Implementation of a Centralized SOC Monitoring Environment and Threat Detection using Wazuh SIEM

Kanchi Kakkad
SOC Task-1

1. SOC Fundamentals and Architecture

The primary purpose of a **Security Operations Center (SOC)** is to provide proactive threat detection, continuous monitoring, and rapid incident response. A modern SOC relies on a specialized hierarchy of personnel:

- **Tier 1 Analysts**: Responsible for initial alert triage and monitoring.
- **Tier 2/3 Analysts**: Handle deep-dive investigations and advanced threat hunting.
- **SOC Managers**: Oversee the entire operation and integrate threat intelligence.

Common frameworks like **NIST SP 800-61** and **MITRE ATT&CK** are used to standardize how these teams identify and respond to attacks.

2. SIEM and Security Monitoring

A **Security Information and Event Management (SIEM)** system, such as Wazuh or Elastic, serves as the "brain" of the SOC.

- **Objectives**: The system is designed to detect anomalies, unauthorized access, and policy violations across the network.

- **Key Metrics**: Performance is measured by **MTTD (Mean Time to Detect)** and the ability to minimize false positives and negatives.

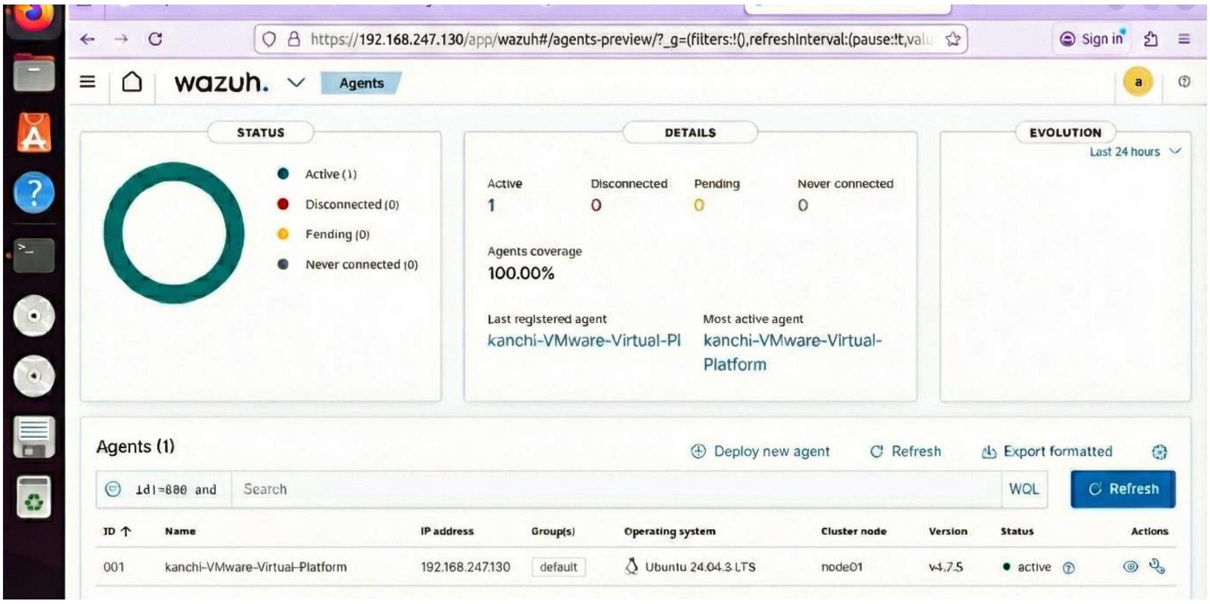
3. Operational Implementation

3.1 Endpoint Synchronization & Deployment

The security perimeter was established by deploying Wazuh agents across two Ubuntu endpoints.

- **Deployment Method:** Leveraged native Linux package management to ensure seamless integration with the host OS.

- **Asset Connectivity:** Both nodes (Agent 001 and Agent 002) were synchronized with the primary Manager, achieving a 100% active operational status.



https://192.168.247.130/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,valu
Sign in
wazuh.
Agents
a

STATUS

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

DETAILS

Active	Disconnected	Pending	Never connected
1	0	0	0

Agents coverage
100.00%

Last reglstered agent
kanchi-VMware-Virtual-Pl

Most active agent
kanchi-VMware-Virtual-Platform

EVOLUTION
Last 24 hours

Agents (1)

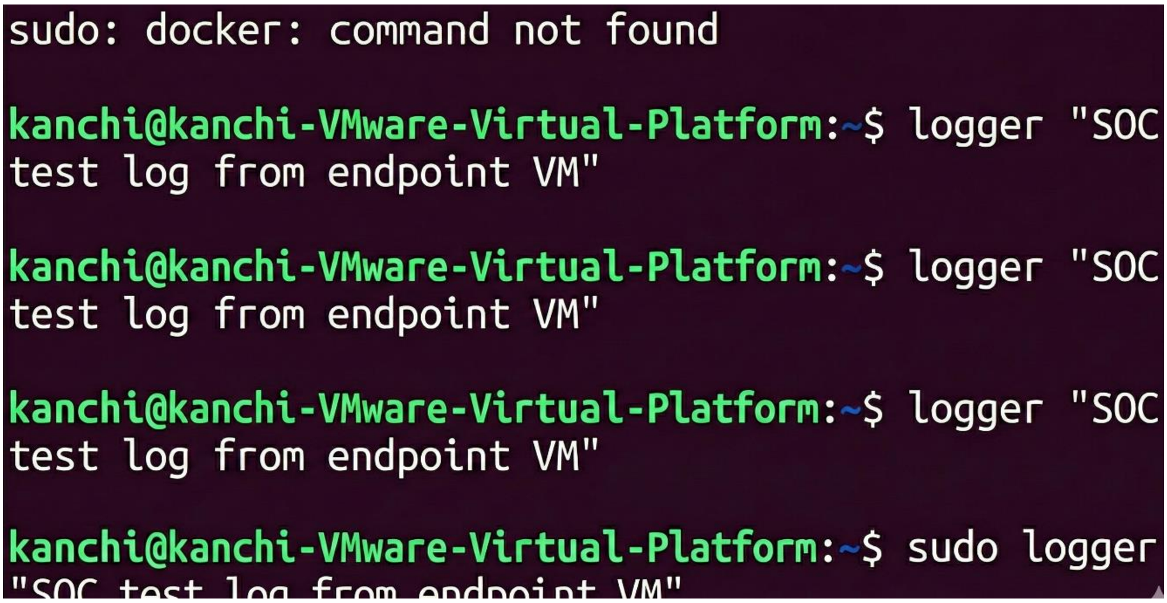
Deploy new agent
Refresh
Export formatted
ıdl=880 and
Search
WQL
Refresh

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	kanchi-VMware-Virtual-Platform	192.168.247.130	default	Ubuntu 24.04.3 LTS	node01	v4.7.5	● active	

3.2 Data Integrity & Log Forwarding Tests

To confirm that the telemetry pipeline was secure and functional, a series of manual log injection tests were performed.

- **Simulation:** Generated custom system logs using the logger command to simulate local system events.
- **Verification:** The Manager successfully captured the string "SOC test log from endpoint VM", validating that the agent-to-manager forwarding path is reliable.



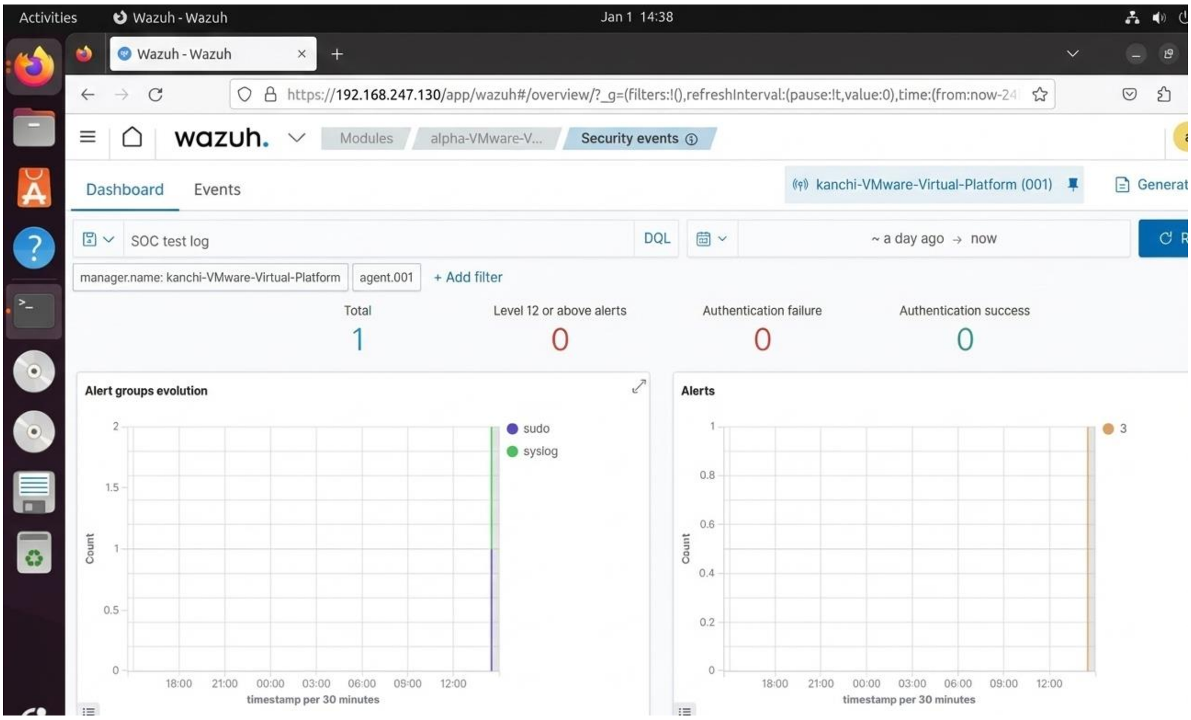
```
sudo: docker: command not found

kanchi@kanchi-VMware-Virtual-Platform:~$ logger "SOC test log from endpoint VM"

kanchi@kanchi-VMware-Virtual-Platform:~$ logger "SOC test log from endpoint VM"

kanchi@kanchi-VMware-Virtual-Platform:~$ logger "SOC test log from endpoint VM"

kanchi@kanchi-VMware-Virtual-Platform:~$ sudo logger "SOC test log from endpoint VM"
```



SOC test log

manager.name: kanchi-VMware-Virtual-Platform agent.001

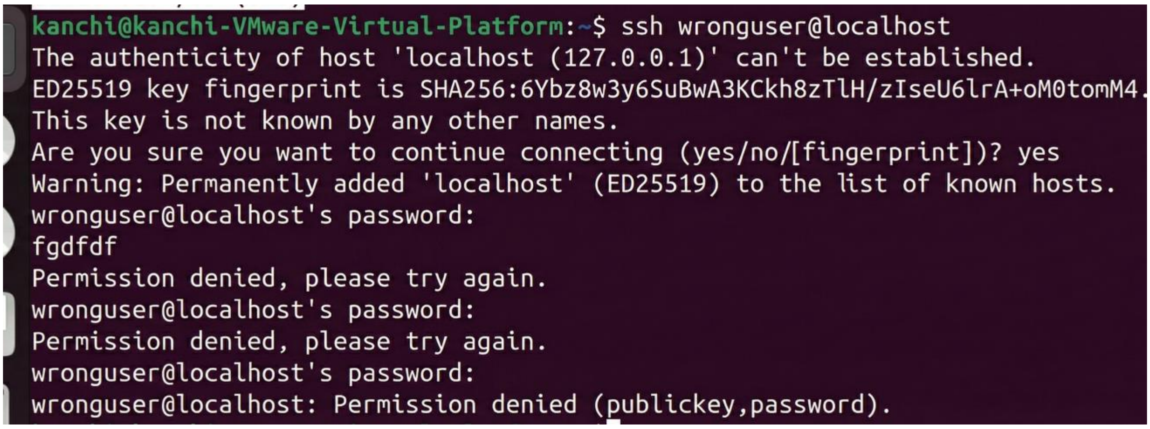
Total	Level 12 or above alerts	Authentication failure	Authentication success
1	0	0	0

4. Threat Detection & Compliance Mapping

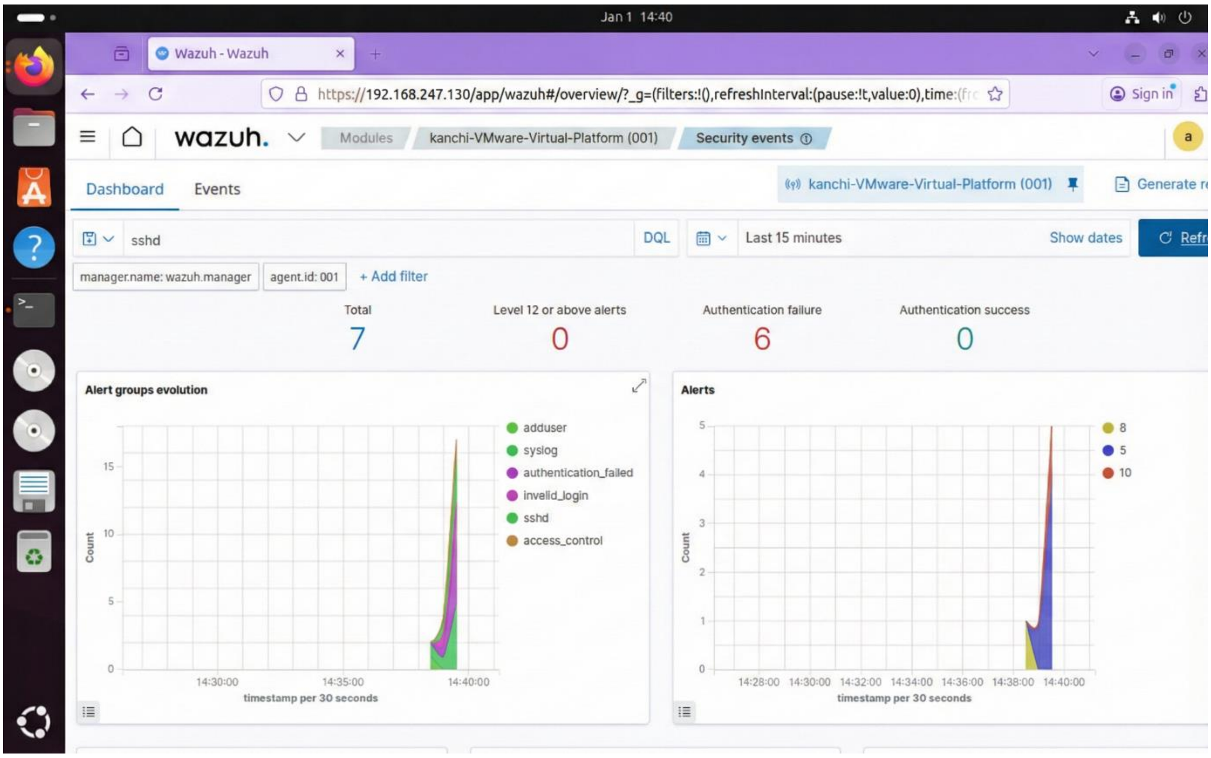
4.1 Brute-Force Authentication Attack Simulation

A controlled security test was conducted to evaluate the SIEM’s detection logic against unauthorized access attempts.

- **The Attack:** Initiated high-frequency SSH connection attempts targeting non-existent user accounts (wronguser).
- **Detection Result:** The system triggered immediate high-priority alerts for "Failed Password" and "Authentication Failure".
- **Log Correlation:** The Manager correlated entries from /var/log/auth.log to identify the source of the malicious activity.



```
kanchi@kanchi-VMware-Virtual-Platform:~$ ssh wronguser@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:6Ybz8w3y6SuBwA3KCkh8zTlH/zIseU6lrA+oM0tomM4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
wronguser@localhost's password:
fgdfdf
Permission denied, please try again.
wronguser@localhost's password:
Permission denied, please try again.
wronguser@localhost's password:
wronguser@localhost: Permission denied (publickey,password).
```



Wazuh - Wazuh

https://192.168.247.130/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(fr

wazuh. Modules / kanchi-VMware-Virtual-Platform (001) / Security events

Dashboard Events

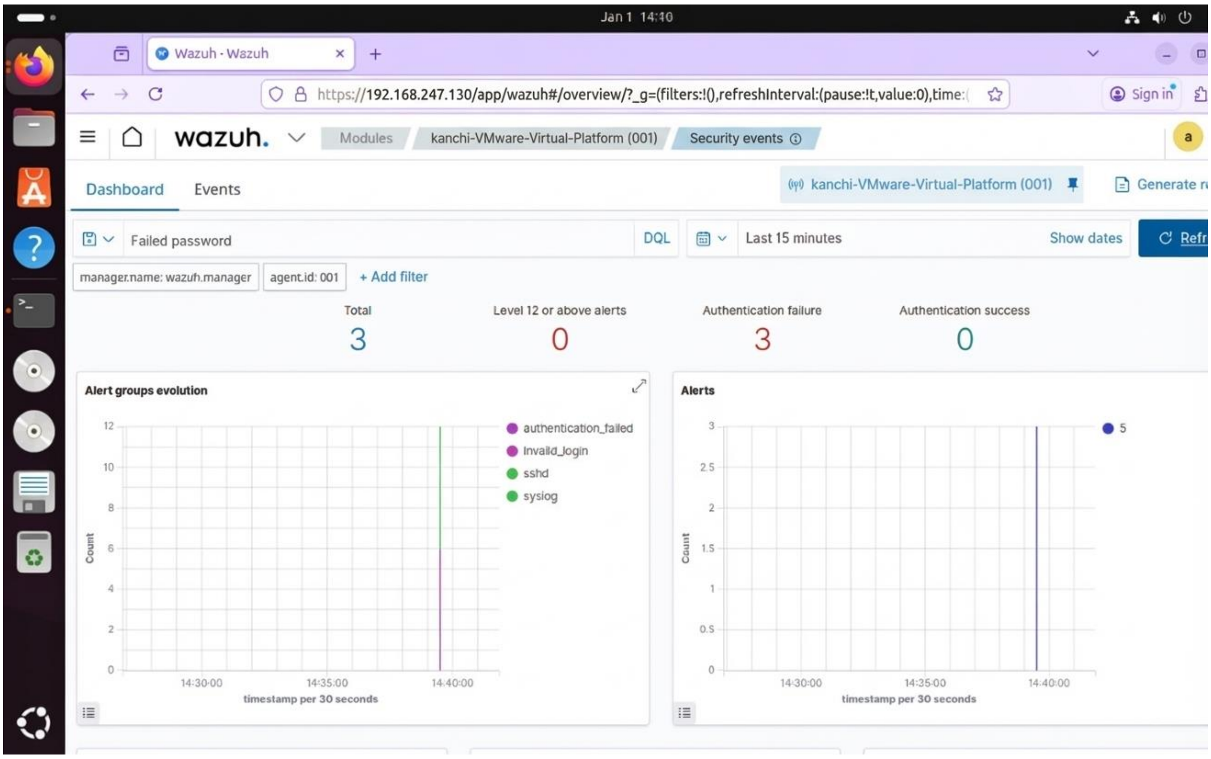
kanchi-VMware-Virtual-Platform (001)

sshd

DQL Last 15 minutes Show dates

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

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



Wazuh - Wazuh

https://192.168.247.130/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(

wazuh. Modules / kanchi-VMware-Virtual-Platform (001) / Security events

Dashboard Events

kanchi-VMware-Virtual-Platform (001)

Failed password

DQL Last 15 minutes Show dates

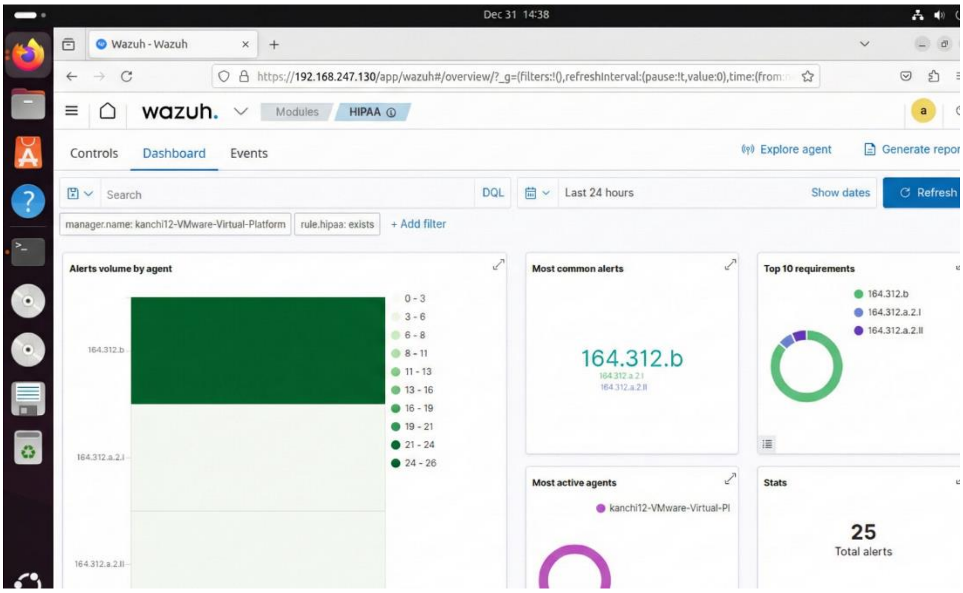
manager.name: wazuh.manager agent.id: 001 + Add filter

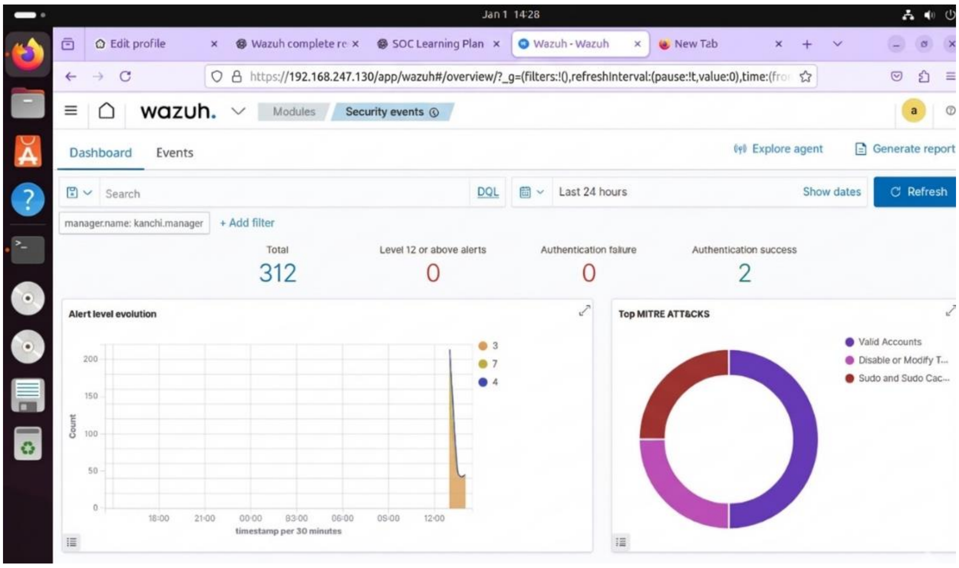
Total	Level 12 or above alerts	Authentication failure	Authentication success
3	0	3	0

3.2 Framework Alignment (MITRE & HIPAA)

To ensure the SOC operations meet global security and legal standards, all triggered events were mapped to standardized frameworks:

- **Credential Access** tactic.
- **Compliance Validation:** Alerts were cross-referenced against **HIPAA 164.312.b**, confirming that the system provides the required audit controls for technical safeguards.

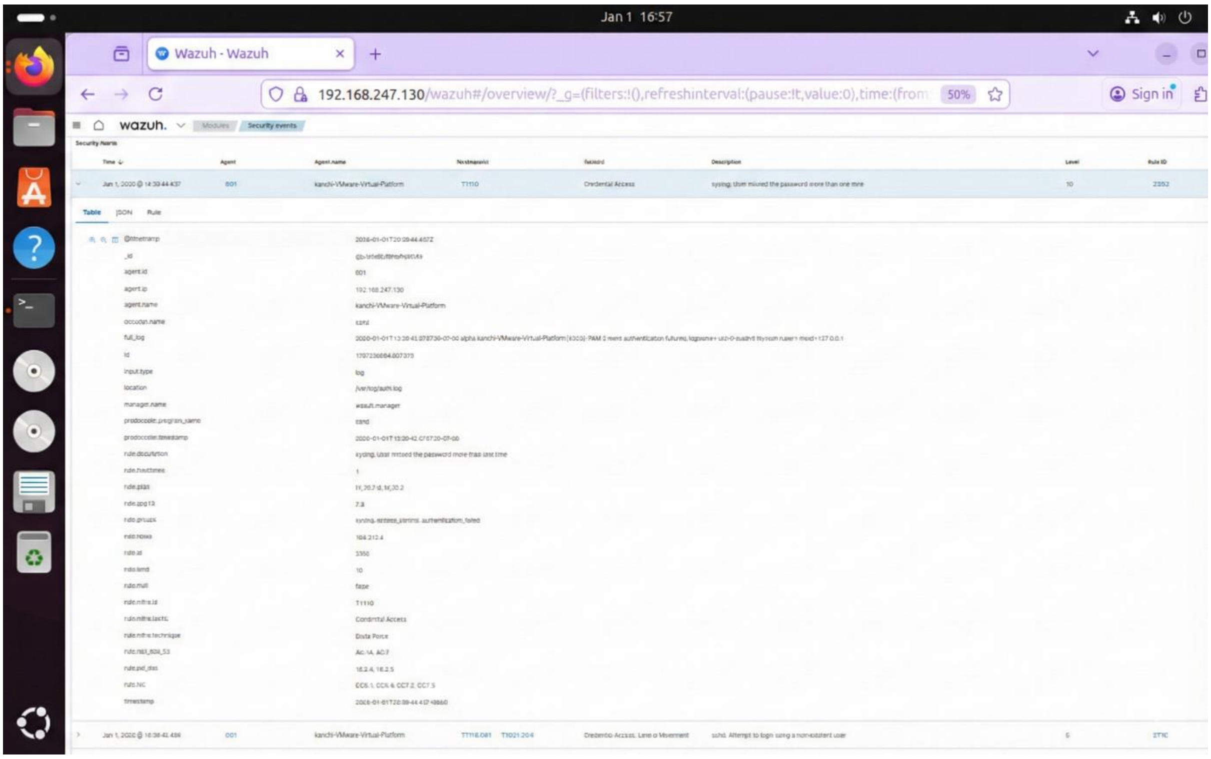




4. Forensic Analysis & System Health

4.1 Granular Event Metadata

Analysis of the raw JSON metadata provided the necessary intelligence for incident response, including the source IP (127.0.0.1), the specific rule IDs triggered (5710, 2502), and the precise timestamp of the intrusion attempt.


Jan 1 16:57
Wazuh - Wazuh
192.168.247.130/wazuh#/overview/?_g=(filters:!(),refreshinterval:(pause:!t,value:0),time:(from
50%
Sign in
wazuh.
Modules
Security events
Security Alerts
Table
JSON
Rule

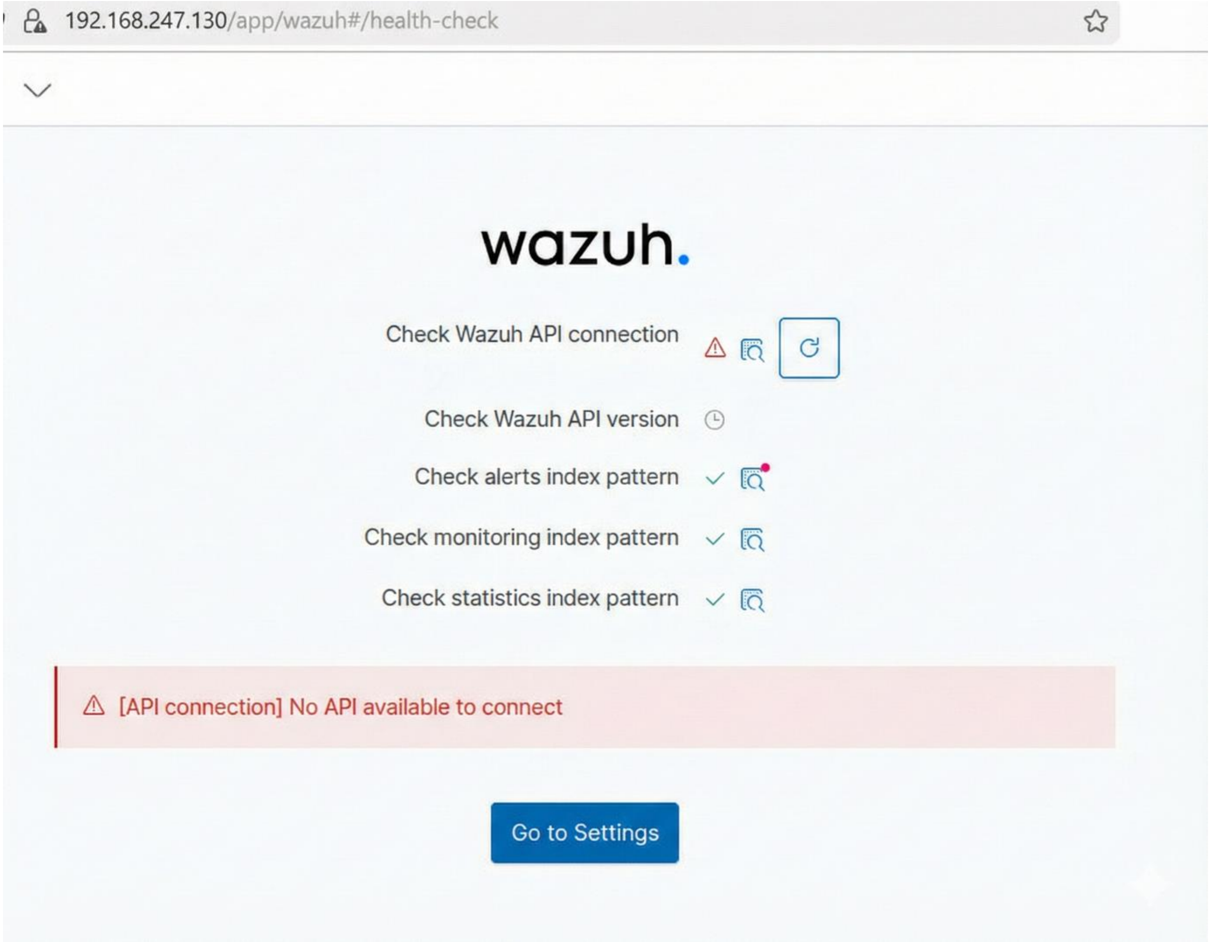
Time ↓	Agent	Agent.name	Nextmapsid	Tacticrd	Description	Level	Rule ID
Jun 1, 2000 @ 14:30:44.437	601	kanchi-VMware-Virtual-Platform	T1110	Credential Access	sysing, Usm miured the password more than one mne	10	2352
Jan 1, 2020 @ 16:38:41.486	001	kanchi-VMware-Virtual-Platform	T1116.081 T1021.204	Credenbo Access, Lene o Movement	sshd. Attempt to login using a non-existent user	5	3710

@timetamp	2026-01-01T20:20:44.407Z
_id	gb-lvbeBLfBmthqstU4a
agent.id	001
agent.ip	192.168.247.130
agent.name	kanchi-VMware-Virtual-Platform
occodsn.name	sand
full_log	2000-01-01T13:20:41.078730-07-00 alpha kanchi-VMware-Virtual-Platform (6300)- PAM 2 ment authentication futured, logpsne+ uid-0-euidn5 ttynsoh ruser+ modd+127.0.0.1
id	1707236664.607379
input.type	log
location	/var/log/auth.log
manager.name	wazuh.manager
prodocoole.pregran_name	sand
prodoccoler.timestamp	2000-01-01T13:20:42.c76720-07-00
rule.docufution	sydng, Ussr mtsed the password more tras last time
rule.heutimes	1
rule.plan	1Y_20.7.d, M_20.2
rule.gpg13	7.8
rule.pruuzk	syding-sntees_sinini. authentication_failed
rule.hows	104.212.4
rule.id	3350
rule.lend	10
rule.mull	fape
rule.mitre.id	T1110
rule.mitre.tactic	Condrntal Accets
rule.mitre.technique	Dista Porce
rule.nist_800_53	Ac.1A, AC.7
rule.pd_dss	18.2.4, 18.2.5
rule.NC	CC6.1, CC6.8, CC7.2, CC7.5
timestamp	2026-01-01T20:39:44.437+0660

4.2 Manager Connectivity Audit

During system validation, a critical health alert was identified concerning the Wazuh API.

- **Finding:** Reported an API connection failure (No API available).
- **Remediation:** Identified the need for a service-level restart on the Ubuntu host to restore full dashboard functionality.



192.168.247.130/app/wazuh#/health-check

wazuh.

Check Wazuh API connection ⚠

Check Wazuh API version

Check alerts index pattern ✓

Check monitoring index pattern ✓

Check statistics index pattern ✓

⚠ [API connection] No API available to connect

5. Final Conclusion

This technical assessment demonstrates that the Wazuh SIEM/XDR environment is fully capable of monitoring Ubuntu-based infrastructures. The system successfully detected and categorized brute-force attacks while simultaneously maintaining compliance with HIPAA standards. These results confirm that the SOC architecture is robust, though proactive monitoring of the API health is recommended to ensure continuous availability.