SOC CAPSTONE – BAZTECH

Defensive Security in a Segmented Network

AGENDA

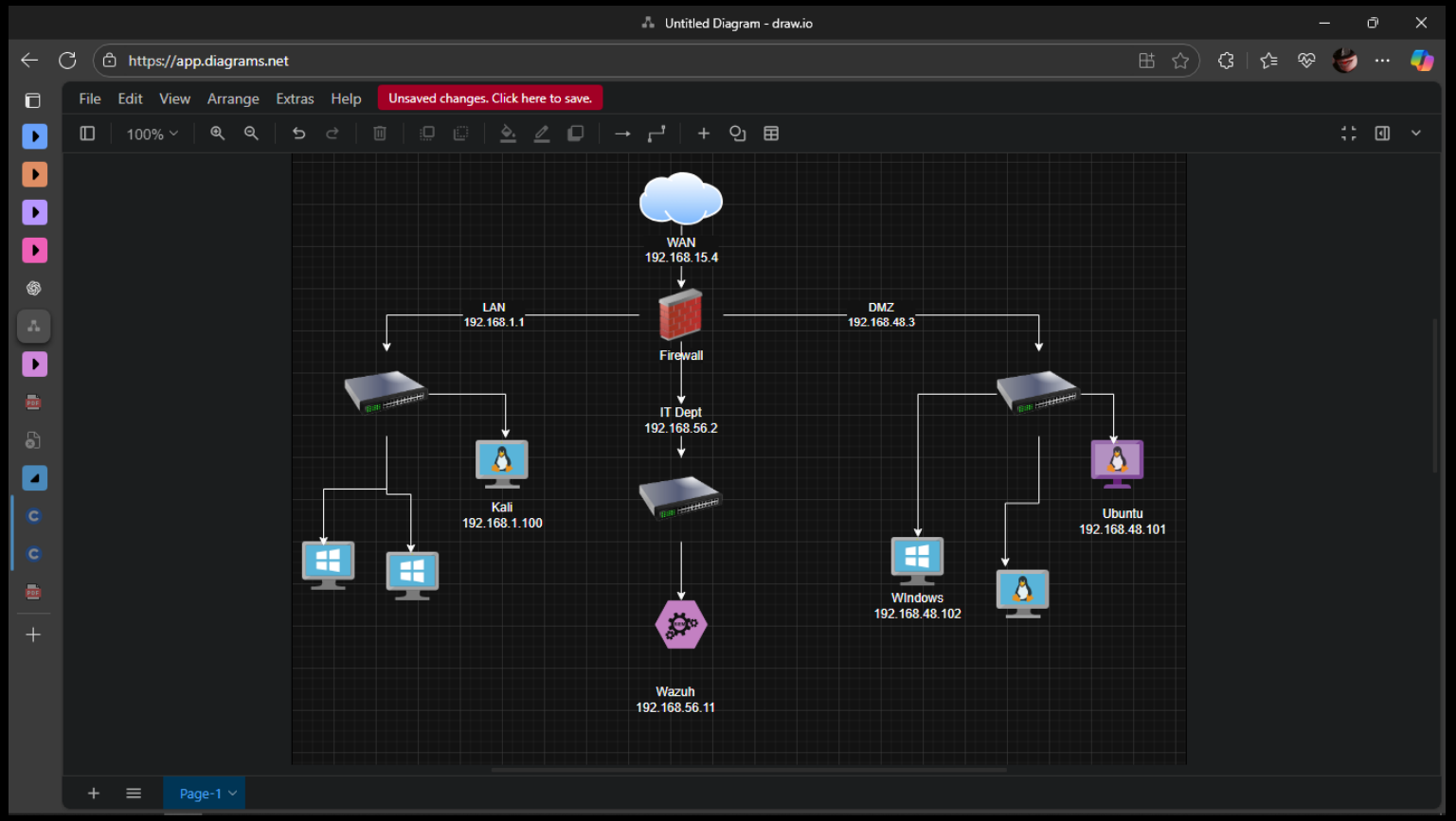
- Introduction
- Lab Environment Setup
- Attack Simulation
- Evidence Collection
- Detection & Correlation
- Recommendations

INTRODUCTION

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

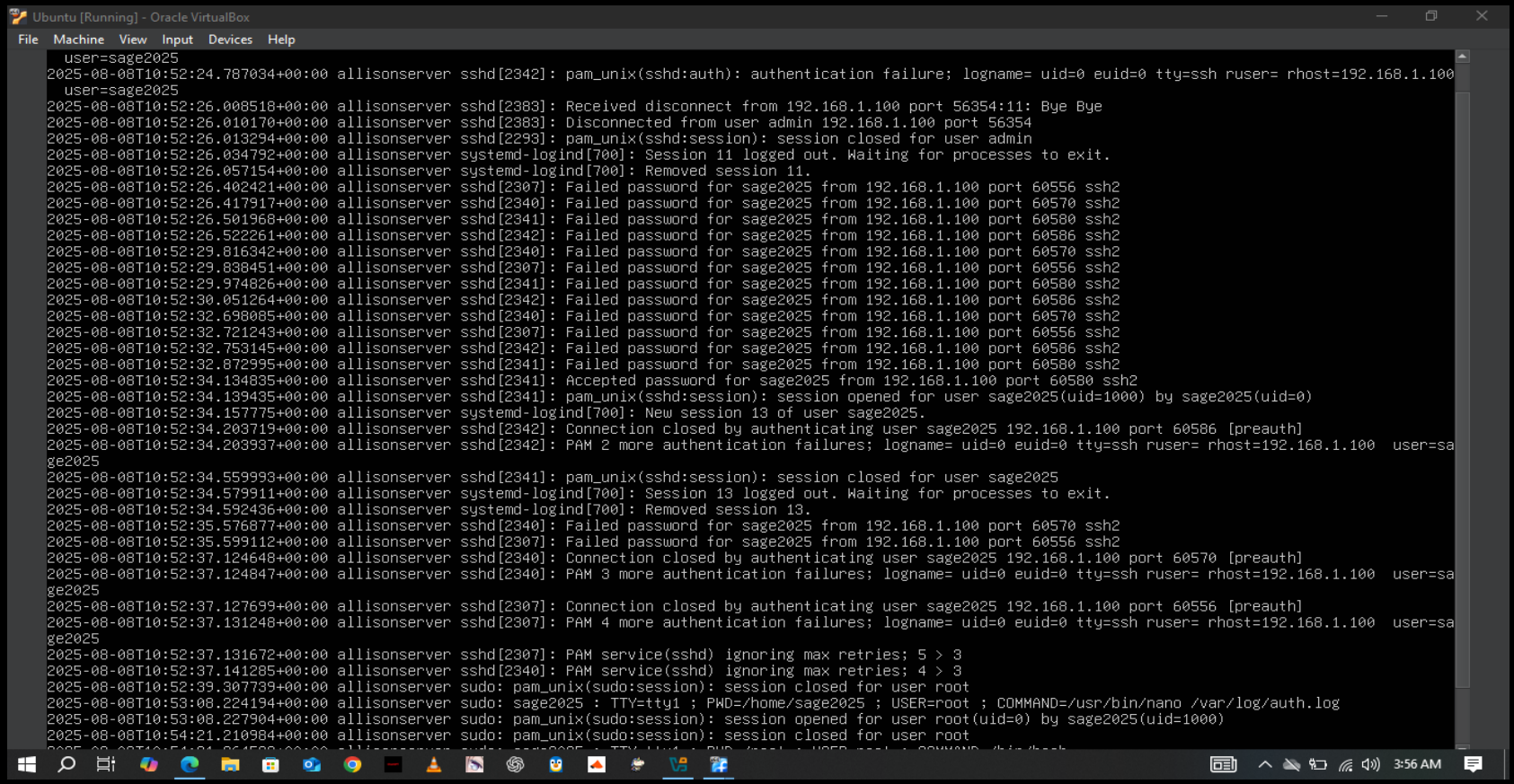
NETWORK DIAGRAM

- BazTech SOC Network Layout



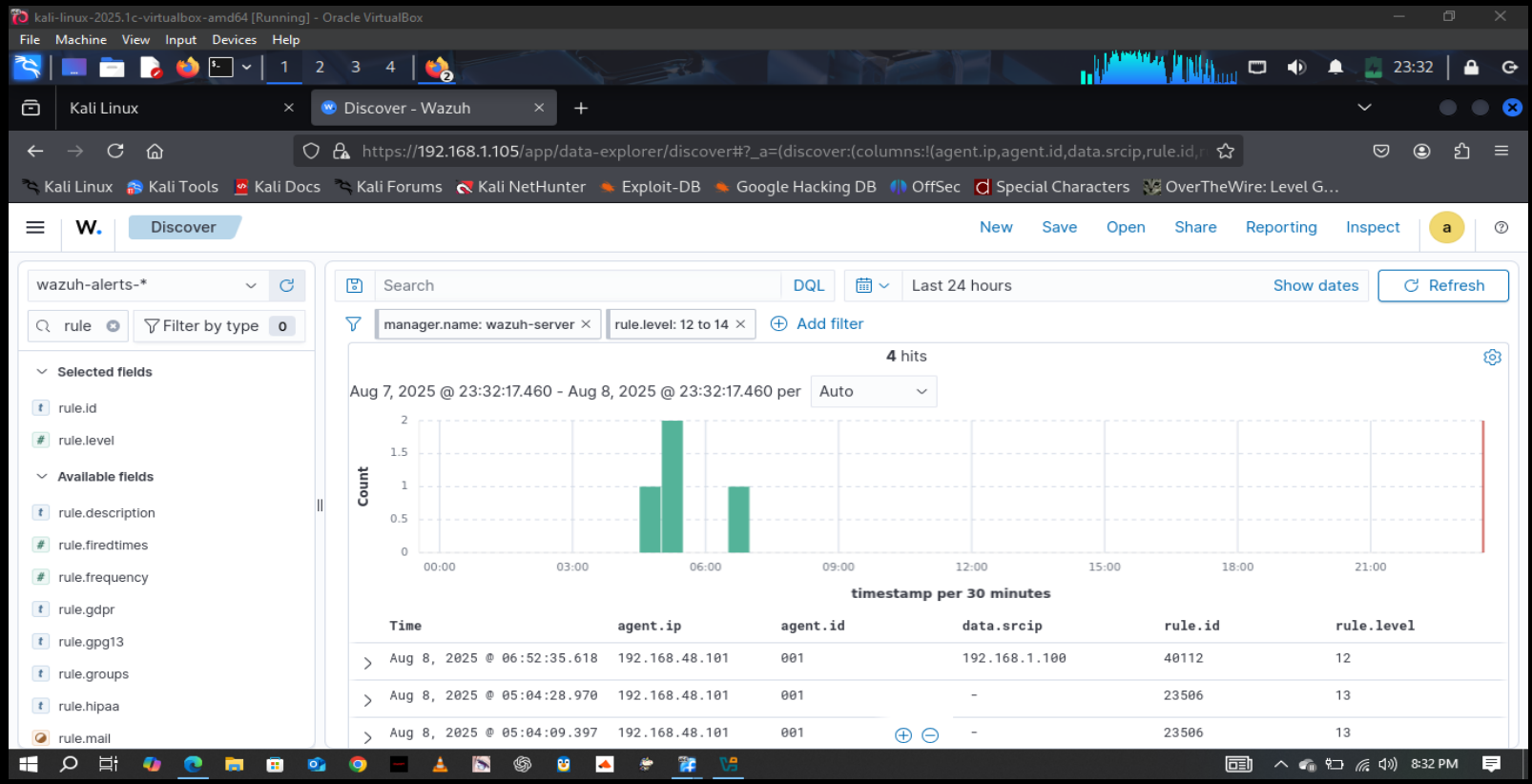
INCIDENT 1: SSH BRUTE FORCE (UBUNTU)

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



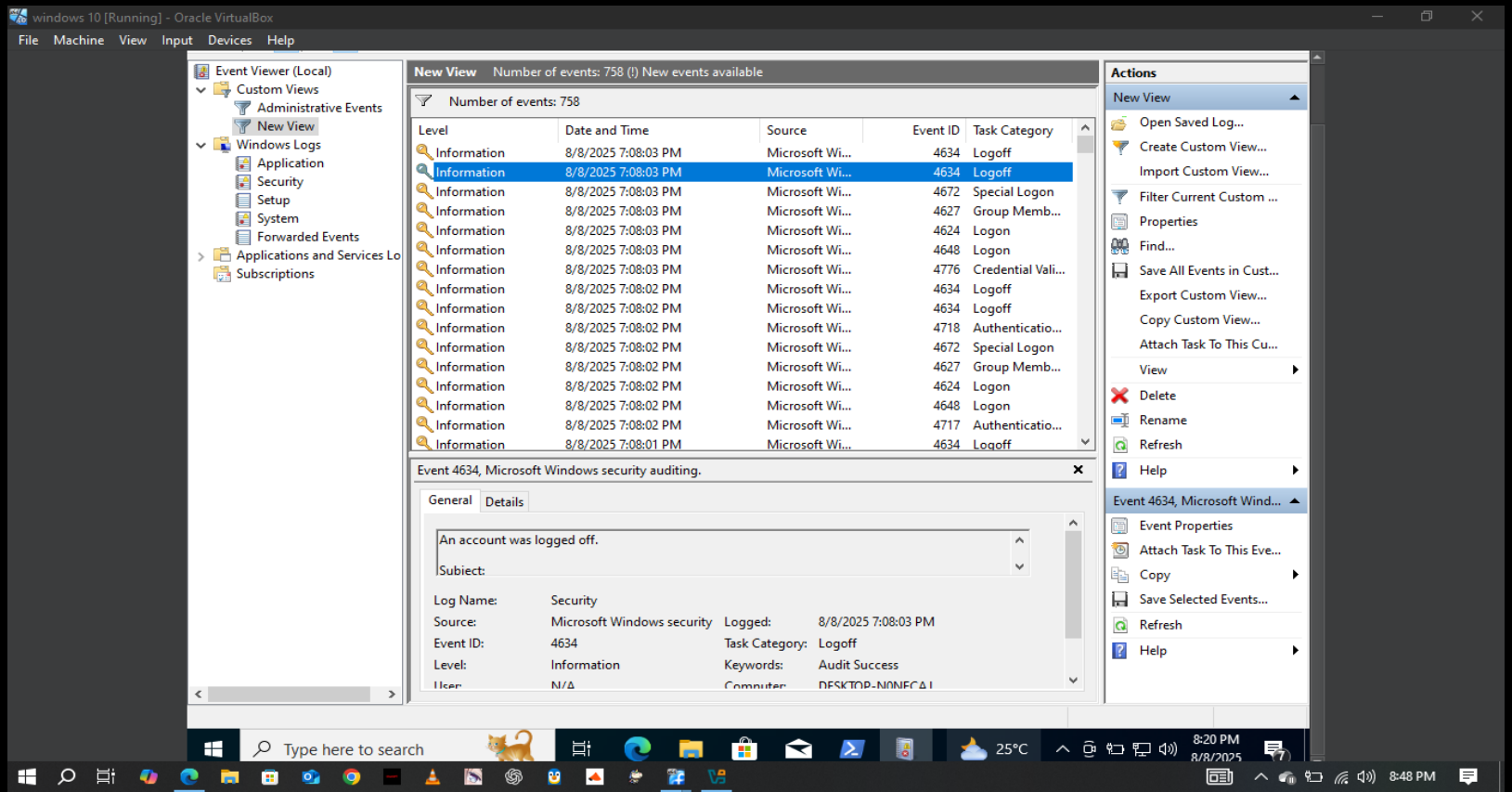
SOC DETECTION: UBUNTU (WAZUH)

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



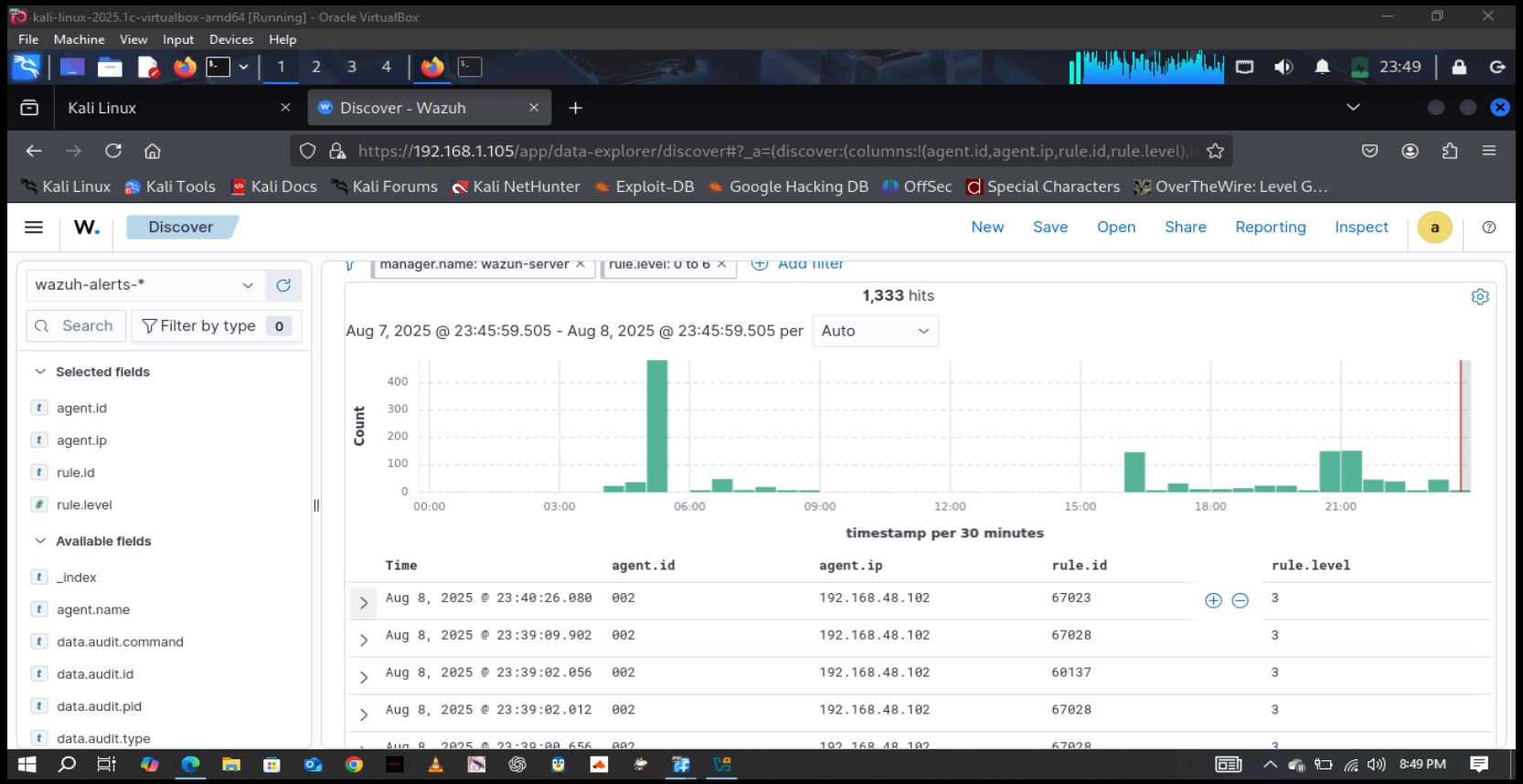
INCIDENT 2: RDP BRUTE FORCE (WINDOWS)

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



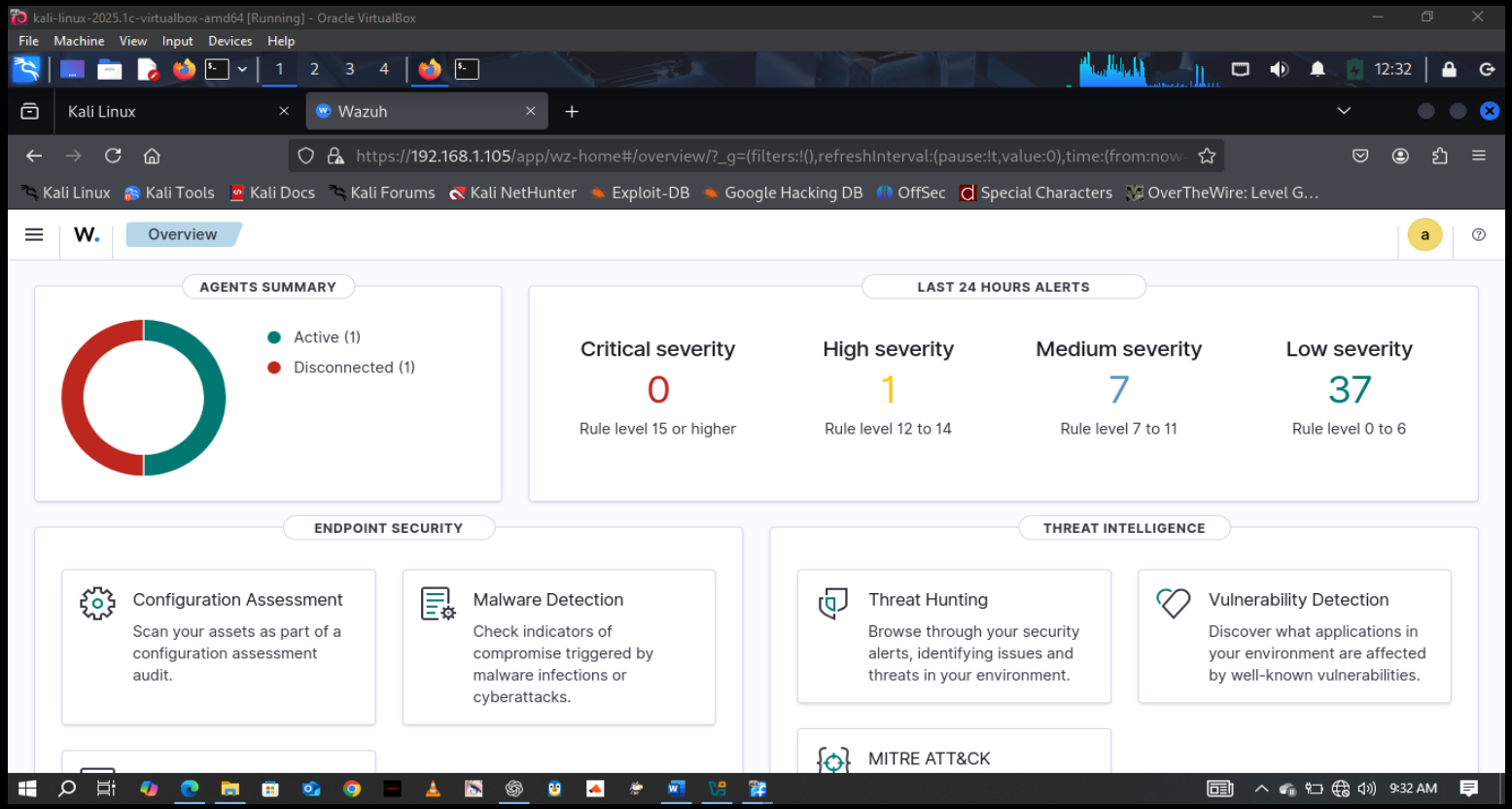
SOC DETECTION: WINDOWS (WAZUH)

- 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