

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.

The screenshot shows the Wazuh Agents preview dashboard at the URL [http://172.20.10.4/app/wazuh#/agents-preview/?_g=\(filters:!\(\),refreshInterval:\(pause:0,value:0\),time:\(from:now-24h,to:now\)\)](http://172.20.10.4/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:0,value:0),time:(from:now-24h,to:now))). The dashboard has three main sections: STATUS, DETAILS, and EVOLUTION.

- STATUS:** A large green circle indicates 1 Active agent. Below it is a legend: Active (1), Disconnected (0), Pending (0), and Never connected (0).
- DETAILS:** Shows the following data:
 - Agents coverage: 100.00%
 - Last registered agent: alpha-VMware-Virtual-Platform
 - Most active agent: alpha-VMware-Virtual-Platform
- EVOLUTION:** A chart showing agent status over the last 24 hours.

Below the dashboard, there is a table titled "Agents (1)" showing the details of the active agent:

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	

At the bottom left, there is a "Rows per page: 10" dropdown. At the bottom right, there are navigation arrows and a page number indicator < 1 >.



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.

The screenshot shows the Wazuh Manager interface. At the top, there is a terminal window displaying a series of log entries:

```
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 VM"
```

Below the terminal, the Wazuh Manager dashboard is visible. It includes a navigation sidebar with icons for Dashboard, Events, Modules, Agents, Security events, and more. The main dashboard area shows summary statistics:

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

Two line charts are displayed below the statistics:

- Alert groups evolution:** A chart showing the count of alerts over time (timestamp per 30 minutes). It shows two data series: sudo (blue dots) and syslog (green dots). The sudo series has one data point at timestamp 0, while the syslog series has three data points at timestamp 1.
- Alerts:** A chart showing the count of alerts over time (timestamp per 30 minutes). It shows a single data point at timestamp 1 with a value of 3.

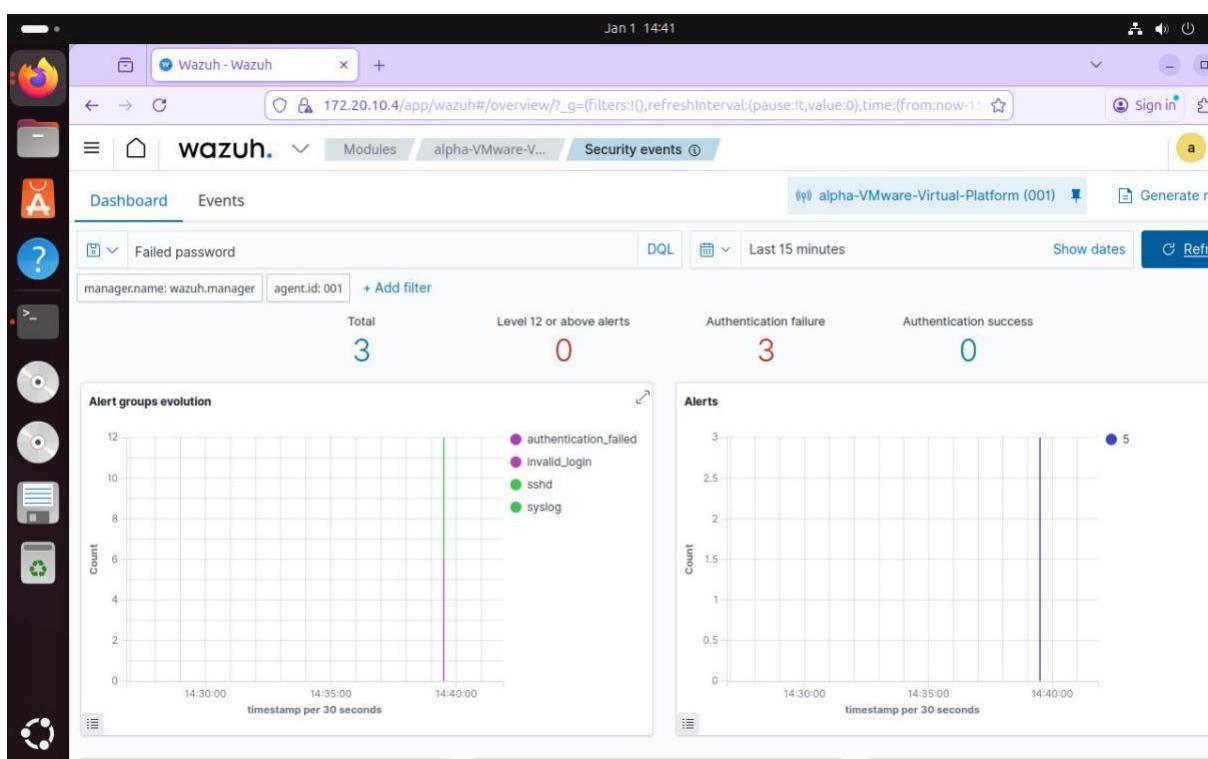
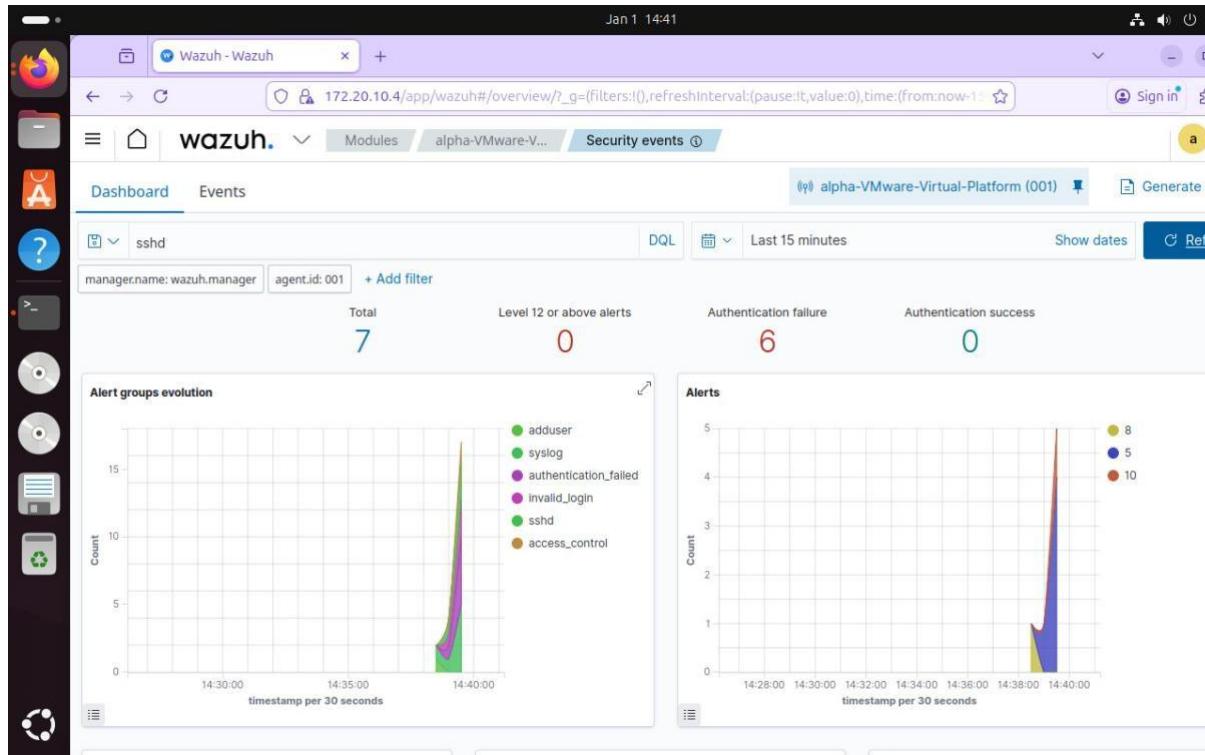


4. Threat Detection and Incident Analysis

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

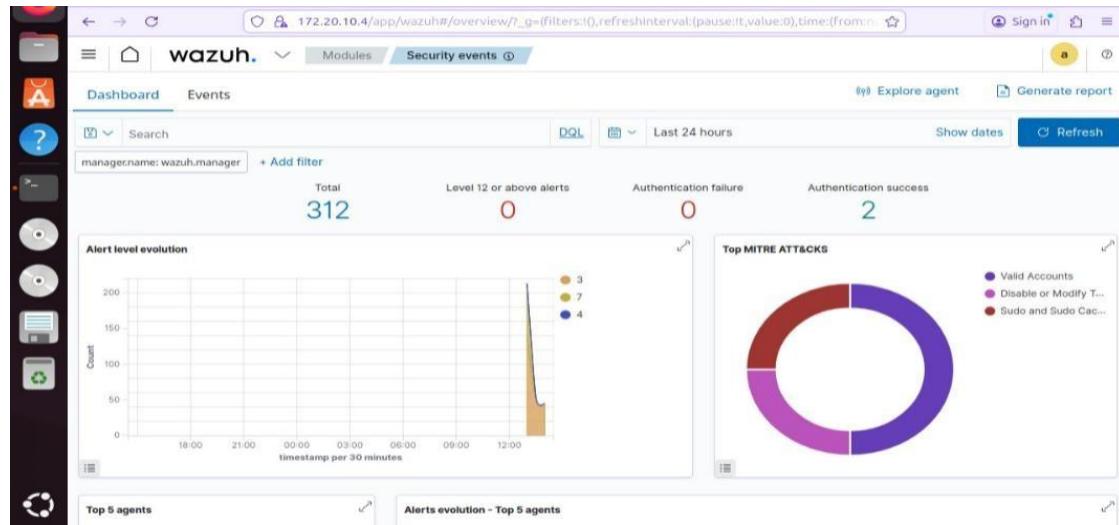


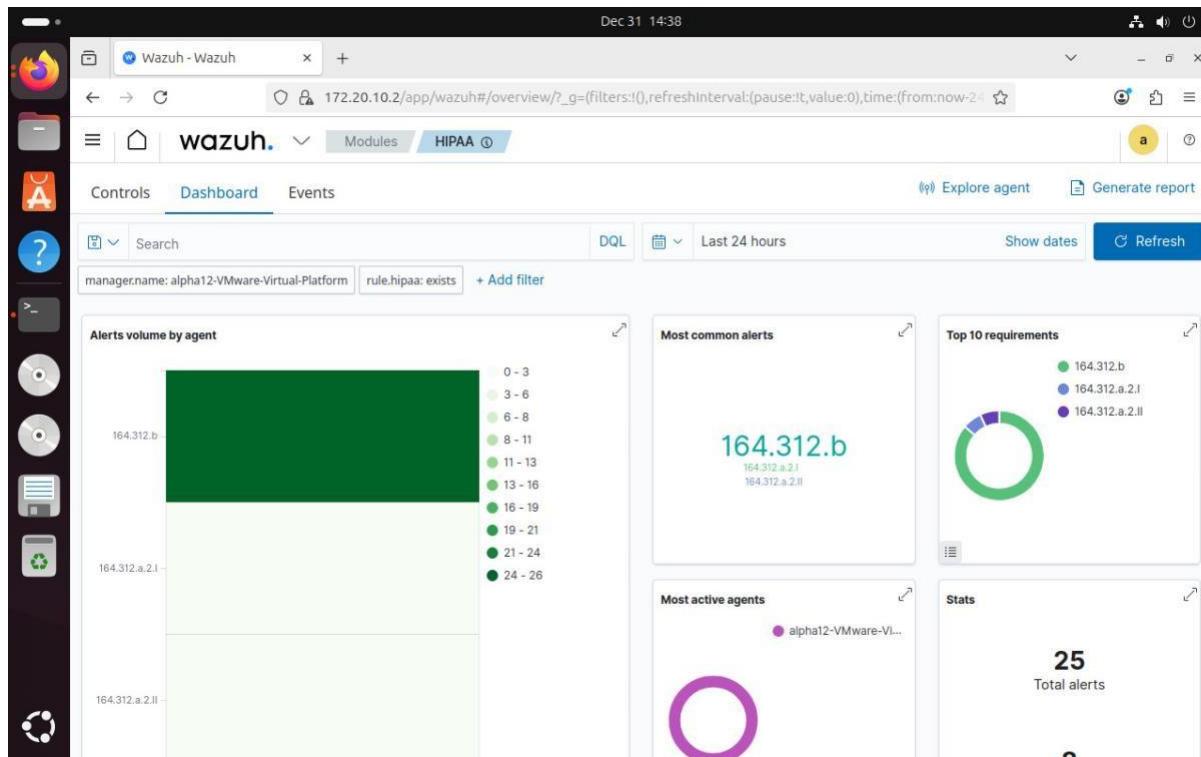


4.2 Framework and Regulatory Mapping

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



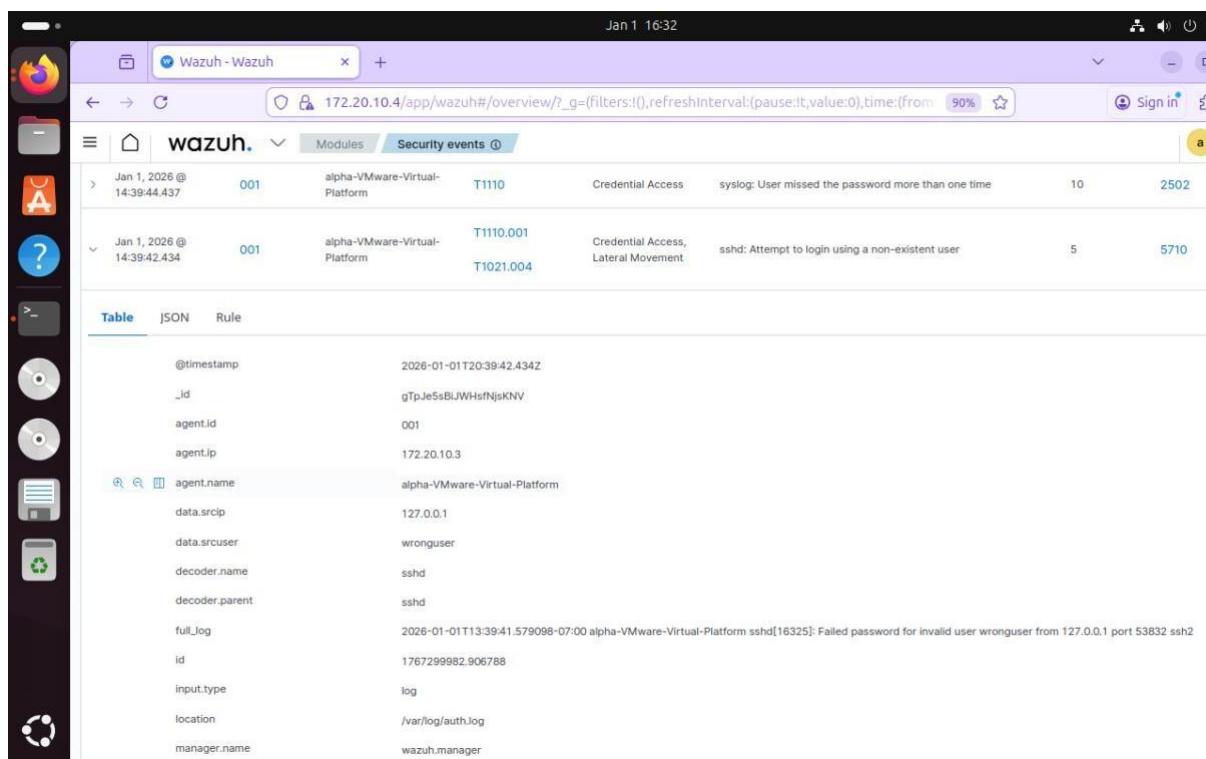


5. Technical Deep-Dive and Health Monitoring

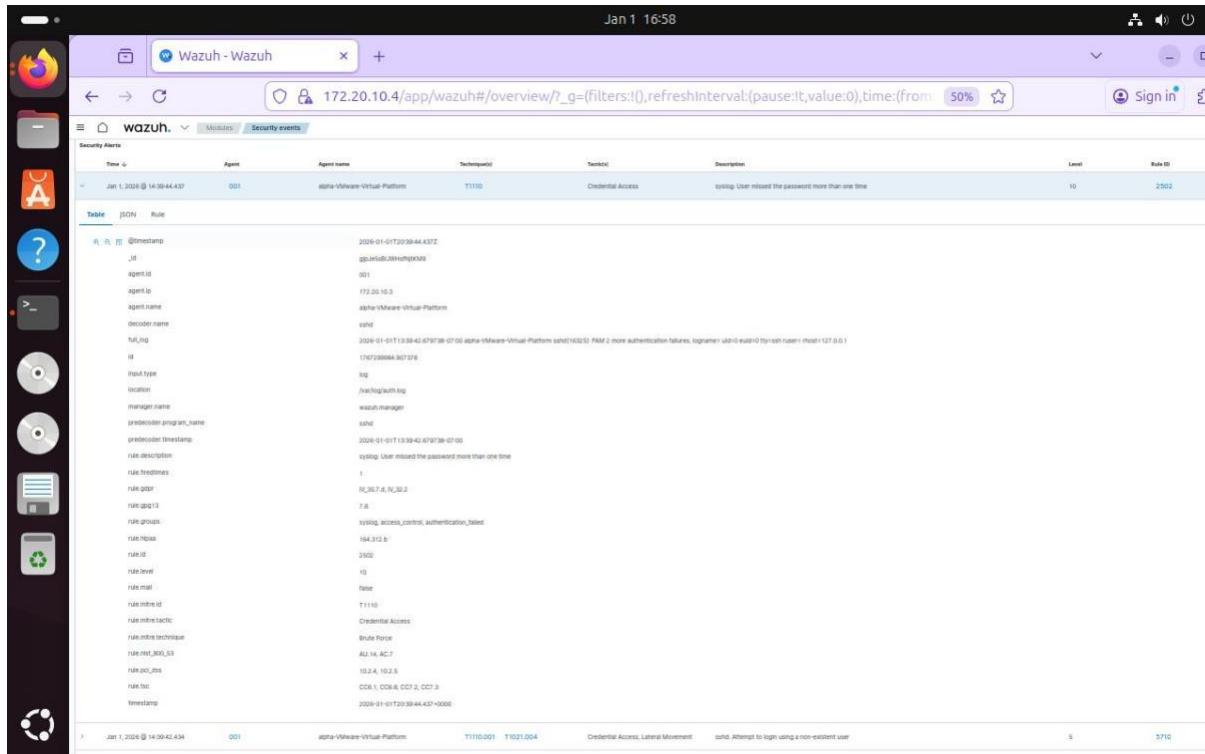
5.1 Forensic Metadata Analysis

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).



Field	Value
@timestamp	2026-01-01T20:39:42.434Z
_id	gTpJe5sBjJWHsfNjsKNV
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	1767299982.06788
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager



The screenshot shows a browser window titled "Wazuh - Wazuh" with the URL "172.20.10.4/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:Jan 1, 2024 at 14:00:44.437,to:Jan 1, 2024 at 14:05:42.434,timezone:UTC))". The main content is a table titled "Security Alerts" with the following data:

Time	Agent	Agent name	TechniqueID	Tactic	Description	Level	Rule ID
Jan 1, 2024 at 14:00:44.437	001	alpha-Vmware-Virtual-Platform	T1110	Credential Access	syslog: User missed the password more than one time	10	2902

The table has a scrollable sidebar on the left containing various log fields such as @timestamp, _id, agent.id, agent.to, agent.name, decoder.name, file, file.raw, id, input.type, location, manager.name, predecoden.program.name, predecoden.timestamp, rule.description, rule.frequency, rule.gid, rule.gid13, rule.groups, rule.hops, rule.id, rule.level, rule.mal, rule.mal_id, rule.mal_tactic, rule.mal_technique, rule.mal_type, rule.mal_type_id, rule.ocid, rule.tct, and timestamp.

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.