

MINOR PROJECT 2 : Wazuh SIEM Implementation & Security Monitoring

Name: Kaushal Jung Thapa

Course: CEH

Sem: 5th Sem

ERP: 6604309

College: Rungta College of
Engineering & Technology,
Bhilai

1. Project Overview

Objective:

To plan, deploy, and configure a Wazuh-based SIEM solution in a Linux environment to enable centralized log collection, real-time threat detection, and security event analysis, while systematically documenting configurations, alerts, and security evidence.

Tools & Environment:

- Ubuntu Server (SIEM VM)
- Wazuh Manager
- Wazuh Agent (VMs)
- Wazuh Dashboard (OpenSearch)
- Web Browser (Chrome/Firefox)

2. Baseline Architecture Document

Component	Purpose
Wazuh Manager	Collects and analyzes logs from agents
Wazuh Agent	Sends system and security logs

	to manager
Wazuh Dashboard	Visualizes alerts, logs, and compliance

3. Implementation Steps

a) Virtual Machine Setup

Commands Used:

```
sudo apt update && sudo apt upgrade -y
```

b) Wazuh Manager Installation

Installed Wazuh manager using the official installation script.

Commands Used:

```
curl -s0 https://packages.wazuh.com/4.7/wazuh-
install.sh
```

```
sudo bash wazuh-install.sh -a
```

Verification:

```
systemctl status wazuh-manager
```

c) Wazuh Dashboard Configuration

Configured OpenSearch dashboard to visualize logs and alerts.

Verification:

Accessed dashboard via browser on port 5601.

The screenshot shows the Wazuh Agents dashboard interface. At the top, there are three cards: 'STATUS' (with a large circle icon), 'DETAILS' (showing 0 Active, 0 Disconnected, 0 Pending, 2 Never connected, and 0.00% Agents coverage), and 'EVOLUTION' (showing 'Last 24 hours' with no results found). Below these is a table titled 'Agents (2)' containing the following data:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	6604309-Kaushal-G25-InternalServer	10.0.1.5	-	-	v4.14.1	never connected	Details	Edit
002	6604309-Kaushal-G25-WebServer	10.0.2.4	-	-	v4.14.1	never connected	Details	Edit

At the bottom left, there is a search bar with the query 'id!=000 and'. On the right, there are buttons for 'Deploy new agent', 'Refresh', 'Export formatted', 'WQL', and another 'Refresh' button. The bottom right corner shows page navigation controls.

d) Agent Installation & Registration

Installed Wazuh agent and authenticated it with the manager.

Commands Used:

```
sudo apt install wazuh-agent -y
```

```
sudo /var/ossec/bin/agent-auth -m <Manager-IP>
```

Verification:

```
systemctl status wazuh-agent
```

e) Log Monitoring & Alert Generation

System activities were monitored and alerts were generated for security-related events.

4. Vulnerability Detection & Observations

Issue No	Observation	Impact	Status
1	Unauthorized login attempts detected	Brute-force risk	Alert Generated
2	File permission change detected	Integrity violation	Alert Generated
3	Service restart activity logged	Configuration monitoring	Logged

7. Remediation Checklist

Task	Status
Install Wazuh Manager	Completed
Configure Dashboard	Completed
Register Agent	Completed

Enable Log Monitoring	Completed
Generate Alerts	Completed
Maintain Evidence	Completed

8. Summary

Wazuh Manager: Installed and operational

Wazuh Agent: Successfully registered

Dashboard: Accessible and functional

Alerts: Generated and analyzed

Monitoring: Active and real-time

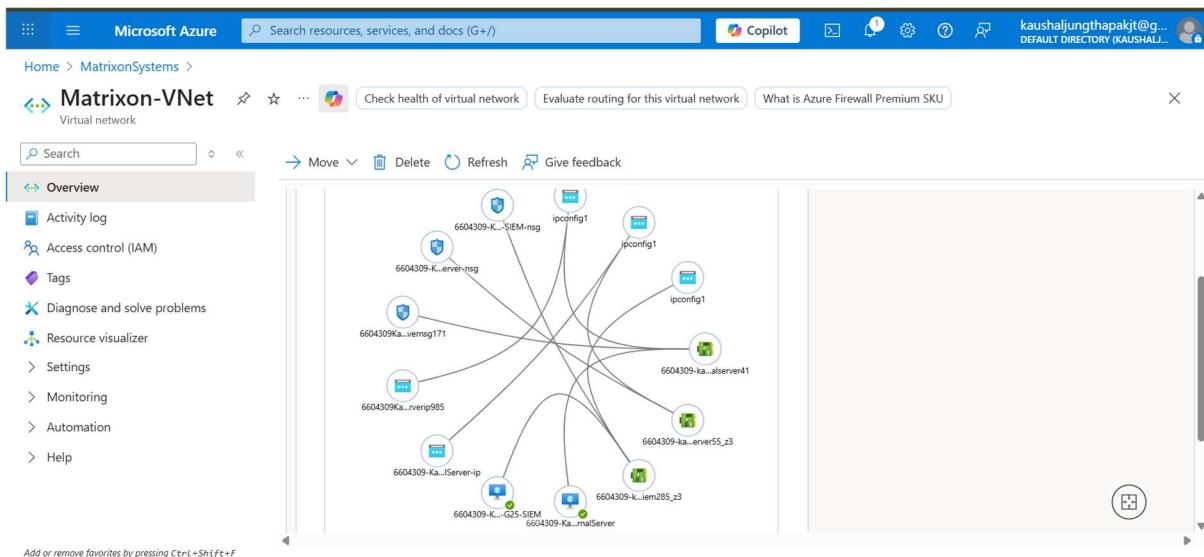
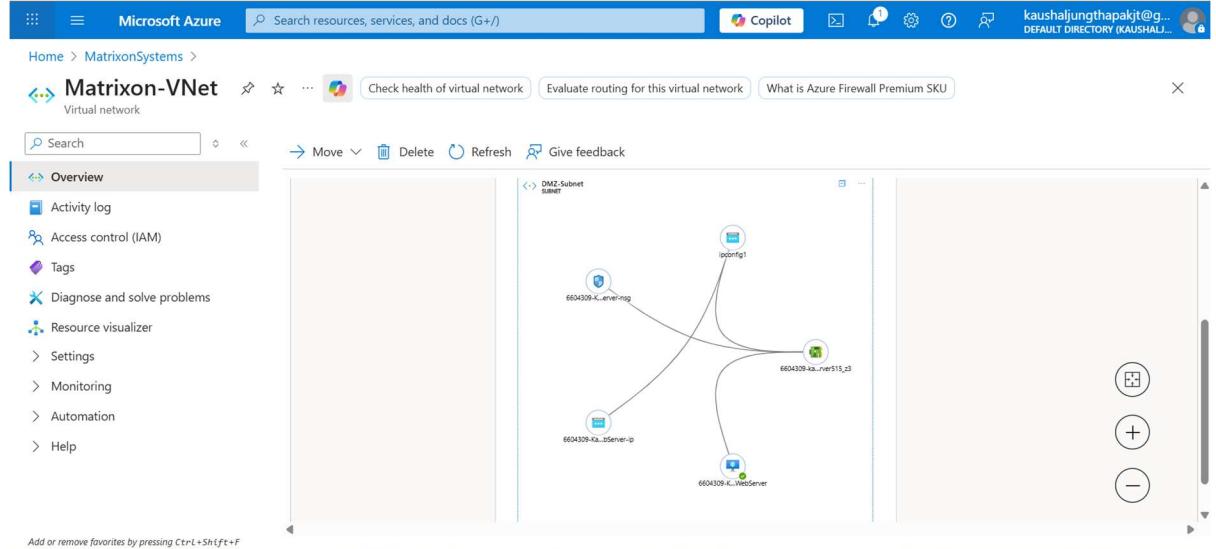
9. Conclusion

This minor project effectively demonstrated the real-world implementation of a SIEM solution based on Wazuh.

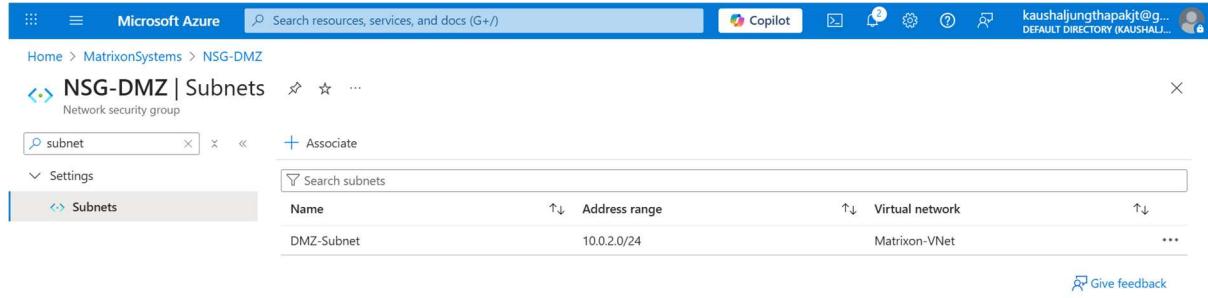
Through practical exercises in log analysis, security monitoring, and alert management, the project enhanced applied knowledge of cybersecurity principles.

10. Supporting Screenshots

Subnets



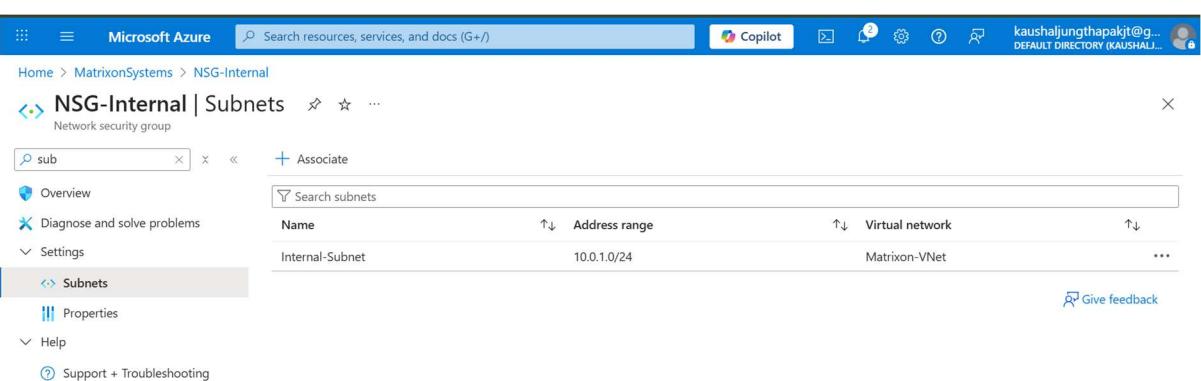
Network Security Groups (NSGs)



The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The top navigation bar includes the Microsoft Azure logo, a search bar, and various account and service icons. The main title is "NSG-DMZ | Subnets". On the left, there's a sidebar with "Subnets" selected under "NSG-DMZ". The main content area displays a table of subnets:

Name	Address range	Virtual network	...
DMZ-Subnet	10.0.2.0/24	Matrixon-VNet	...

A search bar at the top right allows filtering by subnet name. A "Give feedback" link is located at the bottom right.



This screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs), specifically for the "NSG-Internal" group. The top navigation bar and user information are identical to the previous screenshot. The main title is "NSG-Internal | Subnets". The left sidebar shows "Subnets" selected. The main content area displays a table of subnets:

Name	Address range	Virtual network	...
Internal-Subnet	10.0.1.0/24	Matrixon-VNet	...

A search bar at the top right allows filtering by subnet name. A "Give feedback" link is located at the bottom right.

Three Virtual Machines

1) Internal Server

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and user information. Below the navigation is the breadcrumb path 'Home > MatrixonSystems >'. The main content area displays the 'Overview' tab for a virtual machine named '6604309-Kaushal-G25-InternalServer'. The 'Virtual machine' section lists details such as Computer name (6604309-Kaushal-G25-InternalServer), Operating system (Linux (ubuntu 24.04)), VM generation (V2), VM architecture (x64), Agent status (Ready), Agent version (2.15.0.1), Hibernation (Disabled), Host group (-), and Host (-). The 'Networking' section shows a Public IP address (74.225.246.51) and a Private IP address (10.0.1.5), both associated with Network interface 'g25-internalserver41'. The 'Properties' tab is selected.

2) WebServer

The screenshot shows the Microsoft Azure portal interface, similar to the previous one. The top navigation bar and breadcrumb path are identical. The main content area displays the 'Overview' tab for a virtual machine named '6604309-Kaushal-G25-WebServer'. The 'Virtual machine' section lists details such as Computer name (6604309-Kaushal-G25-WebServer), Operating system (Linux (ubuntu 22.04)), VM generation (V2), VM architecture (x64), Agent status (Ready), Agent version (2.15.0.1), Hibernation (Disabled), Host group (-), and Host (-). The 'Networking' section shows a Public IP address (20.193.130.32) and a Private IP address (10.0.2.4), both associated with Network interface 'g25-webserver515_z3'. The 'Properties' tab is selected.

3) SIEM (WAZUH Server)

The screenshot shows the Microsoft Azure portal interface for a virtual machine named "6604309-Kaushal-G25-SIEM". The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, Security, and Backup + disaster recovery. The main content area displays the VM's properties under the "Properties" tab. Key details include:

Virtual machine		Networking	
Computer name	6604309-Kaushal-G25-SIEM	Public IP address	-
Operating system	Linux (ubuntu 24.04)	Private IP address (IPv6)	-
VM generation	V2	Private IP address (IPv6)	10.0.1.6
VM architecture	x64	Virtual network/subnet	Matrixon-VNet/Internal-Subnet
Agent status	Ready	DNS name	-
Agent version	2.15.0.1		
Hibernation	Disabled		
Host group	-		

Below the properties, there are sections for "Size" (Standard B2as v2) and "Monitoring". A note at the top right states: "Your VM has a default outbound IP, which is insecure and will no longer be assigned by default for new subnets after March 2026. To secure your VM and subnets and ensure future compatibility, follow guidance to add an explicit method of outbound and set your subnets to private." Action buttons include Connect, Start, Stop, Hibernate, Capture, Delete, Refresh, Open in mobile, and Feedback.