Project Overview

Project Title: SOC Simulation and Threat Detection for Baztech Using Wazuh SIEM

Baztec Inc., a startup focused on securing data and infrastructure across multiple legal platforms, initiated a Security Operations Center (SOC) simulation to address visibility gaps in its segmented network. Rising cyber threats to critical sectors, including food and agriculture, prompted the need to simulate attacks, centralize log collection, and enable real-time threat detection. The project implemented Wazuh as the central SIEM solution to monitor security logs from diverse devices and departments, correlate events, and detect anomalies. Network segmentation was maintained while enabling centralized monitoring, improving incident detection and response times, and establishing a structured process for handling suspicious activities.

1. Problem Statement

Baztec Inc. operates in a multi-departmental, segmented IT infrastructure to safeguard sensitive legal and cross-sector data. However, its existing environment lacked centralized log management, a defined incident detection process, and adequate visibility into segmented network traffic.

2. Objectives

1. Network segmentation and monitoring
2. Simulate real-world cyber threats across network segments.
3. Centralize log collection from all departments and network devices.
4. Deploy Wazuh SIEM to enable threat detection and response.

3. Tools and Technology used

- Pfsense
- Wazuh
- Ubuntu
- Windows10
- Kali
- Nmap
- Hydra

Steps and Configurations:

1. Four Networks was created on pfsense statically and DHCP was enabled

Network	IP address
• WAN	192.168.15.4
• IT Dept	192.168.50.1
• LAN	192.168.40.1
• DMZ	192.168.60.1

2. Wazuh Deployment

✞ Installed Wazuh Manager in IT Department segment.

- ✞ Installed wazuh agents on endpoints i.e Windows10, Ubuntu (DMZ server)

3. Threat Simulation using kali

- Simulated SSH brute-force attacks with Hydra against the DMZ server

4. Log collation and Analysis

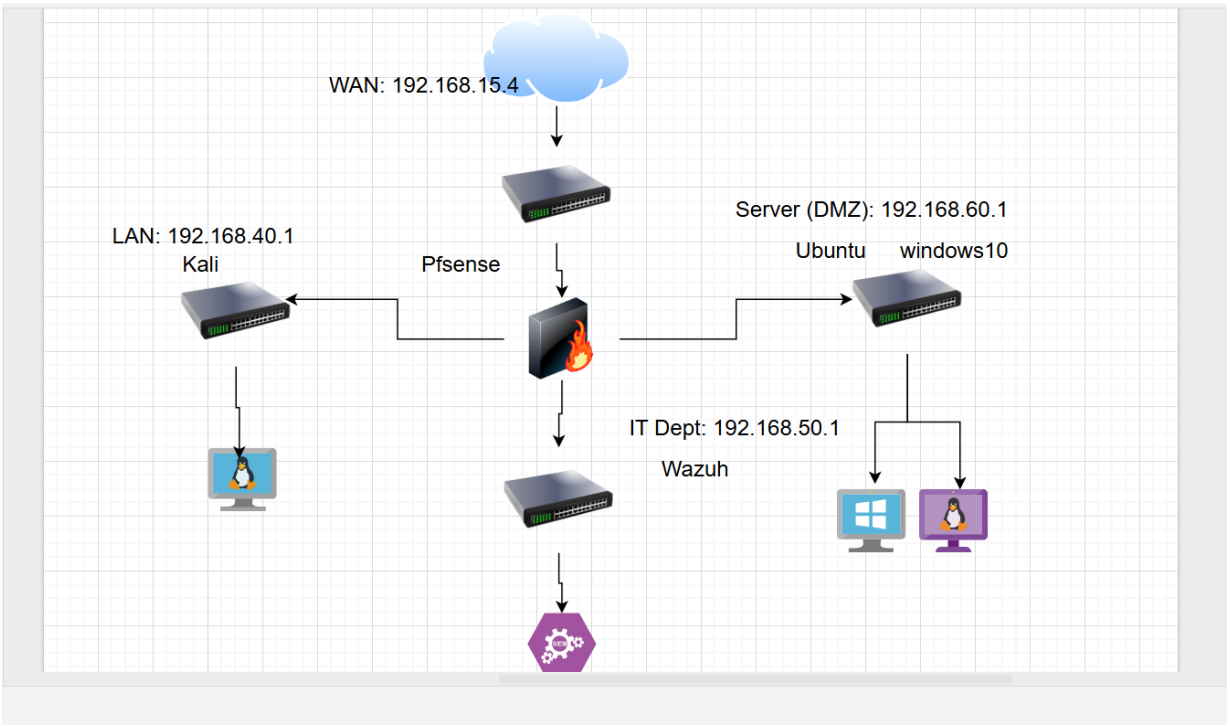
- Collect /var/log/auth.log and windows event logs.
- Analyze logs for suspicious activities i.e IP with most login attempts, IP with most failed logins, lateral movement from LAN to DMZ.

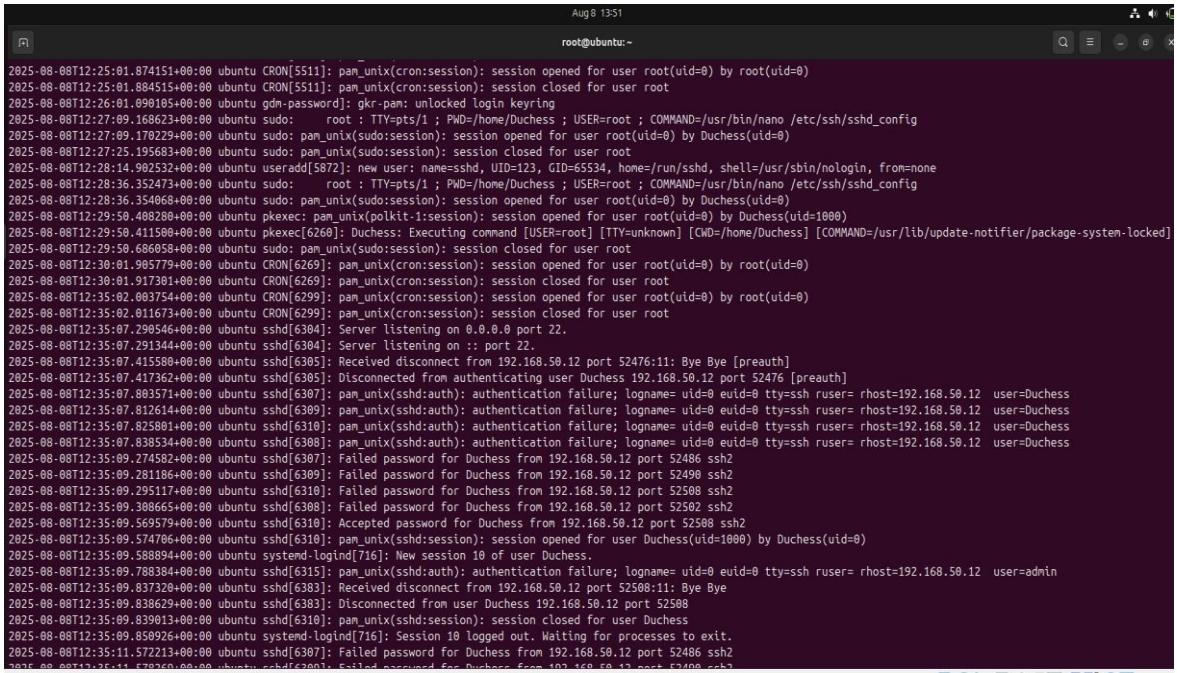
5. Conclusion and Recommendations

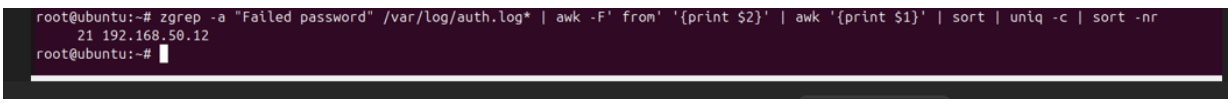
The SOC simulation improved Baztec Inc.'s cybersecurity posture, proving Wazuh's effectiveness in centralized monitoring and rapid threat detection. Future steps include integrating more systems, automating responses, setting up firewall rules to block SSH login attacks and running regular simulations.

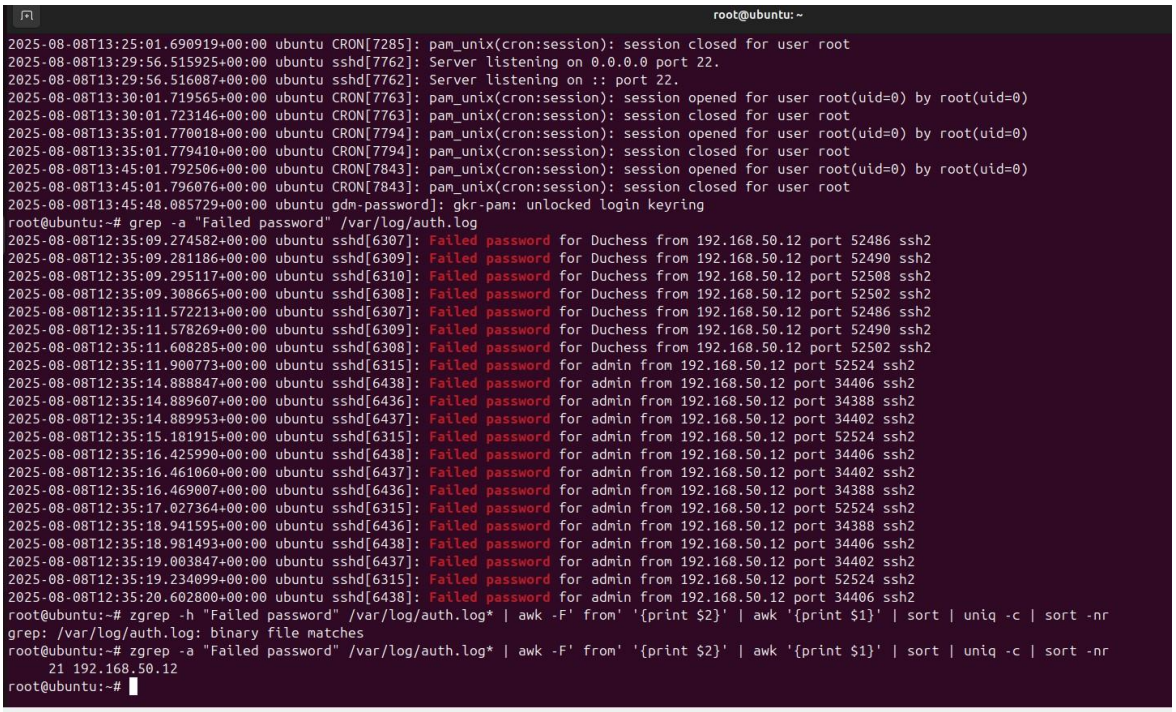
Below are screenshots of:

1. Network segmentation diagram
2. Logs from ubuntu with IP address with most login and failed password attempt
3. Wazuh alerts and dashboard


WAN: 192.168.15.4
LAN: 192.168.40.1
Kali
Pfsense
Server (DMZ): 192.168.60.1
Ubuntu
windows10
IT Dept: 192.168.50.1
Wazuh


Aug 8 13:51
root@ubuntu: ~
2025-08-08T12:25:01.874151+00:00 ubuntu CRON[5511]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-08-08T12:25:01.884515+00:00 ubuntu CRON[5511]: pam_unix(cron:session): session closed for user root
2025-08-08T12:26:01.090105+00:00 ubuntu gdm-password]: gkr-pam: unlocked login keyring
2025-08-08T12:27:09.168623+00:00 ubuntu sudo: root : TTY=pts/1 ; PWD=/home/Duchess ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config
2025-08-08T12:27:09.170229+00:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by Duchess(uid=0)
2025-08-08T12:27:25.195683+00:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root
2025-08-08T12:28:14.902532+00:00 ubuntu useradd[5872]: new user: name=sshd, UID=123, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin, from=none
2025-08-08T12:28:36.352473+00:00 ubuntu sudo: root : TTY=pts/1 ; PWD=/home/Duchess ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config
2025-08-08T12:28:36.354068+00:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by Duchess(uid=0)
2025-08-08T12:29:50.408280+00:00 ubuntu pkexec: pam_unix(polkit-1:session): session opened for user root(uid=0) by Duchess(uid=1000)
2025-08-08T12:29:50.411500+00:00 ubuntu pkexec[6260]: Duchess: Executing command [USER=root] [TTY=unknown] [CWD=/home/Duchess] [COMMAND=/usr/lib/update-notifier/package-system-locked]
2025-08-08T12:29:50.686058+00:00 ubuntu sudo: pam_unix(sudo:session): session closed for user root
2025-08-08T12:30:01.905779+00:00 ubuntu CRON[6269]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-08-08T12:30:01.917301+00:00 ubuntu CRON[6269]: pam_unix(cron:session): session closed for user root
2025-08-08T12:35:02.003754+00:00 ubuntu CRON[6299]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-08-08T12:35:02.011673+00:00 ubuntu CRON[6299]: pam_unix(cron:session): session closed for user root
2025-08-08T12:35:07.290546+00:00 ubuntu sshd[6304]: Server listening on 0.0.0.0 port 22.
2025-08-08T12:35:07.291344+00:00 ubuntu sshd[6304]: Server listening on :: port 22.
2025-08-08T12:35:07.415580+00:00 ubuntu sshd[6305]: Received disconnect from 192.168.50.12 port 52476:11: Bye Bye [preauth]
2025-08-08T12:35:07.417362+00:00 ubuntu sshd[6305]: Disconnected from authenticating user Duchess 192.168.50.12 port 52476 [preauth]
2025-08-08T12:35:07.803571+00:00 ubuntu sshd[6307]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.50.12 user=Duchess
2025-08-08T12:35:07.812614+00:00 ubuntu sshd[6309]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.50.12 user=Duchess
2025-08-08T12:35:07.825801+00:00 ubuntu sshd[6310]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.50.12 user=Duchess
2025-08-08T12:35:07.838534+00:00 ubuntu sshd[6308]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.50.12 user=Duchess
2025-08-08T12:35:09.274582+00:00 ubuntu sshd[6307]: Failed password for Duchess from 192.168.50.12 port 52486 ssh2
2025-08-08T12:35:09.281186+00:00 ubuntu sshd[6309]: Failed password for Duchess from 192.168.50.12 port 52490 ssh2
2025-08-08T12:35:09.295117+00:00 ubuntu sshd[6310]: Failed password for Duchess from 192.168.50.12 port 52508 ssh2
2025-08-08T12:35:09.308665+00:00 ubuntu sshd[6308]: Failed password for Duchess from 192.168.50.12 port 52502 ssh2
2025-08-08T12:35:09.569579+00:00 ubuntu sshd[6310]: Accepted password for Duchess from 192.168.50.12 port 52508 ssh2
2025-08-08T12:35:09.574706+00:00 ubuntu sshd[6310]: pam_unix(sshd:session): session opened for user Duchess(uid=1000) by Duchess(uid=0)
2025-08-08T12:35:09.588894+00:00 ubuntu systemd-logind[716]: New session 10 of user Duchess.
2025-08-08T12:35:09.788384+00:00 ubuntu sshd[6315]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.50.12 user=admin
2025-08-08T12:35:09.837320+00:00 ubuntu sshd[6383]: Received disconnect from 192.168.50.12 port 52508:11: Bye Bye
2025-08-08T12:35:09.838629+00:00 ubuntu sshd[6383]: Disconnected from user Duchess 192.168.50.12 port 52508
2025-08-08T12:35:09.839013+00:00 ubuntu sshd[6310]: pam_unix(sshd:session): session closed for user Duchess
2025-08-08T12:35:09.850926+00:00 ubuntu systemd-logind[716]: Session 10 logged out. Waiting for processes to exit.
2025-08-08T12:35:11.572213+00:00 ubuntu sshd[6307]: Failed password for Duchess from 192.168.50.12 port 52486 ssh2


root@ubuntu:~# zgrep -a "Failed password" /var/log/auth.log* | awk -F' from' '{print $2}' | awk '{print $1}' | sort | uniq -c | sort -nr
21 192.168.50.12
root@ubuntu:~#


root@ubuntu: ~
2025-08-08T13:25:01.690919+00:00 ubuntu CRON[7285]: pam_unix(cron:session): session closed for user root
2025-08-08T13:29:56.515925+00:00 ubuntu sshd[7762]: Server listening on 0.0.0.0 port 22.
2025-08-08T13:29:56.516087+00:00 ubuntu sshd[7762]: Server listening on :: port 22.
2025-08-08T13:30:01.719565+00:00 ubuntu CRON[7763]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-08-08T13:30:01.723146+00:00 ubuntu CRON[7763]: pam_unix(cron:session): session closed for user root
2025-08-08T13:35:01.770018+00:00 ubuntu CRON[7794]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-08-08T13:35:01.779410+00:00 ubuntu CRON[7794]: pam_unix(cron:session): session closed for user root
2025-08-08T13:45:01.792506+00:00 ubuntu CRON[7843]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2025-08-08T13:45:01.796076+00:00 ubuntu CRON[7843]: pam_unix(cron:session): session closed for user root
2025-08-08T13:45:48.085729+00:00 ubuntu gdm-password]: gkr-pam: unlocked login keyring
root@ubuntu:~# grep -a "Failed password" /var/log/auth.log
2025-08-08T12:35:09.274582+00:00 ubuntu sshd[6307]: Failed password for Duchess from 192.168.50.12 port 52486 ssh2
2025-08-08T12:35:09.281186+00:00 ubuntu sshd[6309]: Failed password for Duchess from 192.168.50.12 port 52490 ssh2
2025-08-08T12:35:09.295117+00:00 ubuntu sshd[6310]: Failed password for Duchess from 192.168.50.12 port 52508 ssh2
2025-08-08T12:35:09.308665+00:00 ubuntu sshd[6308]: Failed password for Duchess from 192.168.50.12 port 52502 ssh2
2025-08-08T12:35:11.572213+00:00 ubuntu sshd[6307]: Failed password for Duchess from 192.168.50.12 port 52486 ssh2
2025-08-08T12:35:11.578269+00:00 ubuntu sshd[6309]: Failed password for Duchess from 192.168.50.12 port 52490 ssh2
2025-08-08T12:35:11.608285+00:00 ubuntu sshd[6308]: Failed password for Duchess from 192.168.50.12 port 52502 ssh2
2025-08-08T12:35:11.900773+00:00 ubuntu sshd[6315]: Failed password for admin from 192.168.50.12 port 52524 ssh2
2025-08-08T12:35:14.888847+00:00 ubuntu sshd[6438]: Failed password for admin from 192.168.50.12 port 34406 ssh2
2025-08-08T12:35:14.889607+00:00 ubuntu sshd[6436]: Failed password for admin from 192.168.50.12 port 34388 ssh2
2025-08-08T12:35:14.889953+00:00 ubuntu sshd[6437]: Failed password for admin from 192.168.50.12 port 34402 ssh2
2025-08-08T12:35:15.181915+00:00 ubuntu sshd[6315]: Failed password for admin from 192.168.50.12 port 52524 ssh2
2025-08-08T12:35:16.425990+00:00 ubuntu sshd[6438]: Failed password for admin from 192.168.50.12 port 34406 ssh2
2025-08-08T12:35:16.461060+00:00 ubuntu sshd[6437]: Failed password for admin from 192.168.50.12 port 34402 ssh2
2025-08-08T12:35:16.469007+00:00 ubuntu sshd[6436]: Failed password for admin from 192.168.50.12 port 34388 ssh2
2025-08-08T12:35:17.027364+00:00 ubuntu sshd[6315]: Failed password for admin from 192.168.50.12 port 52524 ssh2
2025-08-08T12:35:18.941595+00:00 ubuntu sshd[6436]: Failed password for admin from 192.168.50.12 port 34388 ssh2
2025-08-08T12:35:18.981493+00:00 ubuntu sshd[6438]: Failed password for admin from 192.168.50.12 port 34406 ssh2
2025-08-08T12:35:19.003847+00:00 ubuntu sshd[6437]: Failed password for admin from 192.168.50.12 port 34402 ssh2
2025-08-08T12:35:19.234099+00:00 ubuntu sshd[6315]: Failed password for admin from 192.168.50.12 port 52524 ssh2
2025-08-08T12:35:20.602800+00:00 ubuntu sshd[6438]: Failed password for admin from 192.168.50.12 port 34406 ssh2
root@ubuntu:~# zgrep -h "Failed password" /var/log/auth.log* | awk -F' from' '{print $2}' | awk '{print $1}' | sort | uniq -c | sort -nr
grep: /var/log/auth.log: binary file matches
root@ubuntu:~# zgrep -a "Failed password" /var/log/auth.log* | awk -F' from' '{print $2}' | awk '{print $1}' | sort | uniq -c | sort -nr
     21 192.168.50.12
root@ubuntu:~#