



SOC CAPSTONE – BAZTECH

Defensive Security in a Segmented Network



AGENDA

- Introduction
- Lab Environment Setup
- Attack Simulation
- Evidence Collection
- Detection & Correlation
- Recommendations

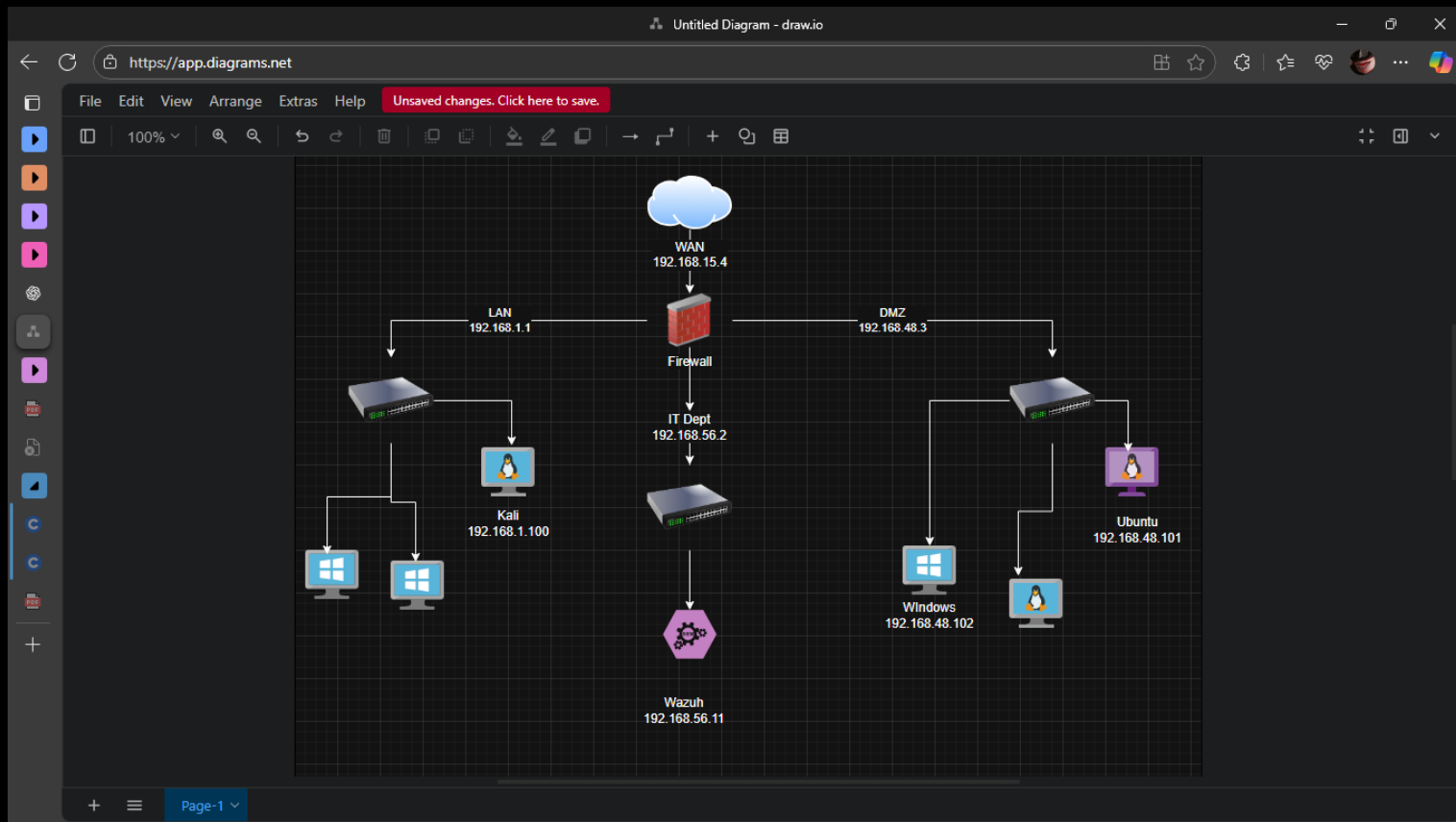


INTRODUCTION

- Simulated SOC environment for BazTech
- Objective: Detect and mitigate threats in a segmented network
- Tools: pfSense, Wazuh, Ubuntu, Windows 10, Kali Linux

NETWORK DIAGRAM

- BazTech SOC Network Layout



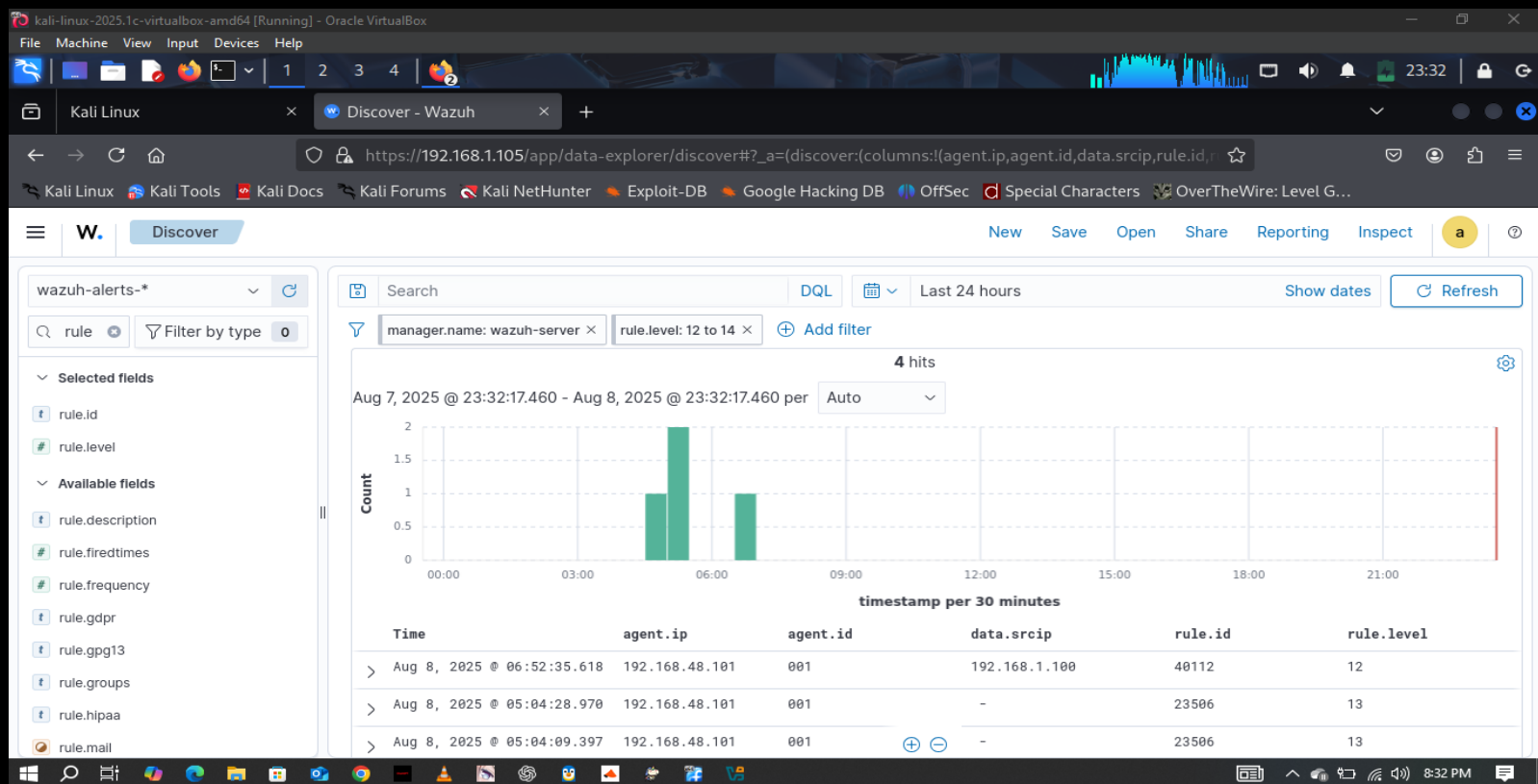
INCIDENT 1: SSH BRUTE FORCE (UBUNTU)

- 45 failed SSH login attempts from 192.168.1.100
- Targeted user: admin, sage2025
- Timeframe: 8/8/2025 10:52pm

```
Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
user=sage2025
2025-08-08T10:52:24.787034+00:00 allisonserver sshd[2342]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100
user=sage2025
2025-08-08T10:52:26.008518+00:00 allisonserver sshd[2383]: Received disconnect from 192.168.1.100 port 56354:11: Bye Bye
2025-08-08T10:52:26.010170+00:00 allisonserver sshd[2383]: Disconnected from user admin 192.168.1.100 port 56354
2025-08-08T10:52:26.013294+00:00 allisonserver sshd[2293]: pam_unix(sshd:session): session closed for user admin
2025-08-08T10:52:26.034792+00:00 allisonserver systemd-logind[700]: Session 11 logged out. Waiting for processes to exit.
2025-08-08T10:52:26.057154+00:00 allisonserver systemd-logind[700]: Removed session 11.
2025-08-08T10:52:26.402421+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:26.417917+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:26.501968+00:00 allisonserver sshd[2341]: Failed password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:26.522261+00:00 allisonserver sshd[2342]: Failed password for sage2025 from 192.168.1.100 port 60586 ssh2
2025-08-08T10:52:29.616342+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:29.838451+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:29.974826+00:00 allisonserver sshd[2341]: Failed password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:30.051264+00:00 allisonserver sshd[2342]: Failed password for sage2025 from 192.168.1.100 port 60586 ssh2
2025-08-08T10:52:32.690805+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:32.721243+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:32.753145+00:00 allisonserver sshd[2342]: Failed password for sage2025 from 192.168.1.100 port 60586 ssh2
2025-08-08T10:52:32.872995+00:00 allisonserver sshd[2341]: Failed password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:34.134035+00:00 allisonserver sshd[2341]: Accepted password for sage2025 from 192.168.1.100 port 60580 ssh2
2025-08-08T10:52:34.139435+00:00 allisonserver sshd[2341]: pam_unix(sshd:session): session opened for user sage2025(uid=1000) by sage2025(uid=0)
2025-08-08T10:52:34.157775+00:00 allisonserver systemd-logind[700]: New session 13 of user sage2025.
2025-08-08T10:52:34.203719+00:00 allisonserver sshd[2342]: Connection closed by authenticating user sage2025 192.168.1.100 port 60586 [preauth]
2025-08-08T10:52:34.203937+00:00 allisonserver sshd[2342]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100 user=sage2025
2025-08-08T10:52:34.559993+00:00 allisonserver sshd[2341]: pam_unix(sshd:session): session closed for user sage2025
2025-08-08T10:52:34.579911+00:00 allisonserver systemd-logind[700]: Session 13 logged out. Waiting for processes to exit.
2025-08-08T10:52:34.592436+00:00 allisonserver systemd-logind[700]: Removed session 13.
2025-08-08T10:52:35.576877+00:00 allisonserver sshd[2340]: Failed password for sage2025 from 192.168.1.100 port 60570 ssh2
2025-08-08T10:52:35.599112+00:00 allisonserver sshd[2307]: Failed password for sage2025 from 192.168.1.100 port 60556 ssh2
2025-08-08T10:52:37.124648+00:00 allisonserver sshd[2340]: Connection closed by authenticating user sage2025 192.168.1.100 port 60570 [preauth]
2025-08-08T10:52:37.124847+00:00 allisonserver sshd[2340]: PAM 3 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100 user=sage2025
2025-08-08T10:52:37.127699+00:00 allisonserver sshd[2307]: Connection closed by authenticating user sage2025 192.168.1.100 port 60556 [preauth]
2025-08-08T10:52:37.131248+00:00 allisonserver sshd[2307]: PAM 4 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.100 user=sage2025
2025-08-08T10:52:37.131672+00:00 allisonserver sshd[2307]: PAM service(sshd) ignoring max retries; 5 > 3
2025-08-08T10:52:37.141285+00:00 allisonserver sshd[2340]: PAM service(sshd) ignoring max retries; 4 > 3
2025-08-08T10:52:39.307739+00:00 allisonserver sudo: pam_unix(sudo:session): session closed for user root
2025-08-08T10:53:08.224194+00:00 allisonserver sudo: sage2025 : TTY=ttty1 : PWD=/home/sage2025 : USER=root : COMMAND=/usr/bin/nano /var/log/auth.log
2025-08-08T10:53:08.227904+00:00 allisonserver sudo: pam_unix(sudo:session): session opened for user root(uid=0) by sage2025(uid=1000)
2025-08-08T10:54:21.210984+00:00 allisonserver sudo: pam_unix(sudo:session): session closed for user root
2025-08-08T10:54:21.214589+00:00 allisonserver sudo: sage2025 : TTY=ttty1 : PWD=/home/sage2025 : USER=root : COMMAND=/usr/bin/nano /var/log/auth.log
```

SOC DETECTION: UBUNTU (WAZUH)

- Rule triggered: Multiple SSH authentication failures
- Rule ID: 40112
- Source IP matches raw logs



INCIDENT 2: RDP BRUTE FORCE (WINDOWS)

- 6 failed RDP login attempts from 192.168.x.x
- Event ID: 4625 (failed logon)
- Source Network Address matches Ubuntu attack

The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Event Viewer (Local)' tree with 'Windows Logs' expanded. The main pane shows a list of events with columns: Level, Date and Time, Source, Event ID, and Task Category. Event 4634 (Logoff) is selected. The right pane shows the 'Actions' menu with options like 'Open Saved Log...', 'Create Custom View...', 'Filter Current Custom ...', 'Properties', 'Find...', 'Save All Events in Cust...', 'Export Custom View...', 'Copy Custom View...', 'Attach Task To This Cu...', 'View', 'Delete', 'Rename', 'Refresh', 'Help', 'Event 4634, Microsoft Wind...', 'Event Properties', 'Attach Task To This Eve...', 'Copy', 'Save Selected Events...', 'Refresh', and 'Help'.

Level	Date and Time	Source	Event ID	Task Category
Information	8/8/2025 7:08:03 PM	Microsoft Wi...	4634	Logoff
Information	8/8/2025 7:08:03 PM	Microsoft Wi...	4634	Logoff
Information	8/8/2025 7:08:03 PM	Microsoft Wi...	4672	Special Logon
Information	8/8/2025 7:08:03 PM	Microsoft Wi...	4627	Group Memb...
Information	8/8/2025 7:08:03 PM	Microsoft Wi...	4624	Logon
Information	8/8/2025 7:08:03 PM	Microsoft Wi...	4648	Logon
Information	8/8/2025 7:08:03 PM	Microsoft Wi...	4776	Credential Vali...
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4634	Logoff
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4634	Logoff
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4718	Authenticatio...
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4672	Special Logon
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4627	Group Memb...
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4624	Logon
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4648	Logon
Information	8/8/2025 7:08:02 PM	Microsoft Wi...	4717	Authenticatio...
Information	8/8/2025 7:08:01 PM	Microsoft Wi...	4634	Logoff

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Subject:

Log Name: Security

Source: Microsoft Windows security

Event ID: 4634

Level: Information

User: N/A

Logged: 8/8/2025 7:08:03 PM

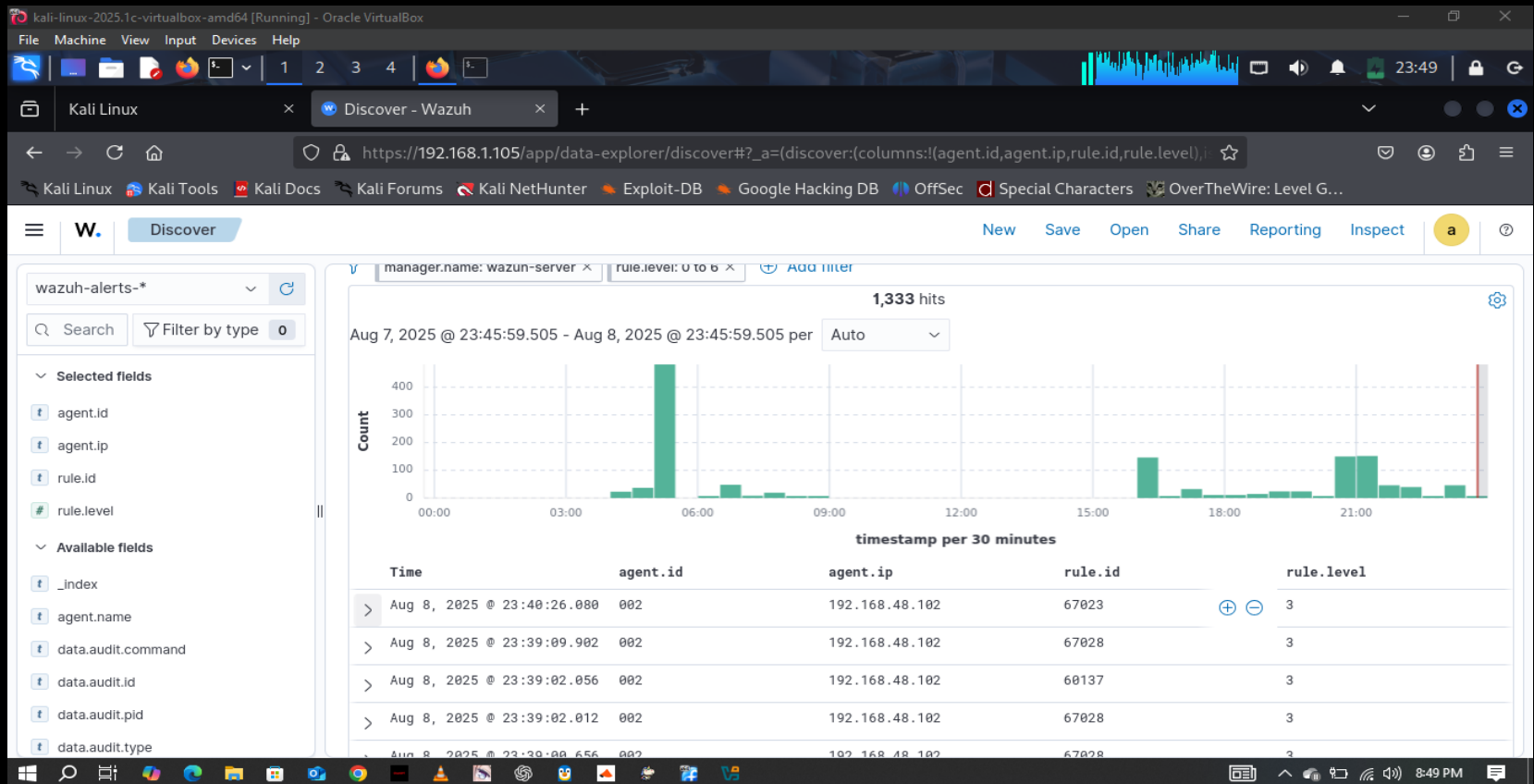
Task Category: Logoff

Keywords: Audit Success

Computer: DESKTOP-N0NFCΔ I

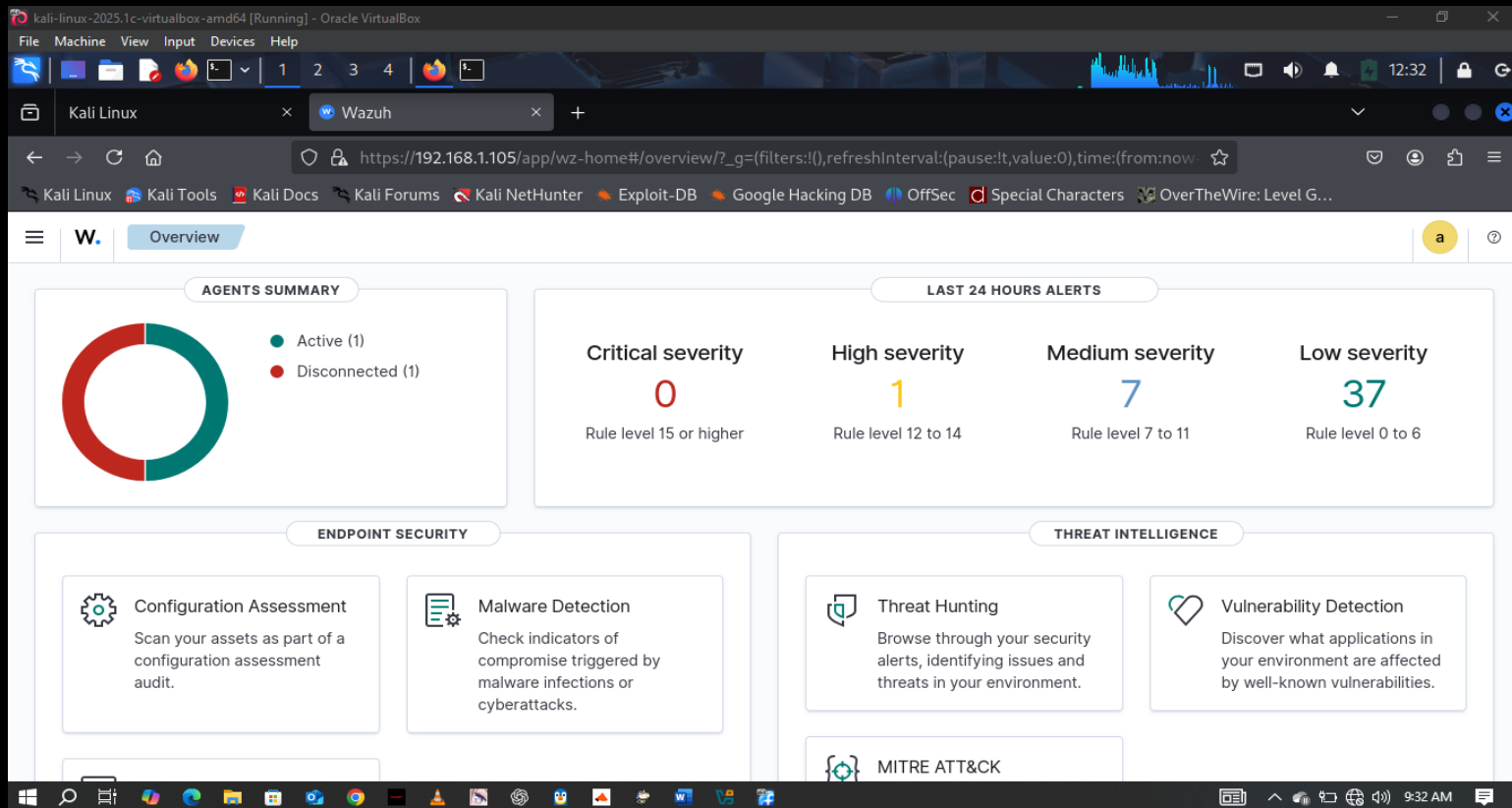
SOC DETECTION: WINDOWS (WAZUH)

- Rule triggered: Multiple RDP authentication failures
- Rule ID: 67823
- Correlates with Ubuntu attack timeframe



CORRELATION ANALYSIS

- Attacker targeted multiple endpoints in quick succession
- Same source IP across SSH and RDP attacks
- Potential reconnaissance or lateral movement attempt



RECOMMENDATIONS

- Implement firewall rules to block SSH & RDP from untrusted networks
- Enable Fail2Ban on Ubuntu (max 3 failed attempts)
- Enforce account lockout on Windows after 3 failed logins
- Restrict RDP access to admin subnet only
- Continue SOC monitoring with Wazuh correlation rules