

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

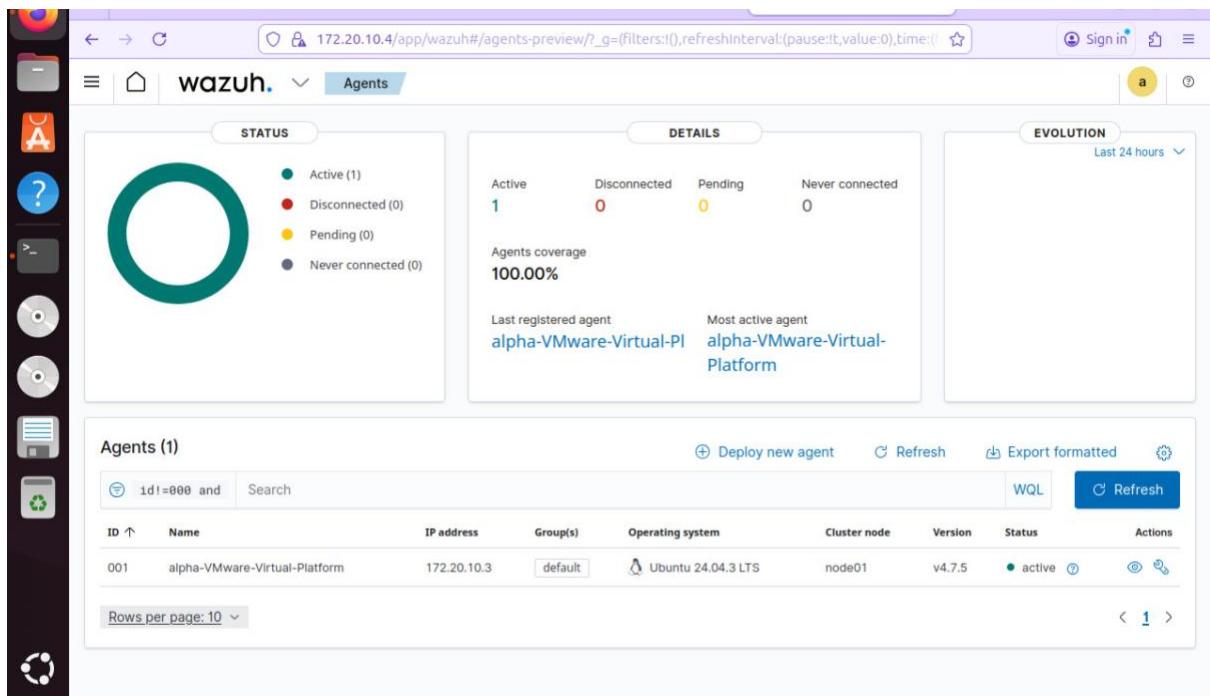
3.1 Agent Deployment and Asset Inventory

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.



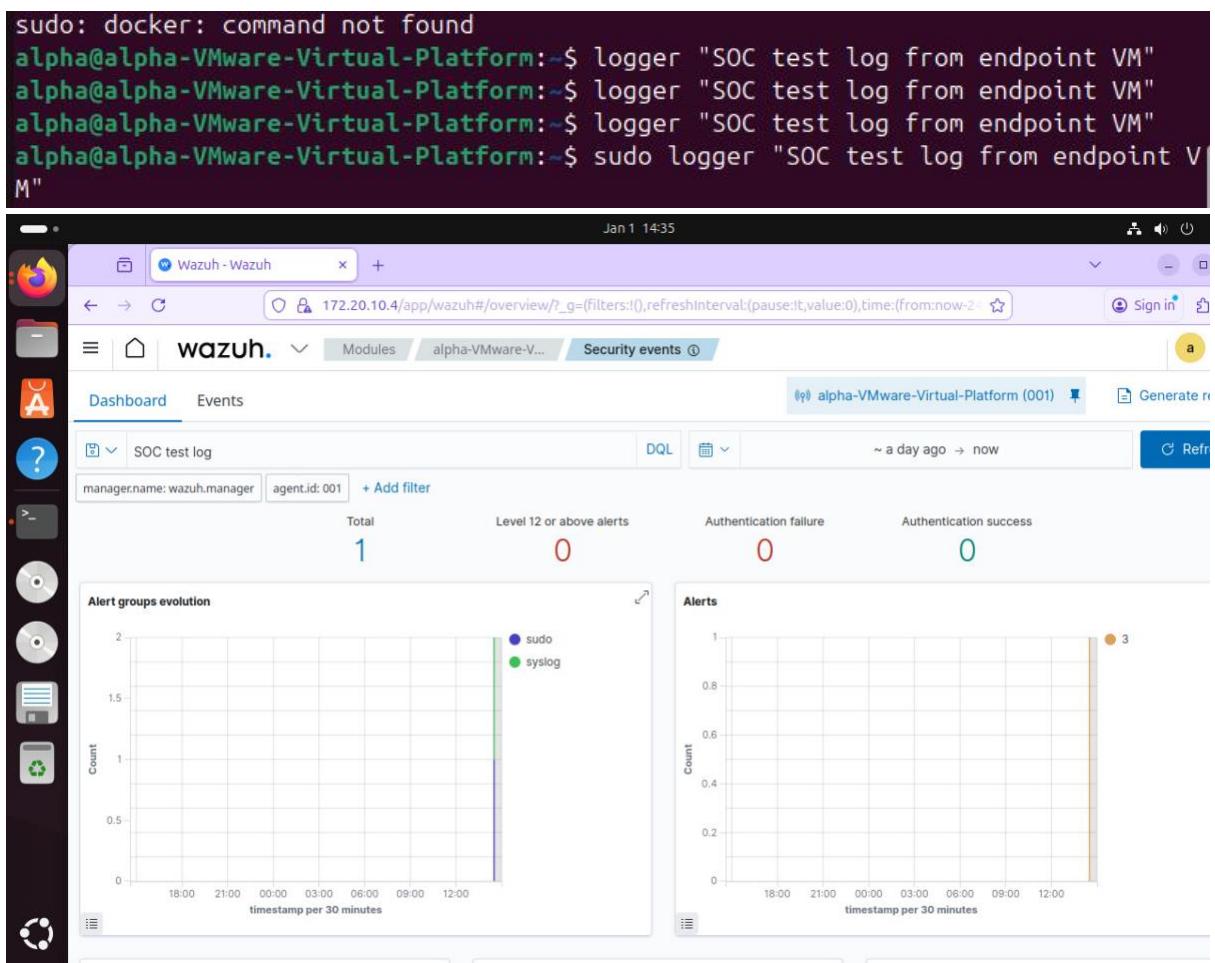
- **Linux Monitoring:** Agent 001 and Agent 002 (Ubuntu 24.04.3 LTS) were configured to communicate with the Manager's IP.
- **Verification:** The SOC dashboard confirmed 100% agent coverage, showing both Ubuntu systems as "Active" and ready for monitoring.



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

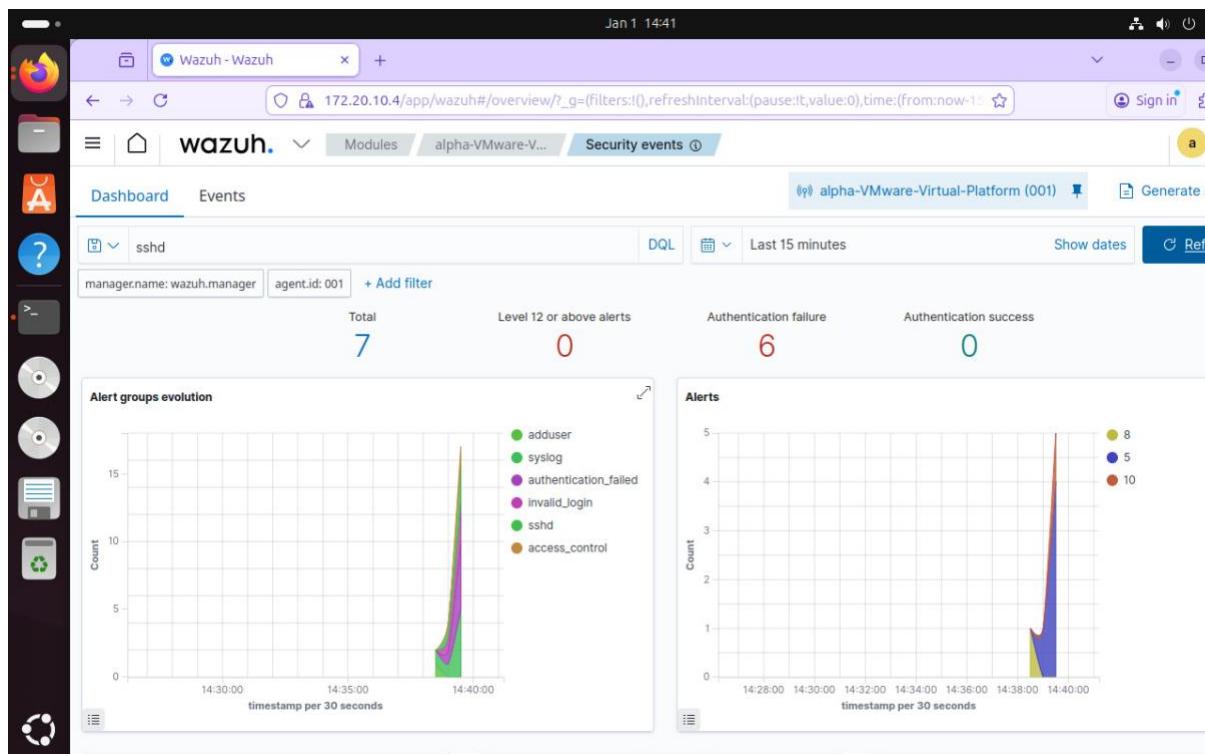
4.1 Brute Force Simulation (SSH on Ubuntu)

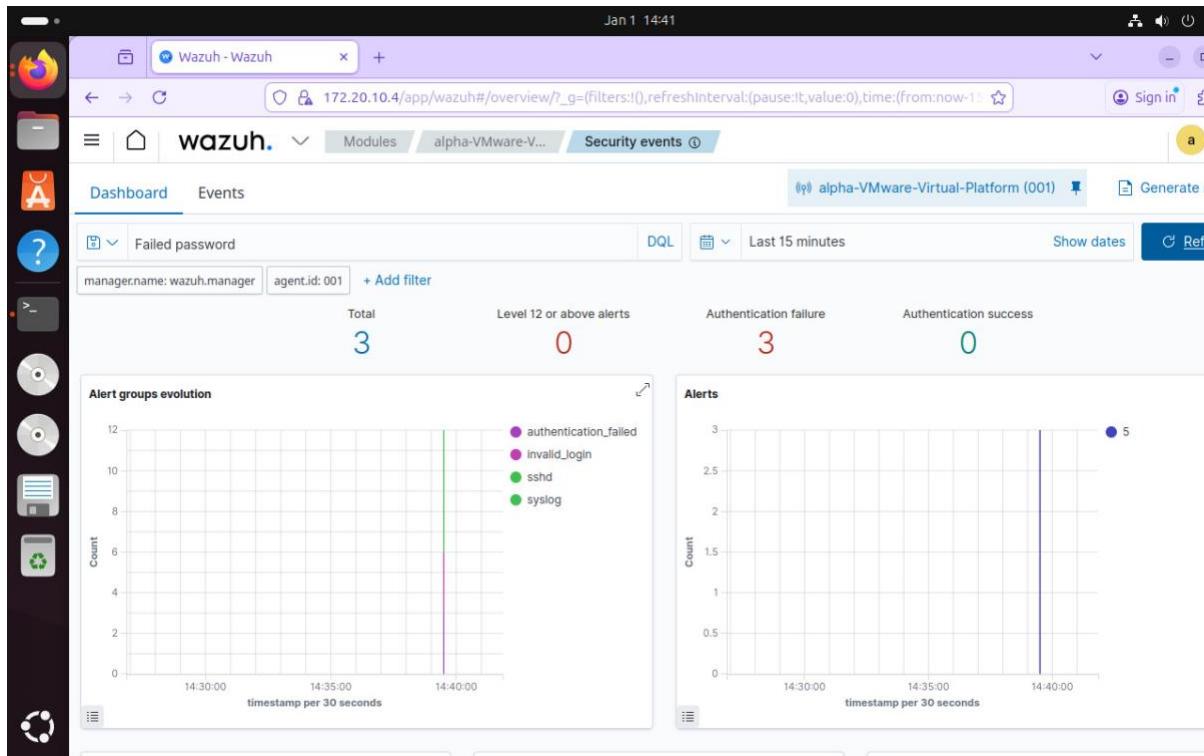
The SOC's primary goal is to detect unauthorized access. We simulated an SSH Brute Force attack targeting one of the Ubuntu agents.

- **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.

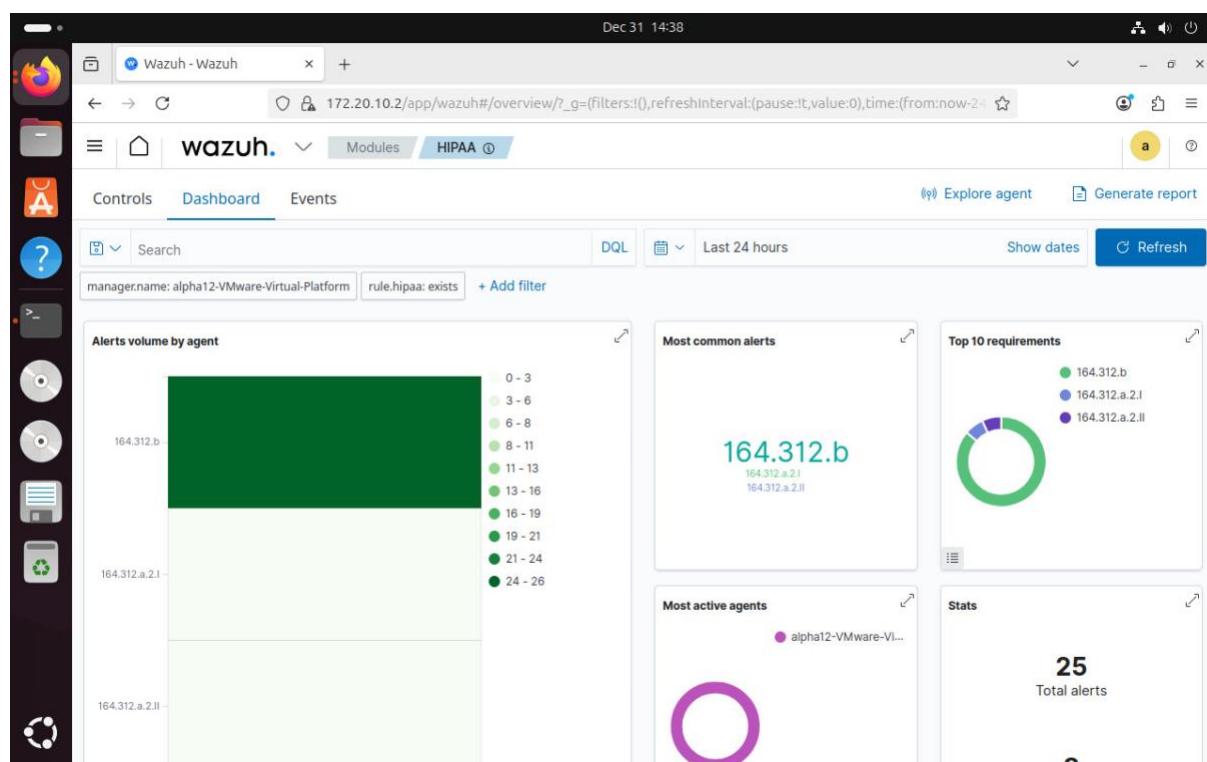
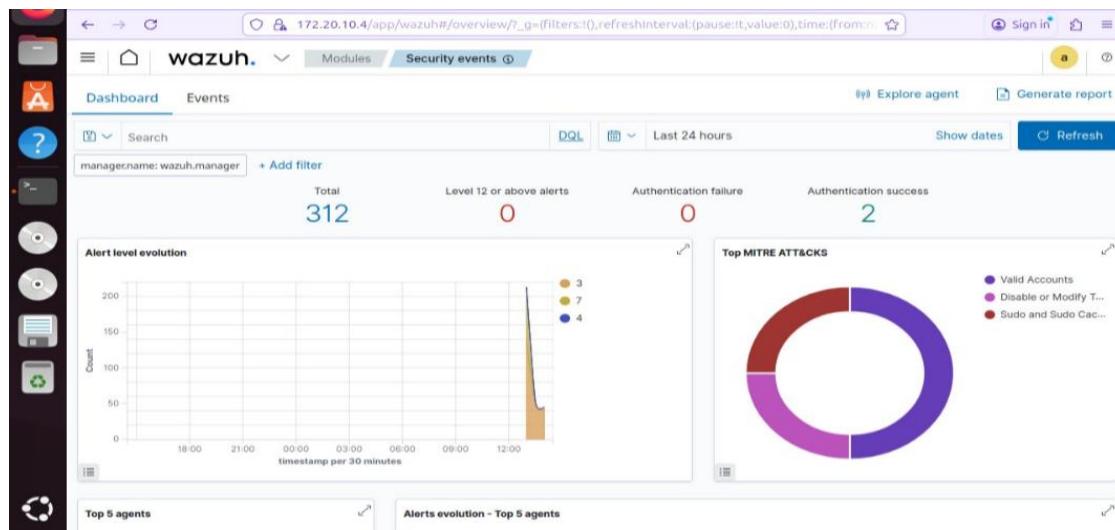




4.2 Framework and Regulatory Mapping

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





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).

The screenshot shows the Wazuh web interface with the URL 172.20.10.4/app/wazuh#/overview/?_g=(filters:(),refreshInterval:(pause:0,value:0),time:(from: Jan 1 16:32)). The interface displays two security events:

Date	User	Host	Rule ID	Description	Severity	Count	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	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5	5710

Below the events, there is a table showing the raw JSON metadata for the second event:

Field	Value
@timestamp	2026-01-01T20:39:42.434Z
_id	gTpJe5sBlJWHstNjsKNV
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:0,value:0),time:(from: 50%, star))

Sign in

wazuh. Modules Security events

Security Alerts

Time	Agent	Agent name	Technique(s)	Tactic	Description	Level	Rule ID
Jan 1, 2024 14:39:44.434	001	alpha-VMware-Virtual-Platform	T1110	Credential Access	syslog: User missed the password more than one time	10	2702

Table JSON Rule

01: 01: 01: @timestamp 2024-01-01T13:39:44.437Z
agent_id 001
agent_ip 172.20.10.3
agent_name alpha-VMware-Virtual-Platform
decoder_name stdh
full_log 2024-01-01T13:39:42.479738-07:00 alpha-VMware-Virtual-Platform stdh|T1110|PAM 2 more authentication failures; logname=ultron|exitid=0|tryauth failed|realm=127.0.0.1|1747299004.907378
id 1
input_type log
location /var/log/auth.log
manager_name wazuh manager
predecoder_program_name wazuh manager
predecoder_timestamp 2024-01-01T13:39:42.479738-07:00
rule_description syslog: User missed the password more than one time
rule_firstrule 1
rule_gpr R_30.7_A, R_32.2
rule_gpt3 7.8
rule_groups syslog, access_control, authentication_failed
rule_ipmask 194.312.0
rule_id 2902
rule_level 10
rule_mail false
rule_min_id T1110
rule_min_tactic Credential Access
rule_min_technique Brute Force
rule_mit_800_53 All_H_A_C_F
rule_out_dos 10.2.4, 10.2.5
rule_out_ses CCIA, CCIA_B, CC7.2, CC7.3
rule_src_ip 2024-01-01T20:39:44.437+0000
timestamp

Jan 1, 2024 14:39:42.434 001 alpha-VMware-Virtual-Platform T1110.001 T1021.004 Credential Access, Lateral Movement stdh, Attempt to login using a non-existent user

5 5702

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.



CYART

inquiry@cyart.io

www.cyart.io