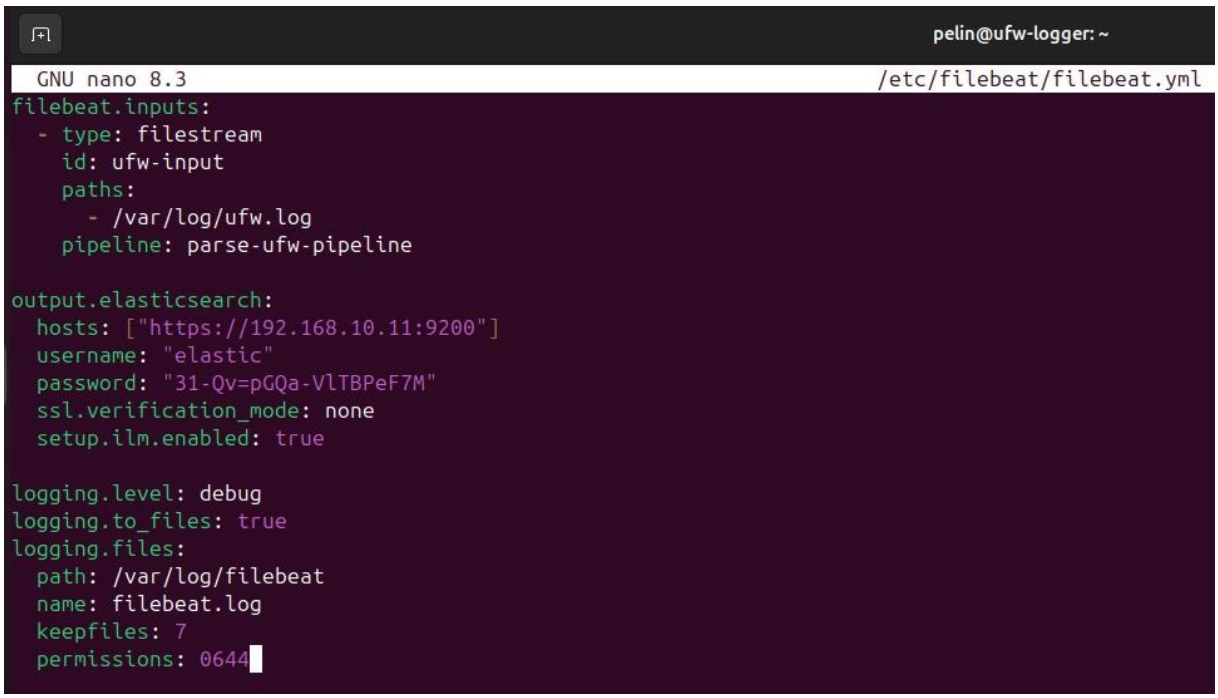
## 7. Attachments

**Configuration Files:**

Filebeat configuration from SNORT machine

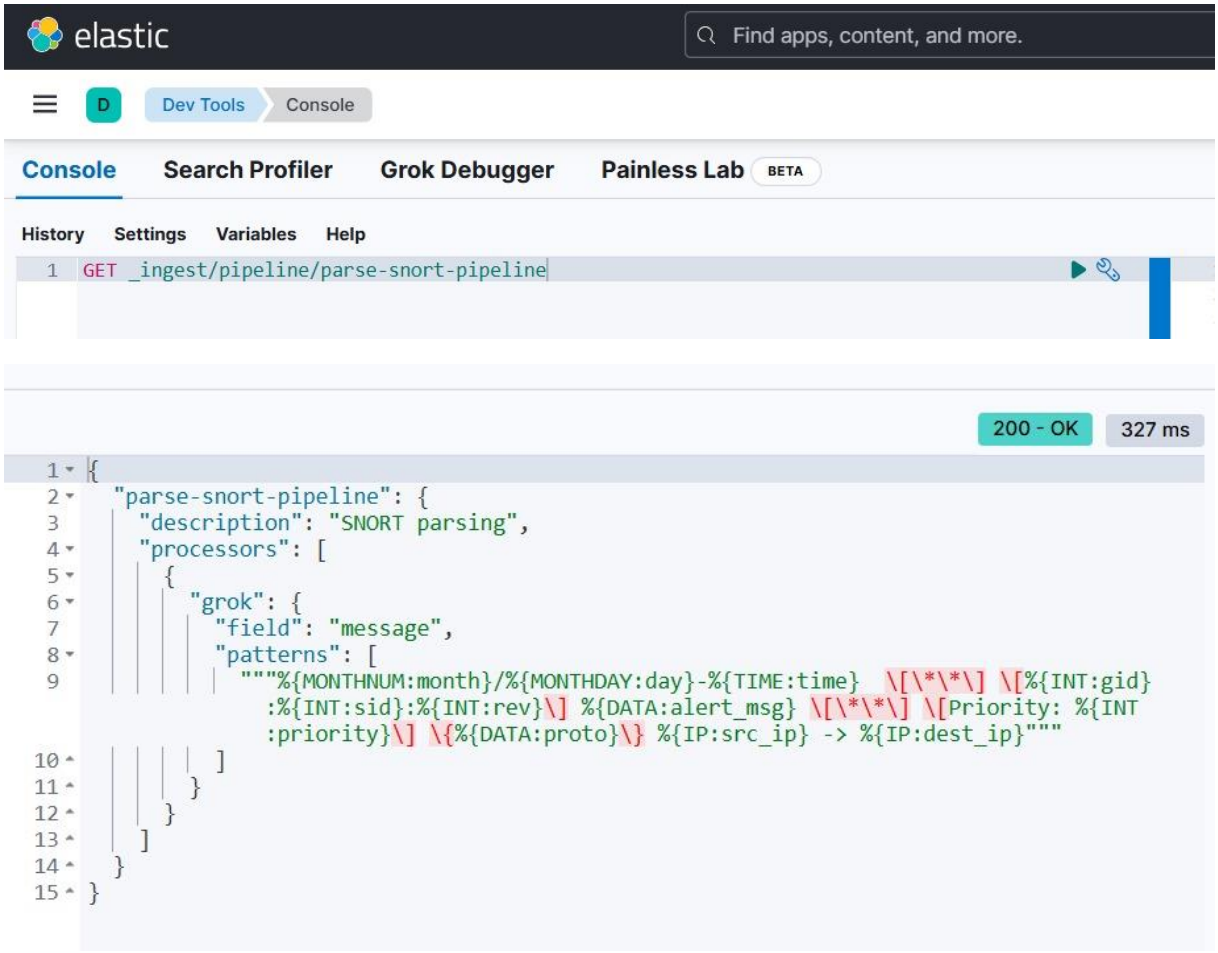



Filebeat configuration from UFW machine

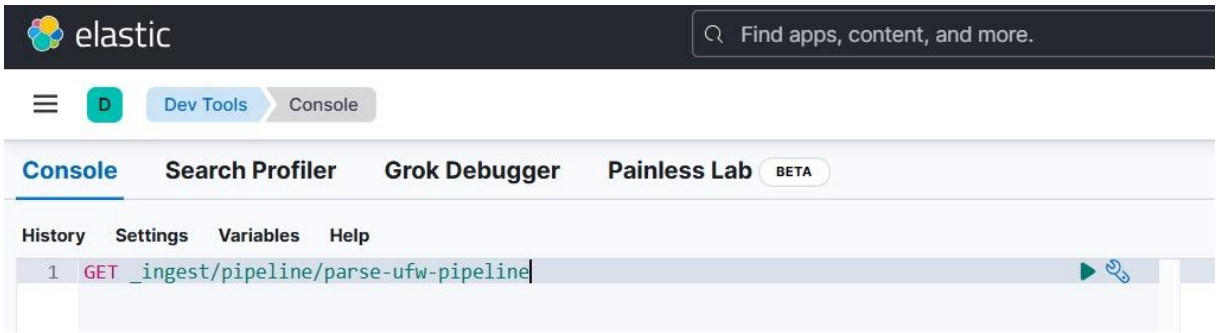


**Ingest Pipelines**

parse-snort-pipel ine JSON export




parse-ufw-pipeline JSON export

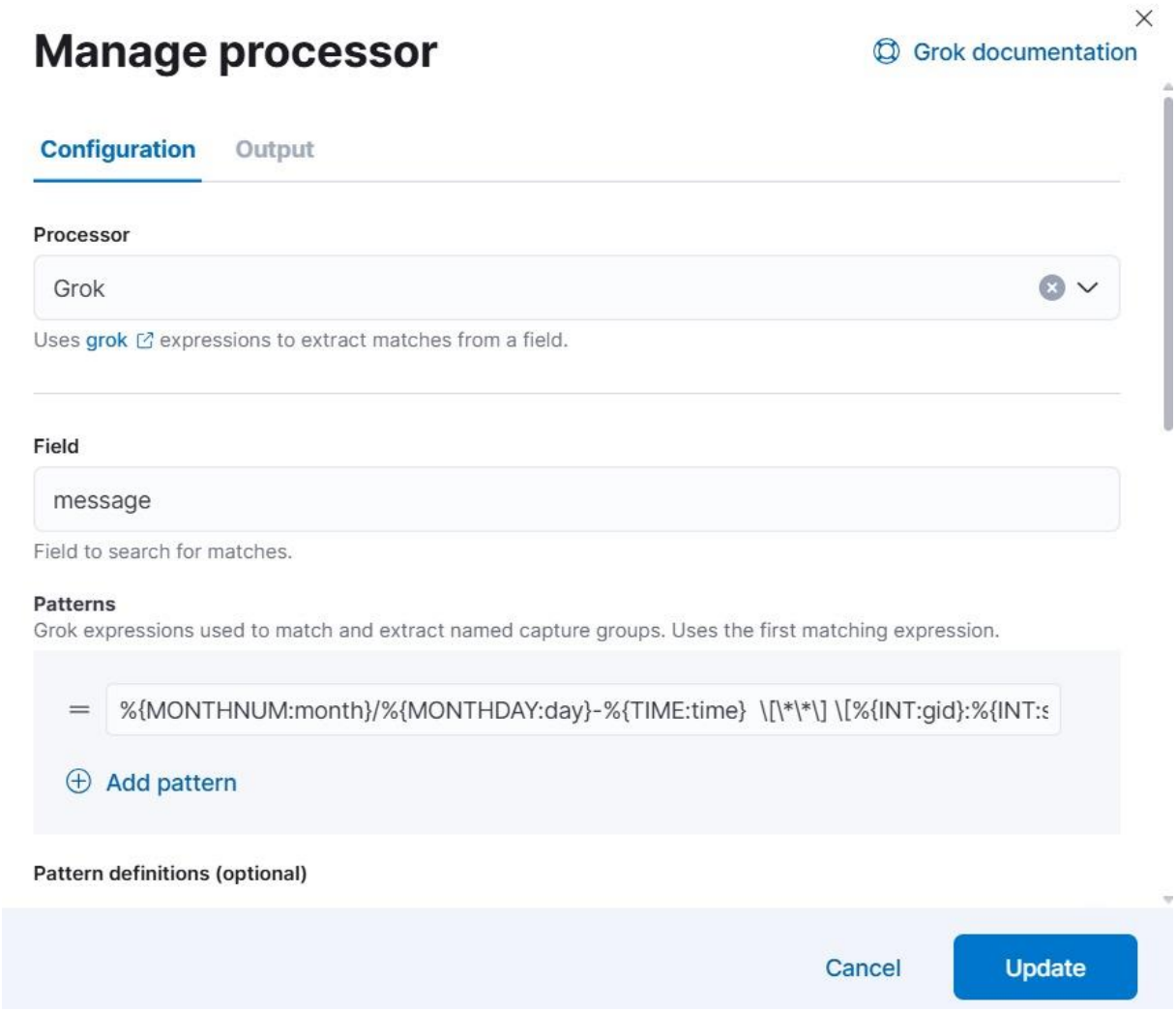


200 - OK 168 ms

```
{
  "parse-ufw-pipeline": {
    "description": "UFW parsing",
    "processors": [
      {
        "grok": {
          "field": "message",
          "patterns": [
            """<%{INT:priority}>%{MONTH} %{MONTHDAY} %{TIME} %{HOSTNAME:hostname}
               kernel: \[UFW %{WORD:action}\] IN=%{WORD:in_interface} OUT=%{WORD
               :out_interface} SRC=%{IP:src_ip} DST=%{IP:dest_ip} PROTO=%{WORD:proto}
               SPT=%{INT:src_port} DPT=%{INT:dest_port}"""
          ]
        }
      }
    ]
  }
}
```

**Parsing Patterns**

parse-snort-pipeline



parse-ufw-pipeline