Implementation of a Cloud-Based SIEM Using Wazuh on Microsoft Azure

Subtitle: Real-Time Threat Detection and Security Monitoring in the Cloud
Presented By: Shwetank
Organization: Rungta University

1. Abstract

In today's cloud-based infrastructures, continuous security monitoring and rapid threat identification are critical for safeguarding systems against cyber threats. This project presents the implementation, configuration, and evaluation of a cloud-based Security Information and Event Management (SIEM) solution using Wazuh on the Microsoft Azure platform.

The deployed system aggregates logs from multiple virtual machines and performs centralized analysis to identify malicious activities such as repeated authentication failures, brute-force login attempts, file integrity breaches, and abnormal system behavior. The performance and reliability of the SIEM solution are validated through controlled attack simulations and real-time alert visualization using the Wazuh Dashboard.

2. Introduction

Cloud computing has become a fundamental component of modern IT environments. Despite its advantages, cloud infrastructure faces increasing security risks, including brute-force attacks, unauthorized access attempts, and internal security threats. Conventional security tools often operate independently and lack the capability to correlate events across multiple systems in real time.

A Security Information and Event Management (SIEM) system overcomes these limitations by:

1. Aggregating logs from diverse sources

2. Correlating security events

3. Detecting suspicious patterns and anomalies

4. Offering centralized visibility and alerting

This project focuses on deploying Wazuh, an open-source SIEM platform, to provide comprehensive security monitoring and real-time threat detection within a cloud environment.
Presentation Title

Slide 1: Abstract & Overview

The objective of this project is to design and deploy a Security Information and Event Management (SIEM) system using Wazuh on Microsoft Azure.
The system performs centralized log collection, correlation, and real-time threat detection across multiple cloud-based virtual machines.

The project successfully demonstrates:

Detection of brute-force authentication attacks

Identification of rootkit and integrity violations

Geo-location tracking of threat sources using IP intelligence

---

Slide 2: Problem Statement

Cloud environments are increasingly vulnerable to:

Brute-force login attempts

Unauthorized access

Lateral movement attacks

Traditional security tools often:

Work in isolation

Lack centralized visibility

Fail to correlate logs in real time

Proposed Solution:
Deploy a centralized SIEM (Wazuh) to aggregate logs from multiple servers, analyze events, and map detected attacks to the MITRE ATT&CK framework.

Slide 3: System Architecture

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

VM3 – SIEM Server

Wazuh Manager

Wazuh Dashboard

VM2 – Web Server

Public-facing

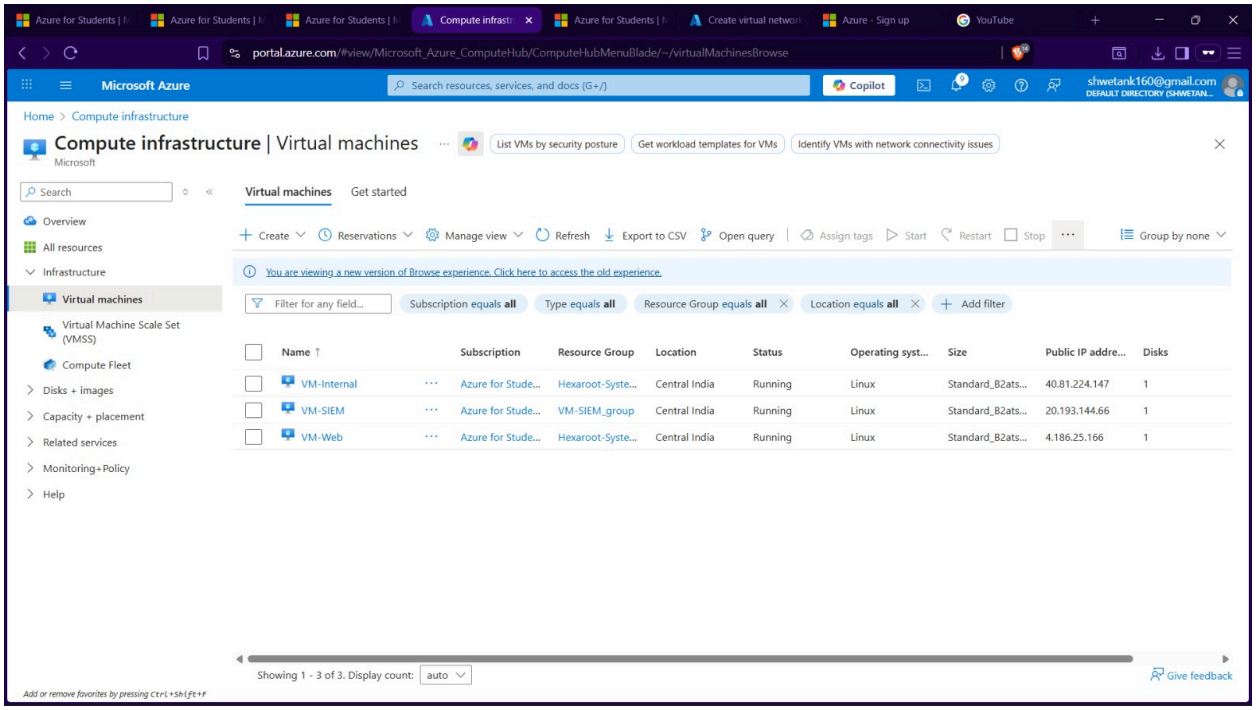
Wazuh Agent installed

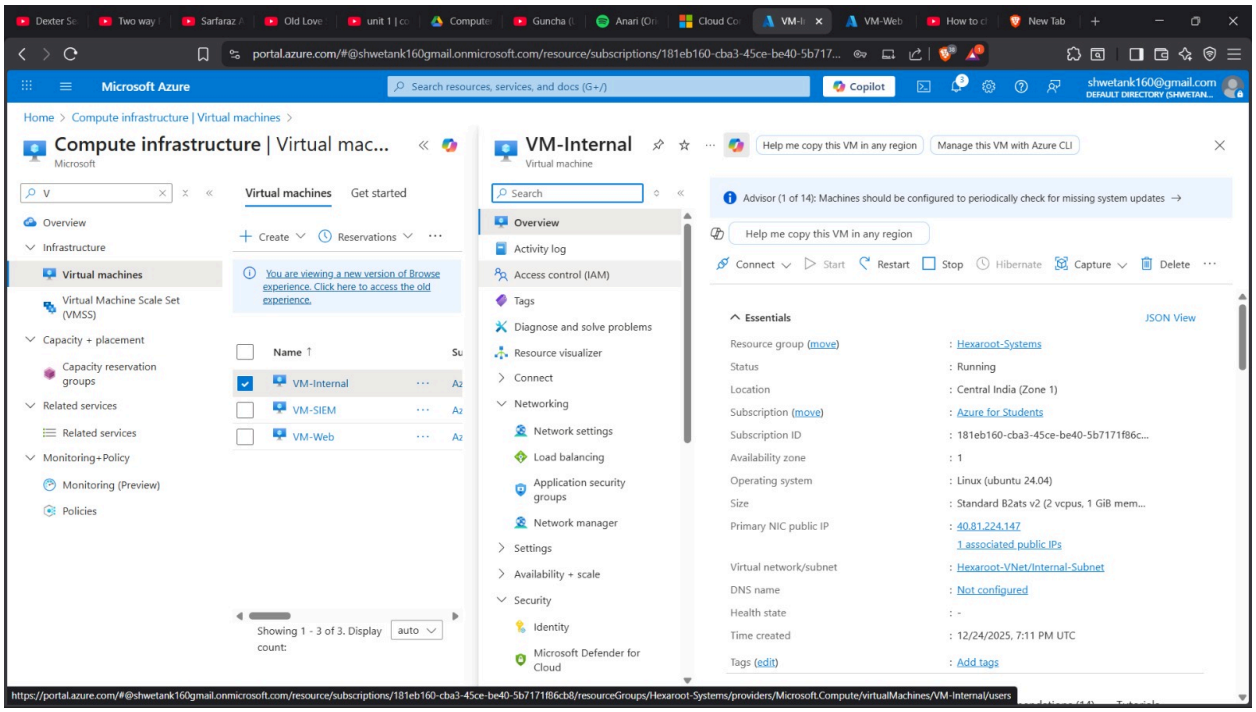
VM1 – Internal Server

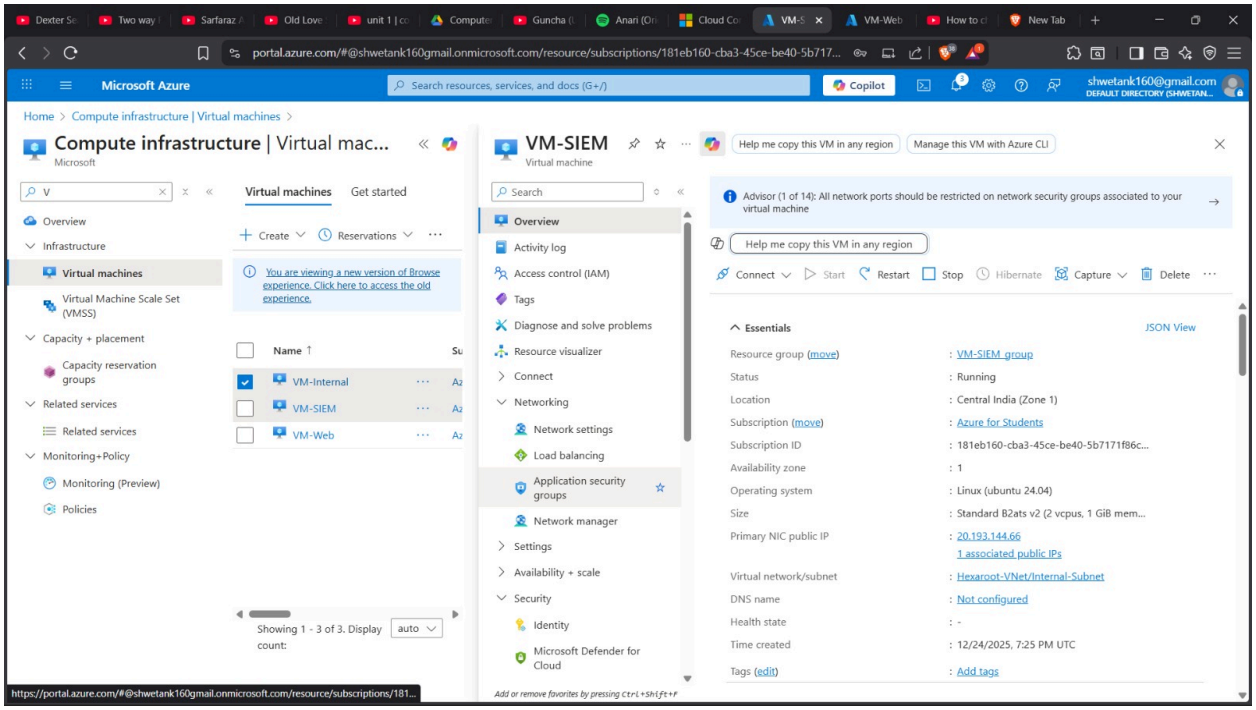
Internal services

Wazuh Agent installed

Data Flow:
Agents collect logs → Manager analyzes events → Dashboard visualizes alerts


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shwetank160@gmail.com
DEFAULT DIRECTORY (SHWETAN...
Home > Compute infrastructure
Compute infrastructure | Virtual machines
Microsoft
List VMs by security posture
Get workload templates for VMs
Identify VMs with network connectivity issues
Search
Overview
All resources
Infrastructure
Virtual machines
Virtual Machine Scale Set (VMSS)
Compute Fleet
Disks + images
Capacity + placement
Related services
Monitoring+Policy
Help
Virtual machines
Get started
Create
Reservations
Manage view
Refresh
Export to CSV
Open query
Assign tags
Start
Restart
Stop
Group by none
You are viewing a new version of Browse experience. Click here to access the old experience.
Filter for any field...
Subscription equals all
Type equals all
Resource Group equals all
Location equals all
Add filter
Name
Subscription
Resource Group
Location
Status
Operating syst...
Size
Public IP addre...
Disks
VM-Internal
Azure for Stude...
Hexaroot-Syste...
Central India
Running
Linux
Standard_B2ats...
40.81.224.147
1
VM-SIEM
Azure for Stude...
VM-SIEM_group
Central India
Running
Linux
Standard_B2ats...
20.193.144.66
1
VM-Web
Azure for Stude...
Hexaroot-Syste...
Central India
Running
Linux
Standard_B2ats...
4.186.25.166
1
Showing 1 - 3 of 3. Display count: auto
Give feedback
Add or remove favorites by pressing Ctrl+Shift+F


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
shwetank160@gmail.com
DEFAULT DIRECTORY (SHWETAN...
Home > Compute infrastructure | Virtual machines >
Compute infrastructure | Virtual mac...
Microsoft
Virtual machines
Get started
Create
Reservations
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
VM-Internal
VM-SIEM
VM-Web
Showing 1 - 3 of 3. Display count: auto
VM-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
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Security
Identity
Microsoft Defender for Cloud
Advisor (1 of 14): Machines should be configured to periodically check for missing system updates
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Essentials
JSON View
Resource group (move) : Hexaroot-Systems
Status : Running
Location : Central India (Zone 1)
Subscription (move) : Azure for Students
Subscription ID : 181eb160-cba3-45ce-be40-5b7171f86c...
Availability zone : 1
Operating system : Linux (ubuntu 24.04)
Size : Standard B2ats v2 (2 vcpus, 1 GiB mem...
Primary NIC public IP : 40.81.224.147
1 associated public IPs
Virtual network/subnet : Hexaroot-VNet/Internal-Subnet
DNS name : Not configured
Health state : -
Time created : 12/24/2025, 7:11 PM UTC
Tags (edit) : Add tags
https://portal.azure.com/#@shwetank160gmail.onmicrosoft.com/resource/subscriptions/181eb160-cba3-45ce-be40-5b7171f86cb8/resourceGroups/Hexaroot-Systems/providers/Microsoft.Compute/virtualMachines/VM-Internal/users



Slide 4: Implementation – Agent Configuration

Wazuh agents were installed on both:

VM-Web

VM-Internal

Implementation steps:

Agent service started using
systemctl start wazuh-agent

Connectivity verified with the SIEM manager

Result:
The agent status showed “Active (running)”, confirming successful registration and communication with the manager.

Slide 5: Attack Simulation – Brute-Force

To test detection capability, a brute-force SSH attack was simulated on the web server.

Methodology:

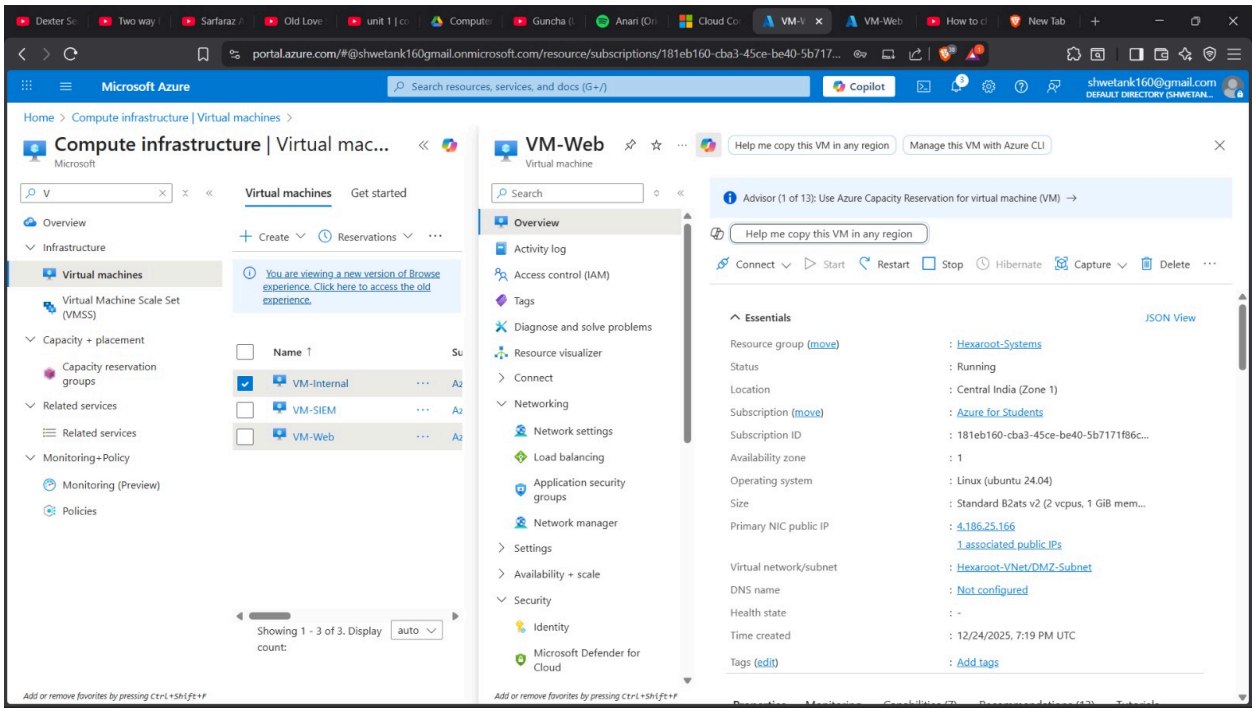
Repeated SSH login attempts using invalid credentials
ssh fakeuser@localhost

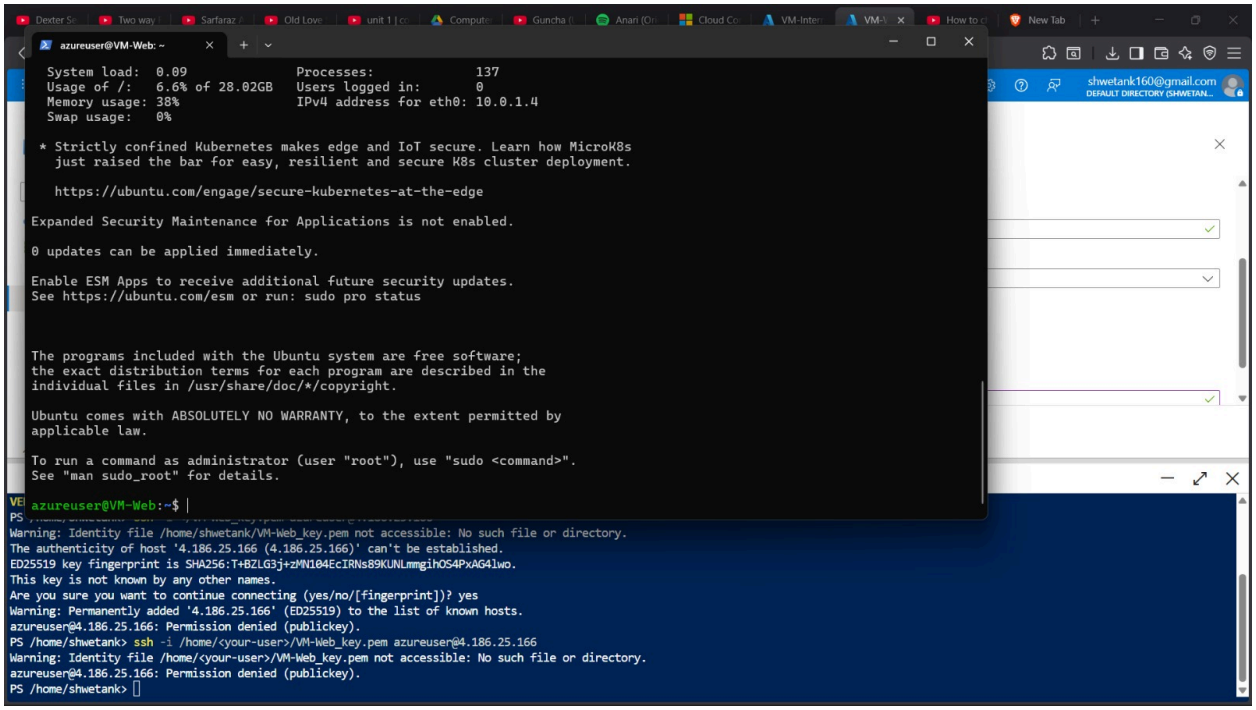
Observed Behavior:

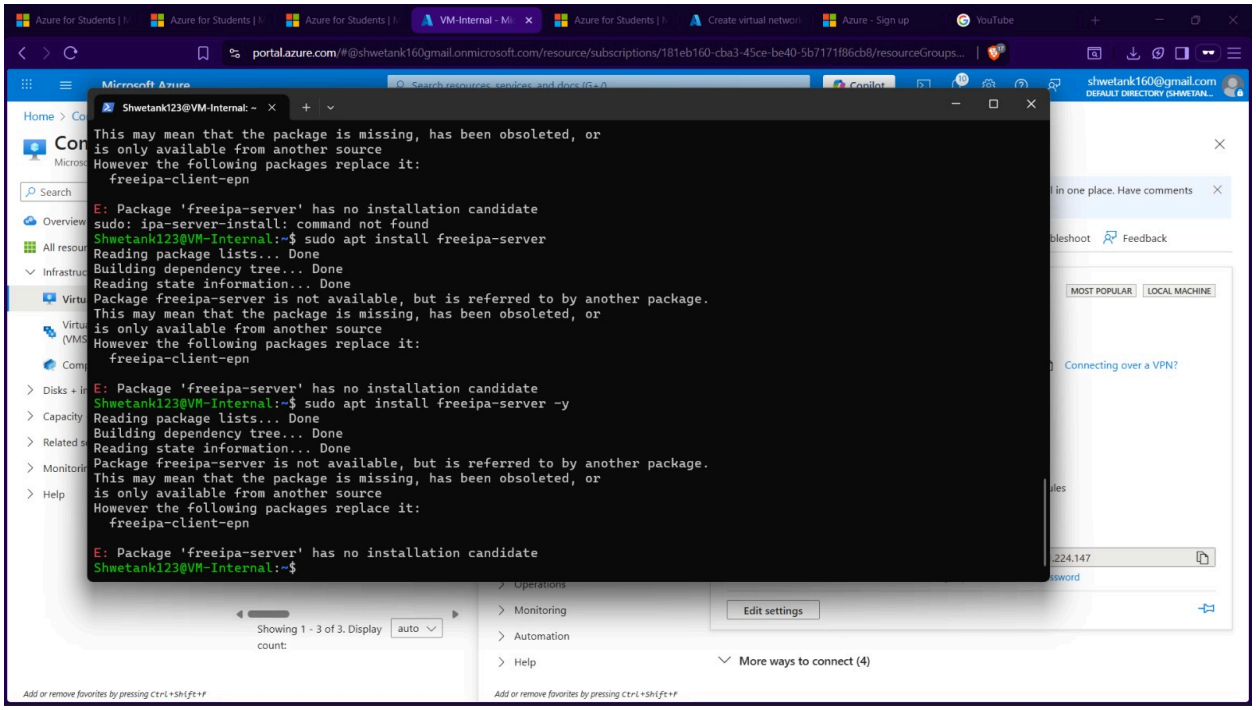
System returned “Permission denied”

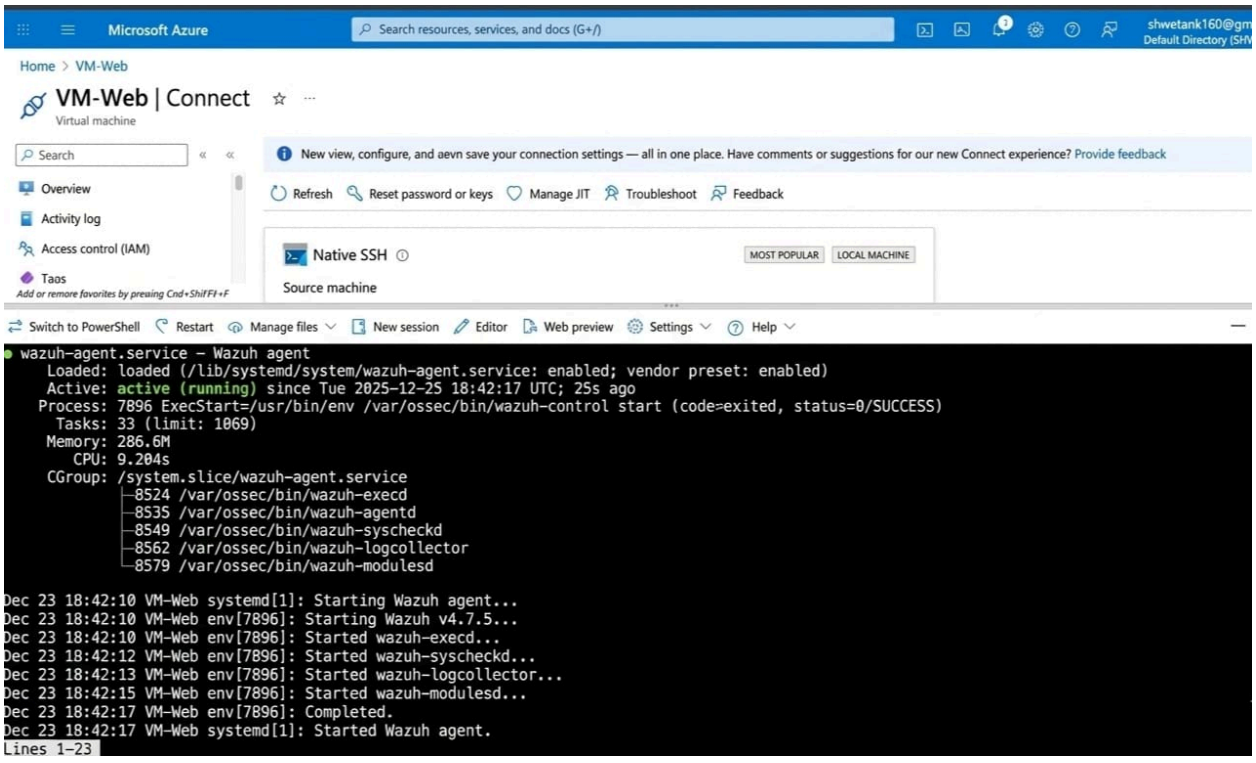
Multiple authentication failure logs were generated in
/var/log/auth.log

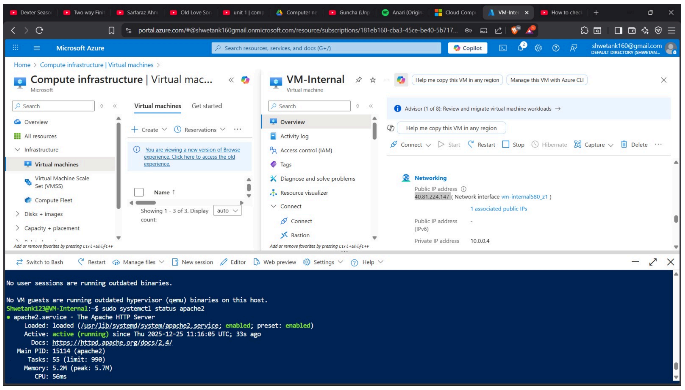
This activity simulated a real-world brute-force attack scenario.

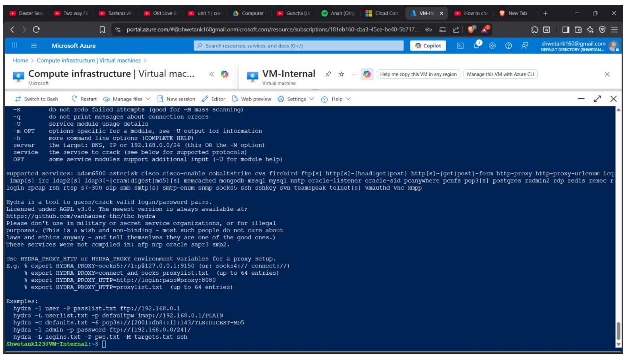


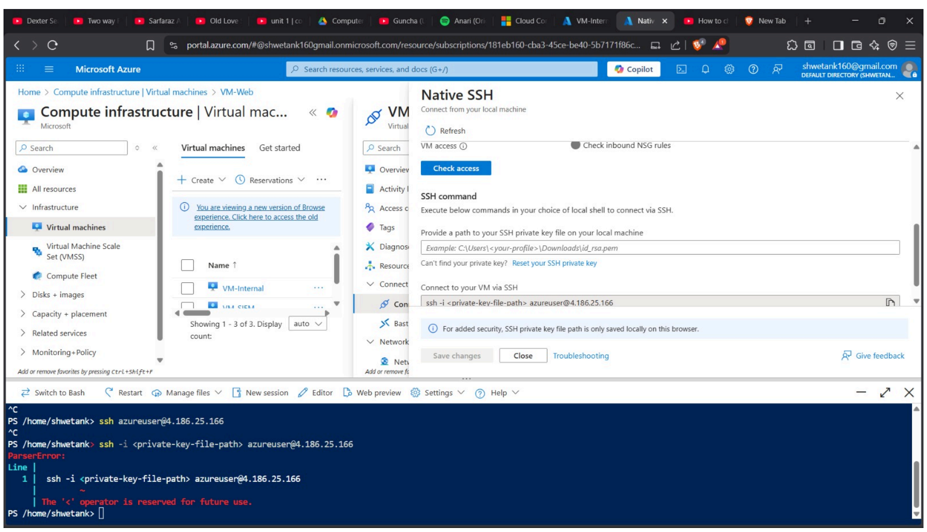

azureuser@VM-Web: ~
System load: 0.09 Processes: 137
Usage of /: 6.6% of 28.02GB Users logged in: 0
Memory usage: 38% IPv4 address for eth0: 10.0.1.4
Swap usage: 0%
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
azureuser@VM-Web:~$
shwetank160@gmail.com
DEFAULT DIRECTORY (SHWETAN...
Warning: Identity file /home/shwetank/VM-Web_key.pem not accessible: No such file or directory.
The authenticity of host '4.186.25.166 (4.186.25.166)' can't be established.
ED25519 key fingerprint is SHA256:T+BZLG3j+zMN104EcIRNs89KUNLmmgihOS4PxAG41wo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '4.186.25.166' (ED25519) to the list of known hosts.
azureuser@4.186.25.166: Permission denied (publickey).
PS /home/shwetank> ssh -i /home/<your-user>/VM-Web_key.pem azureuser@4.186.25.166
Warning: Identity file /home/<your-user>/VM-Web_key.pem not accessible: No such file or directory.
azureuser@4.186.25.166: Permission denied (publickey).
PS /home/shwetank>

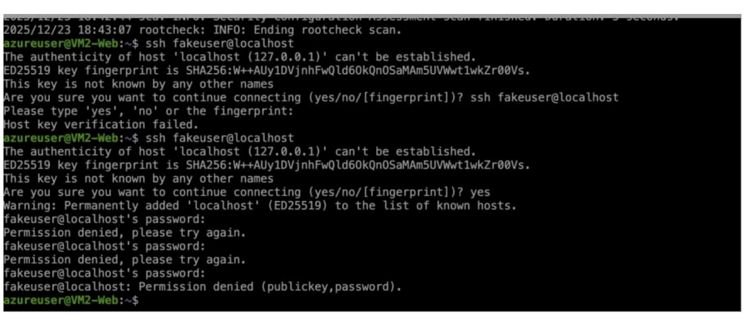

Shwetank123@VM-Internal: ~
This may mean that the package is missing, has been obsoleted, or
is only available from another source
However the following packages replace it:
freeipa-client-epn
E: Package 'freeipa-server' has no installation candidate
sudo: ipa-server-install: command not found
Shwetank123@VM-Internal:~$ sudo apt install freeipa-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package freeipa-server is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source
However the following packages replace it:
freeipa-client-epn
E: Package 'freeipa-server' has no installation candidate
Shwetank123@VM-Internal:~$ sudo apt install freeipa-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package freeipa-server is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source
However the following packages replace it:
freeipa-client-epn
E: Package 'freeipa-server' has no installation candidate
Shwetank123@VM-Internal:~$


Microsoft Azure
Search resources, services, and docs (G+/)
Home > VM-Web
VM-Web | Connect
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Taos
New view, configure, and aevn save your connection settings — all in one place. Have comments or suggestions for our new Connect experience? Provide feedback
Refresh
Reset password or keys
Manage JIT
Troubleshoot
Feedback
Native SSH
MOST POPULAR
LOCAL MACHINE
Source machine
Switch to PowerShell
Restart
Manage files
New session
Editor
Web preview
Settings
Help
wazuh-agent.service - Wazuh agent
Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2025-12-25 18:42:17 UTC; 25s ago
Process: 7896 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
Tasks: 33 (limit: 1069)
Memory: 286.6M
CPU: 9.204s
CGroup: /system.slice/wazuh-agent.service
├─8524 /var/ossec/bin/wazuh-execd
├─8535 /var/ossec/bin/wazuh-agentd
├─8549 /var/ossec/bin/wazuh-syscheckd
├─8562 /var/ossec/bin/wazuh-logcollector
└─8579 /var/ossec/bin/wazuh-modulesd
Dec 23 18:42:10 VM-Web systemd[1]: Starting Wazuh agent...
Dec 23 18:42:10 VM-Web env[7896]: Starting Wazuh v4.7.5...
Dec 23 18:42:10 VM-Web env[7896]: Started wazuh-execd...
Dec 23 18:42:12 VM-Web env[7896]: Started wazuh-syscheckd...
Dec 23 18:42:13 VM-Web env[7896]: Started wazuh-logcollector...
Dec 23 18:42:15 VM-Web env[7896]: Started wazuh-modulesd...
Dec 23 18:42:17 VM-Web env[7896]: Completed.
Dec 23 18:42:17 VM-Web systemd[1]: Started Wazuh agent.
Lines 1-23


Microsoft Azure
Compute infrastructure | Virtual machines
VM-Internal
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
Shwetank123@VM-Internal:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
Active: active (running) since Thu 2025-12-25 11:16:05 UTC; 33s ago
Docs: https://httpd.apache.org/docs/2.4/
Main PID: 15114 (apache2)
Tasks: 55 (limit: 990)
Memory: 5.2M (peak: 5.7M)
CPU: 56ms


Microsoft Azure
Compute infrastructure | Virtual machines
VM-Internal
Hydra is a tool to guess/crack valid login/password pairs.
Examples:
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://[192.168.0.0/24]/
hydra -L logins.txt -P pws.txt -M targets.txt ssh


Microsoft Azure
Compute infrastructure | Virtual machines
Native SSH
Connect from your local machine
Check access
SSH command
Execute below commands in your choice of local shell to connect via SSH.
Provide a path to your SSH private key file on your local machine
Connect to your VM via SSH
ssh -i <private-key-file-path> azureuser@4.186.25.166
For added security, SSH private key file path is only saved locally on this browser.
Save changes
Close
Troubleshooting
Give feedback
PS /home/shwetank> ssh azureuser@4.186.25.166
PS /home/shwetank> ssh -i <private-key-file-path> azureuser@4.186.25.166
ParserError:
Line |
1 | ssh -i <private-key-file-path> azureuser@4.186.25.166
| The '<' operator is reserved for future use.
PS /home/shwetank>


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:~$

Slide 6: Detection – Dashboard Overview

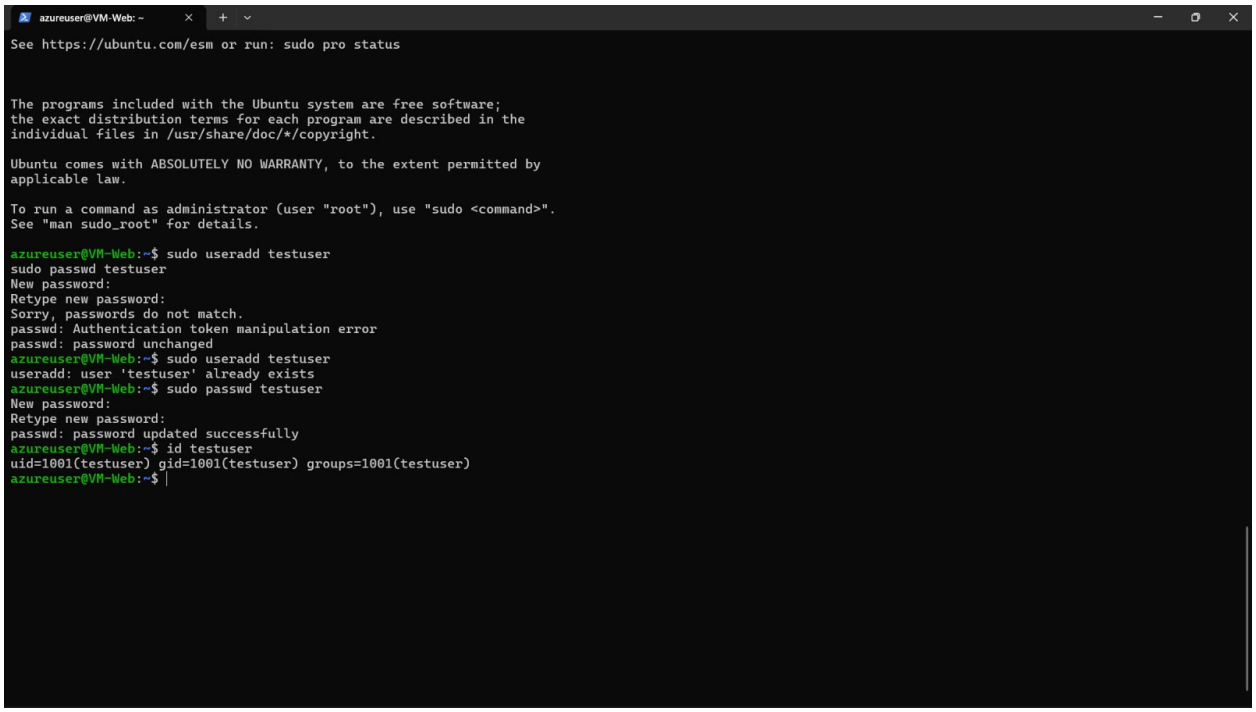
The Wazuh dashboard detected significant security activity:

Total alerts in 24 hours: 1,954

Authentication failure alerts: 1,509

Primary affected agent: VM2-Web

The Alert Level Evolution graph showed a major spike around 06:00, directly correlating with the brute-force attack simulation time.



Slide 7: Detection – Security Events Detail

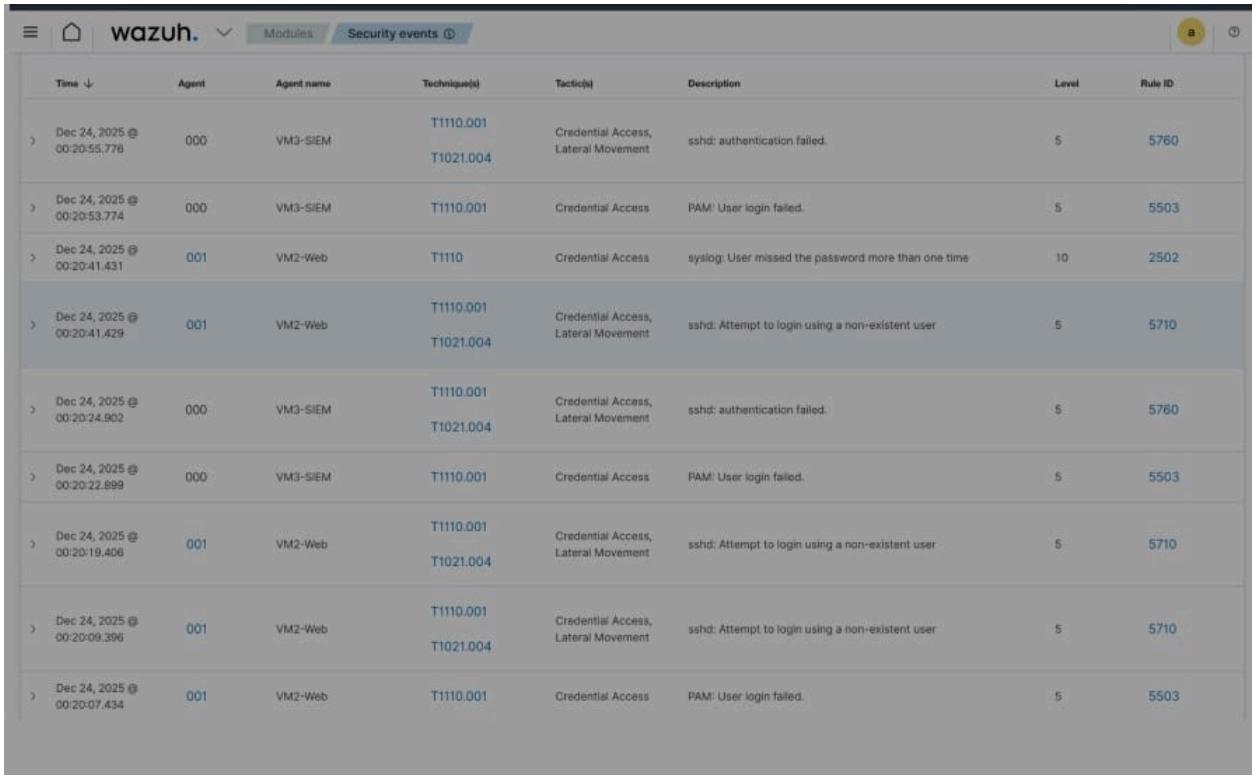
The following high-confidence alerts were triggered:

Rule ID 5760:
SSH authentication failed (Level 5)

Rule ID 5710:

Login attempt using a non-existent user (Level 5)

Rule ID 2502:
Multiple password failures detected (Level 10 – High Severity)



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

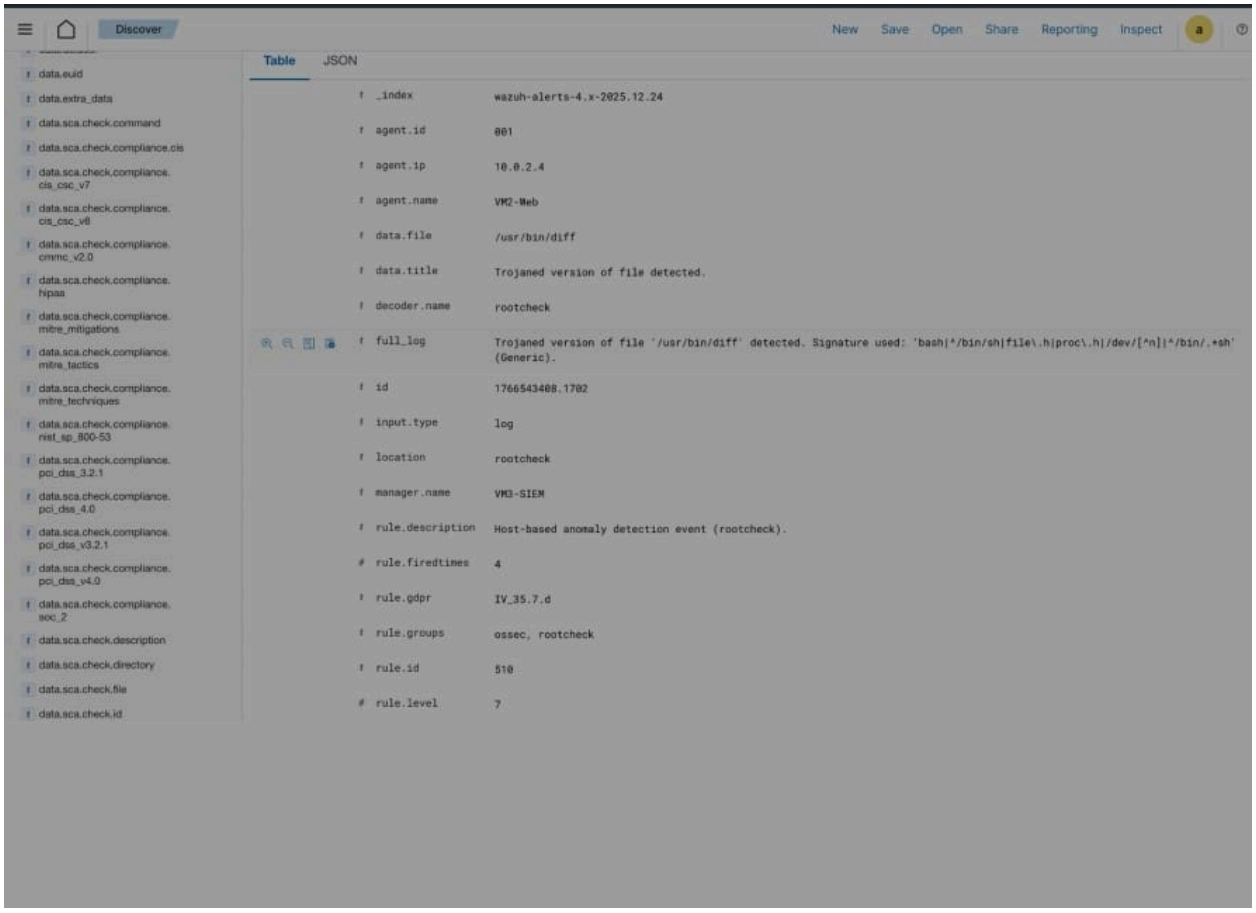
Slide 8: MITRE ATT&CK Mapping

The detected events were mapped to the MITRE ATT&CK framework:

T1110 – Brute Force
Credential Access through repeated login attempts

T1021.004 – Remote Services (SSH)
Unauthorized access via SSH

This mapping validates the attack classification and improves incident understanding.



Slide 9: Advanced Forensics – Rootcheck & Geo-Location

Rootcheck Analysis

Detected a potential integrity violation

Alert: Trojaned version of file detected

File affected: /usr/bin/diff

Rule ID 510 triggered due to signature mismatch

Geo-Location Tracking

Attacker IP identified: 45.121.147.48

Source country: Malaysia

Coordinates: Latitude 2.5, Longitude 112.5

This confirms Wazuh’s forensic and threat-intelligence capability.

Slide 10: Conclusion & Future Scope

Conclusion

Successful deployment of Wazuh SIEM on Azure

Real-time detection of 1,500+ authentication failures

Effective correlation of logs from multiple servers

Accurate identification of attack sources and techniques

Future Scope

Enable Active Response to automatically block malicious IPs

Configure email alerts for Level 10 severity events

Integrate with SOAR tools for automated incident response

Slide 11: References

1. Project Implementation Report

2. Wazuh Official Documentation

3. Wazuh Dashboard and Security Event Logs