

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

Wazuh Dashboard

to manager

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

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

Verification:

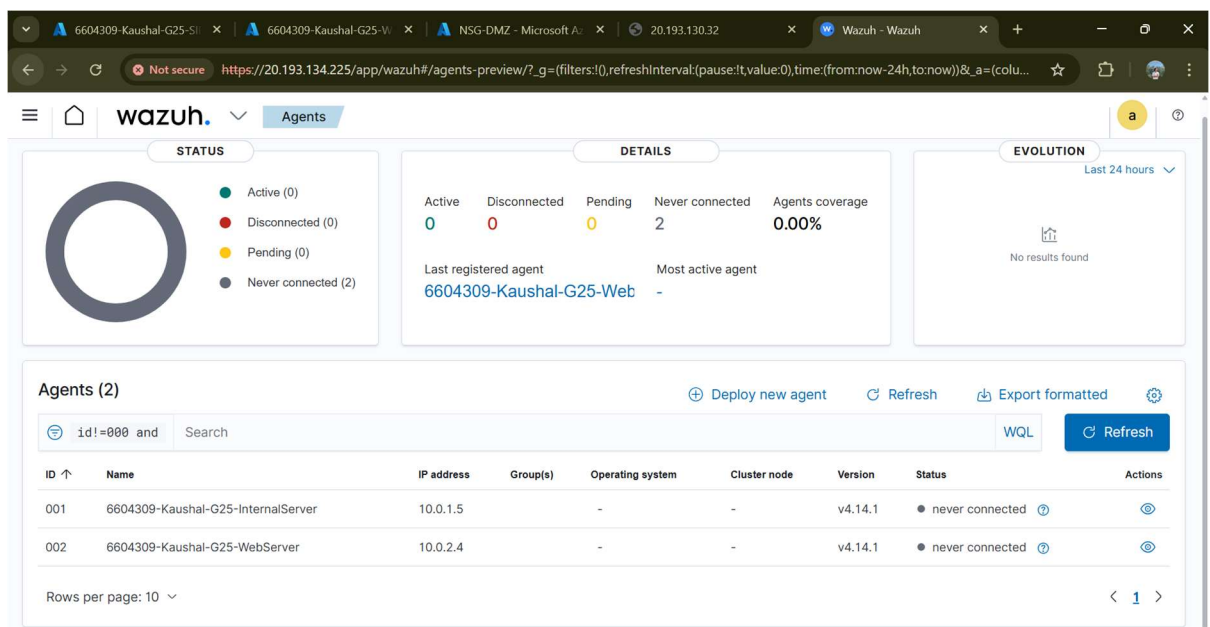
systemctl status wazuh-manager

c) Wazuh Dashboard Configuration

Configured OpenSearch dashboard to visualize logs and alerts.

Verification:

Accessed dashboard via browser on port 5601.



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

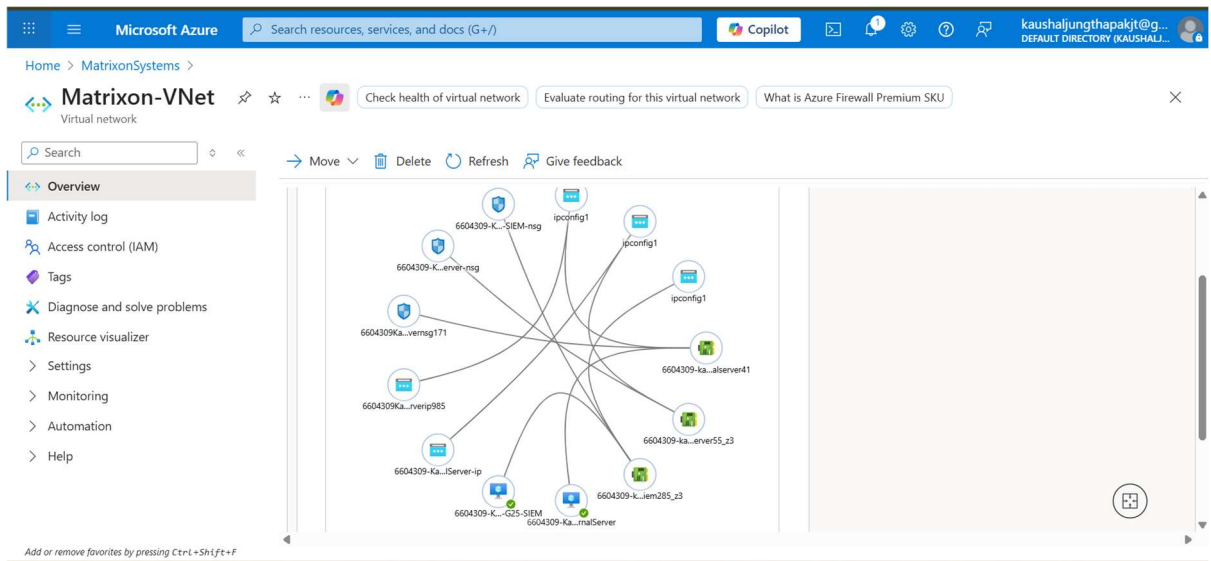
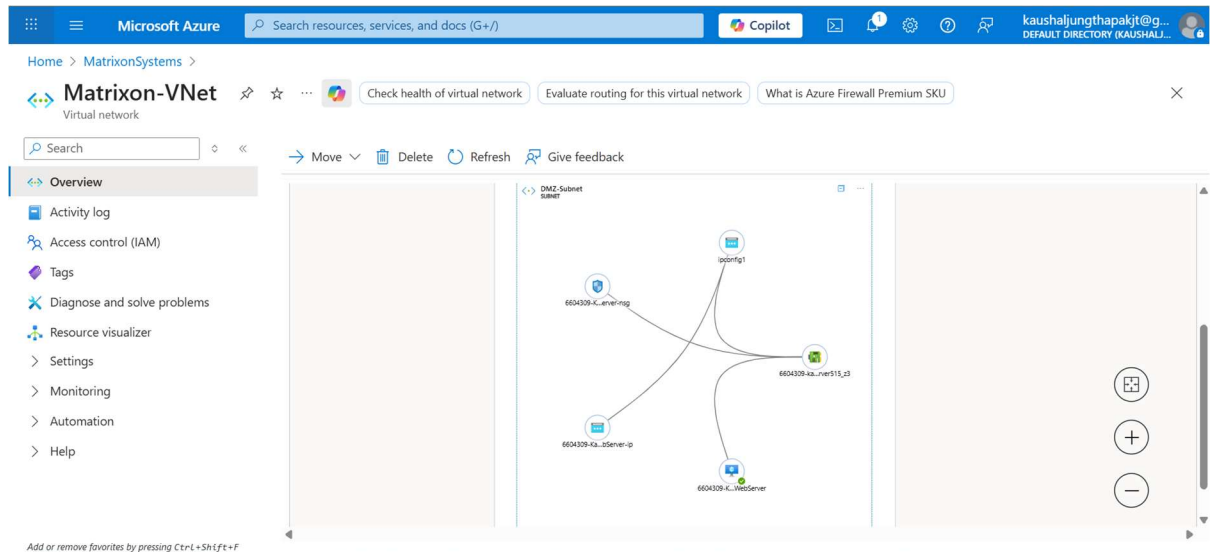
9. Conclusion

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)

Microsoft Azure

Search resources, services, and docs (G+I)

Copilot

kaushaljungthapakit@g...
DEFAULT DIRECTORY (KAUSHALJ...)

Home > MatrixonSystems > NSG-DMZ

NSG-DMZ | Subnets

Network security group

subnet Associate

Settings

Subnets

Search subnets

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

Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Azure

Search resources, services, and docs (G+I)

Copilot

kaushaljungthapakit@g...
DEFAULT DIRECTORY (KAUSHALJ...)

Home > MatrixonSystems > NSG-Internal

NSG-Internal | Subnets

Network security group

sub Associate

Overview

Diagnose and solve problems

Settings

Subnets

Properties

Help

Support + Troubleshooting

Search subnets

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

Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

Three Virtual Machines

1) Internal Server

The screenshot displays the Azure portal interface for a virtual machine. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'kaushaljungthapakjt@g...'. The main header shows the VM name '6604309-Kaushal-G25-InternalServer' and a search bar. The left sidebar lists various management 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 is divided into two panels: 'Virtual machine' and 'Networking'. The 'Virtual machine' panel shows 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' panel shows the Public IP address (74.225.246.51), Private IP address (10.0.1.5), and the Virtual network/subnet (Matrixon-VNet/Internal-Subnet).

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

kaushaljungthapakjt@g...
DEFAULT DIRECTORY (KAUSHALJ...)

Home > MatrixonSystems >

6604309-Kaushal-G25-InternalServer

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Advisor (1 of 6): Use Azure Capacity Reservation for virtual machine (VM) →

Help me copy this VM in any region

Manage this VM with Azure CLI

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback

Properties Monitoring Capabilities (7) Recommendations (6) Tutorials

Virtual machine

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 -

Host -

Networking

Public IP address 74.225.246.51 (Network 6604309-kaushal- interface g25-internalserver41)

1 associated public IPs

Public IP address (IPv6) -

Private IP address 10.0.1.5

Private IP address (IPv6) -

Virtual network/subnet Matrixon-VNet/Internal-Subnet

DNS name Configure

2) WebServer

The screenshot displays the Azure portal interface for a virtual machine. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user profile 'kaushaljungthapakjt@g...'. The main header shows the VM name '6604309-Kaushal-G25-WebServer' and a search bar. The left sidebar lists various management 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 is divided into two panels: 'Virtual machine' and 'Networking'. The 'Virtual machine' panel shows 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' panel shows the Public IP address (20.193.130.32), Private IP address (10.0.2.4), and the Virtual network/subnet (Matrixon-VNet/DMZ-Subnet).

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

kaushaljungthapakjt@g...
DEFAULT DIRECTORY (KAUSHALJ...)

Home > MatrixonSystems >

6604309-Kaushal-G25-WebServer

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Advisor (1 of 6): Use Azure Capacity Reservation for virtual machine (VM) →

Help me copy this VM in any region

Manage this VM with Azure CLI

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback

Properties Monitoring Capabilities (7) Recommendations (6) Tutorials

Virtual machine

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 -

Host -

Networking

Public IP address 20.193.130.32 (Network 6604309-kaushal- interface g25-webserver515_z3)

1 associated public IPs

Public IP address (IPv6) -

Private IP address 10.0.2.4

Private IP address (IPv6) -

Virtual network/subnet Matrixon-VNet/DMZ-Subnet

DNS name Configure

3) SIEM (WAZUH Server)

The screenshot displays the Microsoft Azure portal interface. At the top, the header shows the Microsoft Azure logo, a search bar, and the user's profile (kaushaljungthapakjt@g...). Below the header, the breadcrumb trail indicates the location: Home > MatrixonSystems > 6604309-Kaushal-G25-SIEM. The main content area is titled "Virtual machine" and shows the overview of the VM. A notification banner at the top of the VM page 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." The left sidebar contains a navigation menu with 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 is divided into two columns: "Virtual machine" and "Networking". The "Virtual machine" column lists properties such as Computer name (6604309-Kaushal-G25-SIEM), Operating system (Linux (ubuntu 24.04)), VM generation (V2), VM architecture (x64), Agent status (Ready), Agent version (2.15.0.1), Hibernation (Disabled), and Host group (-). The "Networking" column lists properties such as Public IP address (-), Public IP address (IPv6) (-), Private IP address (10.0.1.6), Private IP address (IPv6) (-), Virtual network/subnet (Matrixon-VNet/Internal-Subnet), and DNS name (-). Below the "Networking" section, the "Size" section shows the VM size as Standard B2as v2.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

kaushaljungthapakjt@g...
DEFAULT DIRECTORY (KAUSHALJ...)

Home > MatrixonSystems > 6604309-Kaushal-G25-SIEM

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Add or remove favorites by pressing Ctrl+Shift+F

Help me copy this VM in any region

Manage this VM with Azure CLI

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.

Help me copy this VM in any region

Connect Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback

Properties Monitoring Capabilities (7) Recommendations Tutorials

Virtual machine

Computer name 6604309-Kaushal-G25-SIEM

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 -

Networking

Public IP address -

Public IP address (IPv6) -

Private IP address 10.0.1.6

Private IP address (IPv6) -

Virtual network/subnet Matrixon-VNet/Internal-Subnet

DNS name -

Size

Size Standard B2as v2