BazTech Inc. SOC Simulation Report

Project Title: A SOC in a Segmented Network

Analyst: Justice Akason

Date: August 2025

Environment: Segmented SOC Lab (Wazuh, Kali, Ubuntu, Windows 10)

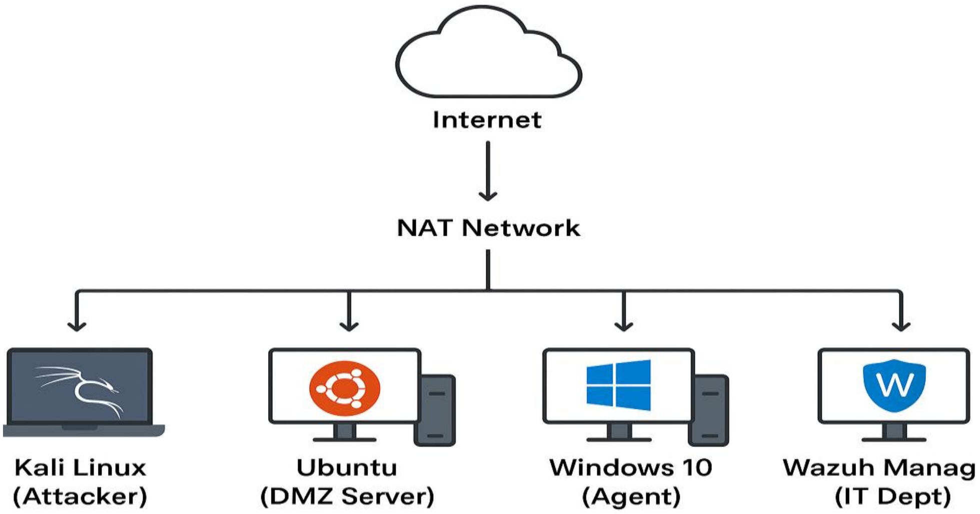
Executive Summary

This report details a simulated SSH brute-force attack within BazTech Inc.'s virtual SOC environment. The exercise validates detection capabilities, incident response workflows, and compliance alignment using Wazuh. It demonstrates my ability to operationalize threat intelligence, correlate logs across platforms, and produce stakeholder-ready documentation under deadline pressure.

Lab Architecture & Segmentation

The SOC lab was designed to mirror enterprise segmentation and simulate adversary behaviour across zones:

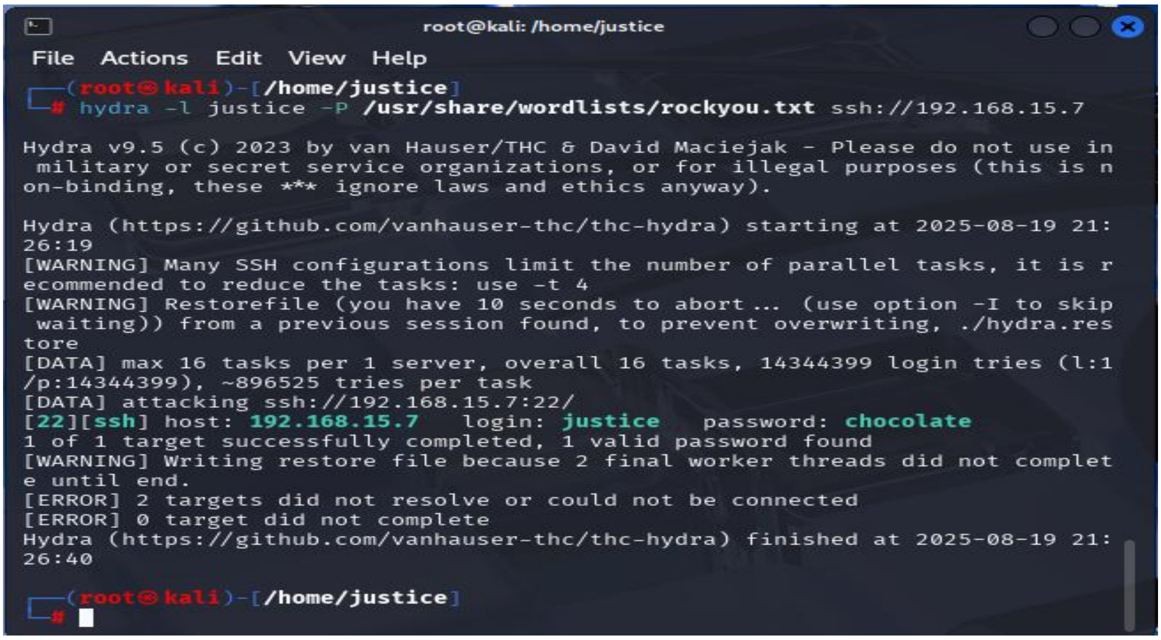
Component	Role	IP Address	Key Functionality
Kali Linux	Attacker	192.168.15.5	Hydra brute-force tool targeting SSH
Ubuntu Server	DMZ Target	192.168.15.7	SSH service with logging enabled
Windows 10 Agent	Internal Host	192.168.15.9	Event log generation, lateral movement test
Wazuh Manager	SIEM	192.168.15.6	Centralized log analysis and alerting



Segmentation Validation:
Firewall rules and traceroute tests confirmed isolation between attacker, DMZ, and internal zones. Only authorized traffic was permitted across interfaces.

Attack Simulation Details

Attack Type: SSH Brute-force
Tool Used: Hydra
Target: Ubuntu Server (192.168.15.7)



```
┌──(root㉿kali)-[/home/justice]
└─# hydra -l justice -P /usr/share/wordlists/rockyou.txt ssh://192.168.15.7

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-19 21:
26:19
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip
 waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1
/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.15.7:22/
[22][ssh] host: 192.168.15.7   login: justice   password: chocolate
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complet
e until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-19 21:
26:40

┌──(root㉿kali)-[/home/justice]
└─# 
```

Command Executed:

hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.15.7

Observed Behaviour:

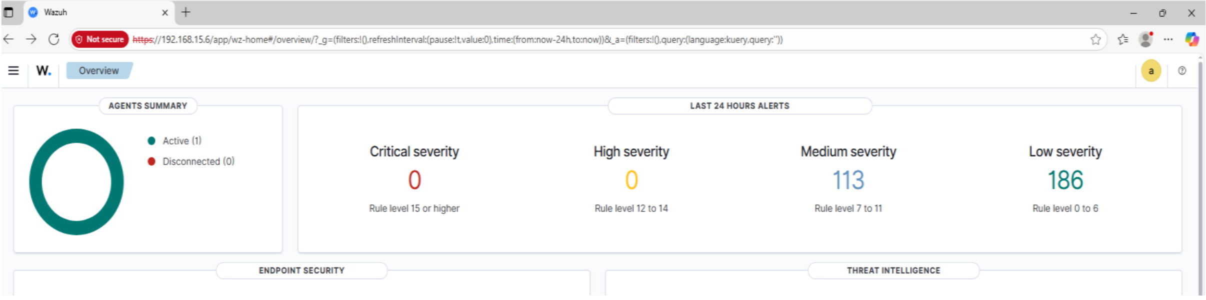
- /var/log/auth.log recorded **22,853 failed login attempts**.
- Wazuh Agent parsed logs and triggered **Rule ID 5715**.
- Alerts were classified as **Brute-force attempt** with MITRE mapping to **T1110**.

Wazuh Detection & Alerting

Dashboard Highlights:

- **Total Alerts:** 299
    - Medium: 113

- Low: 186
- Critical: 0


Wazuh
Not secure
https://192.168.15.6/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!(),query:(language:kuery,query:''))
W.
Overview
a

AGENTS SUMMARY

● Active (1)
● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	113	186
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

THREAT INTELLIGENCE

- **Security Configuration Assessment (SCA):**
- 47 failed hardening checks on Ubuntu
- Weak SSH configuration, missing audit policies

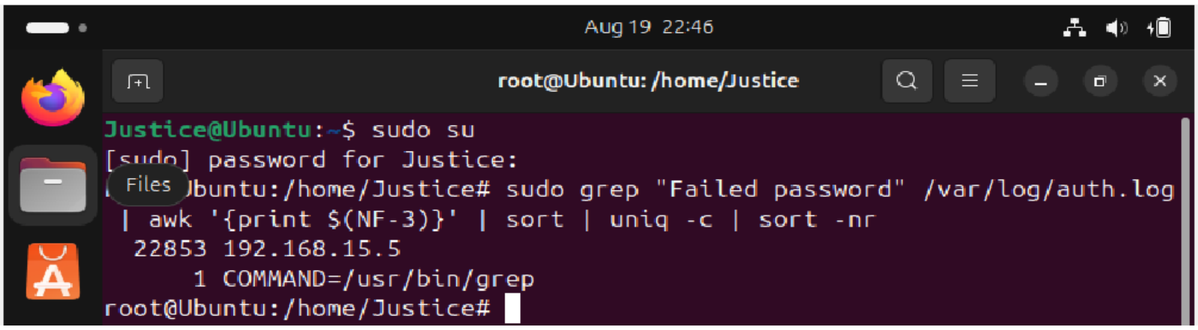
MITRE ATT&CK Mapping:

Technique ID	Name	Phase
T1110	Brute Force	Credential Access
T1003	Credential Dumping	Credential Access
T1082	System Information Discovery	Discovery
T1105	Remote File Copy	Command & Control
T1011	Data Exfiltration	Exfiltration

Log Analysis & Evidence

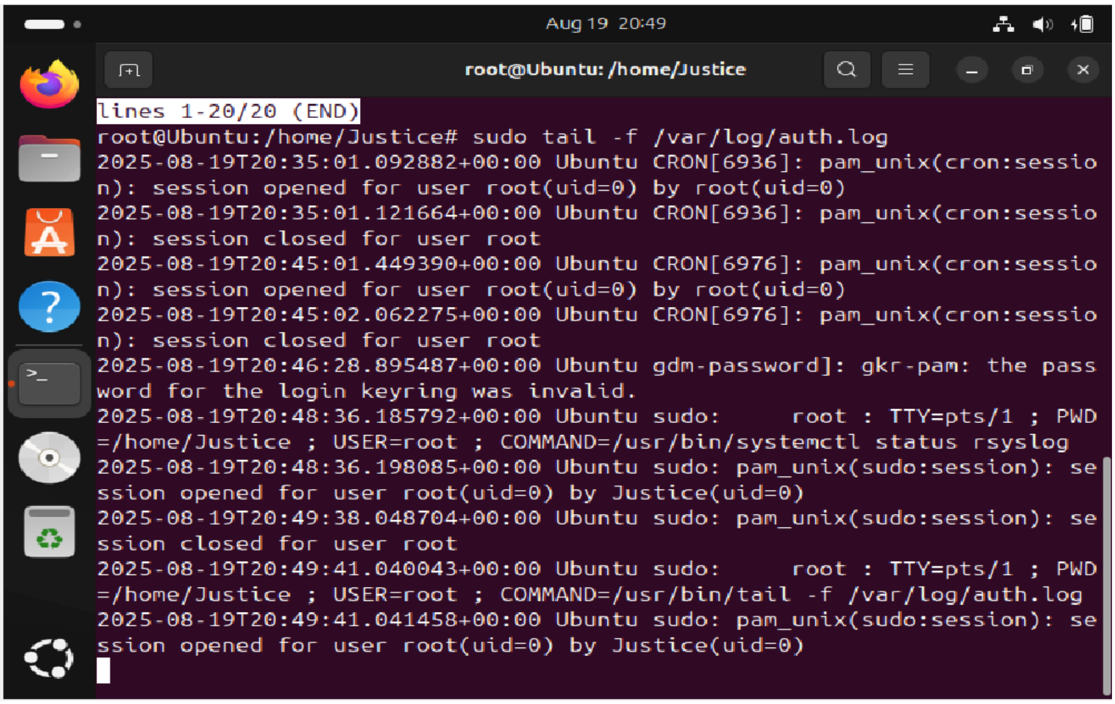
Sample Log Entry from /var/log/auth.log:

Aug 19 22:15:01 ubuntu sshd[1234]: Failed password for root from 192.168.15.5 port 54321 ssh2



```
Justice@Ubuntu:~$ sudo su
[sudo] password for Justice:
root@Ubuntu:/home/Justice# sudo grep "Failed password" /var/log/auth.log
 | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
  22853 192.168.15.5
      1 COMMAND=/usr/bin/grep
root@Ubuntu:/home/Justice#
```

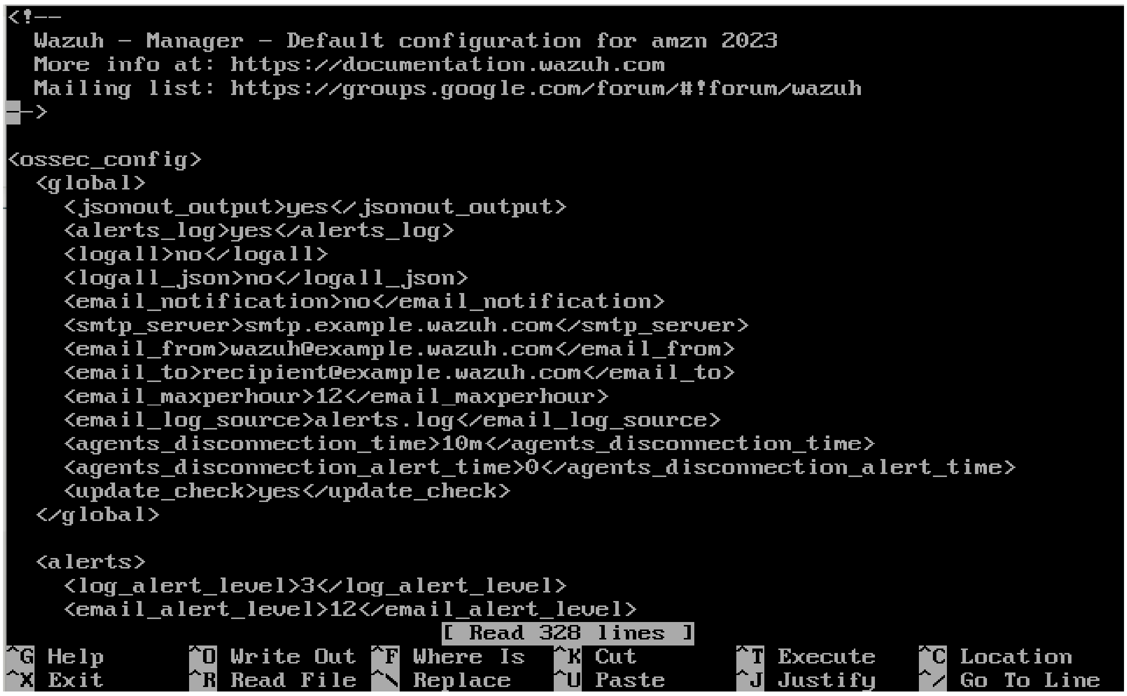
Real-Time Authentication Events: Ubuntu Terminal Output



```
lines 1-20/20 (END)
root@Ubuntu:/home/Justice# sudo tail -f /var/log/auth.log
2025-08-19T20:35:01.092882+00:00 Ubuntu CRON[6936]: pam_unix(cron:sessio
n): session opened for user root(uid=0) by root(uid=0)
2025-08-19T20:35:01.121664+00:00 Ubuntu CRON[6936]: pam_unix(cron:sessio
n): session closed for user root
2025-08-19T20:45:01.449390+00:00 Ubuntu CRON[6976]: pam_unix(cron:sessio
n): session opened for user root(uid=0) by root(uid=0)
2025-08-19T20:45:02.062275+00:00 Ubuntu CRON[6976]: pam_unix(cron:sessio
n): session closed for user root
2025-08-19T20:46:28.895487+00:00 Ubuntu gdm-password]: gkr-pam: the pass
word for the login keyring was invalid.
2025-08-19T20:48:36.185792+00:00 Ubuntu sudo:     root : TTY=pts/1 ; PWD
=/home/Justice ; USER=root ; COMMAND=/usr/bin/systemctl status rsyslog
2025-08-19T20:48:36.198085+00:00 Ubuntu sudo: pam_unix(sudo:session): se
ssion opened for user root(uid=0) by Justice(uid=0)
2025-08-19T20:49:38.048704+00:00 Ubuntu sudo: pam_unix(sudo:session): se
ssion closed for user root
2025-08-19T20:49:41.040043+00:00 Ubuntu sudo:     root : TTY=pts/1 ; PWD
=/home/Justice ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2025-08-19T20:49:41.041458+00:00 Ubuntu sudo: pam_unix(sudo:session): se
ssion opened for user root(uid=0) by Justice(uid=0)
```

Wazuh Alert JSON:

{ "rule": { "id": "5715", "level": 10, "description": "Possible SSH brute-force attack" }, "srcip": "192.168.15.5", "location": "/var/log/auth.log" }

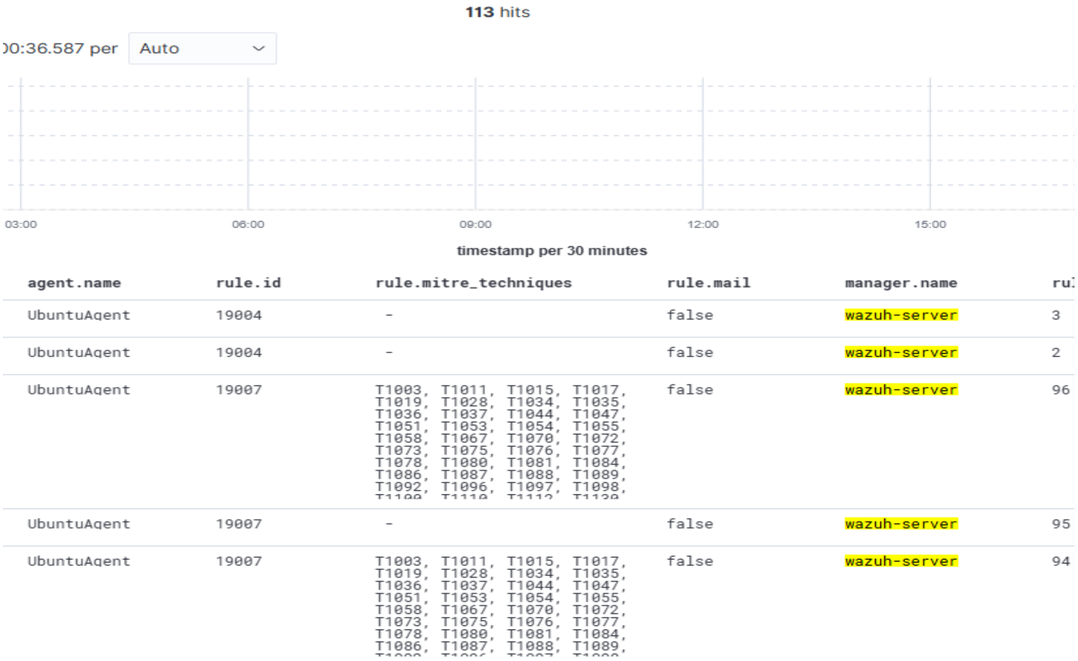


```
<!--
  Wazuh - Manager - Default configuration for amzn 2023
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
                                              [ Read 328 lines ]
^G Help         ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit         ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

Visual Evidence:
Annotated screenshots of Wazuh dashboard, alert breakdown, and SCA results were captured and included in stakeholder documentation.



agent.name	rule.id	rule.mitre_techniques	rule.mail	manager.name	ru
UbuntuAgent	19004	-	false	wazuh-server	3
UbuntuAgent	19004	-	false	wazuh-server	2
UbuntuAgent	19007	T1003, T1011, T1015, T1017, T1019, T1028, T1034, T1035, T1036, T1037, T1044, T1047, T1051, T1053, T1054, T1055, T1058, T1067, T1070, T1072, T1073, T1075, T1076, T1077, T1078, T1080, T1081, T1084, T1086, T1087, T1088, T1089, T1092, T1096, T1097, T1098, T1100, T1110, T1112, T1130,	false	wazuh-server	96
UbuntuAgent	19007	-	false	wazuh-server	95
UbuntuAgent	19007	T1003, T1011, T1015, T1017, T1019, T1028, T1034, T1035, T1036, T1037, T1044, T1047, T1051, T1053, T1054, T1055, T1058, T1067, T1070, T1072, T1073, T1075, T1076, T1077, T1078, T1080, T1081, T1084, T1086, T1087, T1088, T1089,	false	wazuh-server	94

Mitigation & Hardening Actions

Action Taken	Description
IP Blocking	iptables -A INPUT -s 192.168.15.5 -j DROP
SSH Hardening	Disabled password auth; enforced key-based login
Network Access Control	Restricted SSH to trusted IP ranges via Firewall
Wazuh Rule Tuning	Elevated brute-force alerts; enabled active response
SCA Remediation	Applied CIS benchmarks; reduced failed checks

Documentation & Stakeholder Deliverables

I produced the following artifacts:

- Annotated diagrams of attack flow and segmentation
- Markdown checklist of vulnerabilities and remediation steps
- Executive summary tailored for non-technical stakeholders
- MITRE mapping table for compliance and audit teams

- Log excerpts and alert evidence for forensic validation

Lessons Learned & Analyst Reflection

- **Detection Depth:** Wazuh effectively correlated logs across zones, but tuning was required to reduce noise and elevate critical alerts.
- **Segmentation Success:** firewall rules prevented lateral movement, validating network isolation.
- **Documentation Impact:** Clear, visual reporting accelerated stakeholder understanding and decision-making.
- **Analyst Growth:** This simulation sharpened my skills in adversary emulation, SIEM tuning, and stakeholder communication under pressure.

Conclusion

This capstone simulation demonstrates my ability to design, execute, and document a full-cycle SOC workflow—from attack emulation to detection, mitigation, and reporting. The deliverables reflect operational clarity, technical rigor, and strategic alignment with compliance frameworks like ISO 27001 and GDPR.