

SECURING THE PERIMETER



STEVEN REJI GEORGE
CBS-0141

SUBMITTED ON: 26-03-2025

Project Scenario

Overview

XYZ is the premier cryptocurrency exchange. They transact over a billion trades everyday and are considered to be one of the most reliable and secure exchanges in the world. Due to their rapid growth, they've faced challenges in scaling their security posture.

The largest challenge they've faced is with their Perimeter Network Security being secure. The networking team was overburdened with the rapid growth and a majority of the network infrastructure was built insecurely.

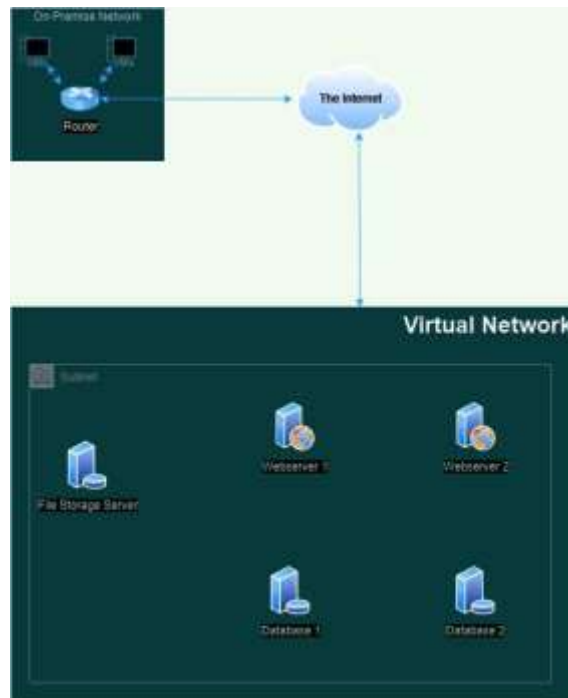
Due to a lack of visibility and a lack of proper access control setup on the network, it was inevitable that a breach took place! XYZ was hit with a massive attack in which their network was breached and their internal servers were compromised resulting in over 500 Bitcoin being stolen!

Needing to get the bottom of this breach and resolving their current perimeter issues they've contracted you from SecureCorp, a world renowned cybersecurity consulting firm. Your job is to redesign their network architecture securely and set up a SIEM to monitor against future attacks.

Section 1:

Designing a secure
Network Architecture

Network Description



- *The on-premise network is connected to a virtual network through the internet.*
- *All five servers are located within a single virtual network and in one subnet.*
- *All servers have direct connections to the internet.*
- *The two web servers are required to communicate with the two database servers to function correctly.*
- *The file storage server only needs to be accessible from the on-premise network.*

Identify Network Vulnerabilities

1. Web servers are exposed directly

Webservers are directly exposed to internet and connected to the virtual n/w via the internet.

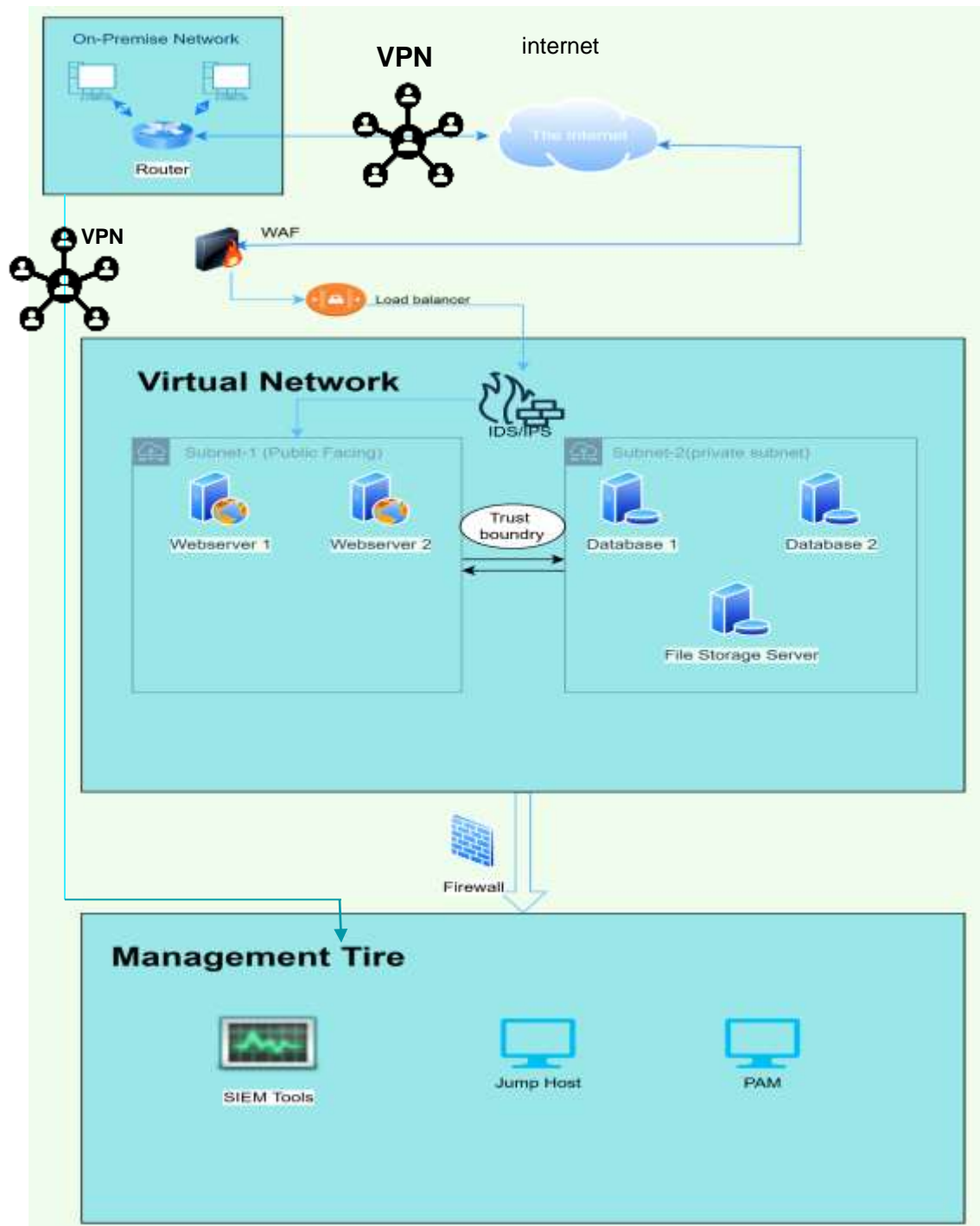
2. No Firewall

No firewall between the internet and internal servers, therefore the ports are openly exposed and the traffic coming from the internet are not filtered. This lead to the easy exploitation of open ports by bad actors

3. No VPN for secure tunneling

Without a VPN, organization face significant security risks, including data breaches, unauthorized access and malware infection, especially remote workers accessing the system

Network Redesign



Convince the Stakeholders

Why do we need to add firewalls to our network?

A firewall is a network security ,that provides an initial layer of protection against cyber attacks, if our organization is vulnarable by installing the firewall is can't be avioded., because:

1.It blocks unauthorised access

2.Prevent DDos attacks.

3Prevent malware & Exploits

What is the benefit of having different areas in our network for web servers and database servers?

In our new architecture web servers are in Public faced subnet and the DB servers are in private subnet ,by implementing this the main advantages are:

1.Improved security: If public servers are attacked we can prevent the attackers from accessing the DB server which contain confidential information like credentials

2.Enhanced Performance and load management: Implementing load balancers to distribute more traffics ,efficient data handling (webserver and DB servers are in diff. Subnets)

3.Compliance and data protection Isolating databases from public access minimizes the risk of unauthorized access.
Logging and monitoring (SIEM tools) can be targeted at various layers.

5. Minimized Attack Surface

Even if an attacker gains control of a web server, they still cannot directly access the databases.

Convince the Stakeholders

What does a VPN do for our connection to the file storage server?

A Virtual Private Network(VPN) offers a secure encrypted network between remote users and system and internal network ,such as File storage server .It also allow remote workers to operate the management tire(SIEM...) securely .the security cannot be compromised while accessing the system remotely

Section 2:

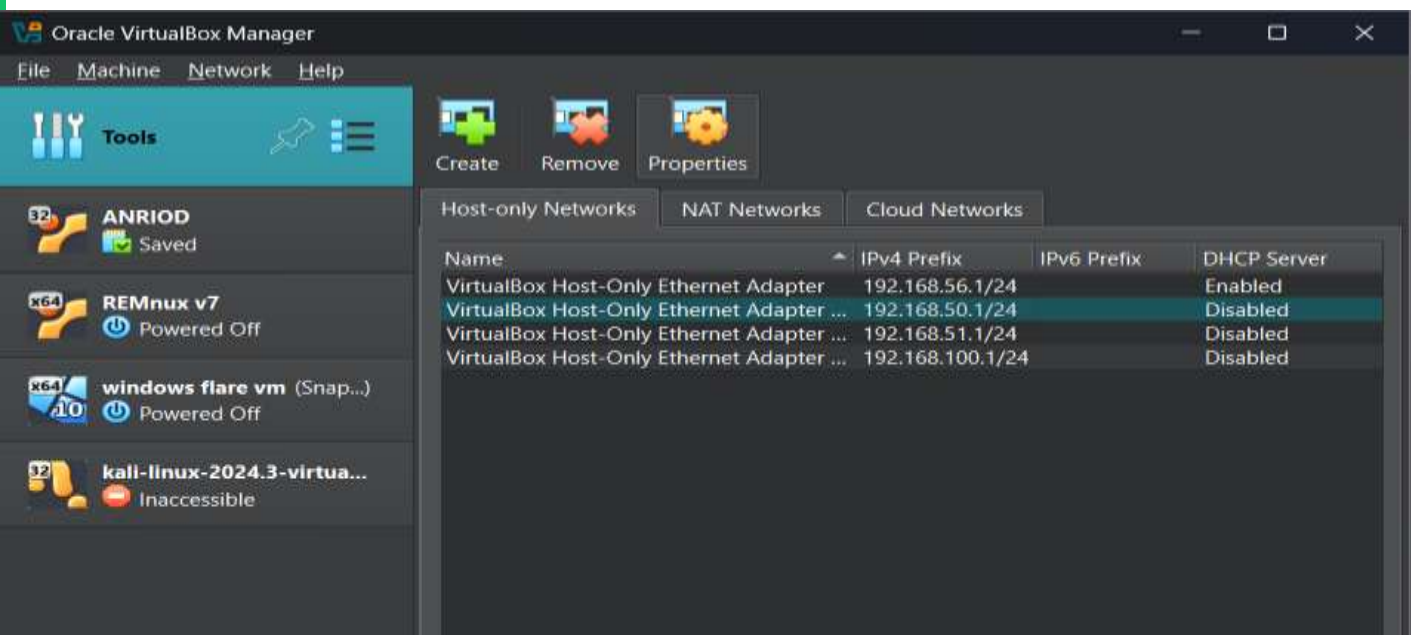
Building a secure Network
Architecture in VirtualBox

Network Setup

Following the favorable reception of your network diagram, management is keen to see this blueprint come to life in a test environment. They have chosen VirtualBox as the platform to host this venture into the cloud. Your next task is to build the test network, which is detailed below.

- *Construct two VirtualBox virtual networks (VNet):*
 - *Name the first VNet DMZ. Within it, create two subnets:*
 - *Public-DMZ for future web servers.*
 - *Private-DMZ for database servers.*
 - *Name the second VNet Internal and create one subnet within it called Internal-Subnet.*
- *Take and submit a screenshot of the DMZ Virtual Network with the two subnets*
- *Take and submit a screenshot of the Internal Virtual Network with the subnet*

Network Setup



Network Identification Guide

Default VirtualBox Name	IPv4 Prefix	Purpose (Your Design)	DHCP Status
VirtualBox Host-Only Ethernet Adapter ...	192.168.50.1 /24	Public-DMZ (Web Servers)	Disabled
VirtualBox Host-Only Ethernet Adapter ...	192.168.51.1 /24	Private-DMZ (Databases)	Disabled
VirtualBox Host-Only Ethernet Adapter ...	192.168.100.1 /24	Internal (Management)	Disabled

There is no option to change the name of subnets therefore a network guide is provided above.

Section 3:

Continuous Monitoring with a SIEM

Understanding SIEM Benefits

1. Real Time thread detection

SIEM tools actively collect and analyze log information from networks, servers, firewall and all other endpoints in real time. It discovers suspicious patterns, alert prioritization i.e., identify high risk events

2. Compliance & Audit support

Automated Reporting, produces compliance reports, regulations, this report can be further used for auditing, system modification and for forensic analysis.

3. Quick Incident Response

Quick responses against attacks like IP blocking, quarantining infected devices to mitigate attacks

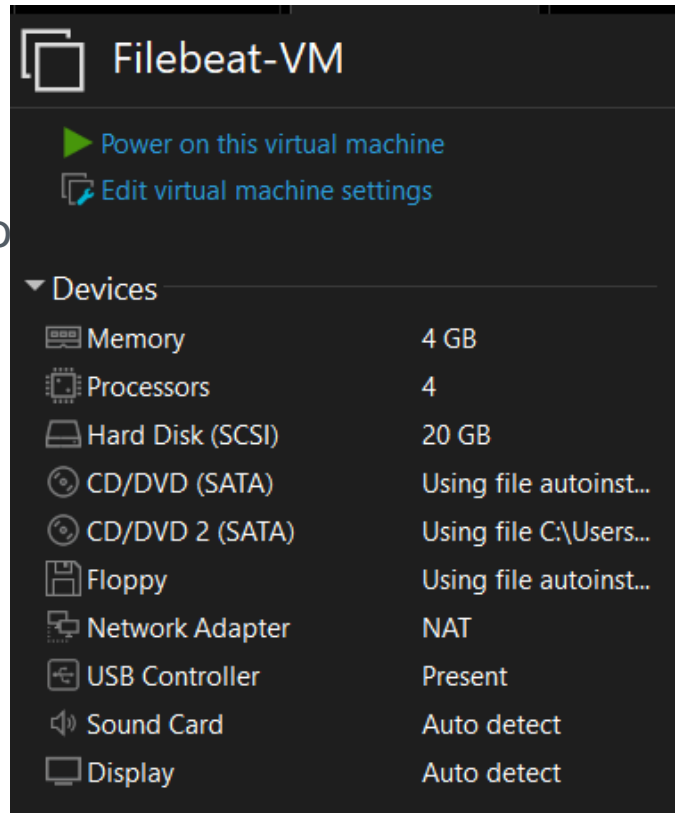
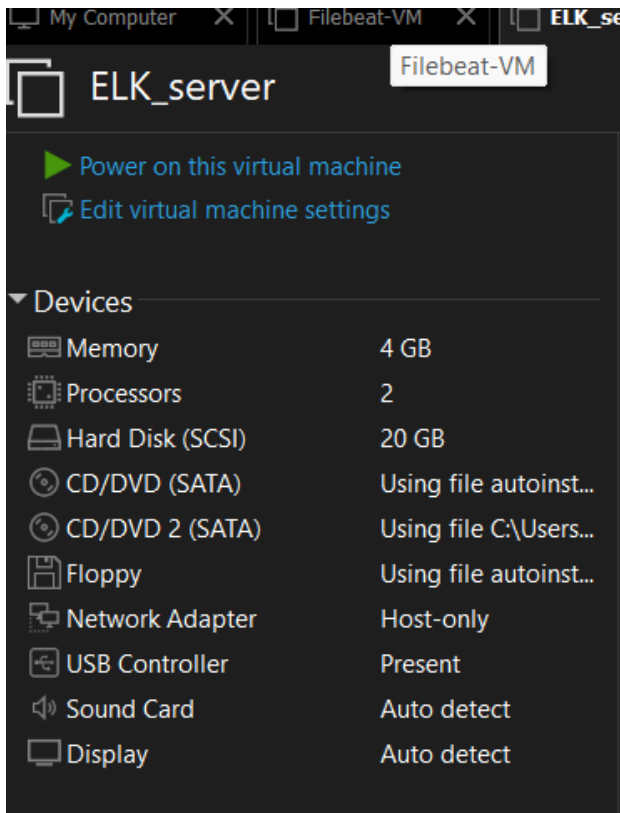
Deploy SIEM Components in VirtualBox

To give management a tangible understanding of how a Security Information and Event Management (SIEM) system operates, we're going to set up a demonstration in our VirtualBox test environment. This setup will involve deploying a virtual machine for the ELK server within the private subnet and a virtual machine for Filebeat within the public subnet. These components will work in tandem to illustrate the power of centralized logging and real-time analysis.

- *Deploy a virtual machine named Elk-Server in the Private-DMZ subnet of the DMZ VNet for the ELK stack.*
- *Deploy a virtual machine named Filebeat-VM in the Public-DMZ subnet of the DMZ VNet for Filebeat.*
- *Take and submit screenshots of the VM instances confirming their creation and network placement.*

Deploy SIEM Components in VirtualBox

Screenshots of the VM instances confirming their creation and network placement.



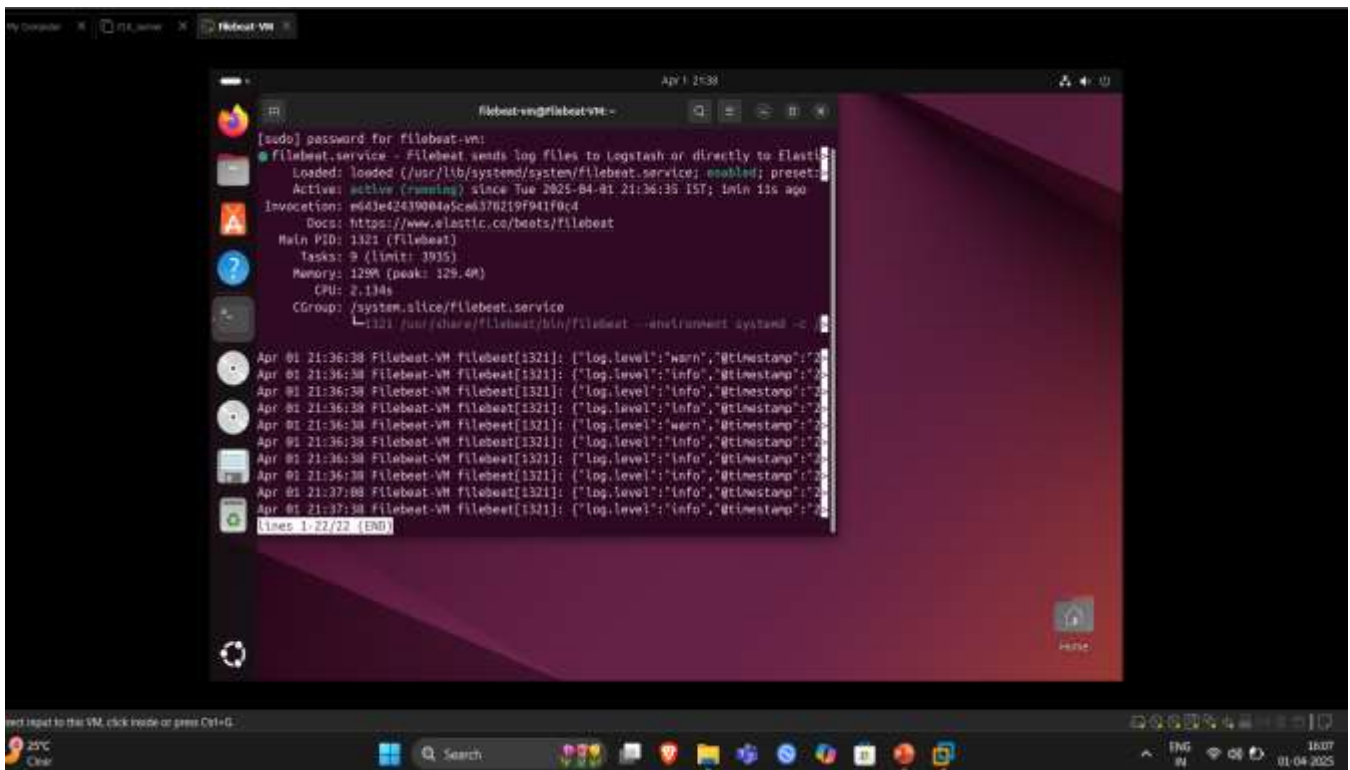
Setup Monitoring

To fully showcase our SIEM's capabilities, we will set up the ELK (Elasticsearch, Logstash, Kibana) server, install Filebeat on our web server, and ensure that web server logs are correctly forwarded and displayed in Kibana. This comprehensive task is pivotal for demonstrating effective real-time monitoring and analysis of web server activity, which is essential for maintaining operational health and security within our infrastructure.

- *Install and configure the ELK server on a VM within the Private-DMZ subnet.*
- *Install Filebeat on the web server in the Public-DMZ subnet.*
- *Configure Filebeat to forward logs to the ELK server's Elasticsearch.*
- *Generate traffic on the web server to create log data (i.e. access the server).*
- *Verify logs are forwarded to Elasticsearch and visible in Kibana.*
- *Create screenshots to confirm that the services are running:*
 - *Filebeat service running on the web server*
 - *Make it from the CLI, with the 'systemctl status filebeat'*
 - *Kibana receives logs from the Filebeat host*
 - *From Kibana site SIEM/Hosts/Filebeat-VM*

Setup Monitoring

Screenshot of the Filebeat service on the web server
(command: 'systemctl status filebeat')



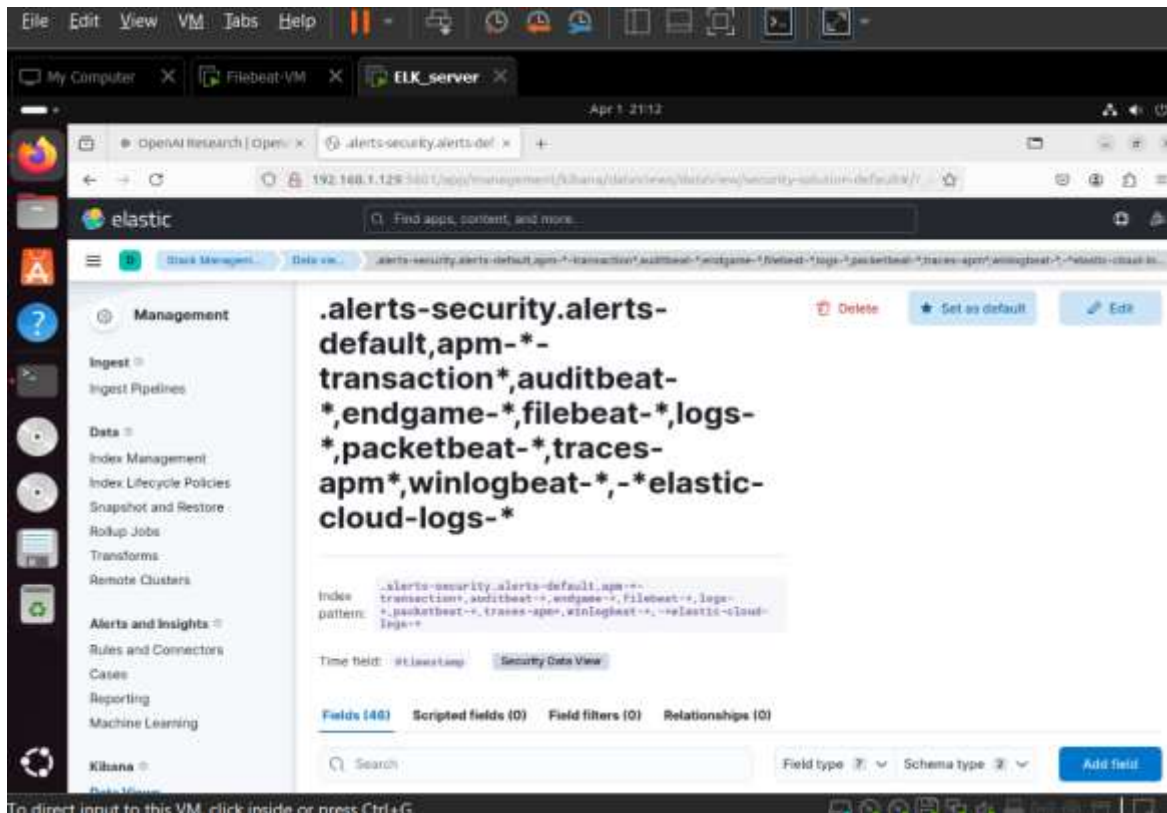
```
filebeat-vn@filebeat-vn:~$ [sudo] password for filebeat-vn:
● filebeat.service - Filebeat sends log files to Logstash or directly to Elastic
   Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset:
   Active: active (running) since Tue 2025-04-01 21:36:35 IST; 1min 11s ago
 Invocation: m643e42430004a5c66376219f941f0c4
    Docs: https://www.elastic.co/beats/filebeat
   Main PID: 1321 (Filebeat)
      Tasks: 9 (limit: 3935)
    Memory: 129M (peak: 129.4M)
       CPU: 2.134s
    CGroup: /system.slice/filebeat.service
           └─1321 /usr/share/filebeat/bin/filebeat --hostname=systemd -c

Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"warn","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":1}
Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":2}
Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":3}
Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":4}
Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"warn","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":5}
Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":6}
Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":7}
Apr 01 21:36:38 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:36:38.000Z","log.offset":8}
Apr 01 21:37:08 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:37:08.000Z","log.offset":9}
Apr 01 21:37:38 Filebeat-VN filebeat[1321]: {"log.level":"info","@timestamp":"2025-04-01T21:37:38.000Z","log.offset":10}
lines 1-22/22 (END)
```

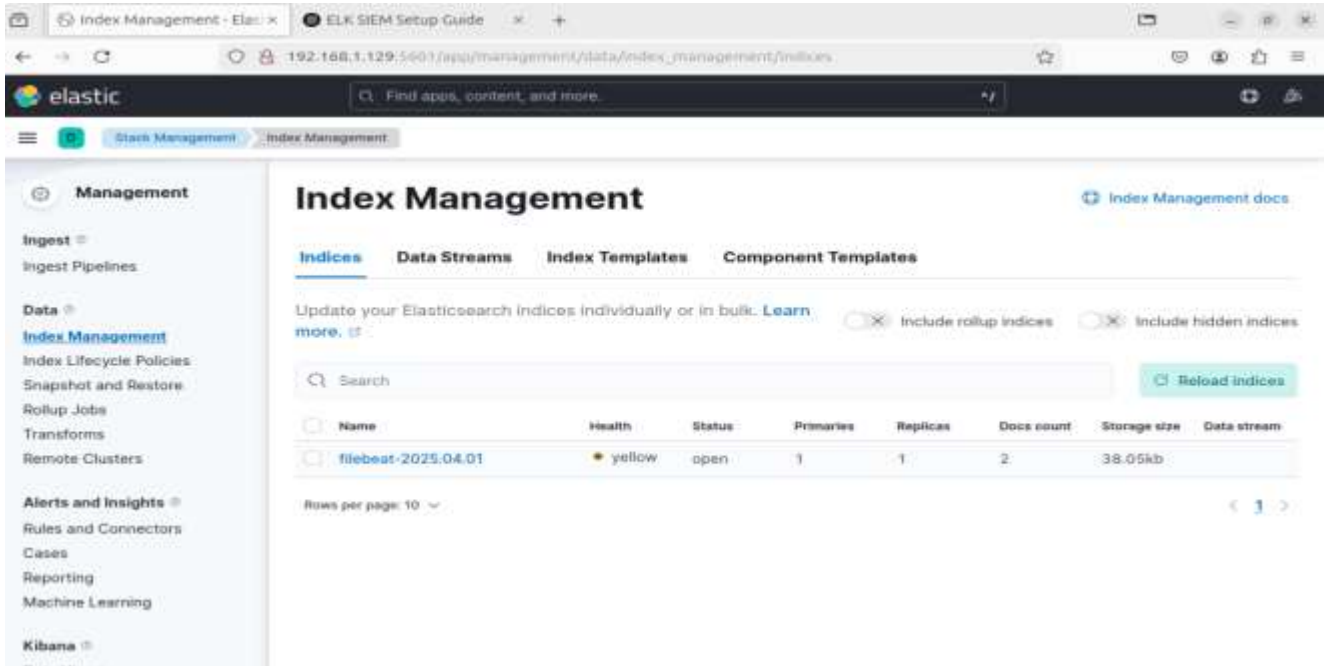
Setup Monitoring

Screenshot showing that Kibana receives logs from the Filebeat host (SIEM/Hosts/Filebeat-VM)

```
lk@elk-admin:~/elk$ sudo docker ps
sudo] password for elk:
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS
PORTS
dfea02cb864    docker.elastic.co/kibana/kibana:8.7.1  "/bin/tini -- /usr/L..."  2 hours ago   Up 9 minutes
0.0.0.0:5601->5601/tcp, :::5601->5601/tcp    kibana
d3737e4c3e2    docker.elastic.co/logstash/logstash:8.7.1  "/usr/local/bin/dock..."  2 hours ago   Up 9 minutes
0.0.0.0:5044->5044/tcp, :::5044->5044/tcp, 9600/tcp    logstash
8e625ff317b    docker.elastic.co/elasticsearch/elasticsearch:8.7.1  "/bin/tini -- /usr/L..."  2 hours ago   Up 9 minutes
0.0.0.0:9200->9200/tcp, :::9200->9200/tcp, 9300/tcp    elasticsearch
lk@elk-admin:~/elk$
```



Setup Monitoring



The screenshot shows the Elastic Index Management interface. The left sidebar contains navigation links for Management, Ingest, Data, Alerts and Insights, and Kibana. The main content area is titled 'Index Management' and includes tabs for Indices, Data Streams, Index Templates, and Component Templates. Below the tabs, there is a search bar and a table of indices. The table has columns for Name, Health, Status, Primaries, Replicas, Docs count, Storage size, and Data stream. One index is listed: 'filebeat-2025.04.01' with a yellow health status and an open status. The bottom of the page shows 'Rows per page: 10' and a pagination control.

Index Management

[Index Management docs](#)

Indices Data Streams Index Templates Component Templates

Update your Elasticsearch Indices individually or in bulk. [Learn more.](#) ☒ Include rollup indices ☒ Include hidden indices

Search [Reload indices](#)

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
<input type="checkbox"/> filebeat-2025.04.01	yellow	open	1	1	2	38.05kb	

Rows per page: 10 < 1 >

Section 4:

Zero Trust

Zero Trust Comparison

Following a significant security breach at XYZ, the necessity to reassess and strengthen our network security architecture is paramount. A comparison between the emerging Zero Trust architecture and traditional network security models will highlight the potential enhancements Zero Trust can offer. Your task involves selecting three key principles from Zero Trust architecture, comparing them to traditional models, and evaluating the benefits of Zero Trust. This analysis is crucial for guiding XYZ towards a more resilient cybersecurity framework.

- Select three principles of Zero Trust architecture (you can find them in the classroom and in the next page)
- Compare each selected principle to its counterpart in traditional network security models, focusing on:
 - Differences in approach
 - Potential benefits of Zero Trust over traditional methods

Zero Trust Principles

Select three principles to use in the comparison:

- Consideration of all resources: Every device, software, and system is a potential security vector.
- Secured communication: Encrypt all data transfers, irrespective of location.
- Per-session access: Grant access to resources only for the duration of a session.
- Dynamic access policy: Access is based on real-time evaluations of multiple factors.
- Continuous monitoring: Real-time assessment of asset integrity and security.
- Dynamic authentication: Ongoing verification before allowing access.
- Extensive data collection: Gather detailed information for security enhancement.

Zero Trust Comparison

1. NEVER TRUST ,ALWAYS VERIFY

Zero Trust Approach: Each user or device within or outside the network must authenticate and authorize itself before it allowed access

Traditional Approach: Devices or users found within the network are allowed defaultly without any authorization.

Benefits of Zero Trust:

- *less lateral movement The attackers can't simply travel laterally along the network since every access needs new authentication
- *Reduce thread inside: Reduce insider entities need to continuously demonstrate trust boundries.
- * Increase in security

2. Small Segmented networks

Zero Trust Approach: Divide the networks into entirly small ,isolated networks ,each network uses strict access control ,so that every user can't access specific resources.

Traditional Approach: Larger networks tends to use larger Subnets offering large attack surface for the user .if the security of one subnet is compermised the entire network need to be compermised.

Benefits of Zero Trust:

- *Fine grained Control since the network is divided into small segments decreasing attack surface.
- *Mitigation against attacks : If one part is attacked small segment isolated them from entering other spaces.
- *Easy audicting

Zero Trust Comparison

3. LEAST PRIVILEGE ACCESS

Zero Trust Approach: Users and machines are given only least number of permissions ,i.e permission need for their own roles

Traditional Approach: Static RBA in which users have more previlages ,here users allow access to all connected resources

Benefits of Zero Trust:

- #Reduced attack surface
- #Compliance enhanced
- #Adaptive enforsment

The Zero Trust Model

Following your analysis of Zero Trust versus traditional security models, it's clear that a Zero Trust framework is essential for enhancing XYZ's network security. The challenge now shifts to selecting the most appropriate Zero Trust model for XYZ from three distinct options: Device Agent & Gateway, Enclave Gateway, or Resource Portal. This selection is critical, as it must align with the unique challenges and goals of the company. Your task is to make an informed choice and articulate why this model stands out as the best fit for XYZ, considering their need for a robust response to recent security vulnerabilities.

- Choose one Zero Trust model for XYZ from the following options:
 - Device Agent & Gateway
 - Enclave Gateway
 - Resource Portal
- Justify why the selected model is the best fit for XYZ's current network challenges and security objectives.

Zero Trust Model

Enclave model

Enclave model is the best practice to follow here because:

1.Improved security for vital resouces: Recent security flaws at XYZ company are probably the result of lack of security ,network segmentation.

2.More robust microperimeters & segmentation: The model establishes microperimeter around critical assets(which requires more security).

3.Minimal intrupts to End – users :