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

Sumit Solanki
SOC Task-1

1. Security Operations Center (SOC)

A Security Operations Center (SOC) is a centralized facility responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents in real time. The SOC continuously observes logs, alerts, and events generated by endpoints, servers, and network devices to identify suspicious or malicious activities.
The SOC follows a structured workflow that includes event detection, alert triage, investigation, escalation, and reporting.

2. SIEM and Its Role in SOC

A Security Information and Event Management (SIEM) system acts as the backbone of a SOC. It aggregates logs from multiple sources, applies correlation rules, and generates alerts when predefined security conditions are met.

SIEM systems enable:

- Centralized log monitoring
- Detection of attack patterns
- Real-time alerting
- Visualization of security posture

In this experiment, Wazuh is used as the SIEM platform.

3. Methodology and Implementation

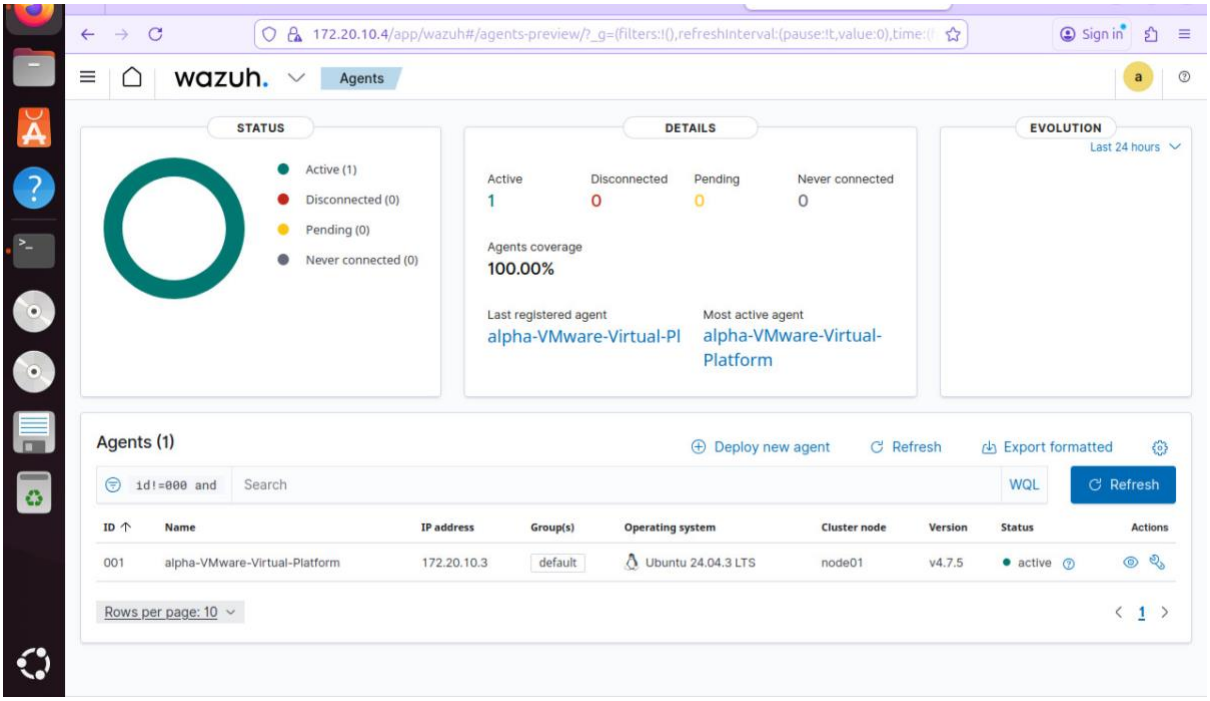
3.1 Agent Deployment and Asset Inventory

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.

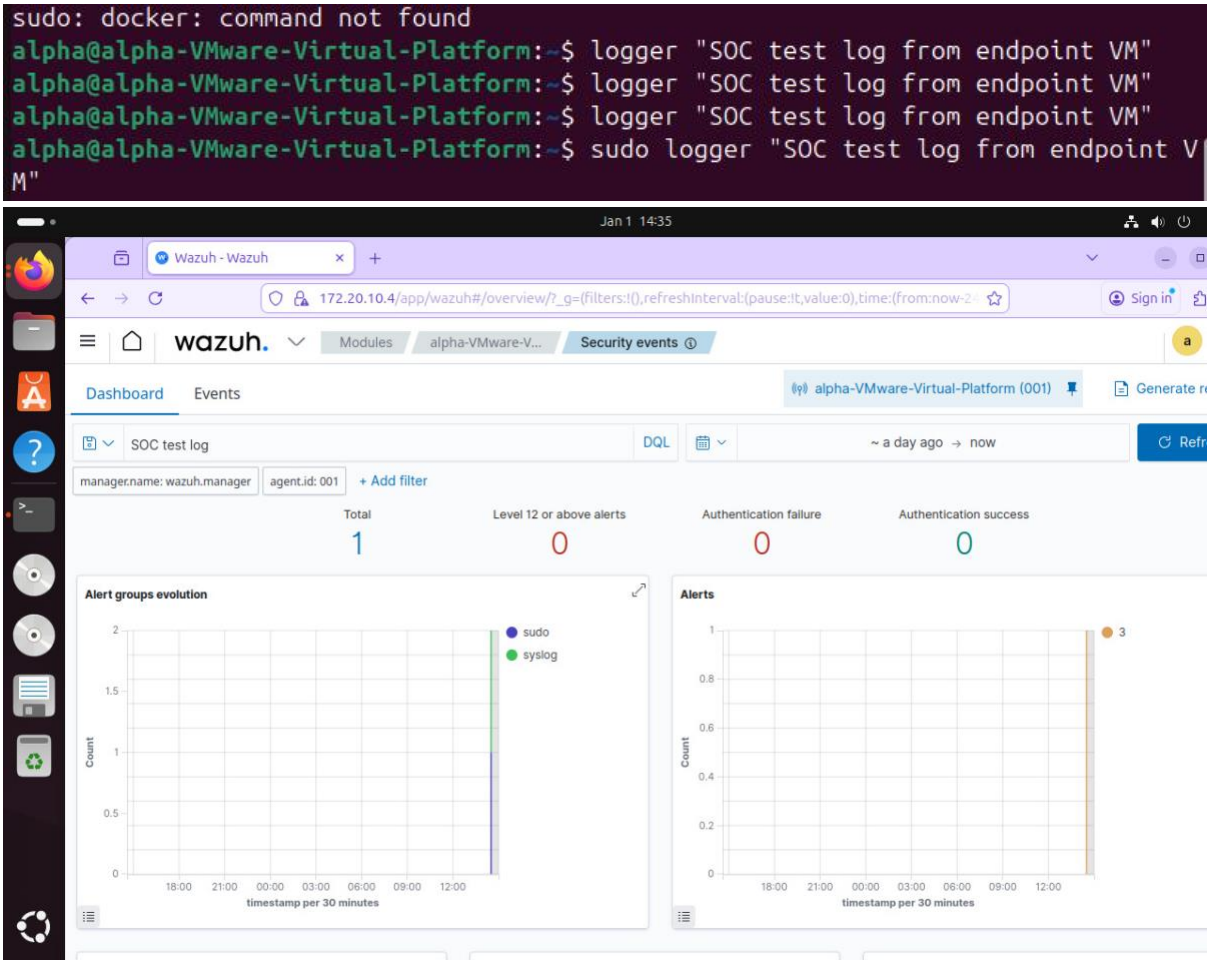


3.2 Log Pipeline Verification (Proof of Concept)

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 data.



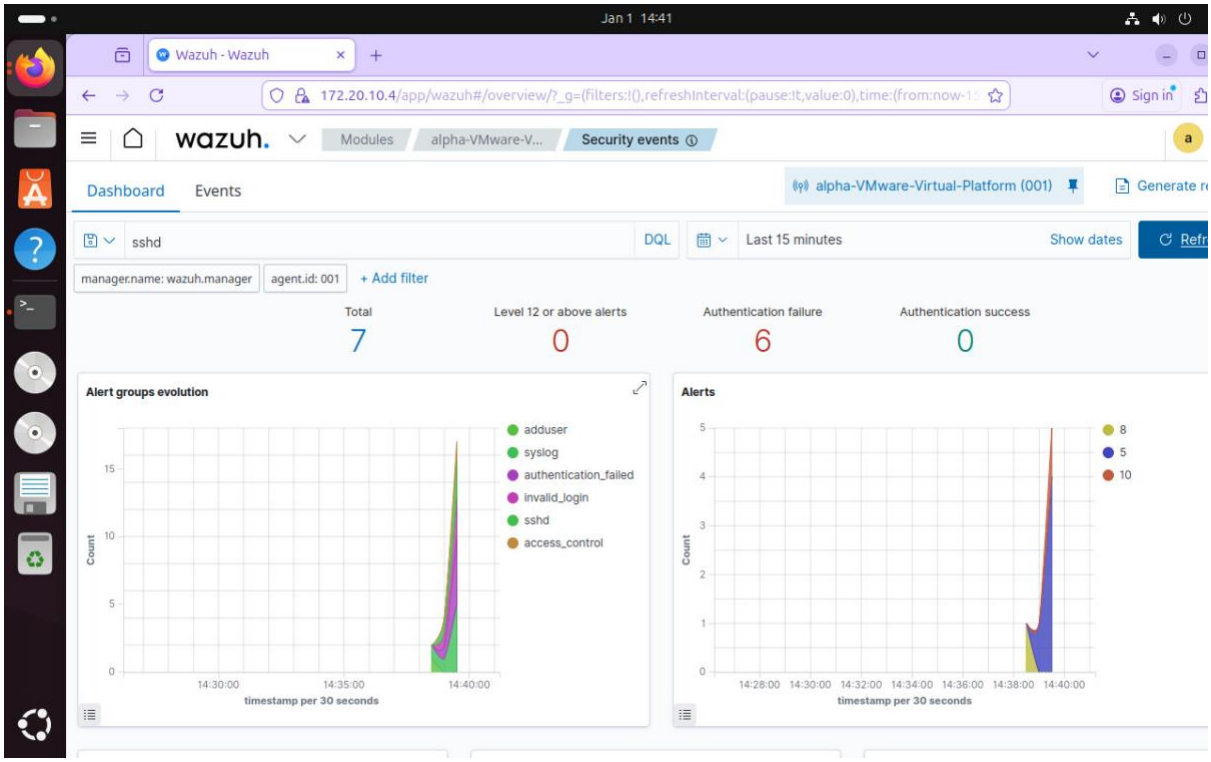
4. Threat Detection and Incident Analysis

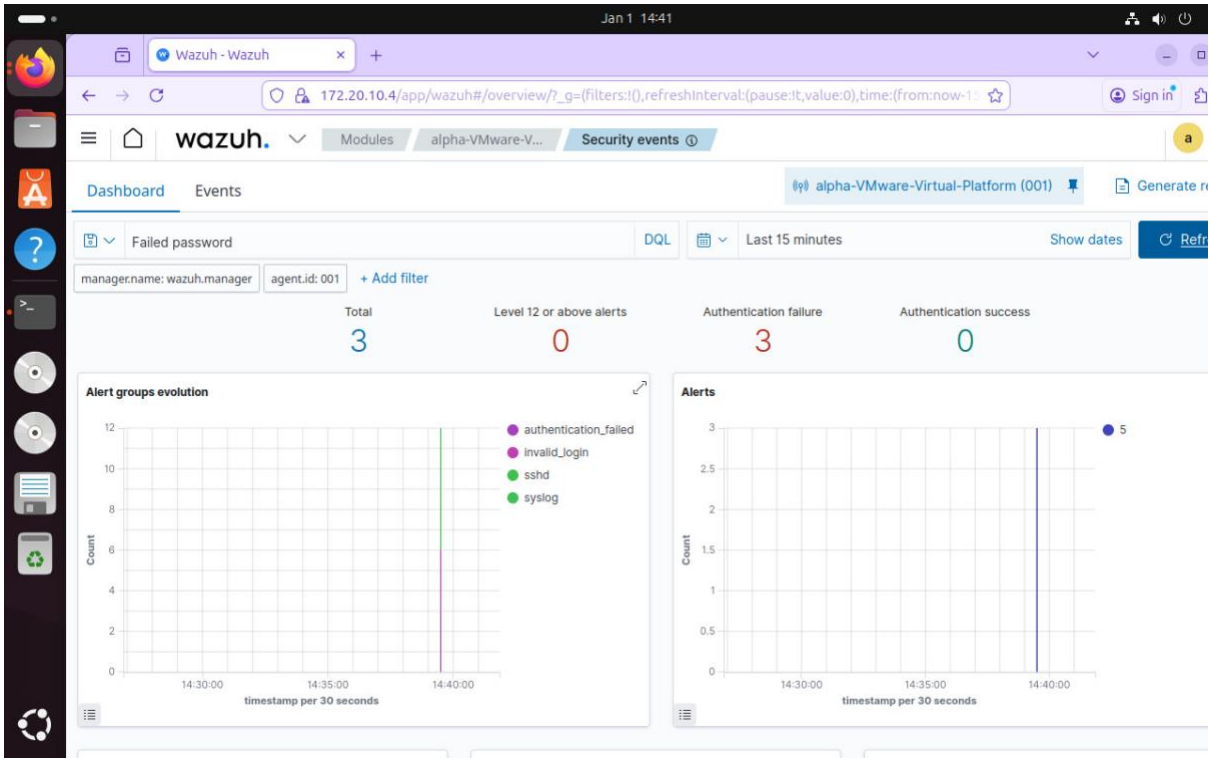
4.1 Brute Force Simulation (SSH on Ubuntu)

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.



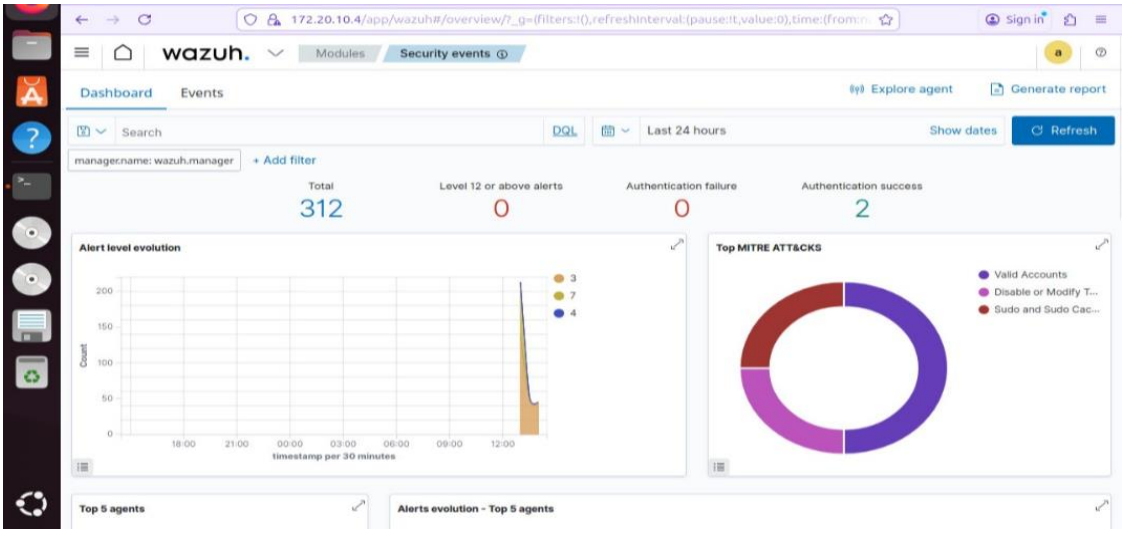


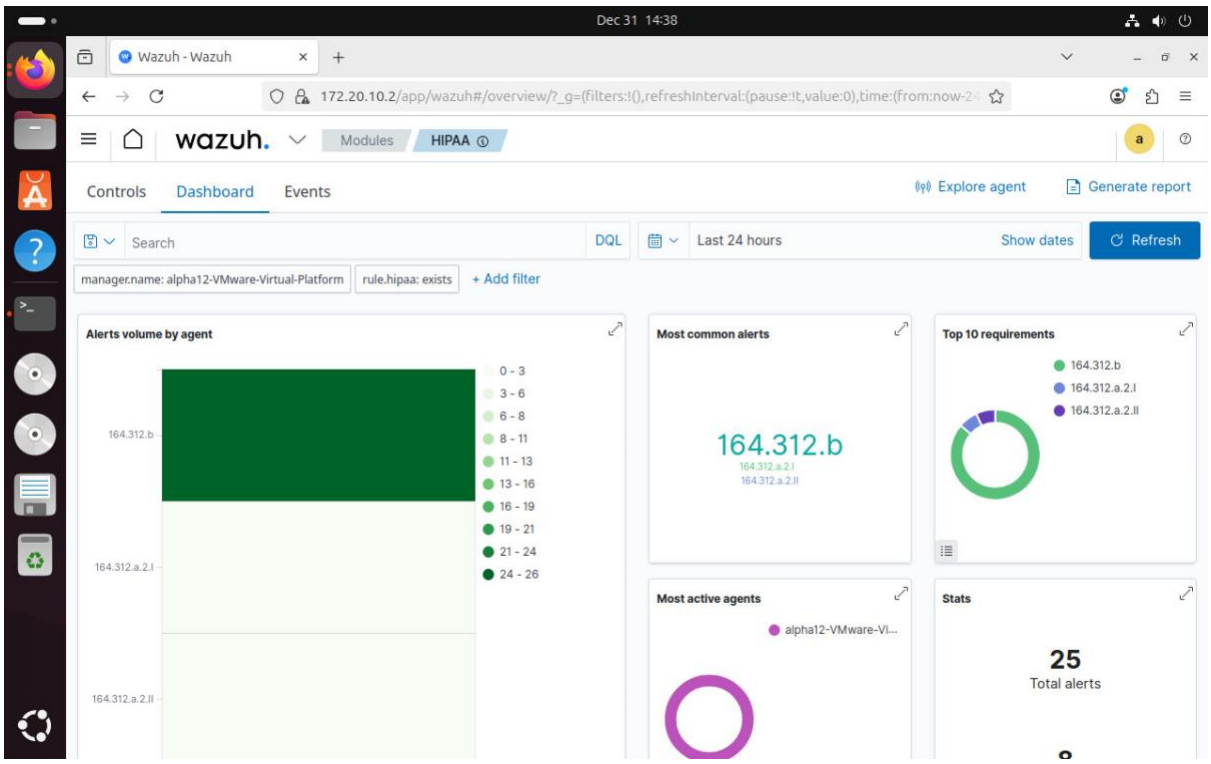
4.2 Framework and Regulatory Mapping

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


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
Top MITRE ATT&CKS
Valid Accounts
Disable or Modify T...
Sudo and Sudo Cac...
Top 5 agents
Alerts evolution - Top 5 agents

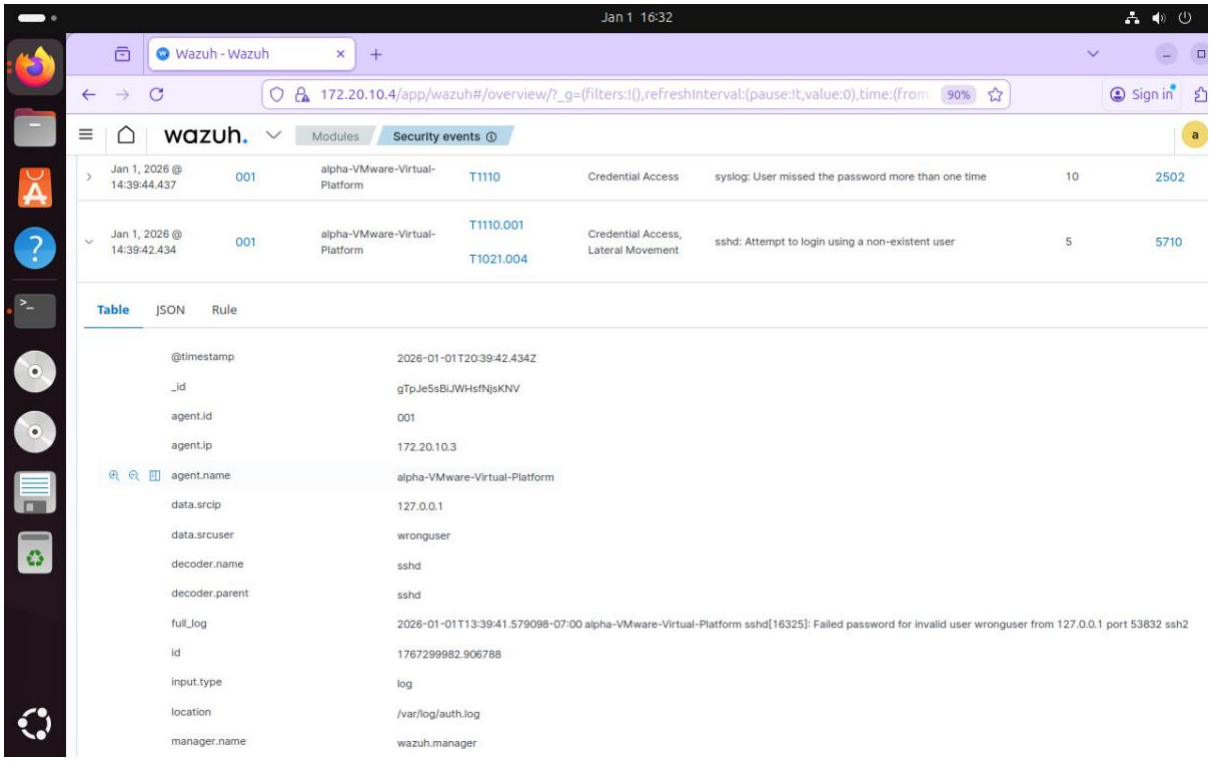

Dec 31 14:38
Wazuh - Wazuh
wazuh.
Modules
HIPAA
Controls
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: alpha12-VMware-Virtual-Platform
rule.hipaa: exists
+ Add filter
Alerts volume by agent
Most common alerts
164.312.b
Top 10 requirements
164.312.b
164.312.a.2.I
164.312.a.2.II
Most active agents
Stats
25
Total alerts

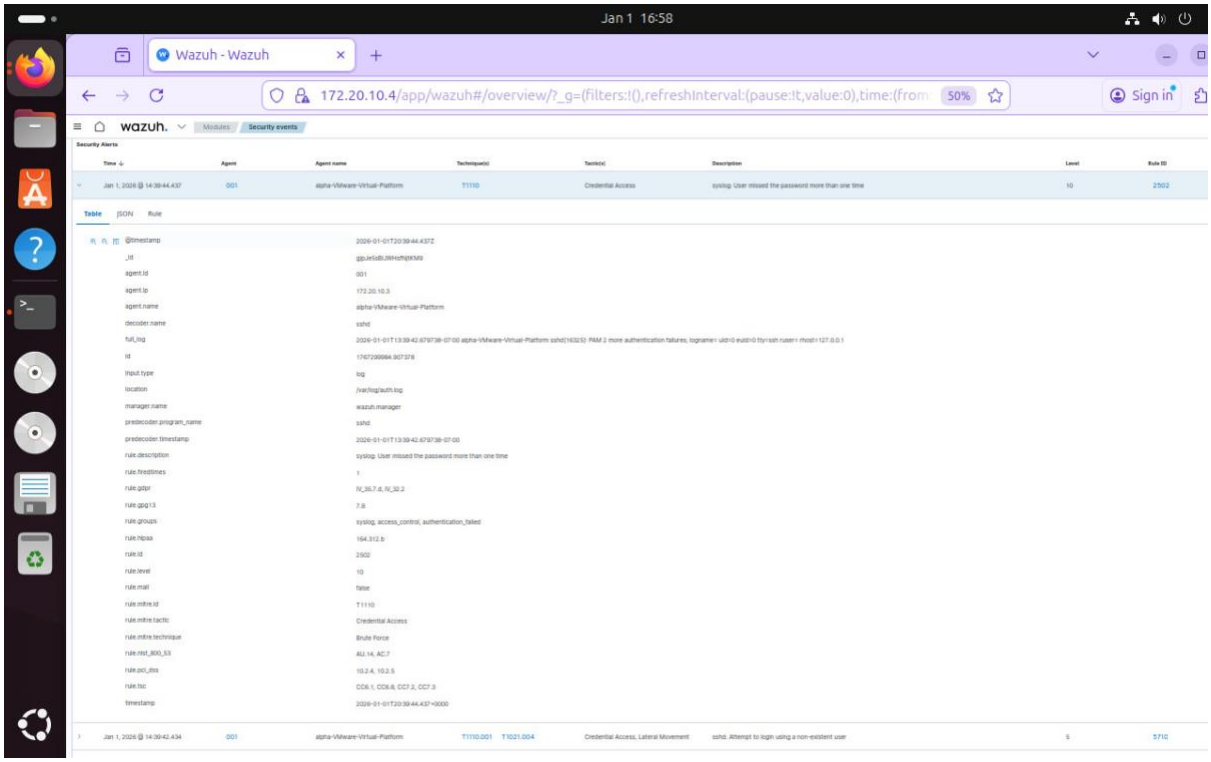
5. Technical Deep-Dive and Health Monitoring

5.1 Forensic 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).





5.2 System 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.