Security Monitoring, Log Analysis, and Incident Response using Wazuh SIEM

Meet Tank
SOC Task-1

1. Security Operations Center (SOC)

A Security Operations Center (SOC) is a centralized unit within an organization that is responsible for continuous monitoring, detection, analysis, and response to cybersecurity threats. The primary goal of a SOC is to protect an organization's digital assets, including systems, networks, applications, and sensitive data, from cyberattacks and security breaches. A SOC follows a structured operational workflow to handle security events effectively. This workflow begins with event detection, where security tools generate alerts based on predefined rules or abnormal behavior. Next, alert triage is performed to determine whether the alert is a false positive or a real security issue. Once confirmed, analysts conduct an investigation to understand the scope, impact, and root cause of the incident. If the incident is severe, it is escalated to higher-level analysts or incident response teams for containment and remediation

The SOC operates 24/7 and uses a combination of people, processes, and technology to identify potential security incidents in real time. It continuously collects and analyzes data from multiple sources such as endpoints, servers, firewalls, routers, intrusion detection systems (IDS), intrusion prevention systems (IPS), and applications. By monitoring these sources, the SOC can quickly detect unusual activities that may indicate threats like malware infections, unauthorized access attempts, data exfiltration, or denial-of-service attacks.

2. SIEM and Its Role in SOC

A Security Information and Event Management (SIEM) system plays a critical role in the functioning of a SOC and is often considered its core technology. SIEM solutions collect, store, normalize, and analyze log data from various sources across the organization's IT infrastructure. These sources include operating systems, network devices, security tools, databases, and applications.

The main function of a SIEM is to provide centralized visibility into security events by aggregating logs into a single platform. It applies correlation rules and analytics to identify patterns that may indicate malicious activity. For example, multiple failed login attempts followed by a successful login from an unusual location may trigger an alert for a possible brute-force attack.

SIEM systems support SOC operations in several important ways. They enable centralized log monitoring, which helps analysts review events without accessing individual systems. They assist in the detection of attack patterns by correlating events across different sources. SIEM platforms also provide real-time alerting, allowing SOC teams to respond quickly to incidents before they cause significant damage. Additionally, SIEM tools offer dashboards and visualizations that display the overall security posture of the organization, making it easier to identify trends and recurring threats.

3. Methodology and Implementation

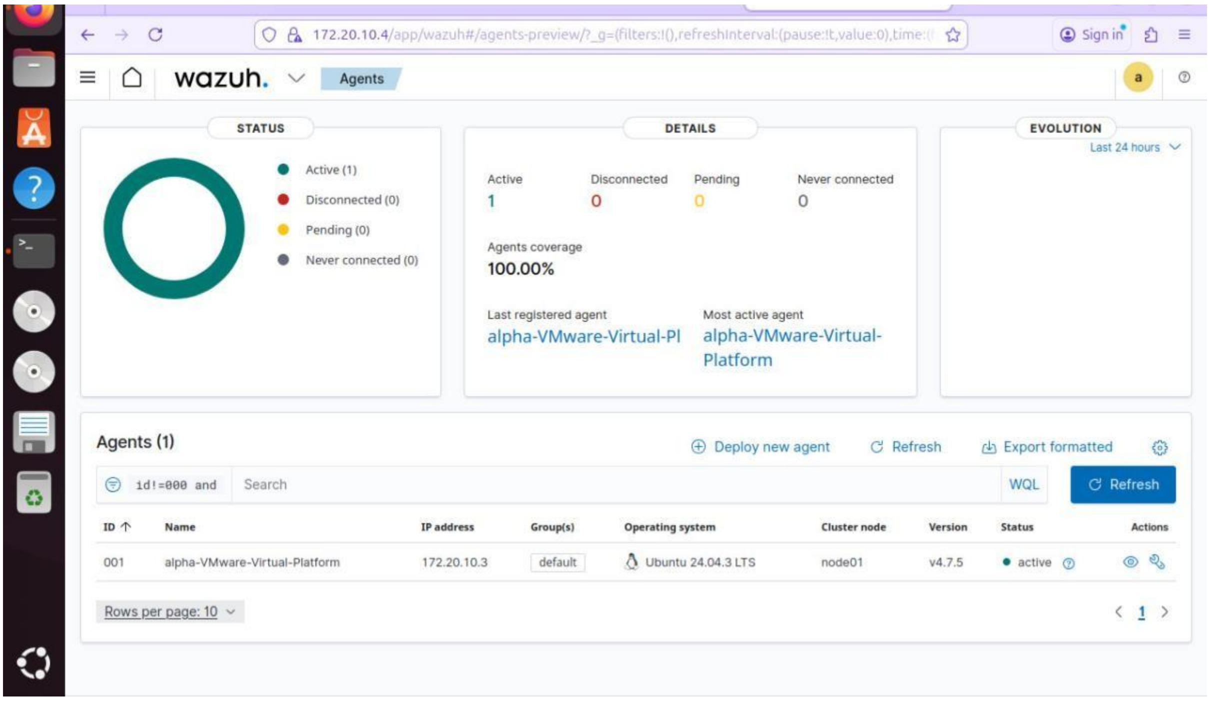
3.1 Agent Deployment and Asset Inventory

The foundation of the SOC is visibility into endpoints. We utilized the Wazuh Manager (Ubuntu Host) to generate deployment scripts for our Ubuntu agents.

- **Ubuntu Onboarding**: The agents were installed on the two Ubuntu endpoints using the native .deb package manager and registered with the Manager.

- **Linux Monitoring**: Agent 001 and Agent 002 (Ubuntu 24.04.3 LTS) were configured to communicate with the Manager's IP.

- **Verification**: The SOC dashboard confirmed 100% agent coverage, showing both Ubuntu systems as "Active" and ready for monitoring.



STATUS

- ● Active (1)
- ● Disconnected (0)
- ● Pending (0)
- ● Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected
1	0	0	0

Agents coverage
100.00%

Last registered agent
alpha-VMware-Virtual-Pl

Most active agent
alpha-VMware-Virtual-Platform

Agents (1)

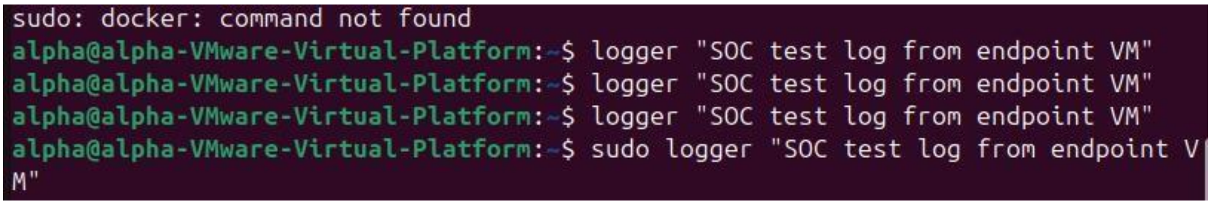
id!=000 and Search

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	alpha-VMware-Virtual-Platform	172.20.10.3	default	Ubuntu 24.04.3 LTS	node01	v4.7.5	● active	

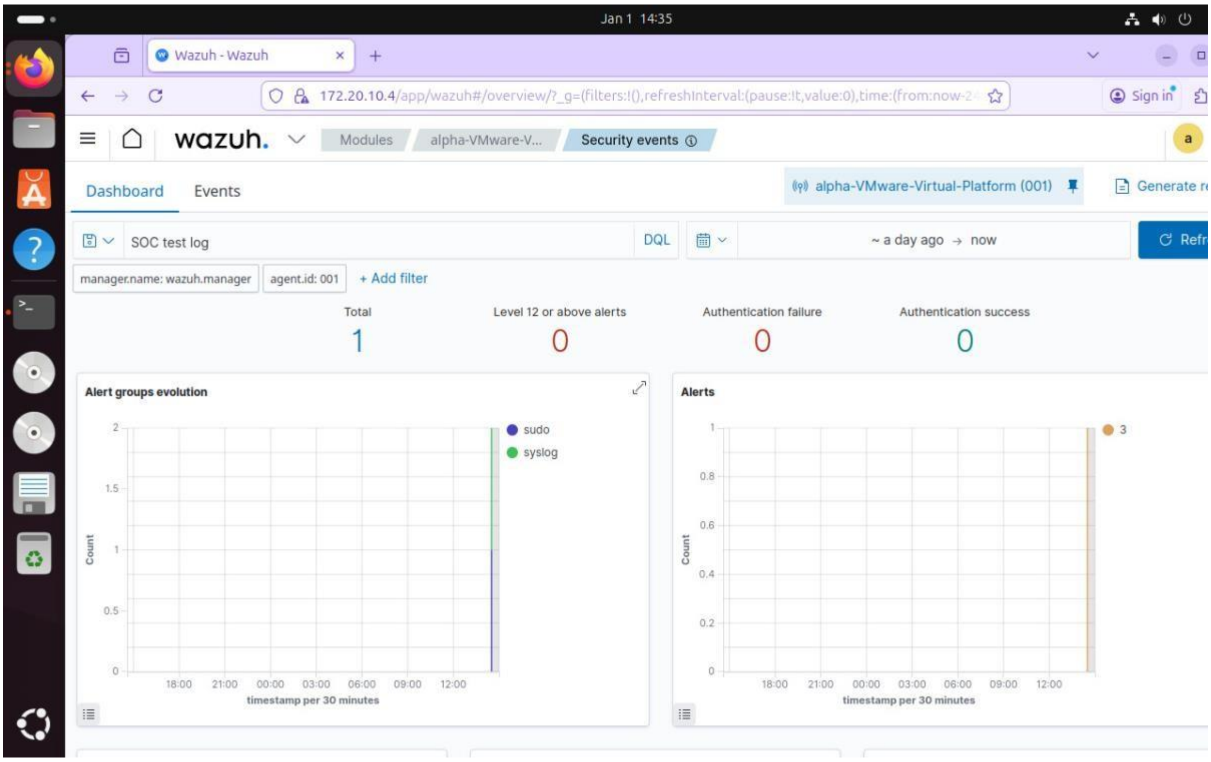
3.2 Log Pipeline Verification (Proof of Concept)

To ensure the SIEM was correctly receiving data from the Ubuntu endpoints, a manual "Heartbeat" test was performed.

- Action: The logger utility was used on an Ubuntu agent to push a custom string: "SOC test log from endpoint VM".
- Result: The event was successfully indexed by the Manager, proving that the syslog pipeline is functional and that the Wazuh agent is correctly forwarding local /var/log/syslog da



```
sudo: docker: command not found
alpha@alpha-VMware-Virtual-Platform:~$ logger "SOC test log from endpoint VM"
alpha@alpha-VMware-Virtual-Platform:~$ logger "SOC test log from endpoint VM"
alpha@alpha-VMware-Virtual-Platform:~$ logger "SOC test log from endpoint VM"
alpha@alpha-VMware-Virtual-Platform:~$ sudo logger "SOC test log from endpoint V
M"
```



Jan 1 14:35

Wazuh - Wazuh

172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-2

wazuh. Modules alpha-VMware-V... Security events

Dashboard Events alpha-VMware-Virtual-Platform (001) Generate r

SOC test log DQL ~ a day ago → now

manager.name: wazuh.manager agent.id: 001 + Add filter

Total	Level 12 or above alerts	Authentication failure	Authentication success
1	0	0	0

Threat Detection and Incident Analysis

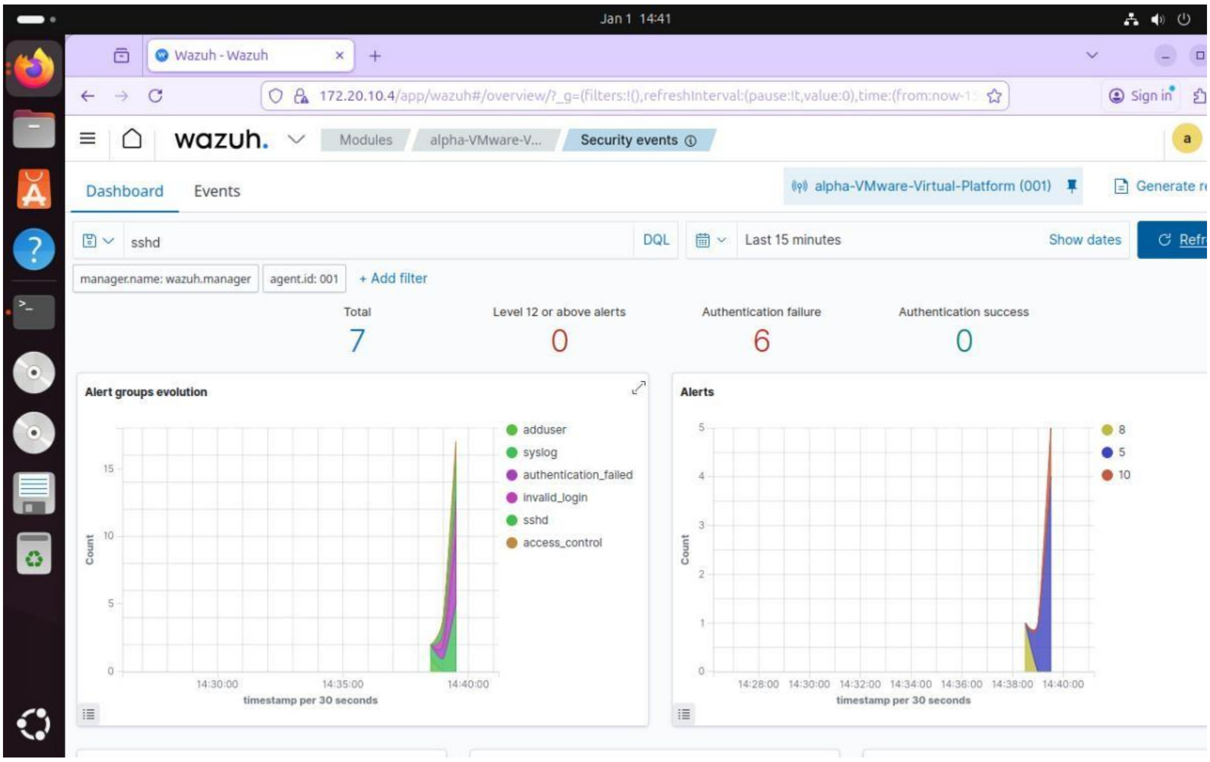
1.1 Brute Force Simulation (SSH on Ubuntu)

The SOC's primary goal is to detect unauthorized access. We simulated an SSH Brute Force attack targeting one of the Ubuntu agents.

- **Attack Technique**: Multiple failed authentication attempts were made using a non-existent user account (wrong user) via SSH.

- **Detection Logic**: Wazuh triggered high-severity alerts (Level 10) for "Authentication failure" and "Failed password" attempts found in /var/log/auth.log.

- **Telemetry**: The dashboard displayed a sharp spike in authentication failure counts, indicating a sustained attack attempt.



172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-1

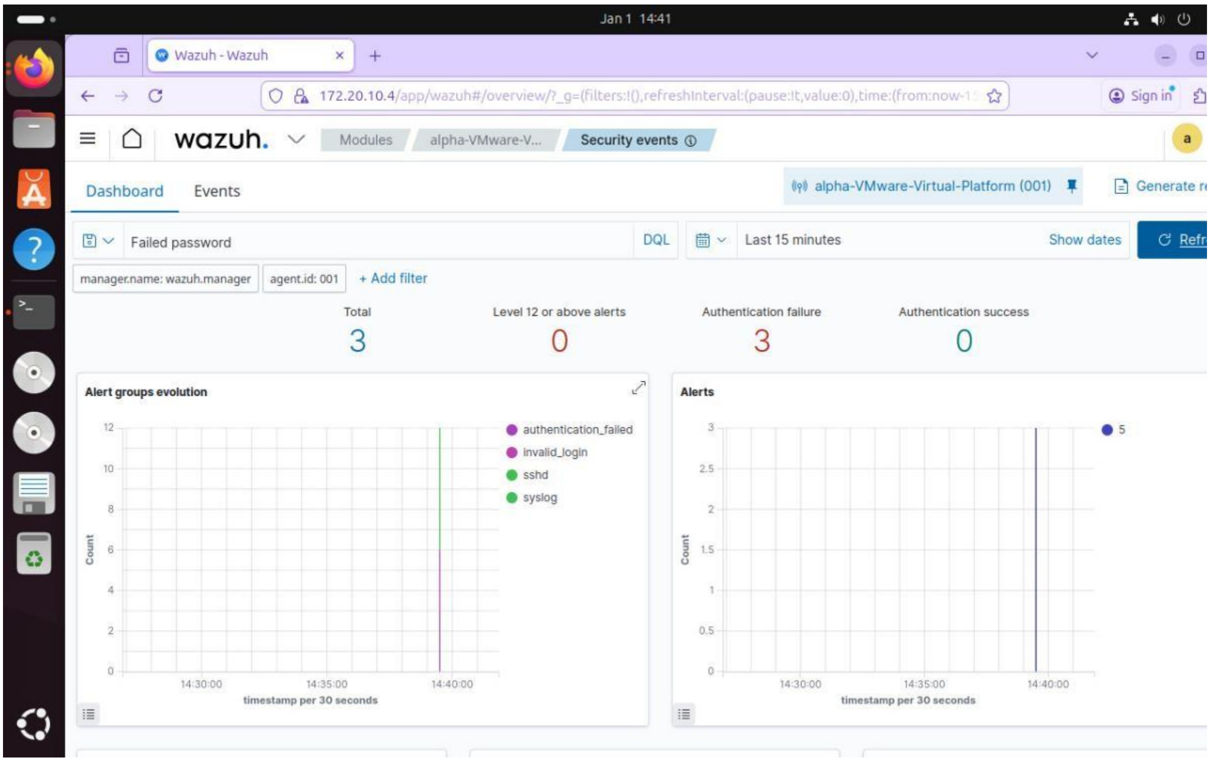
sshd

Last 15 minutes

manager.name: wazuh.manager
agent.id: 001

alpha-VMware-Virtual-Platform (001)

Total	Level 12 or above alerts	Authentication failure	Authentication success
7	0	6	0



Failed password

Last 15 minutes

manager.name: wazuh.manager

agent.id: 001

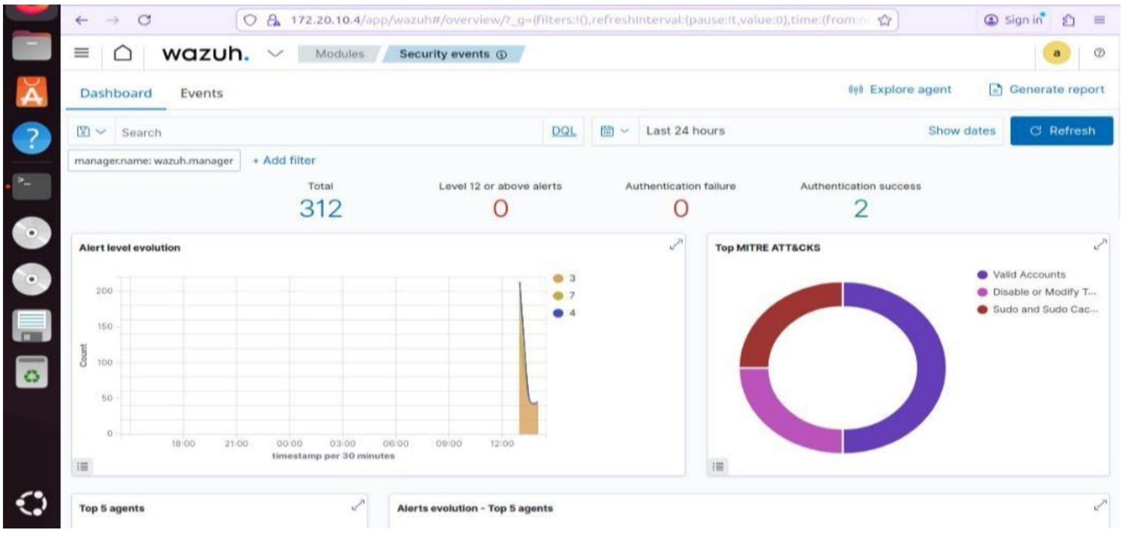
Total	Level 12 or above alerts	Authentication failure	Authentication success
3	0	3	0

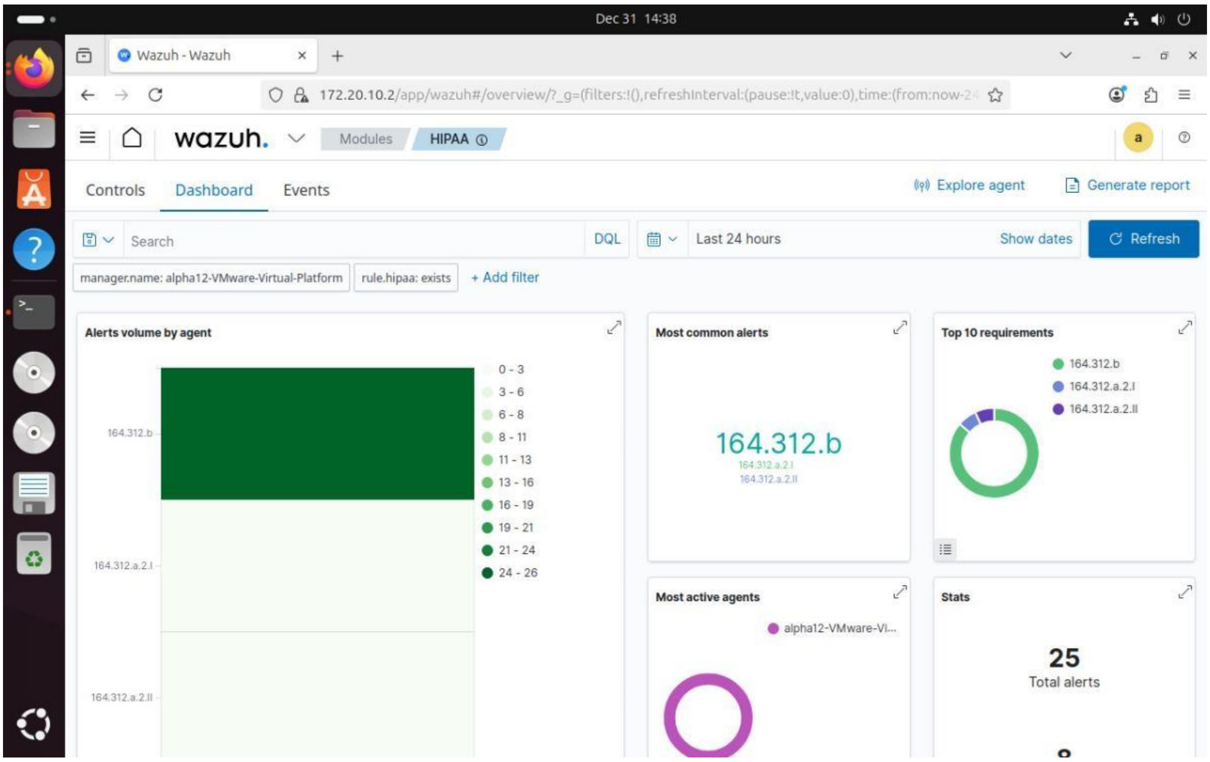
1.1 Framework and Regulatory Mapping

Every alert was contextualized using global frameworks to determine the stage of the attack and meet legal requirements.

- **MITRE ATT&CK**: The attack was mapped to Tactic: **Credential Access** and Technique: **T1110 (Brute Force)**.

- **Regulatory Compliance (HIPAA)**: Used the HIPAA dashboard to visualize how these events impact security standards (Technical Safeguards 164.312.b regarding


172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:n
Sign in
wazuh.
Modules
Security events
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh.manager
+ Add filter
Total
312
Level 12 or above alerts
0
Authentication failure
0
Authentication success
2
Alert level evolution
200
150
100
50
0
Count
18:00
21:00
00:00
03:00
06:00
09:00
12:00
timestamp per 30 minutes
3
7
4
Top MITRE ATT&CKS
Valid Accounts
Disable or Modify T...
Sudo and Sudo Cac...
Top 5 agents
Alerts evolution - Top 5 agents

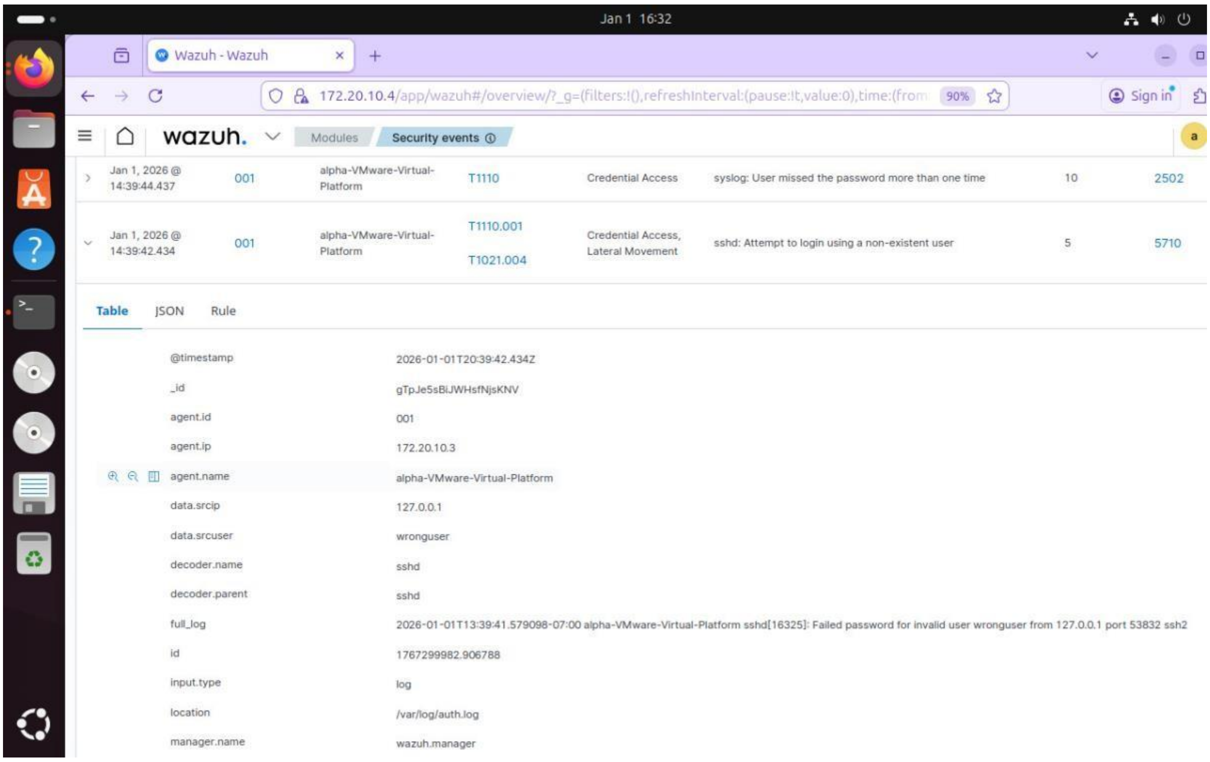

Dec 31 14:38
Wazuh - Wazuh
172.20.10.2/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24
wazuh.
Modules
HIPAA
Controls
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: alpha12-VMware-Virtual-Platform
rule.hipaa: exists
+ Add filter
Alerts volume by agent
164.312.b
164.312.a.2.I
164.312.a.2.II
0 - 3
3 - 6
6 - 8
8 - 11
11 - 13
13 - 16
16 - 19
19 - 21
21 - 24
24 - 26
Most common alerts
164.312.b
164.312.a.2.I
164.312.a.2.II
Top 10 requirements
164.312.b
164.312.a.2.I
164.312.a.2.II
Most active agents
alpha12-VMware-Vi...
Stats
25
Total alerts
8

1. Technical Deep-Dive and Health Monitoring

1.1Forensic Metadata Analysis

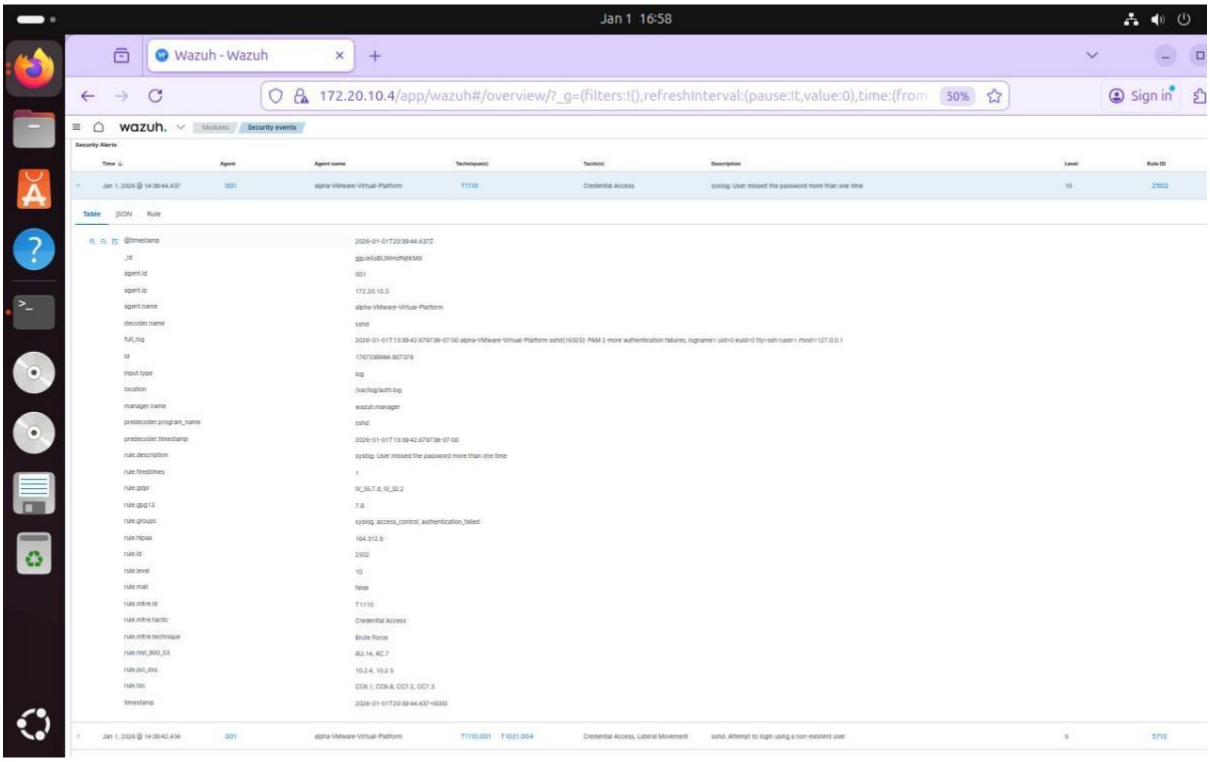
For detailed incident response, we analyzed the raw JSON metadata of the triggered alerts.

- **Source IP**: 127.0.0.1 (Internal test simulation).
- **Target User**: wronguser.
- **Log Source**: /var/log/auth.log (The standard authentication log for Ubuntu).
- **Rule IDs**: 5710 (SSHD login attempt) and 2502 (Syslog password failure).


Jan 1 16:32
Wazuh - Wazuh
172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from
90%
Sign in
wazuh.
Modules
Security events
a
Table
JSON
Rule

Jan 1, 2026 @ 14:39:44.437	001	alpha-VMware-Virtual-Platform	T1110	Credential Access	syslog: User missed the password more than one time	10	2502
Jan 1, 2026 @ 14:39:42.434	001	alpha-VMware-Virtual-Platform	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

@timestamp	2026-01-01T20:39:42.434Z
_id	gTpJe5sBiJWHsfNjsKNV
agent.id	001
agent.ip	172.20.10.3
agent.name	alpha-VMware-Virtual-Platform
data.srcip	127.0.0.1
data.srcuser	wronguser
decoder.name	sshd
decoder.parent	sshd
full_log	2026-01-01T13:39:41.579098-07:00 alpha-VMware-Virtual-Platform sshd[16325]: Failed password for invalid user wronguser from 127.0.0.1 port 53832 ssh2
id	1767299982.906788
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager



Jan 1 16:58
Wazuh - Wazuh
172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from
50%
Sign in
wazuh.
Modules
Security events
Table
JSON
Rule

Security Alerts

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 1, 2026 @ 14:39:44.437	001	alpha-VMware-Virtual-Platform	T1110	Credential Access	syslog: User missed the password more than one time	10	2502
Jan 1, 2026 @ 14:39:42.434	001	alpha-VMware-Virtual-Platform	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

@timestamp	2026-01-01T20:39:44.437Z
_id	gjpJe5sBIJWHsfNjtKM9
agent.id	001
agent.ip	172.20.10.3
agent.name	alpha-VMware-Virtual-Platform
decoder.name	sshd
full_log	2026-01-01T13:39:42.679738-07:00 alpha-VMware-Virtual-Platform sshd[16325]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
id	1767299984.907378
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager
predecoder.program_name	sshd
predecoder.timestamp	2026-01-01T13:39:42.679738-07:00
rule.description	syslog: User missed the password more than one time
rule.firedtimes	1
rule.gdpr	IV_35.7.d, IV_32.2
rule.gpg13	7.8
rule.groups	syslog, access_control, authentication_failed
rule.hipaa	164.312.b
rule.id	2502
rule.level	10
rule.mail	false
rule.mitre.id	T1110
rule.mitre.tactic	Credential Access
rule.mitre.technique	Brute Force
rule.nist_800_53	AU.14, AC.7
rule.pci_dss	10.2.4, 10.2.5
rule.tsc	CC6.1, CC6.8, CC7.2, CC7.3
timestamp	2026-01-01T20:39:44.437+0000

1.2System Reliability Issues

A Health Check revealed an API connectivity failure within the Ubuntu host.

- **Finding**: The Manager reported [API connection] No API available.
- **Resolution Step**: This indicates a service outage on the Wazuh indexer or manager, requiring a restart of the services on the Ubuntu host.

5. Conclusion

This technical exercise successfully demonstrated the lifecycle of a security event within an all-Ubuntu SOC environment. We proved that the environment is capable of onboarding assets via native agent deployment, validating data integrity through manual log generation, and detecting suspicious activity like SSH Brute Force in real-time. Furthermore, the ability to map these events to MITRE ATT&CK and HIPAA standards ensures that the SOC meets both operational and regulatory requirements.