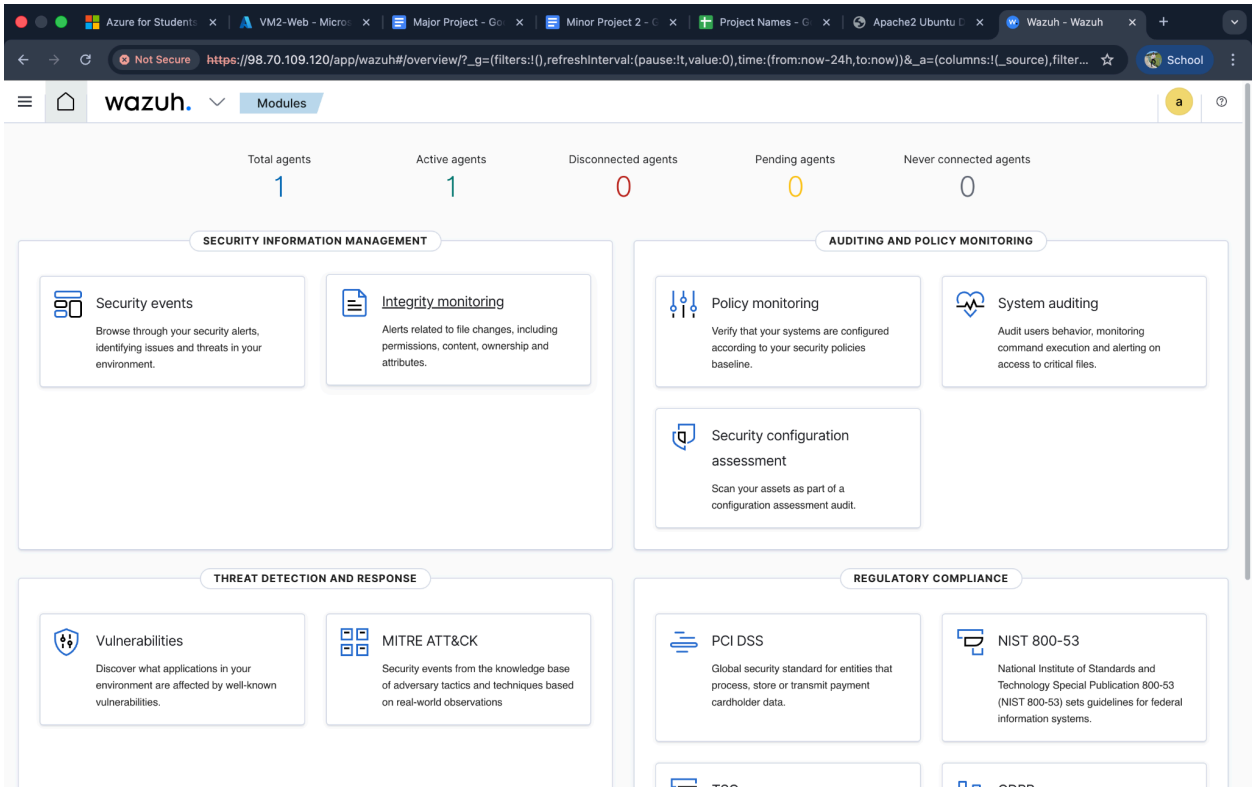
📘 PROJECT REPORT

Implementation of Cloud-Based SIEM Using Wazuh on Microsoft Azure

1. ABSTRACT

In modern cloud environments, continuous monitoring and real-time threat detection are essential to protect systems from cyber-attacks. This project focuses on the **design, deployment, and validation of a Security Information and Event Management (SIEM) solution using Wazuh on Microsoft Azure**.

The system collects logs from multiple virtual machines, analyzes them centrally, and detects suspicious activities such as **authentication failures, brute-force attempts, file integrity violations, and system anomalies**. The effectiveness of the SIEM solution is demonstrated through **attack simulations and real-time alert visualization** using the Wazuh Dashboard.



2. INTRODUCTION

Cloud computing has become the backbone of modern IT infrastructure. However, cloud systems are exposed to various cyber threats such as brute-force attacks, unauthorized access, and insider threats. Traditional security tools are insufficient to detect and correlate such attacks in real time.

A **Security Information and Event Management (SIEM)** system addresses this issue by:

1.Collecting logs from multiple sources
2.Correlating events
3.Detecting anomalies
4.Providing centralized monitoring and alerting
This project implements **Wazuh SIEM**, an open-source security monitoring platform, in a **Microsoft Azure cloud environment**.

4. SYSTEM ARCHITECTURE

4.1 Architecture Overview

The system is designed using a **three-tier architecture** deployed on Microsoft Azure:

1.VM3 – SIEM Server

→ Hosts Wazuh Manager, Wazuh Indexer, and Wazuh Dashboard

2.VM2 – Web Server

→ Public-facing Apache web server

→ Wazuh Agent installed

3.VM1 – Internal Server

→ Internal monitored system

→ Wazuh Agent installed

All virtual machines are deployed within a **custom Azure Virtual Network (VNet)** with **DMZ and Internal subnets**.

Azure for Students | Microsoft | Nexyra-VNet-1766496425710 | Major Project - Google Docs | Minor Project 2 - Google Doc | Project Names - Google Shee

portal.azure.com/?Microsoft_Azure_Education_correlationId=b226f876-3ce7-4c28-a51c-bc94d7d1239d#view/HubsExtension/DeploymentDetailsBlade/...

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | 6604985@rungta.org DEFAULT DIRECTORY (ASHIDEEP...

Home >

Nexyra-VNet-1766496425710 | Overview

Deployment

Search

- Overview
- Inputs
- Outputs
- Template

Delete | Cancel | Redeploy | Download | Refresh

Deployment succeeded

Deployment 'Nexyra-VNet-1766496425710' to resource group 'Nexyra-Technologies' was successful.

Go to resource | Pin to dashboard

Your deployment is complete

Deployment name : Nexyra-VNet-1766496425710
Subscription : Azure for Students
Resource group : Nexyra-Technologies

Start time : 23/12/2025, 18:57:42
Correlation ID : 2c0e948c-f2e8-41e8-8fef-4e75a2b362f7

Deployment details

Next steps

Go to resource

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

Find an Azure expert >

Add or remove favorites by pressing Cmd+Shift+F

Azure for Students | Mic | Nexyra-VNet - Microsof | Major Project - Google | Minor Project 2 - Googl | Project Names - Google | Apache2 Ubuntu Defaul

portal.azure.com/?Microsoft_Azure_Education_correlationId=b226f876-3ce7-4c28-a51c-bc94d7d1239d#@ashideepakoutlook.onmicrosoft.com/resource...

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | 6604985@rungta.org DEFAULT DIRECTORY (ASHIDEEP...

Home >

Nexyra-VNet | Subnets

Virtual network

Check health of virtual network | Diagnose issues with this virtual network | Retrieve detailed routing information for troubleshooting

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Address space
  - Connected devices
  - Subnets
  - Bastion
  - DDoS protection
  - Firewall
  - Microsoft Defender for Cloud

Subnet | Refresh | Manage users | Delete | Export to CSV

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

Search subnets

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
Internal-Subnet	10.0.1.0/24	-	249	-	-	-
DMZ-Subnet	10.0.2.0/24	-	250	-	-	-

Showing 2 subnets

Give feedback

Add or remove favorites by pressing Cmd+Shift+F

Switch to PowerShell | Restart | Manage files | New session | Editor | Web preview | Settings | Help

```
Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
deepak [ ~ ]$ sudo systemctl status apache2
sudo: The "no new privileges" flag is set, which prevents sudo from running as root.
sudo: If sudo is running in a container, you may need to adjust the container configuration to disable the flag.
deepak [ ~ ]$
```

Azure for Students | Microsoft | VM1-Internal - Microsoft Azure | Major Project - Google Docs | Minor Project 2 - Google Doc | Project Names - Google Shee

portal.azure.com/?Microsoft_Azure_Education_correlationId=b226f876-3ce7-4c28-a51c-bc94d7d1239d#@ashideepakoutlook.onmicrosoft.com/resource...

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | 6604985@rungta.org DEFAULT DIRECTORY (ASHIDEEP...

Home >

VM1-Internal
Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh | Open in mobile | Feedback | CLI / PS

Essentials JSON View

Resource group (move)	: Nexyra-Technologies	Operating system	: Linux (ubuntu 22.04)
Status	: Running	Size	: Standard B2ats v2 (2 vcpus, 1 GiB memory)
Location	: Central India	Primary NIC public IP	: 74.225.170.199
Subscription (move)	: Azure for Students		1 associated public IPs
Subscription ID	: f792c2f8-da86-4c66-b267-b1cb12113ecb	Virtual network/subnet	: Nexyra-VNet/Internal-Subnet
		DNS name	: Not configured
		Health state	: -
		Time created	: 23/12/2025, 15:40 UTC

Tags (edit) : Add tags

Properties | Monitoring | Capabilities (7) | Recommendations | Tutorials

Virtual machine

Computer name	VM1-Internal
Operating system	Linux (ubuntu 22.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.15.0.1
Hibernation	Disabled

Networking

Public IP address	74.225.170.199 (Network interface vm1-internal703)
	1 associated public IPs
Public IP address (IPv6)	-
Private IP address	10.0.1.4
Private IP address (IPv6)	-
Virtual network/subnet	Nexyra-VNet/Internal-Subnet
DNS name	Configure

Add or remove favorites by pressing Cmd+Shift+F

Azure for Students | Microsoft | VM2-Web - Microsoft Azure | Major Project - Google Docs | Minor Project 2 - Google Doc | Project Names - Google Shee

portal.azure.com/?Microsoft_Azure_Education_correlationId=b226f876-3ce7-4c28-a51c-bc94d7d1239d#@ashideepakoutlook.onmicrosoft.com/re...

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | 6604985@rungta.org DEFAULT DIRECTORY (ASHIDEEP...

Home >

VM2-Web
Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh | Open in mobile | Feedback | CLI / PS

Essentials JSON View

Resource group (move)	: Nexyra-Technologies	Operating system	: Linux (ubuntu 22.04)
Status	: Running	Size	: Standard B2ats v2 (2 vcpus, 1 GiB memory)
Location	: Central India	Primary NIC public IP	: 4.213.59.253
Subscription (move)	: Azure for Students		1 associated public IPs
Subscription ID	: f792c2f8-da86-4c66-b267-b1cb12113ecb	Virtual network/subnet	: Nexyra-VNet/DMZ-Subnet
		DNS name	: Not configured
		Health state	: -
		Time created	: 23/12/2025, 15:51 UTC

Tags (edit) : Add tags

Properties | Monitoring | Capabilities (7) | Recommendations | Tutorials

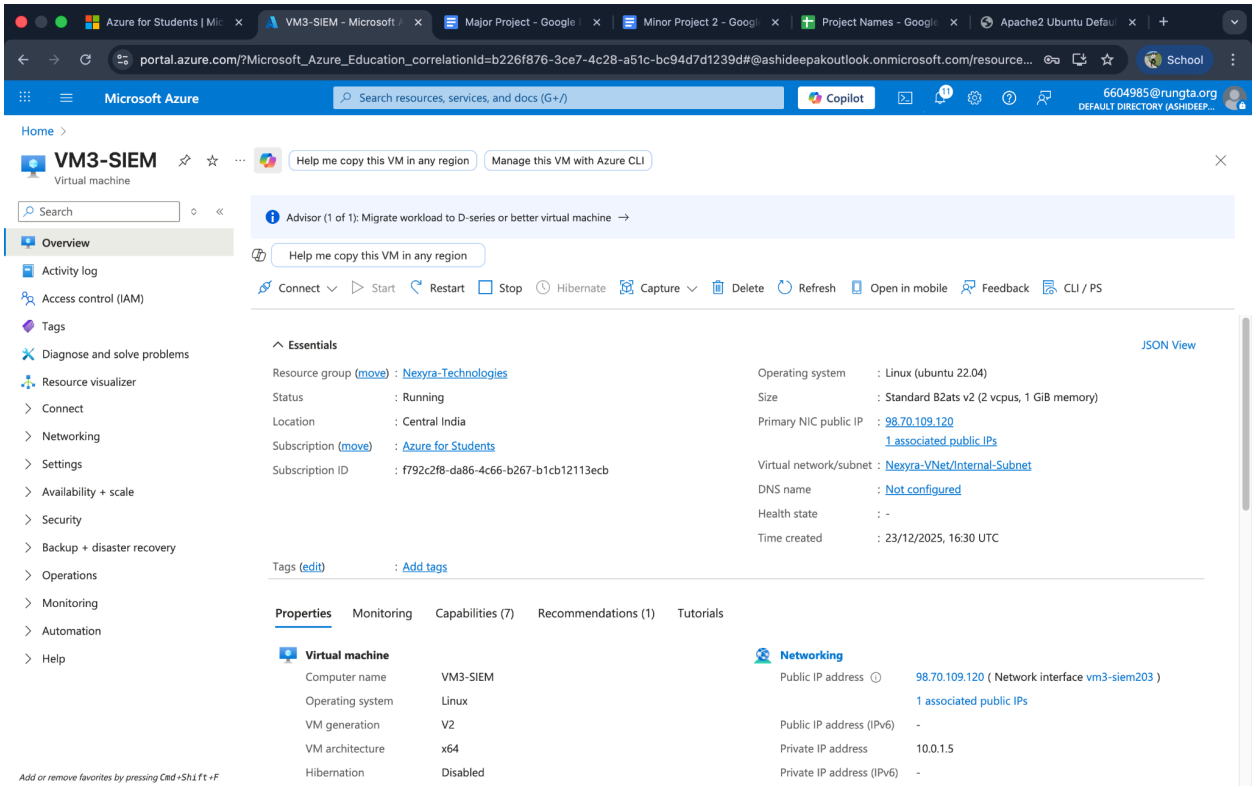
Virtual machine

Computer name	VM2-Web
Operating system	Linux (ubuntu 22.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.15.0.1
Hibernation	Disabled

Networking

Public IP address	4.213.59.253 (Network interface vm2-web117)
	1 associated public IPs
Public IP address (IPv6)	-
Private IP address	10.0.2.4
Private IP address (IPv6)	-
Virtual network/subnet	Nexyra-VNet/DMZ-Subnet
DNS name	Configure

Add or remove favorites by pressing Cmd+Shift+F



4.2 Architecture Flow

Attack Activity

↓

Wazuh Agent (VM2-Web / VM1-Internal)

↓

Wazuh Manager (VM3-SIEM)

↓

Wazuh Indexer (OpenSearch)

↓

Wazuh Dashboard (Visualization & Alerts)

5. TOOLS AND TECHNOLOGIES USED

Technology	Description
Microsoft Azure	Cloud platform
Ubuntu 22.04 LTS	Operating system
Wazuh SIEM	Security monitoring
Wazuh Agent	Log collection

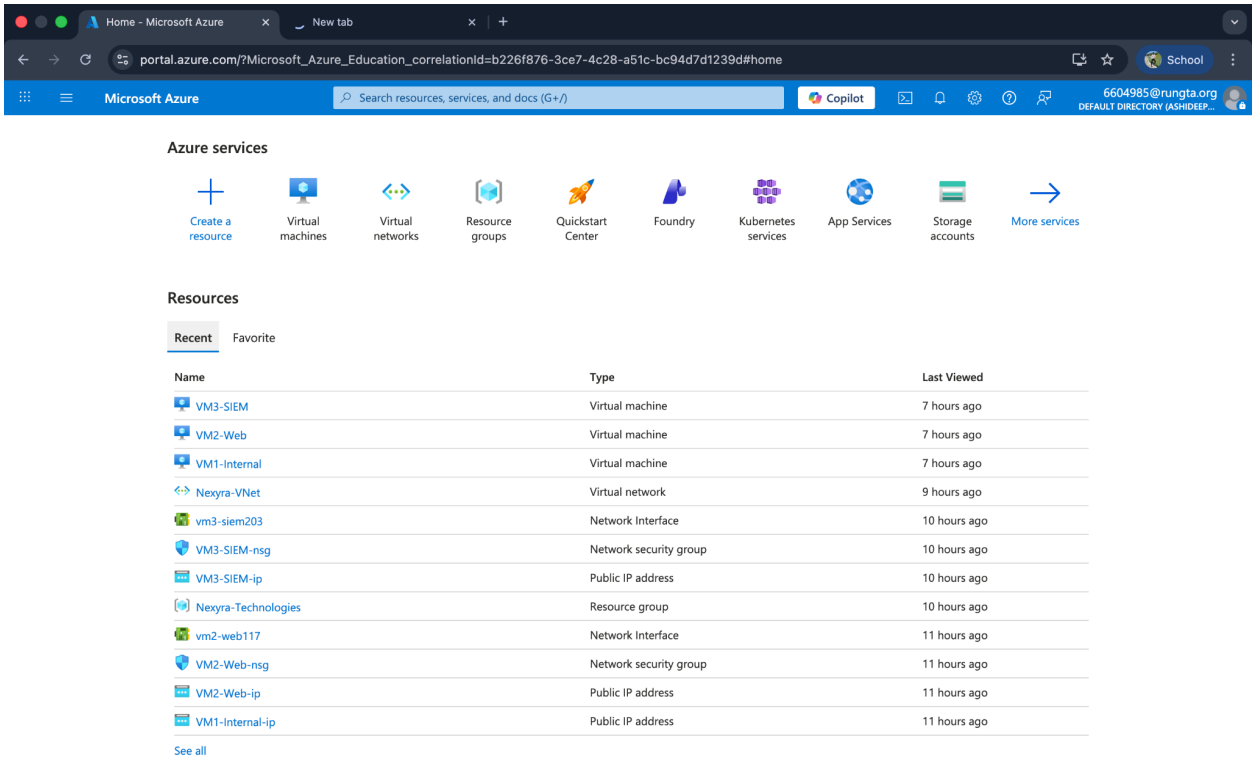
OpenSearch	**Log indexing**
Apache Web Server	**Target service**
SSH	**Secure remote access**
MITRE ATT&CK	**Threat classification**

6. IMPLEMENTATION DETAILS

6.1 Azure Infrastructure Setup

Three Ubuntu virtual machines were created using the Azure portal. Network Security Groups (NSGs) were configured to allow:

- **SSH (Port 22)**
- **HTTPS (Port 443)**
- **Wazuh Dashboard (Port 5601)**



6.2 Wazuh SIEM Installation

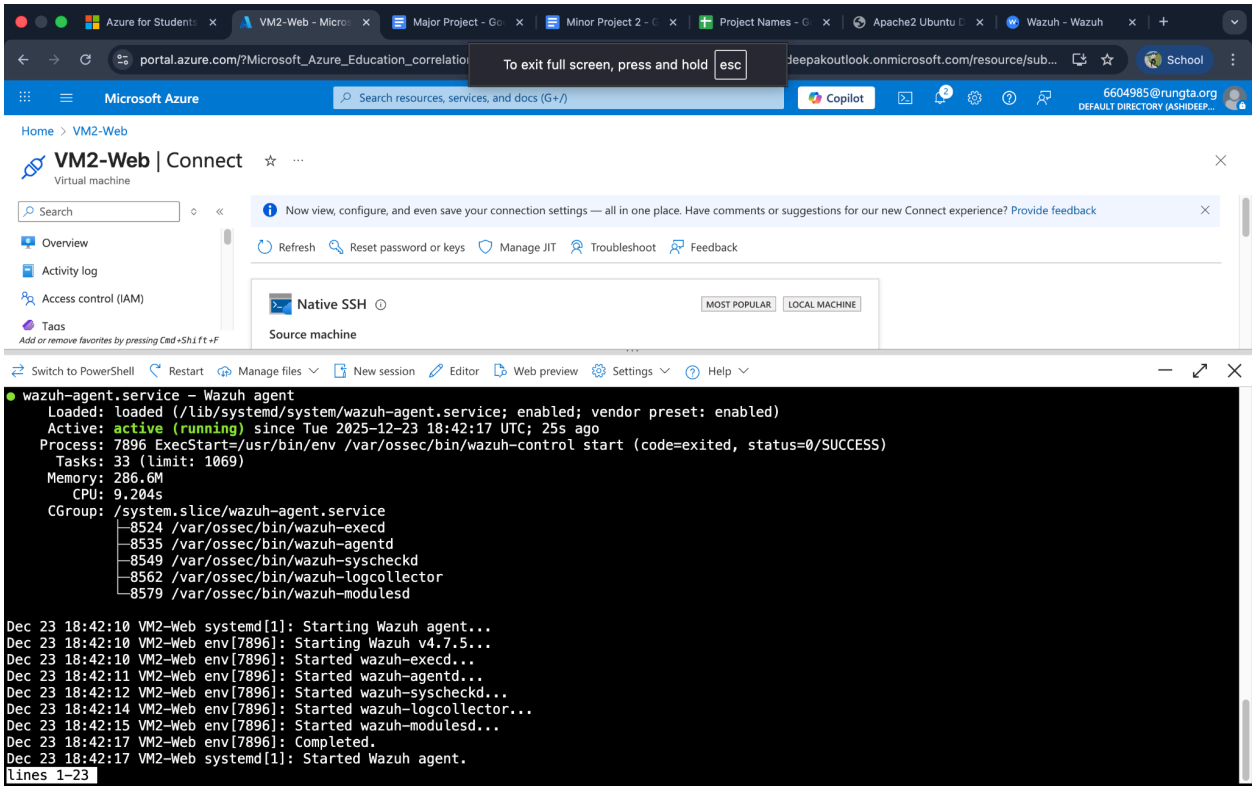
Wazuh was installed on VM3-SIEM using the official installation script. The installation included:

- **Wazuh Manager**
- **Wazuh Indexer**
- **Wazuh Dashboard**

All services were verified using `systemctl`.

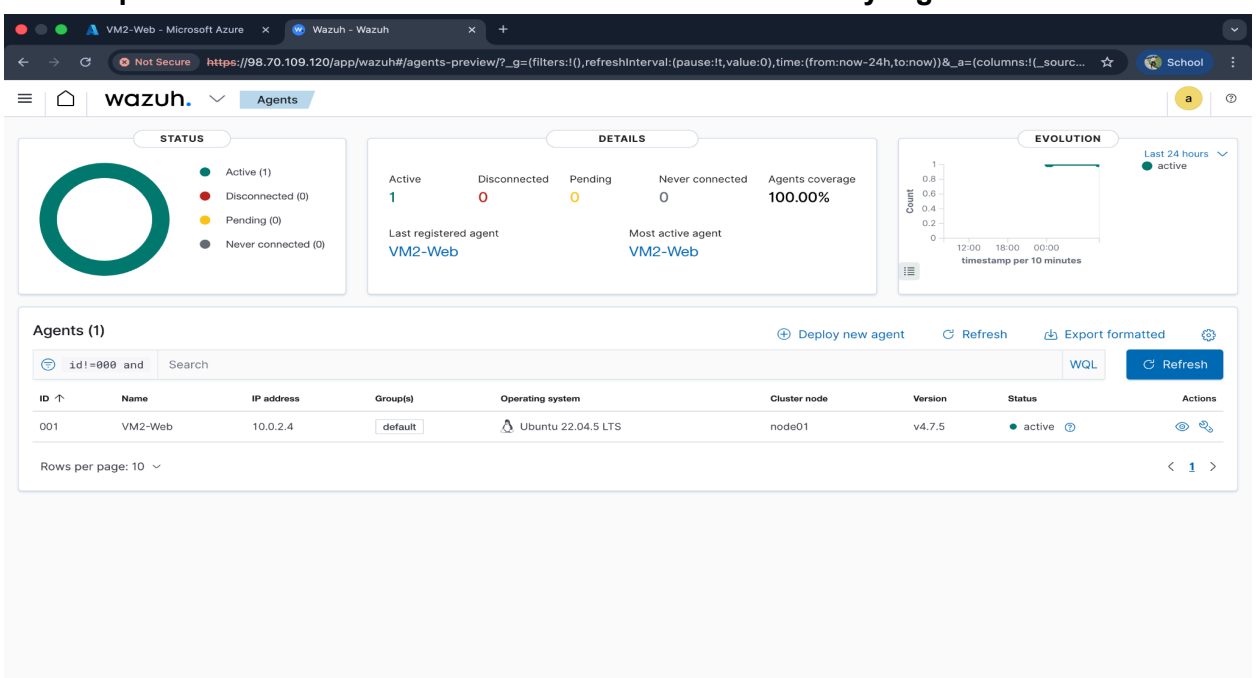
6.3 Agent Installation and Registration

Wazuh Agents were installed on VM2-Web and VM1-Internal. Each agent was configured with the private IP address of the SIEM server and successfully registered.



6.3 Agent Installation and Registration

Wazuh Agents were installed on VM2-Web and VM1-Internal. Each agent was configured with the private IP address of the SIEM server and successfully registered.



7. ATTACK SIMULATION

7.1 SSH Brute-Force Simulation

Multiple failed SSH login attempts were generated to simulate a brute-force attack. These attempts triggered authentication failure alerts.

Command - ssh fakeuser@localhost

```
2025/12/23 18:43:07 rootcheck: INFO: Ending rootcheck scan.
azureuser@VM2-Web:~$ ssh fakeuser@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:W++AUy1DVjnhFwQld6OkQnOSaMAm5UVWwt1wkZr00Vs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? ssh fakeuser@localhost
Please type 'yes', 'no' or the fingerprint:
Host key verification failed.
azureuser@VM2-Web:~$ ssh fakeuser@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:W++AUy1DVjnhFwQld6OkQnOSaMAm5UVWwt1wkZr00Vs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
fakeuser@localhost: Permission denied (publickey,password).
azureuser@VM2-Web:~$
```

7.2 File Integrity Monitoring (FIM)

Unauthorized file creation and modification were performed to test file integrity monitoring.

sudo touch /etc/hacked_by_student
sudo echo "attack simulation" >> /etc/hacked_by_student

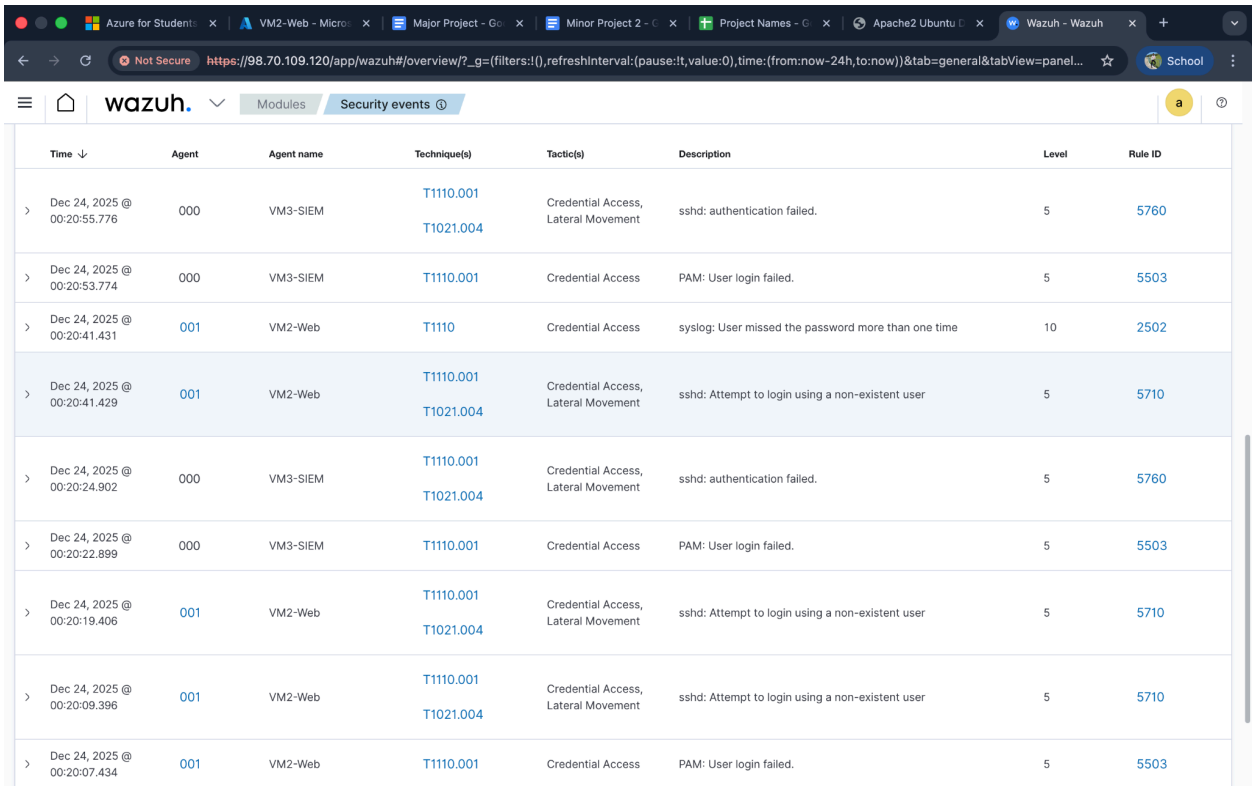
8. DETECTION AND MONITORING

All attack activities were successfully detected by Wazuh. Alerts were visible in:

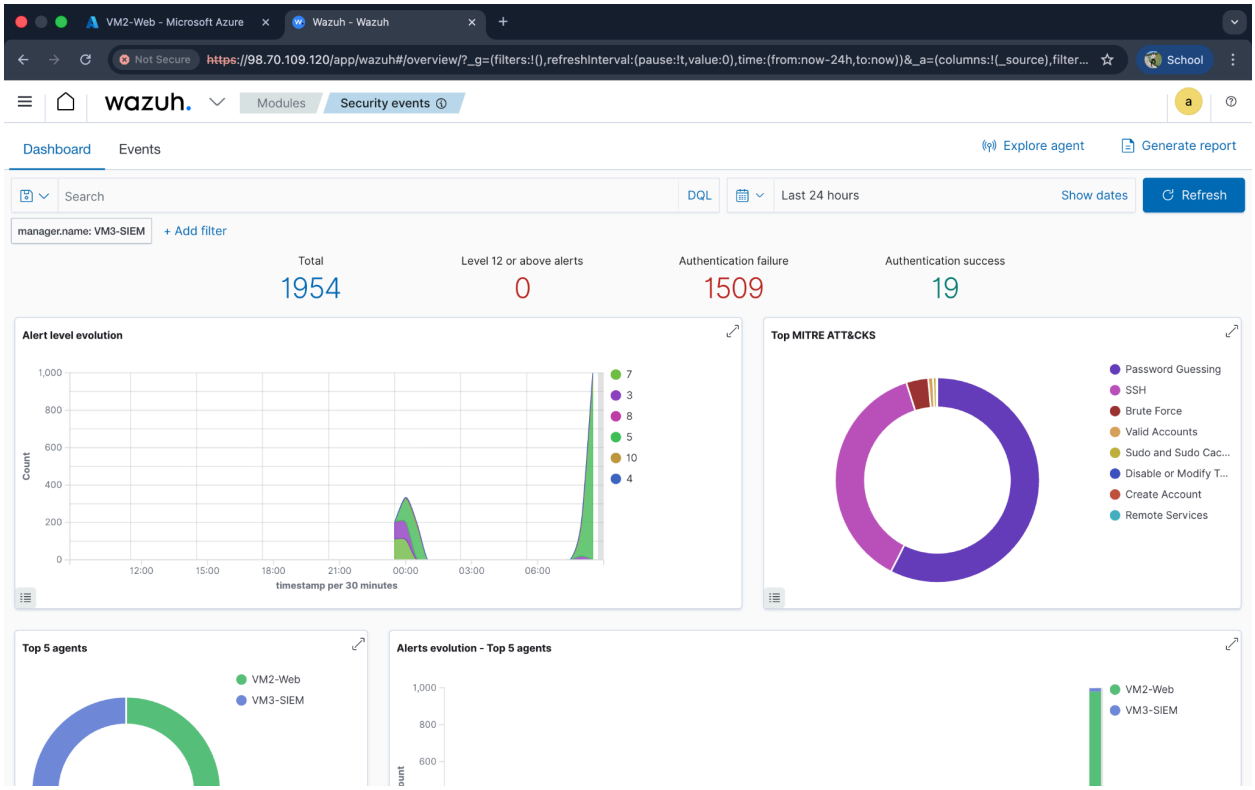
- Security Events
- Discover
- Integrity Monitoring

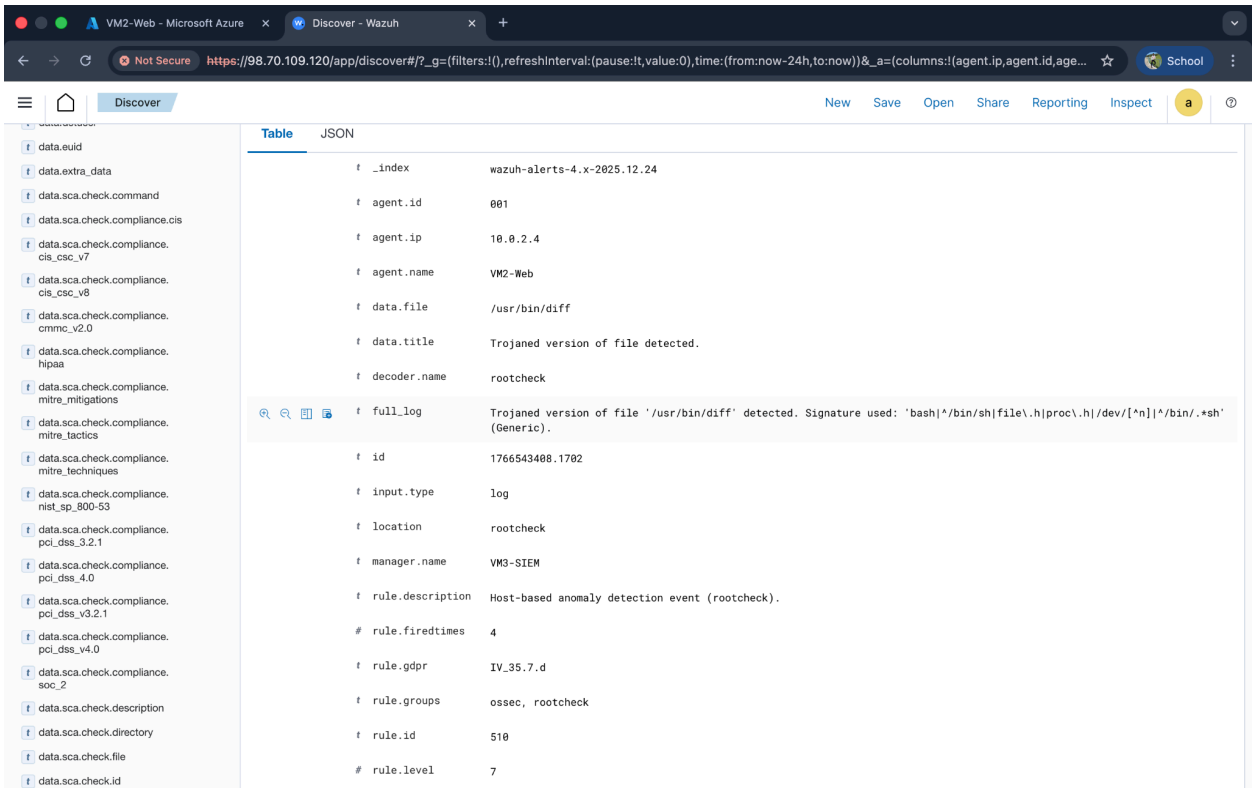
Detected events included:

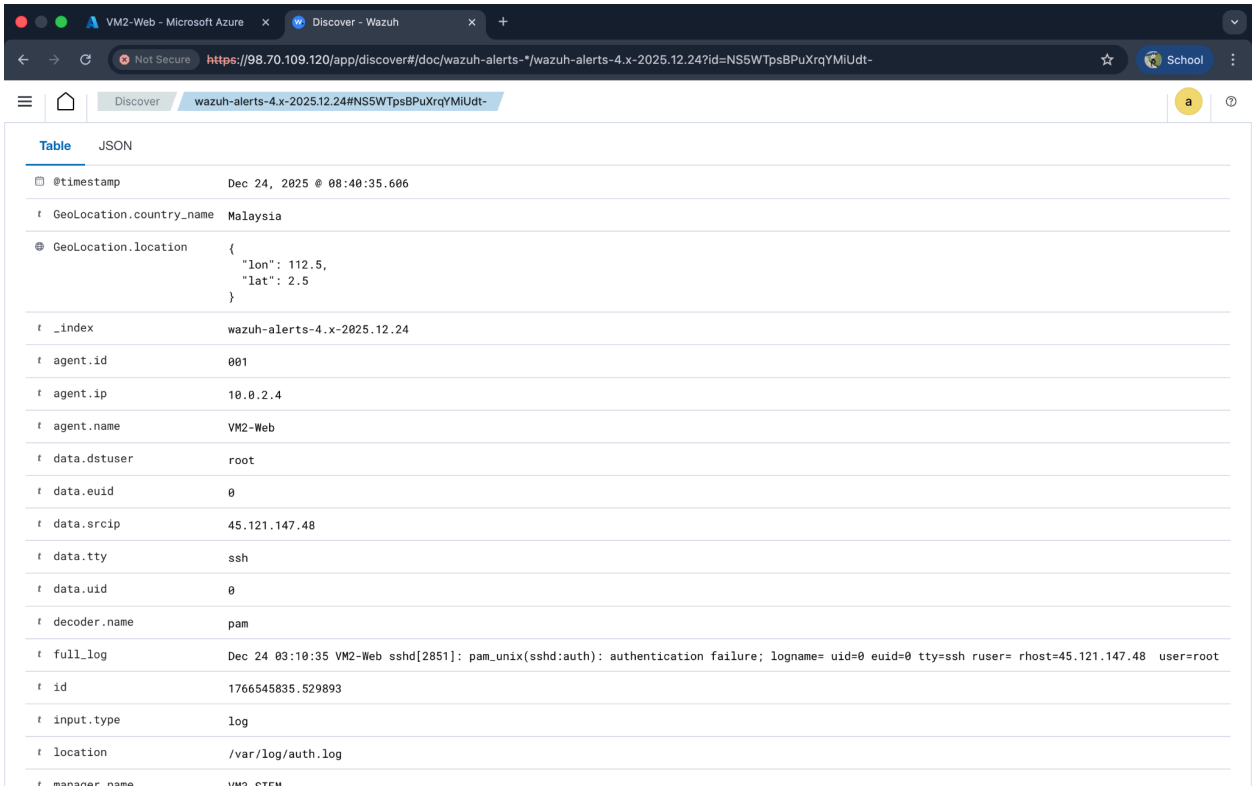
- Authentication failures
- SSH brute-force attempts
- Rootcheck alerts
- File integrity violations



Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Dec 24, 2025 @ 00:20:55.776	000	VM3-SIEM	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
Dec 24, 2025 @ 00:20:53.774	000	VM3-SIEM	T1110.001	Credential Access	PAM: User login failed.	5	5503
Dec 24, 2025 @ 00:20:41.431	001	VM2-Web	T1110	Credential Access	syslog: User missed the password more than one time	10	2502
Dec 24, 2025 @ 00:20:41.429	001	VM2-Web	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 00:20:24.902	000	VM3-SIEM	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
Dec 24, 2025 @ 00:20:22.899	000	VM3-SIEM	T1110.001	Credential Access	PAM: User login failed.	5	5503
Dec 24, 2025 @ 00:20:19.406	001	VM2-Web	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 00:20:09.396	001	VM2-Web	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710
Dec 24, 2025 @ 00:20:07.434	001	VM2-Web	T1110.001	Credential Access	PAM: User login failed.	5	5503


VM2-Web - Microsoft Azure
Wazuh - Wazuh
Not Secure
https://98.70.109.120/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filter...
School
wazuh.
Modules
Security events
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: VM3-SIEM
+ Add filter
Total
1954
Level 12 or above alerts
0
Authentication failure
1509
Authentication success
19
Alert level evolution
Count
timestamp per 30 minutes
Top MITRE ATT&CKS
Password Guessing
SSH
Brute Force
Valid Accounts
Sudo and Sudo Cac...
Disable or Modify T...
Create Account
Remote Services
Top 5 agents
VM2-Web
VM3-SIEM
Alerts evolution - Top 5 agents


VM2-Web - Microsoft Azure
Discover - Wazuh
Not Secure
https://98.70.109.120/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(agent.ip,agent.id,age...
School
Discover
New
Save
Open
Share
Reporting
Inspect
Table
JSON
data.euid
data.extra_data
data.sca.check.command
data.sca.check.compliance.cis
data.sca.check.compliance.cis_csc_v7
data.sca.check.compliance.cis_csc_v8
data.sca.check.compliance.cmmc_v2.0
data.sca.check.compliance.hipaa
data.sca.check.compliance.mitre_mitigations
data.sca.check.compliance.mitre_tactics
data.sca.check.compliance.mitre_techniques
data.sca.check.compliance.nist_sp_800-53
data.sca.check.compliance.pci_dss_3.2.1
data.sca.check.compliance.pci_dss_4.0
data.sca.check.compliance.pci_dss_v3.2.1
data.sca.check.compliance.pci_dss_v4.0
data.sca.check.compliance.soc_2
data.sca.check.description
data.sca.check.directory
data.sca.check.file
data.sca.check.id
_index wazuh-alerts-4.x-2025.12.24
agent.id 001
agent.ip 10.0.2.4
agent.name VM2-Web
data.file /usr/bin/diff
data.title Trojaned version of file detected.
decoder.name rootcheck
full_log Trojaned version of file '/usr/bin/diff' detected. Signature used: 'bash|^/bin/sh|file\.h|proc\.h|/dev/[^n]|^/bin/.*sh' (Generic).
id 1766543408.1702
input.type log
location rootcheck
manager.name VM3-SIEM
rule.description Host-based anomaly detection event (rootcheck).
rule.firedtimes 4
rule.gdpr IV_35.7.d
rule.groups ossec, rootcheck
rule.id 510
rule.level 7



9. RESULTS AND OBSERVATIONS

- Centralized monitoring was achieved
- Real-time alerts were generated
- Attack sources were identified with IP and geo-location
- SIEM effectively detected simulated attacks

---

10. ADVANTAGES OF THE SYSTEM

- Real-time security monitoring
- Centralized log analysis
- Open-source and cost-effective
- Scalable cloud deployment
- MITRE-based threat classification

---

11. LIMITATIONS

- Requires sufficient system resources
- Initial configuration complexity
- Manual alert tuning required

---

12. FUTURE SCOPE

- Automated incident response
- Email/SMS alerting
- Integration with IDS tools (Suricata)
- Machine learning-based anomaly detection

---

13. CONCLUSION

This project successfully demonstrates a **cloud-based SIEM implementation using Wazuh on Microsoft Azure**. Through real attack simulations and alert analysis, the system proves its capability to monitor, detect, and analyze security threats in a modern cloud environment.

---

14. REFERENCES

1. https://documentation.wazuh.com
2. https://learn.microsoft.com/azure
3. https://attack.mitre.org