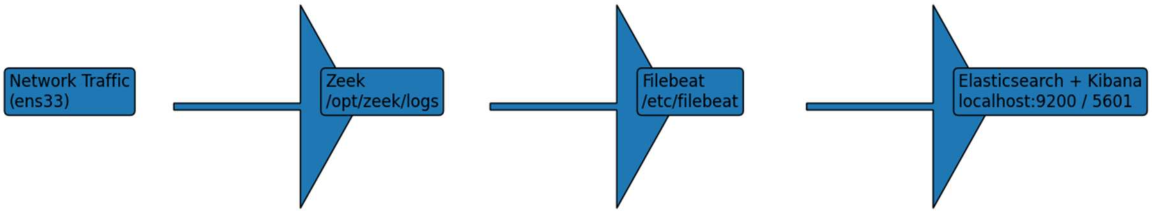
END-TO-END SIEM PIPELINE DEPLOYMENT USING ZEEK, FILEBEAT AND ELK STACK ON UBUNTU

Prepared by: Aman Kumar
Platform: Ubuntu 24.04 LTS
Project: SIEM Deployment

1. SIEM Architecture Overview



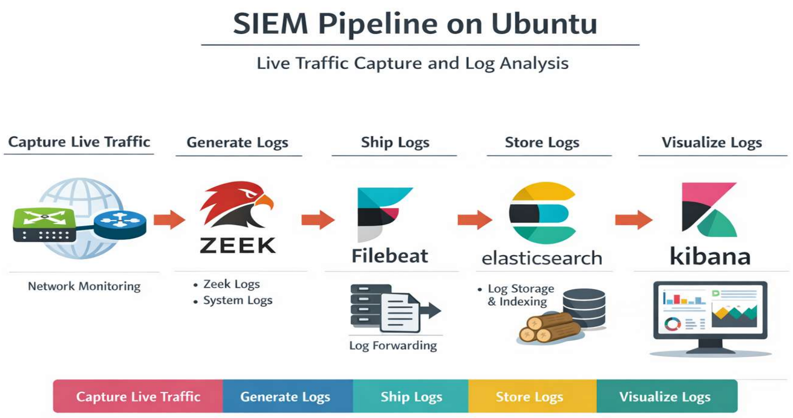
This architecture captures live traffic using Zeek, ships logs using Filebeat,
stores logs in Elasticsearch, and visualizes logs using Kibana.

2. Introduction

SIEM systems provide centralized security monitoring. This project deploys a complete SIEM pipeline using Zeek, Filebeat, Elasticsearch, and Kibana on Ubuntu.

Objective:

- Capture live traffic
- Generate logs
- Ship logs
- Store logs
- Visualize logs



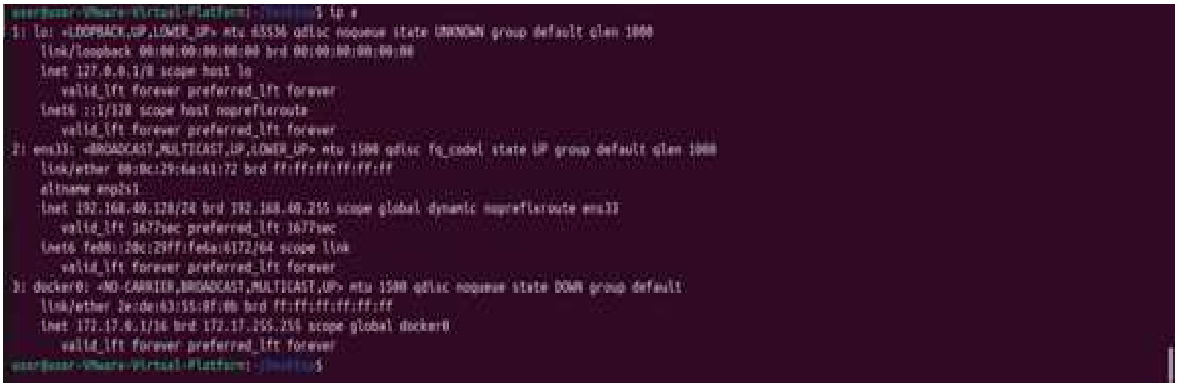
3. System Environment

Operating System: Ubuntu 24.04 LTS
Zeek Path: /opt/zeek
Filebeat Path: /etc/filebeat
Elasticsearch: localhost:9200
Kibana: localhost:5601

Command:
ip a

Output:
ens33: inet 192.168.1.100

Explanation:
ens33 is the active network interface.



```
user@user-VMware-Virtual-Platform:~/[illegible]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6a:61:72 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.40.128/24 brd 192.168.40.255 scope global dynamic noprefixroute ens33
       valid_lft 1677sec preferred_lft 1677sec
    inet6 fe80::20c:29ff:fe6a:6172/64 scope link
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 2e:de:63:55:0f:0b brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
user@user-VMware-Virtual-Platform:~/[illegible]$
```

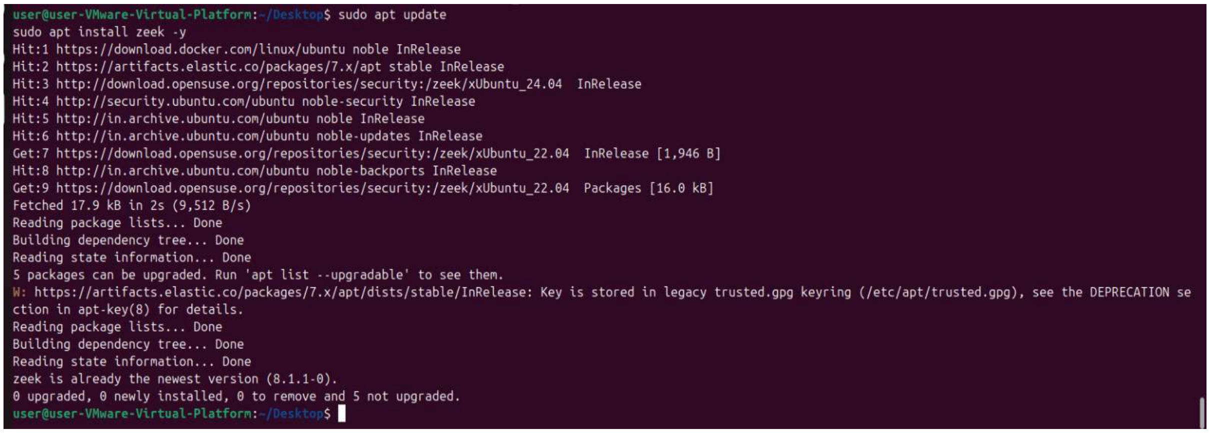
4. Zeek Deployment

Command:
sudo /opt/zeek/bin/zeekctl deploy

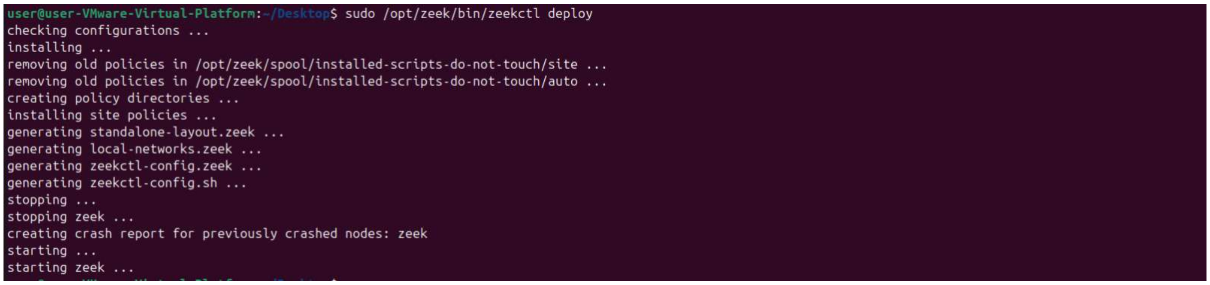
Explanation line-by-line:

sudo → administrator privilege
zeekctl → Zeek control tool
deploy → starts monitoring

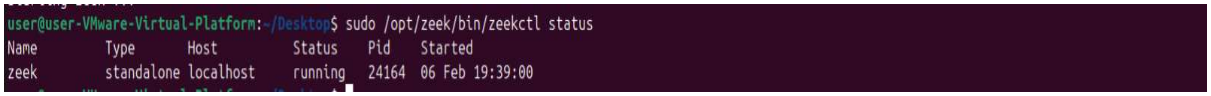
Output:
starting zeek ...



```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo apt update
sudo apt install zeek -y
Hit:1 https://download.docker.com/linux/ubuntu noble InRelease
Hit:2 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:3 http://download.opensuse.org/repositories/security:/zeek/xUbuntu_24.04  InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:5 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:6 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Get:7 https://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04  InRelease [1,946 B]
Hit:8 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:9 https://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04  Packages [16.0 kB]
Fetched 17.9 kB in 2s (9,512 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
5 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION se
ction in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zeek is already the newest version (8.1.1-0).
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
user@user-VMware-Virtual-Platform:~/Desktop$
```



```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo /opt/zeek/bin/zeekctl deploy
checking configurations ...
installing ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
creating crash report for previously crashed nodes: zeek
starting ...
starting zeek ...
```



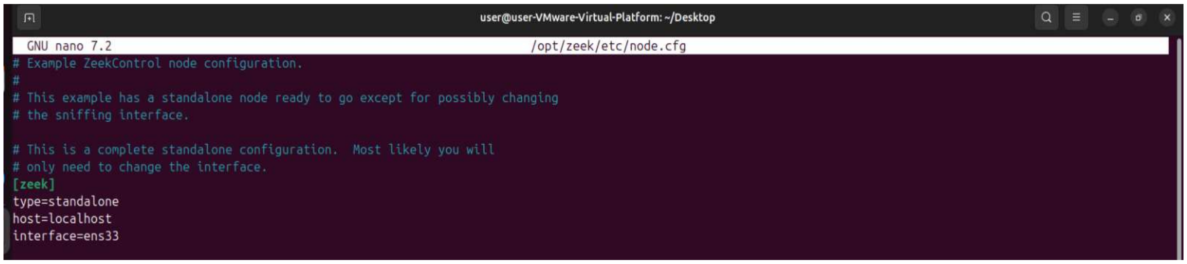
```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo /opt/zeek/bin/zeekctl status
Name         Type       Host          Status    Pid    Started
zeek         standalone localhost     running   24164  06 Feb 19:39:00
```

5. Zeek Configuration

File:
/opt/zeek/etc/node.cfg

Configuration:
interface=ens33

Explanation:
Defines capture interface.



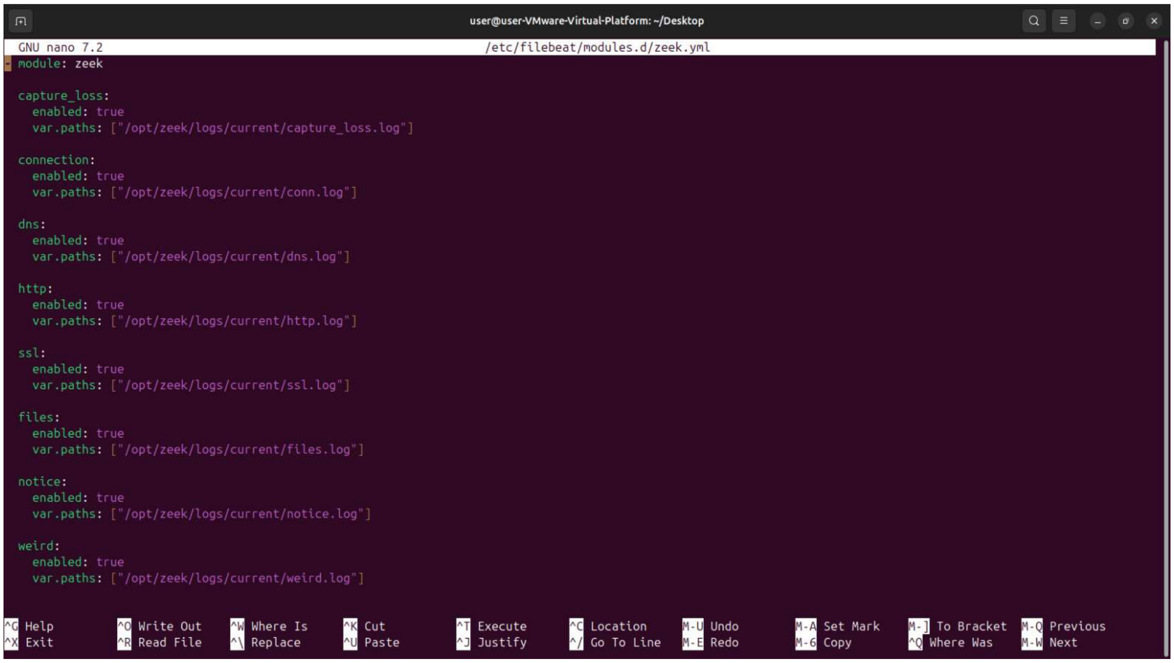
```
# Example ZeekControl node configuration.
#
# This example has a standalone node ready to go except for possibly changing
# the sniffing interface.

# This is a complete standalone configuration.  Most likely you will
# only need to change the interface.
[zeek]
type=standalone
host=localhost
interface=ens33
```

6. Zeek Log Generation

Command:
ls /opt/zeek/logs/current

Output:
conn.log
dns.log
http.log

Explanation:
Confirms successful capture.

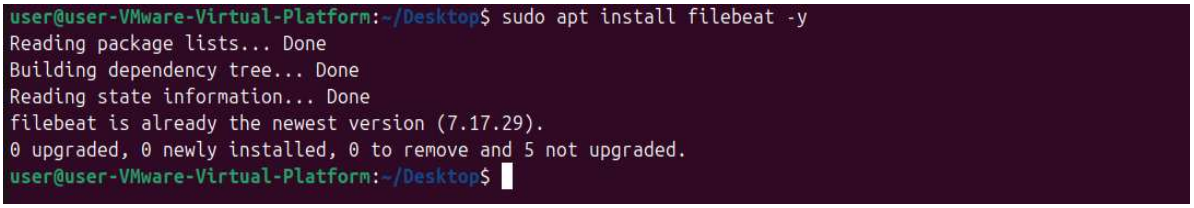

user@user-VMware-Virtual-Platform: ~/Desktop
GNU nano 7.2
/etc/filebeat/modules.d/zeek.yml

```
- module: zeek

  capture_loss:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/capture_loss.log"]

  connection:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/conn.log"]

  dns:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/dns.log"]

  http:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/http.log"]

  ssl:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/ssl.log"]

  files:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/files.log"]

  notice:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/notice.log"]

  weird:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/weird.log"]
```

7. Filebeat Installation

Command:
sudo apt install filebeat -y

Output:
filebeat installed



```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo apt install filebeat -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
filebeat is already the newest version (7.17.29).
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
user@user-VMware-Virtual-Platform:~/Desktop$ 
```

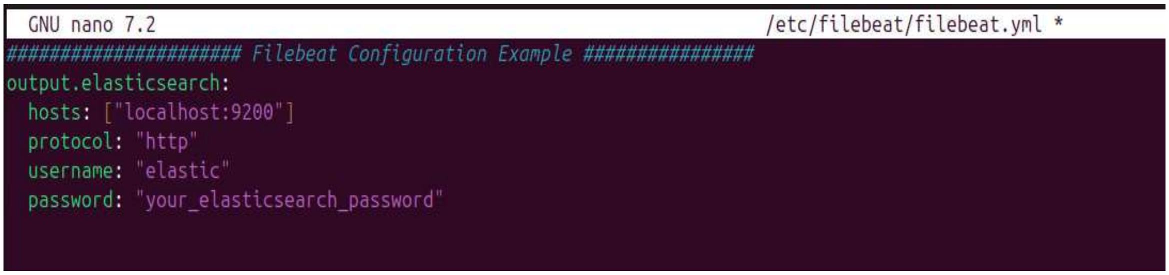
8. Filebeat Configuration

File:
/etc/filebeat/filebeat.yml

Configuration:
output.elasticsearch:
 hosts: ["localhost:9200"]

Explanation line-by-line:

output.elasticsearch → output destination
hosts → Elasticsearch server

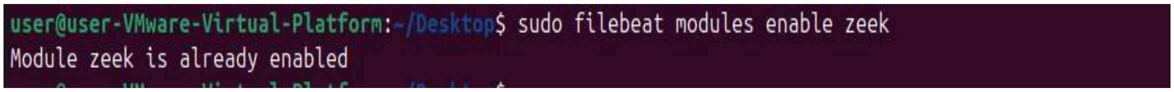


```
  GNU nano 7.2                                        /etc/filebeat/filebeat.yml *
###################### Filebeat Configuration Example ################
output.elasticsearch:
  hosts: ["localhost:9200"]
  protocol: "http"
  username: "elastic"
  password: "your_elasticsearch_password"
```

9. Enable Zeek Module

Command:
sudo filebeat modules enable zeek

Explanation:
Enables Zeek log parsing.

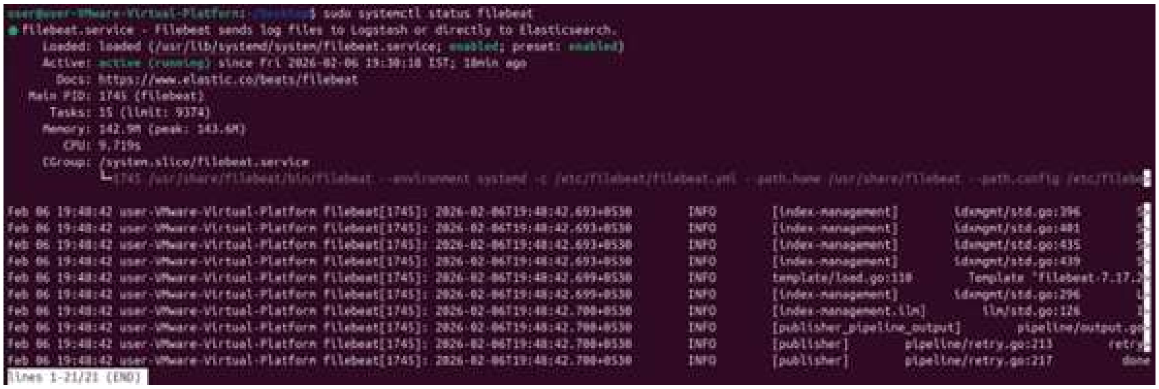


```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo filebeat modules enable zeek
Module zeek is already enabled
```

10. Start Filebeat

Command:
sudo systemctl start filebeat

Output:
active (running)



```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
     Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset: enabled)
     Active: active (running) since Fri 2026-02-06 19:30:18 IST; 18min ago
       Docs: https://www.elastic.co/beats/filebeat
   Main PID: 1745 (filebeat)
      Tasks: 15 (limit: 9374)
     Memory: 142.9M (peak: 143.6M)
        CPU: 9.719s
     CGroup: /system.slice/filebeat.service
             └─1745 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc/filebe

Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.693+0530       INFO      [index-management]       idxmgmt/std.go:396
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.693+0530       INFO      [index-management]       idxmgmt/std.go:401
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.693+0530       INFO      [index-management]       idxmgmt/std.go:435
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.693+0530       INFO      [index-management]       idxmgmt/std.go:439
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.699+0530       INFO      template/load.go:110       Template "filebeat-7.17.
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.699+0530       INFO      [index-management]       idxmgmt/std.go:296
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.700+0530       INFO      [index-management.ilm]       ilm/std.go:126
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.700+0530       INFO      [publisher_pipeline_output]       pipeline/output.go
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.700+0530       INFO      [publisher]       pipeline/retry.go:213       retry
Feb 06 19:48:42 user-VMware-Virtual-Platform filebeat[1745]: 2026-02-06T19:48:42.700+0530       INFO      [publisher]       pipeline/retry.go:217       done
lines 1-21/21 (END)
```

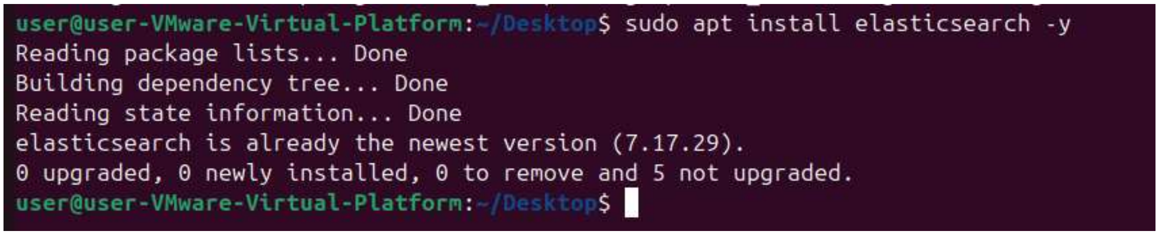
11. Elasticsearch Verification

Command:
curl http://localhost:9200

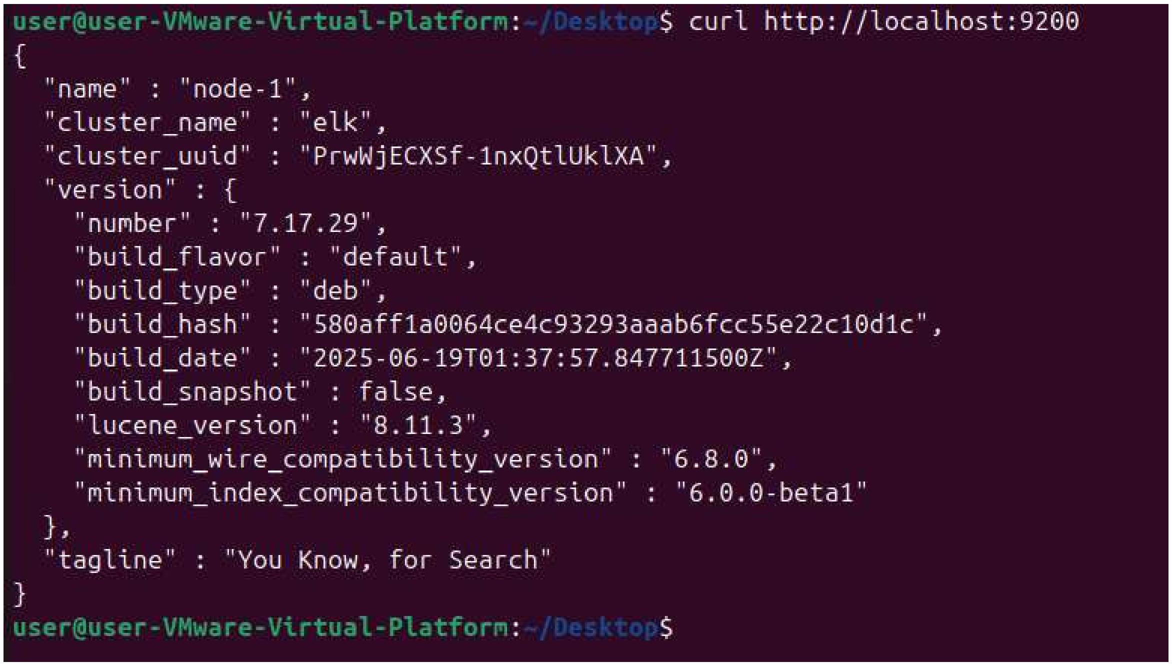
Output:
cluster running

Explanation:

Confirms Elasticsearch active.



```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo apt install elasticsearch -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
elasticsearch is already the newest version (7.17.29).
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
user@user-VMware-Virtual-Platform:~/Desktop$ 
```



```
user@user-VMware-Virtual-Platform:~/Desktop$ curl http://localhost:9200
{
  "name" : "node-1",
  "cluster_name" : "elk",
  "cluster_uuid" : "PrwWjECXSf-1nxQtlUklXA",
  "version" : {
    "number" : "7.17.29",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "580aff1a0064ce4c93293aaab6fcc55e22c10d1c",
    "build_date" : "2025-06-19T01:37:57.847711500Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
user@user-VMware-Virtual-Platform:~/Desktop$
```

12. Verify Elasticsearch Index

Command:

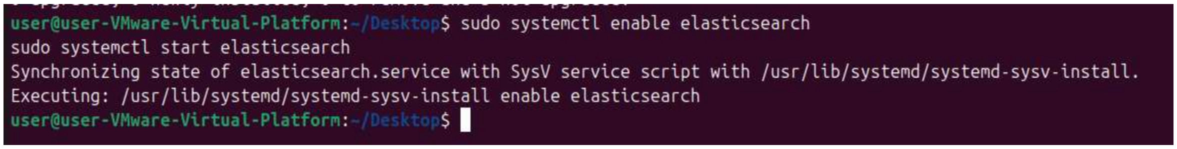
curl http://localhost:9200/_cat/indices/filebeat*?v

Output:

filebeat-2026

Explanation:

Confirms logs stored.

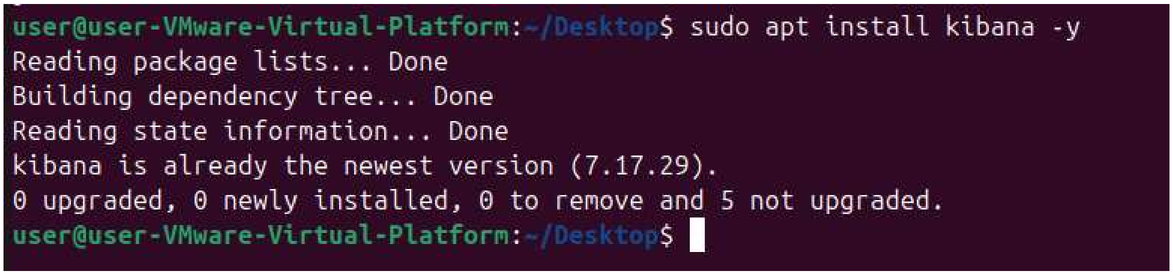


```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch
user@user-VMware-Virtual-Platform:~/Desktop$
```

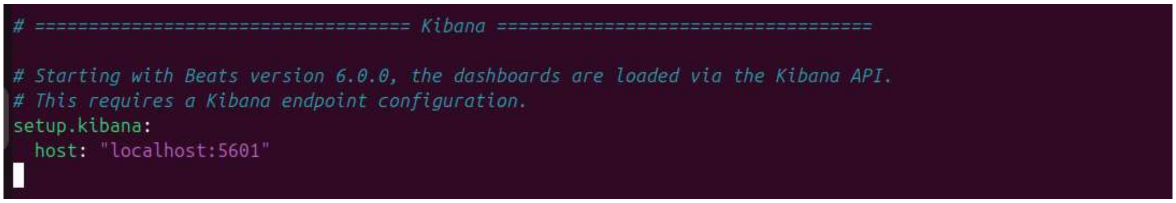
13. Kibana Deployment

Access:
http://localhost:5601

Explanation:
Kibana displays logs.



```
user@user-VMware-Virtual-Platform:~/Desktop$ sudo apt install kibana -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
kibana is already the newest version (7.17.29).
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
user@user-VMware-Virtual-Platform:~/Desktop$
```

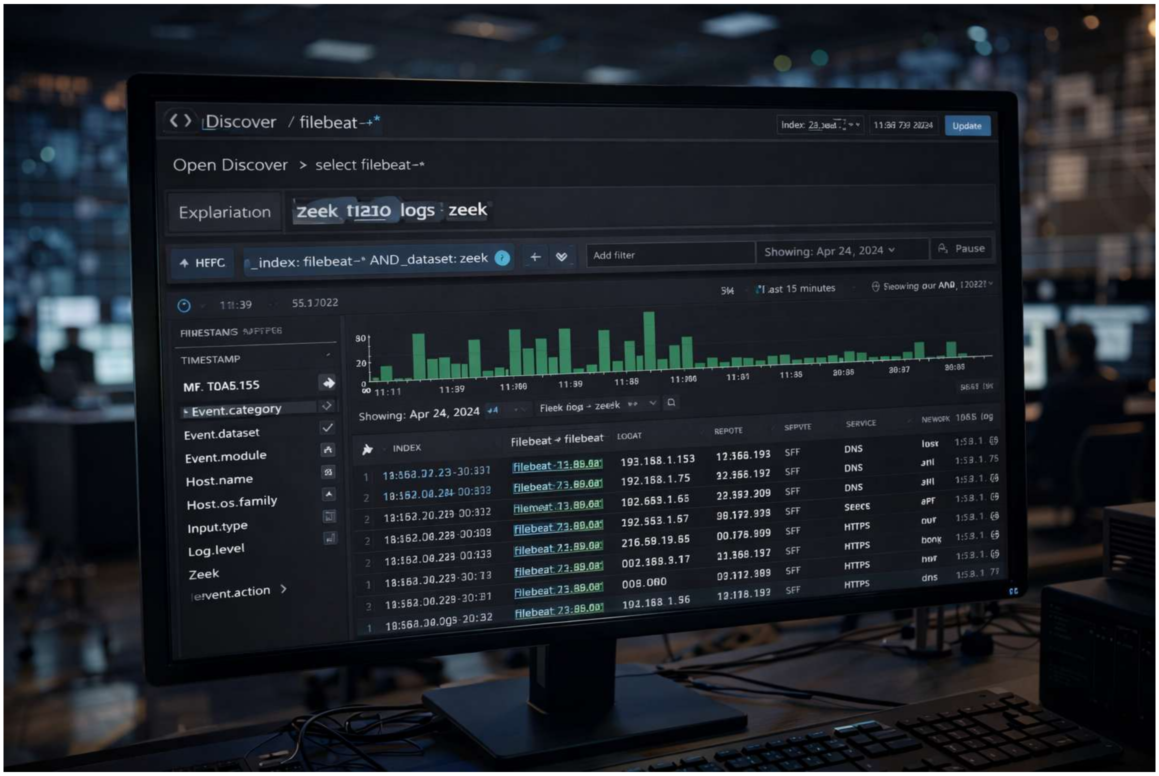


```
# ================================== Kibana ===================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "localhost:5601"
```

14. Kibana Log Analysis

Open Discover → select filebeat-*

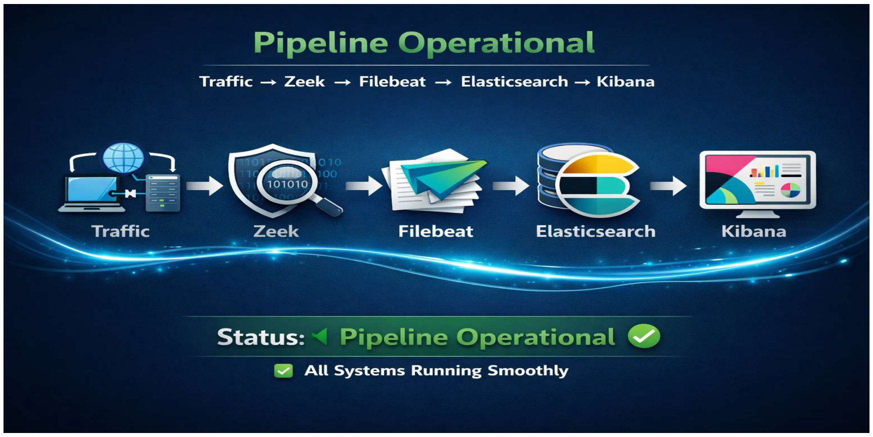
Explanation:
Displays Zeek logs.



15. Full Pipeline Verification

Flow:
Traffic → Zeek → Filebeat → Elasticsearch → Kibana

Result:
Pipeline operational.



Pipeline Operational

Traffic → Zeek → Filebeat → Elasticsearch → Kibana

Traffic → Zeek → Filebeat → Elasticsearch → Kibana

Status: Pipeline Operational ✓

✓ All Systems Running Smoothly

16. Security Monitoring Capability

Detectable events:
DNS queries
HTTP traffic
Suspicious connections

17. Results

System successfully captures and processes logs.
All components working.

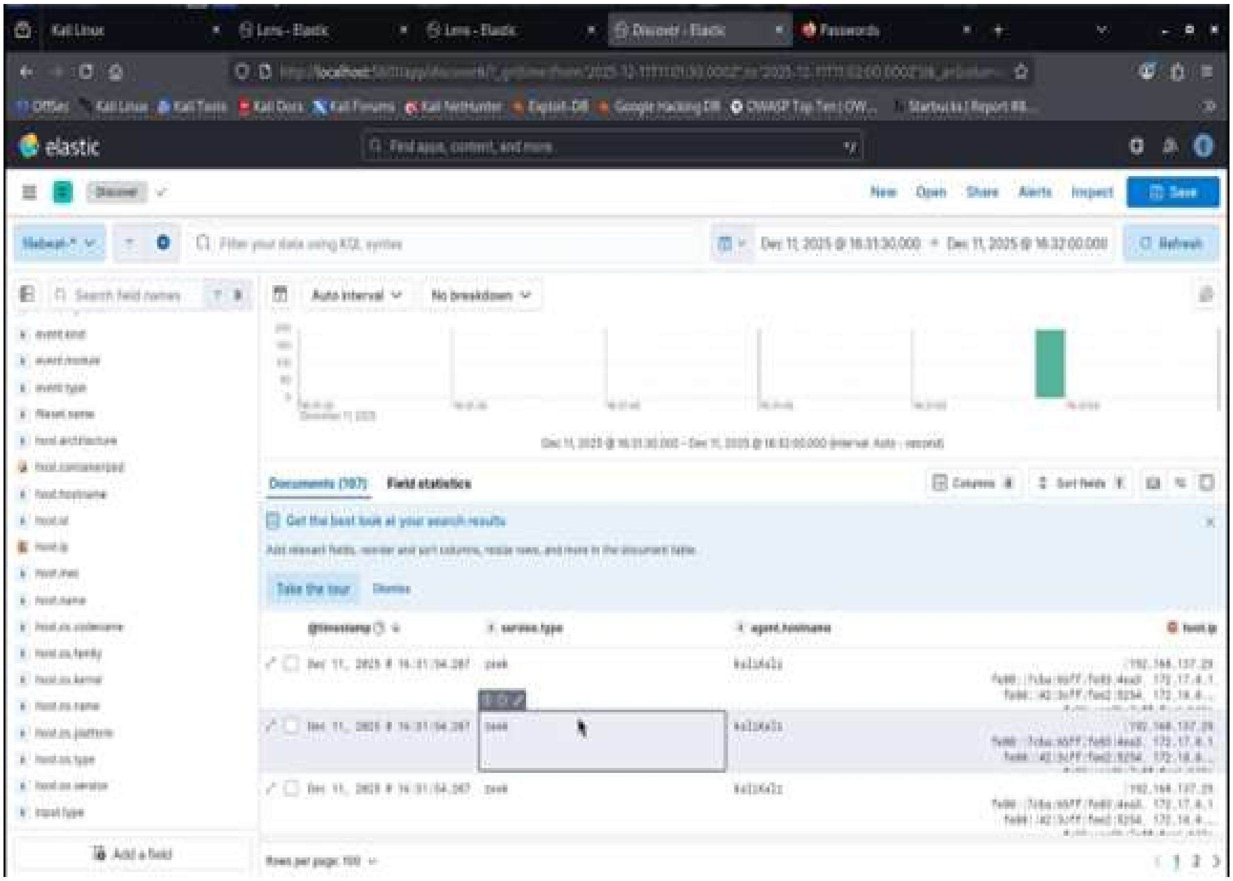
```
111:79:20:50  System Checkpoint Completed!
111:79:20:50  User Authenticated: ID 54322.
111:79:20:50  Data Backup Successful:
111:79:20:39  Service Health Check OK:'
111:79:20:50  Service Health Check: OK'
111:79:20:50  API Request Processed!
111:79:20:50  System Checkpoint Completed:
111:73:20:50  User Authenticated: ID 54337.
111:73:20:50  YATA Retoee Processed!'
```

■ LOGS RECEIVED: 2563 ENTRIES ■ DATA PROCESSING: NORMAL ■ NETWORK 'CONNECTED

18. Conclusion

The SIEM deployment was successfully completed on Ubuntu.

This system provides real-time monitoring and SOC-level analysis.



Discover - Elastic
elastic
Find apps, content, and more
New
Open
Share
Alerts
Inspect
Save
filebeat-*
Filter your data using KQL syntax
Dec 11, 2025 @ 16:31:30.000 → Dec 11, 2025 @ 16:32:00.000
Refresh
Auto interval
No breakdown
Documents (187)
Field statistics
Get the best look at your search results
Take the tour
Add a field

@timestamp	service.type	agent.hostname	host.ip
Dec 11, 2025 @ 16:31:54.287	zeek	[illegible]	192.168.137.29 [illegible]
Dec 11, 2025 @ 16:31:54.287	zeek	[illegible]	192.168.137.29 [illegible]
Dec 11, 2025 @ 16:31:54.287	zeek	[illegible]	192.168.137.29 [illegible]

19. Detailed Technical Explanation

- Zeek captures packets and converts them into logs.
- Filebeat reads logs and sends them to Elasticsearch.
- Elasticsearch indexes logs for fast searching.
- Kibana visualizes logs for analysis.
- Each component performs a critical role in the SIEM pipeline.

20. Final Summary

- This project demonstrates real-world SIEM deployment using Ubuntu.
- The pipeline successfully captures, ships, stores, and visualizes logs.
- This deployment is suitable for SOC environments and cybersecurity operations.