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

Riddhi Vekariya
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.

- Security monitoring aims to detect:
  Brute-force login attempts
  Unauthorized access
  Malware behavior
  Policy violations

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.

- In this experiment, Wazuh was used as the SIEM platform to:
  Collect logs from Ubuntu endpoints
  Detect SSH brute-force attempts
  Generate real-time alerts
  Provide MITRE ATT&CK and HIPAA compliance mapping

Support investigation through detailed JSON event data

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.

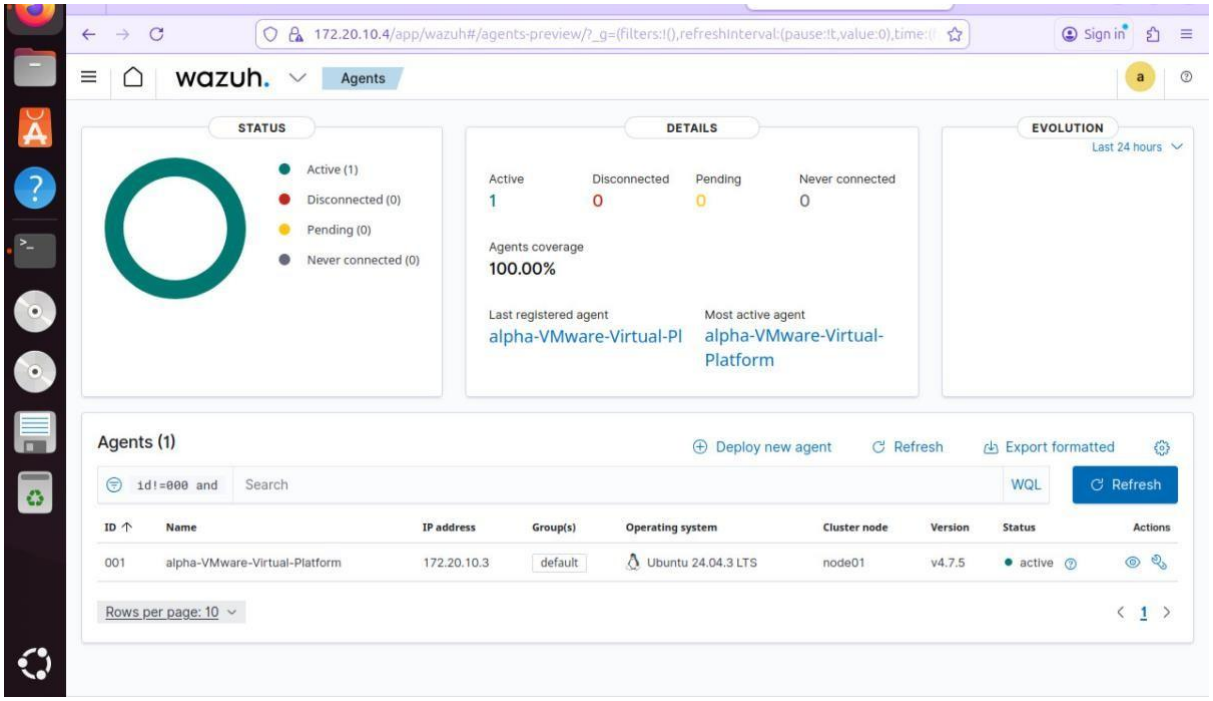
- **Ubuntu Onboarding**: The agents were installed on the two Ubuntu endpoints using the native .deb package manager and registered with the Manager.

➢ In this experiment, Wazuh acted as:

Agent Manager – handling secure onboarding
Log Collector – receiving endpoint telemetry
Asset Inventory System – tracking active Ubuntu endpoints

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

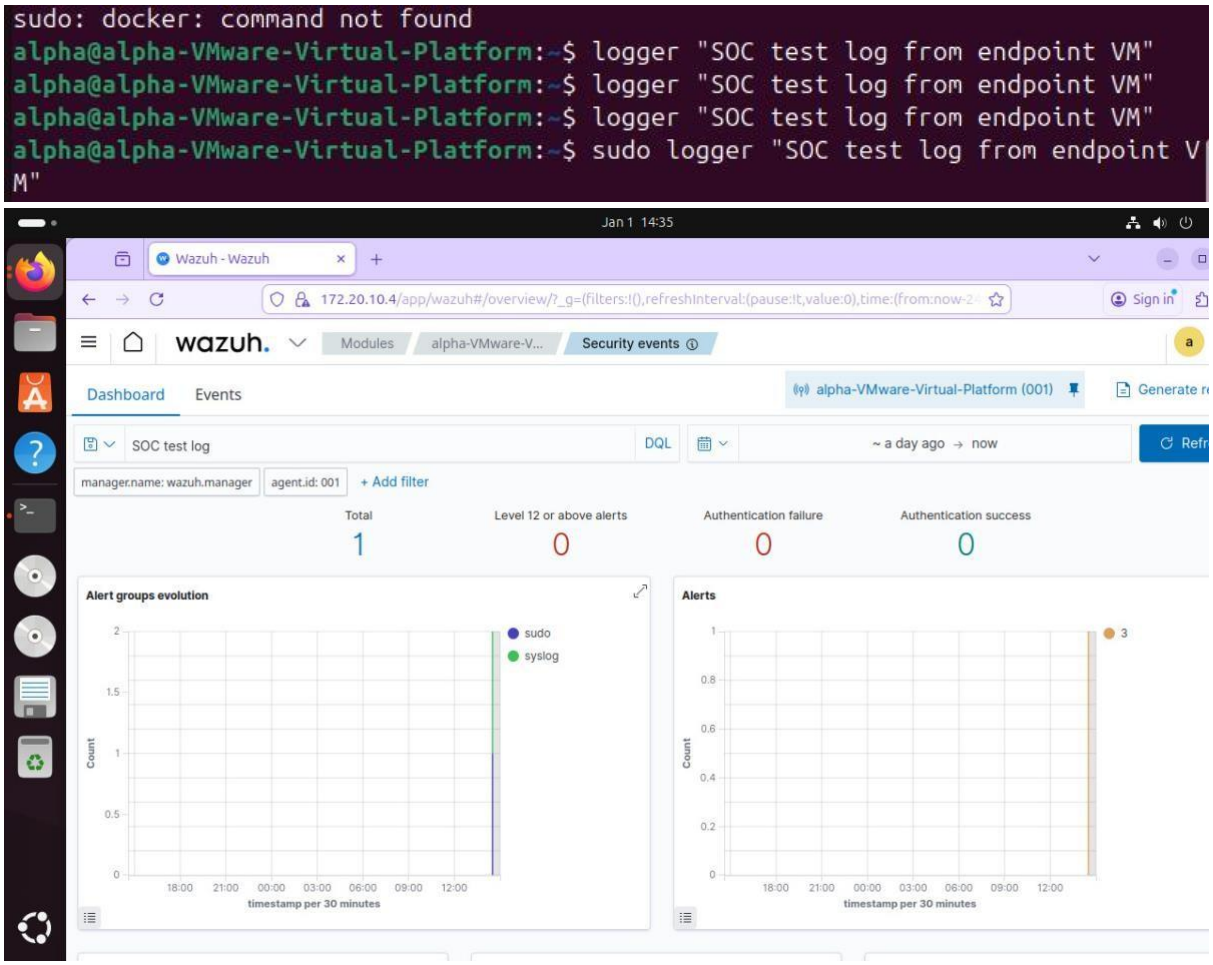
- **Verification**: The SOC dashboard confirmed 100% agent coverage, showing both Ubuntu systems as "Active" and ready for monitoring.



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)

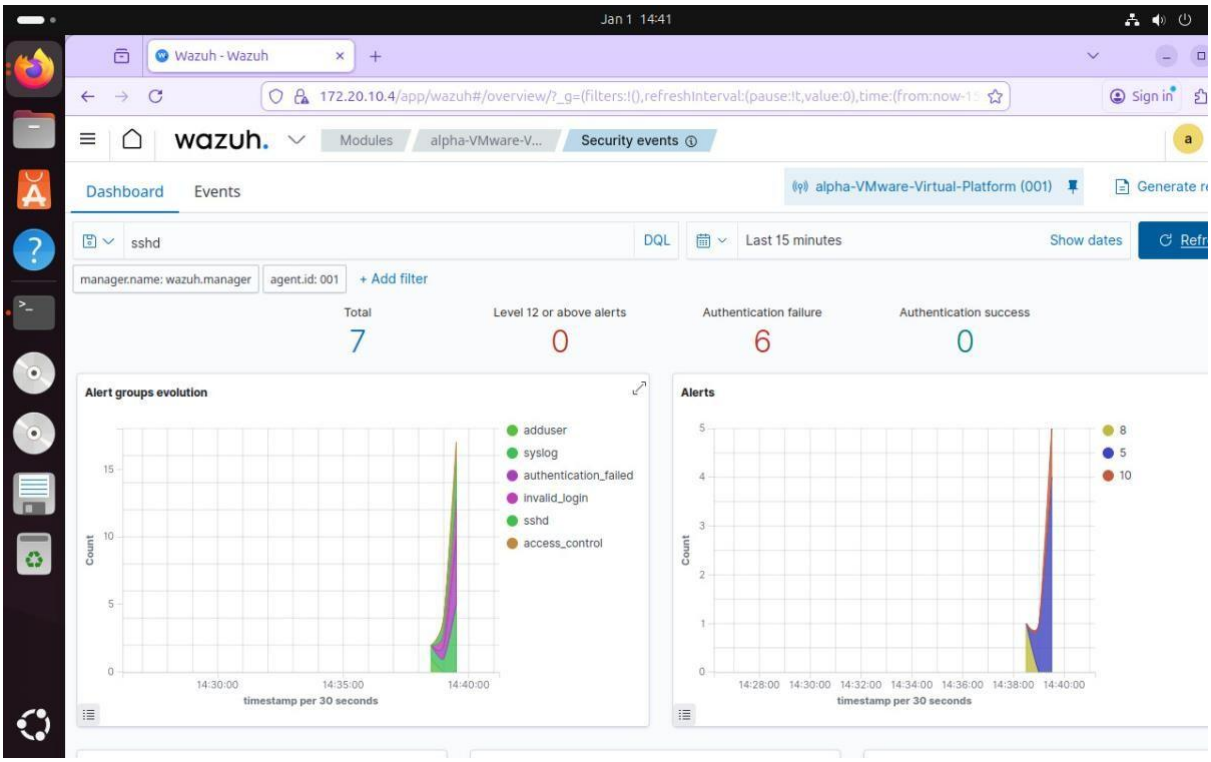
The SOC's primary goal is to detect unauthorized access. We simulated an SSH Brute Force attack targeting one of the Ubuntu agents.

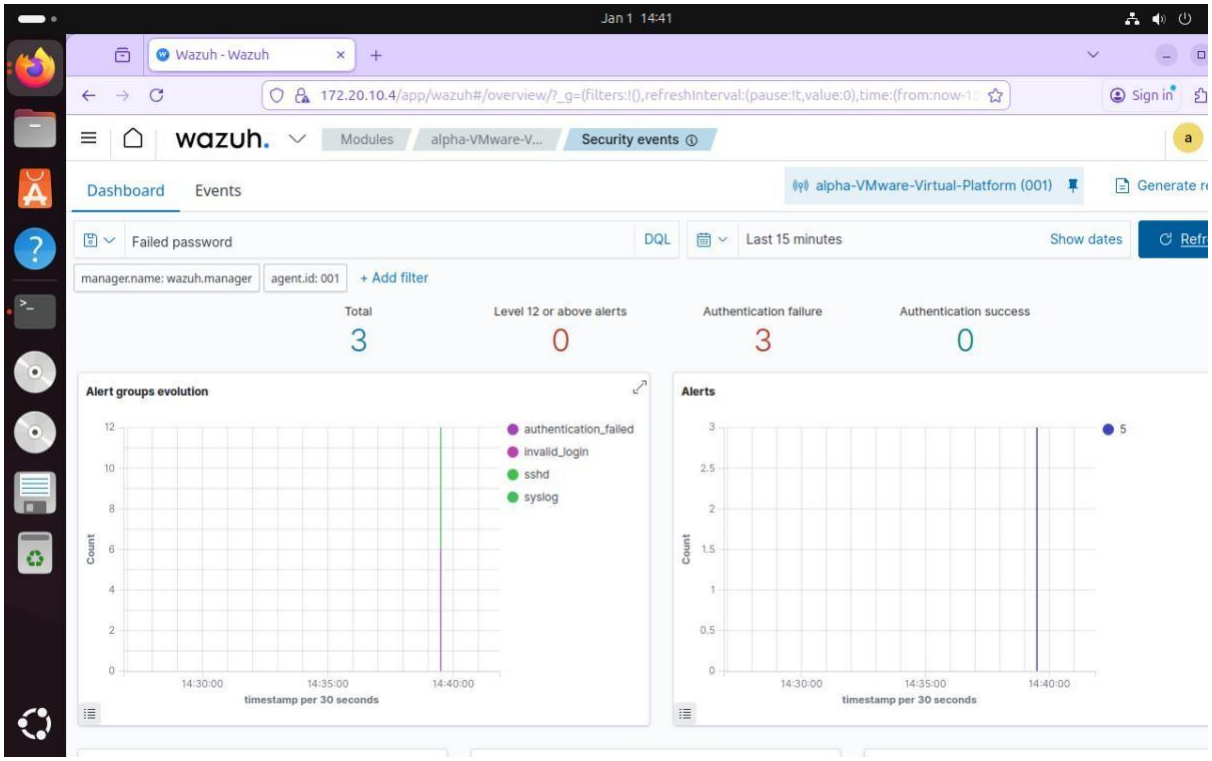
- **Attack Technique**: Multiple failed authentication attempts were made using a non-existent user account (wrong user) via SSH.

- **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.

  ➢ Mapping the incident to the MITRE ATT&CK framework provides:
  Standardized attack classification
  Improved threat intelligence sharing
  Better incident reporting and analysis


Jan 1 14:41
Wazuh - Wazuh
172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15
Sign in
wazuh.
Modules
alpha-VMware-V...
Security events
Dashboard
Events
alpha-VMware-Virtual-Platform (001)
Generate r
sshd
DQL
Last 15 minutes
Show dates
Refr
manager.name: wazuh.manager
agent.id: 001
+ Add filter
Total
7
Level 12 or above alerts
0
Authentication failure
6
Authentication success
0
Alert groups evolution
adduser
syslog
authentication_failed
invalid_login
sshd
access_control
Count
timestamp per 30 seconds
Alerts
8
5
10
14:28:00
14:30:00
14:32:00
14:34:00
14:36:00
14:38:00
14:40:00

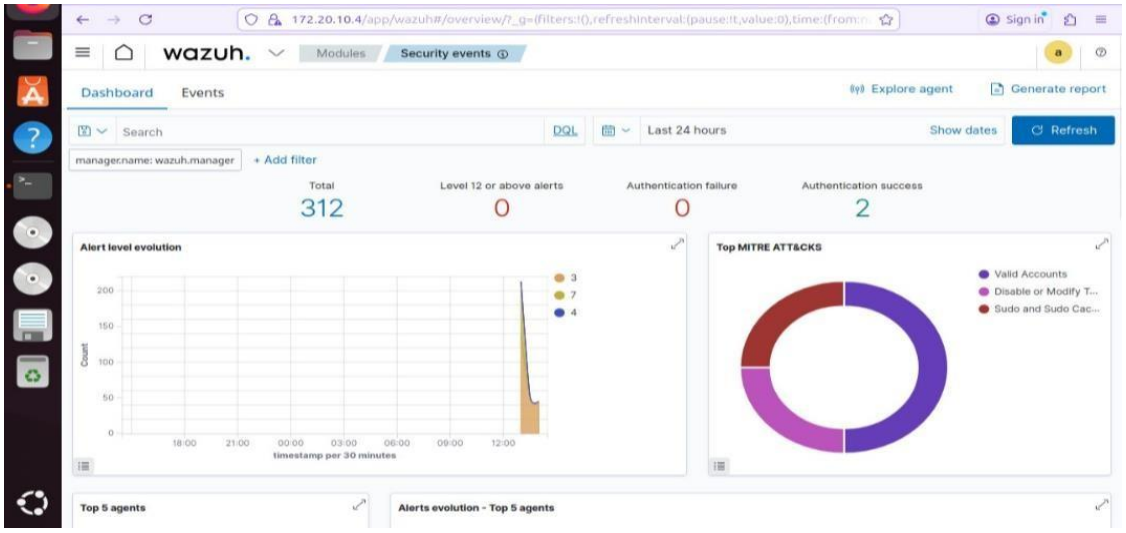

Jan 1 14:41
Wazuh - Wazuh
172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15
Sign in
wazuh.
Modules
alpha-VMware-V...
Security events
Dashboard
Events
alpha-VMware-Virtual-Platform (001)
Generate r
Failed password
DQL
Last 15 minutes
Show dates
Refr
manager.name: wazuh.manager
agent.id: 001
+ Add filter
Total
3
Level 12 or above alerts
0
Authentication failure
3
Authentication success
0
Alert groups evolution
authentication_failed
invalid_login
sshd
syslog
Count
timestamp per 30 seconds
Alerts
5
14:30:00
14:35:00
14:40:00

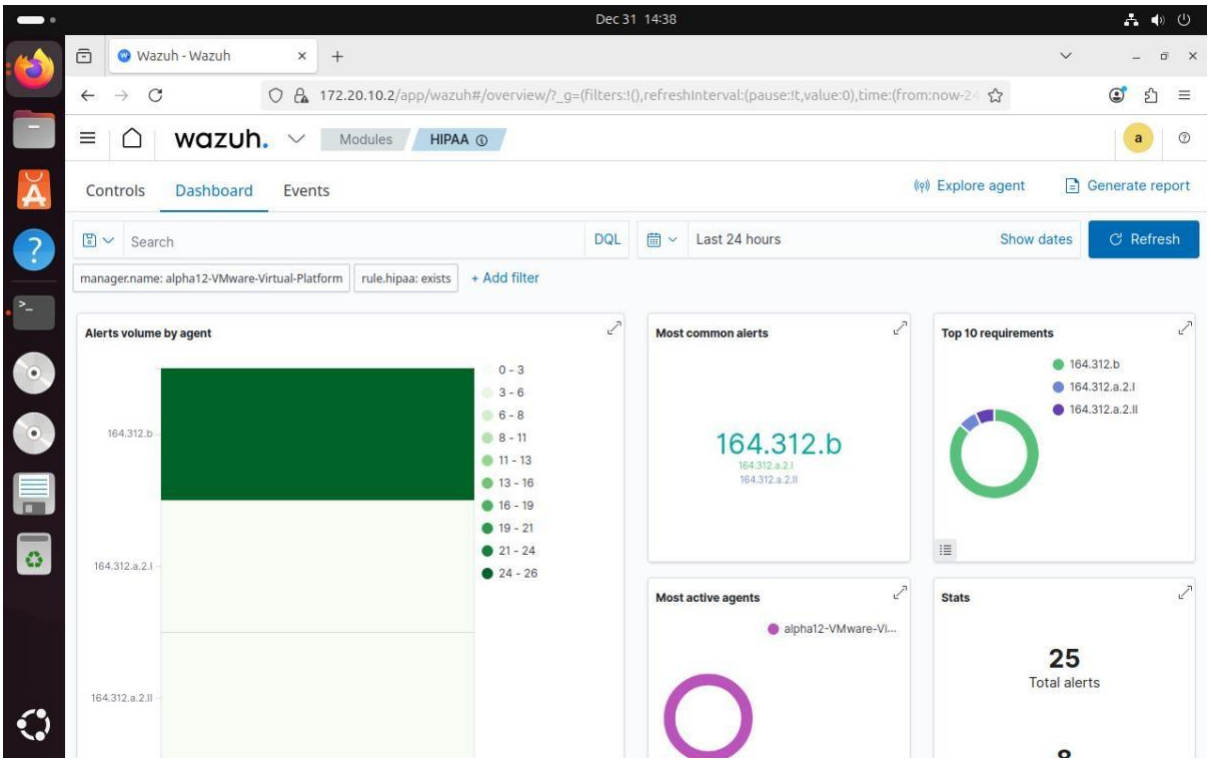
4.2 Framework and Regulatory Mapping

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



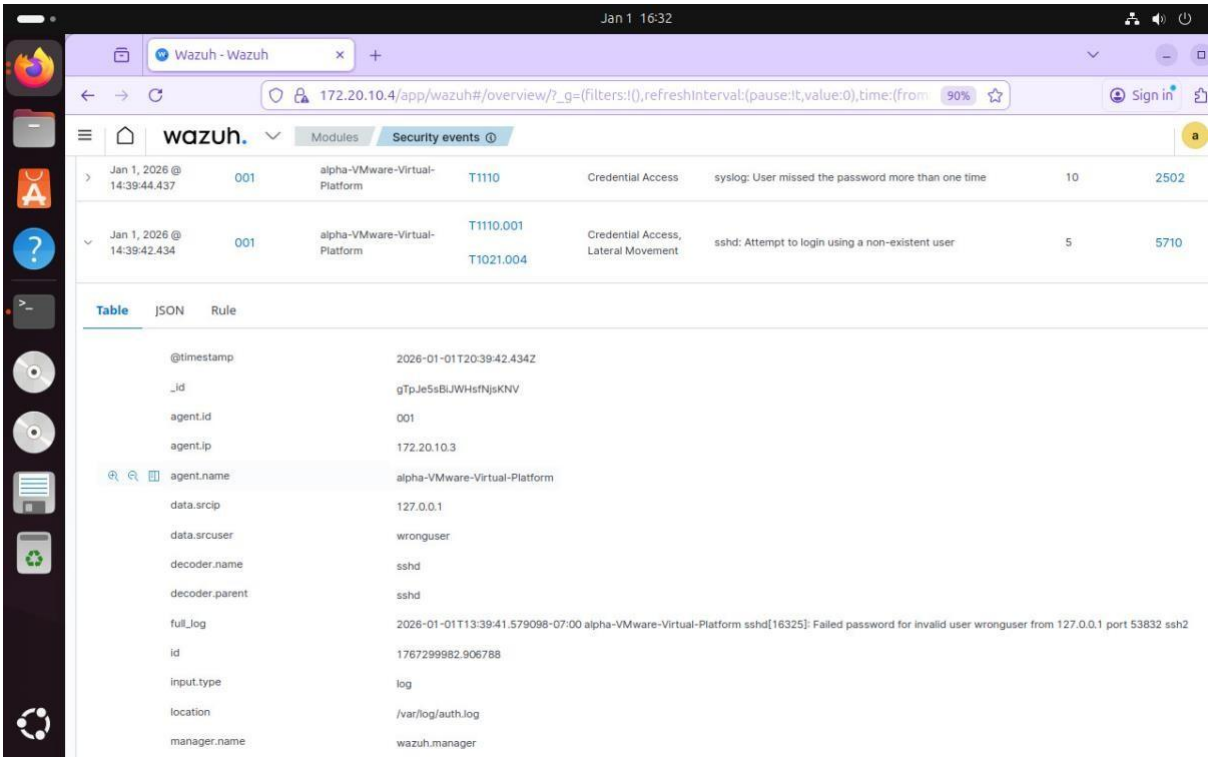

Dec 31 14:38
Wazuh - Wazuh
172.20.10.2/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-2
wazuh.
Modules
HIPAA
Controls
Dashboard
Events
Explore agent
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: alpha12-VMware-Virtual-Platform
rule.hipaa: 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

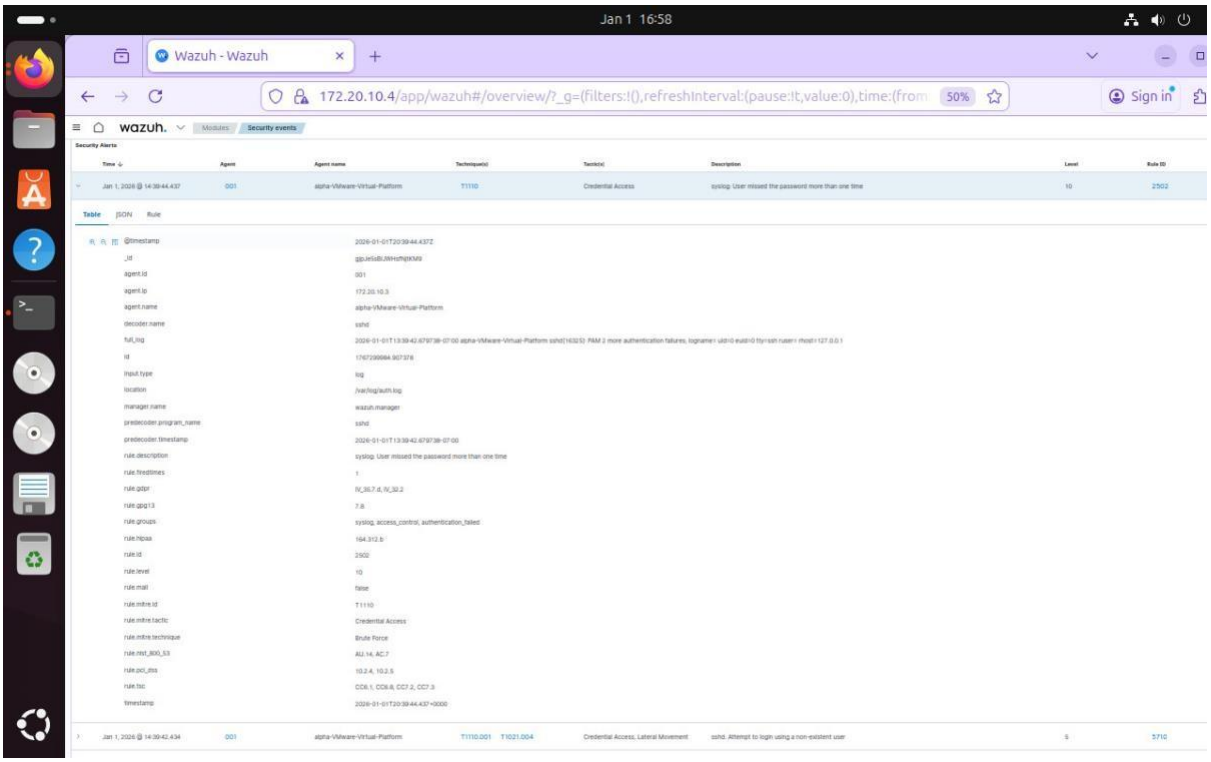
5. Technical Deep-Dive and Health Monitoring

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.

➢ After an alert is generated, a SOC does not stop at detection. Detailed forensic analysis is required to understand the who, what, where, and how of the security incident.

5. Conclusion

The theoretical component established a strong foundation in key areas such as SOC roles and responsibilities, SIEM functionality, security monitoring objectives, log lifecycle management, and core security principles including the CIA triad, defense-in-depth, and zero trust. Industry-standard frameworks such as NIST and MITRE ATT&CK were used to structure detection and response activities, ensuring alignment with real-world SOC practices.

Overall, this task effectively bridged the gap between theory and practice, providing practical insight into real-world SOC workflows, security monitoring, and incident response processes. The knowledge and skills gained through this exercise form a strong foundation for advanced SOC operations, cybersecurity analysis, and professional roles such as SOC Analyst or Incident Responder.