

# **Zeek + Filebeat + Elasticsearch (ELK) Deployment Report**

---

## **1. Introduction (Purpose of the Project)**

The objective of this project is to deploy a complete network monitoring and SIEM pipeline using **Zeek, Filebeat, Elasticsearch, and Kibana**.

This setup is designed specifically for **Security Operations Center (SOC)** use cases such as:

- Network traffic monitoring
- Suspicious activity detection
- Log analysis and investigation
- Centralized visibility of network events

This project simulates a **real-world SOC environment**, where logs are continuously collected, processed, stored, and visualized for effective security analysis and incident investigation.

---

## **2. Why We Use Only These Software (SOC Perspective)**

### **2.1 Why Zeek**

Zeek is a **Network Security Monitor**, not just a packet sniffer.

Key reasons for using Zeek:

- Converts raw network traffic into structured security logs
- Produces human-readable logs such as:
  - conn.log – connection metadata
  - dns.log – DNS activity
  - http.log – HTTP request details

SOC analysts work with **events**, not raw packets, making Zeek ideal for SOC environments.

### **2.2 Why Not Wireshark**

- Wireshark is packet-based and requires manual analysis
  - Not suitable for continuous, large-scale SOC monitoring
  - No centralized log management
- 

### **2.3 Why Filebeat**

Filebeat is used for **secure and reliable log shipping**.

Advantages:

- Automatically reads Zeek log files
- Handles log rotation efficiently
- Prevents data loss
- Provides a built-in Zeek module
- Industry-standard log shipper for SOC environments

### **2.4 Why Not Custom Scripts**

- Custom scripts may crash or fail silently
  - No retry or fault-tolerance mechanism
  - Not considered SOC-standard or enterprise-ready
- 

## 2.5 Why Elasticsearch

Elasticsearch acts as the **SIEM data storage and search engine**.

Benefits:

- Stores massive volumes of security logs
- High-speed indexing and searching
- Optimized for time-based log analysis

## 2.6 Why Not SQL Databases

- SQL databases are not optimized for log analytics
  - Slower querying for time-series security data
  - Poor scalability for SOC workloads
- 

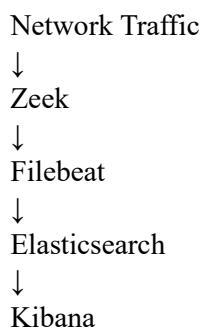
## 2.7 Why Kibana

Kibana serves as the **SOC analyst interface**.

Features:

- Interactive dashboards
  - Advanced searching and filtering
  - Timeline-based investigations
  - No command-line requirement for analysts
- 

## 3. Architecture Overview (SOC Data Flow)



This architecture represents a **standard SOC / SIEM pipeline** used in enterprise environments.

---

## 4. System Environment

Operating System: Ubuntu 24.04 LTS

Zeek Version: 8.0.4

Filebeat Version: 7.17.29 / 8.19.8

Elasticsearch Version: 7.17.29

Kibana Version: 7.17.29  
Network Interface: ens33

---

## 5. Step-by-Step Deployment with Explanation

### Step 1: Identify Network Interface

Command:

```
ip a
```

Reason:

Zeek must listen on the correct network interface.  
Incorrect interface selection prevents packet capture.

---

### Step 2: Configure Zeek Interface

Configuration File:

```
/opt/zeek/etc/node.cfg
```

Change:

```
interface=eth0
```

To:

```
interface=ens33
```

Reason:

Ensures Zeek captures live network traffic and avoids startup errors.

---

### Step 3: Deploy Zeek

Commands:

```
sudo /opt/zeek/bin/zeekctl deploy
```

```
sudo /opt/zeek/bin/zeekctl status
```

Reason:

- Starts Zeek services
  - Applies configuration changes
  - Confirms Zeek is running successfully
- 

### Step 4: Verify Zeek Logs

Command:

```
sudo ls /opt/zeek/logs/current
```

Reason:  
SOC monitoring depends entirely on log generation.  
No logs means no security visibility.

---

## 6. Issues Faced and Resolution

### Issue 1: Zeek Interface Error

Error:

pcap\_error: No such device exists

Cause:  
Incorrect network interface configured.

Solution:  
• Updated interface name in node.cfg  
• Redeployed Zeek

---

### Issue 2: Zeek Logs Not Accessible

Error:

Permission denied

Cause:  
• Zeek logs owned by root  
• Filebeat runs as a non-root user

Solution Commands:

sudo useradd filebeat

sudo chgrp -R filebeat /opt/zeek/logs

sudo chmod -R 750 /opt/zeek/logs

Reason:  
• Follows principle of least privilege  
• Allows Filebeat to safely read logs

---

### Issue 3: JSON Parsing Error

Error:

json: cannot unmarshal number into Go value

Cause:  
Zeek logs are generated in **TSV format**, not JSON.

Solution:  
• Enabled Zeek module in Filebeat  
• Disabled manual JSON parsing

Configuration File:

/etc/filebeat/modules.d/zeek.yml

---

## Issue 4: Kibana Dashboard Import Error

Error:

Saved objects are not backwards compatible

Cause:

Filebeat version newer than Kibana.

Resolution:

- Skipped dashboard import
- Used Kibana Discover for analysis

Reason:

Log ingestion was successful; visualization through Discover was sufficient.

---

## 7. Filebeat Configuration and Start

Commands:

sudo filebeat test config

sudo systemctl restart filebeat

sudo systemctl status filebeat

Reason:

- Validates configuration
  - Starts log shipping to Elasticsearch
  - Confirms Filebeat service health
- 

## 8. Elasticsearch Verification

**Service Check:** curl http://localhost:9200

Reason:

Confirms Elasticsearch is running.

Index Verification:

curl http://localhost:9200/\_cat/indices/filebeat\*?v

Reason:

Confirms logs are indexed successfully.

This proves SIEM ingestion is working.

---

## 9. Kibana Access and SOC Validation

**Access URL:** http://localhost:5601

Discover Configuration:

- Index pattern: filebeat-\*
- Filter:

event.module : zeek

Reason:

SOC analysts validate logs through Kibana to ensure data is searchable and usable.

---

## 10. SOC Analysis Use Case

With this deployment, a SOC analyst can:

- Detect suspicious DNS queries
  - Analyze abnormal network connections
  - Investigate HTTP traffic
  - Perform timeline-based incident analysis
- 

## 11. Final Deployment Checklist

Zeek capturing traffic – ✓

Logs generated – ✓

Filebeat shipping logs – ✓

Elasticsearch indexing data – ✓

Kibana visualizing logs – ✓

---

## 12. Conclusion

The **Zeek–Filebeat–ELK Stack** was successfully deployed for SOC analysis.

All issues related to network interface configuration, permissions, log format handling, and version compatibility were resolved through systematic troubleshooting.

This deployment represents a **real-world SOC / SIEM monitoring architecture**, making it highly suitable for **security internships, academic projects, and practical SOC operations**.

---