Project Title: Azure Cloud Security Lab - Investigation Phase

Role: Blue Team (SOC Analyst)

Date: December 25, 2025

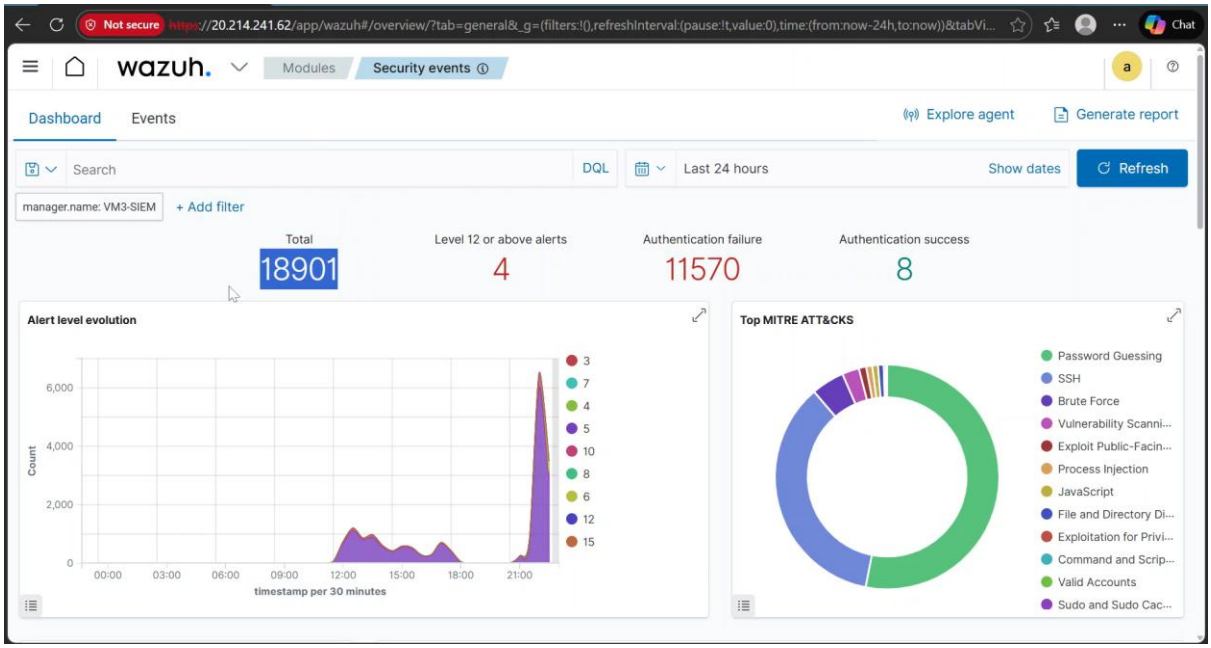
Team Members Name Involved in Blue Teaming

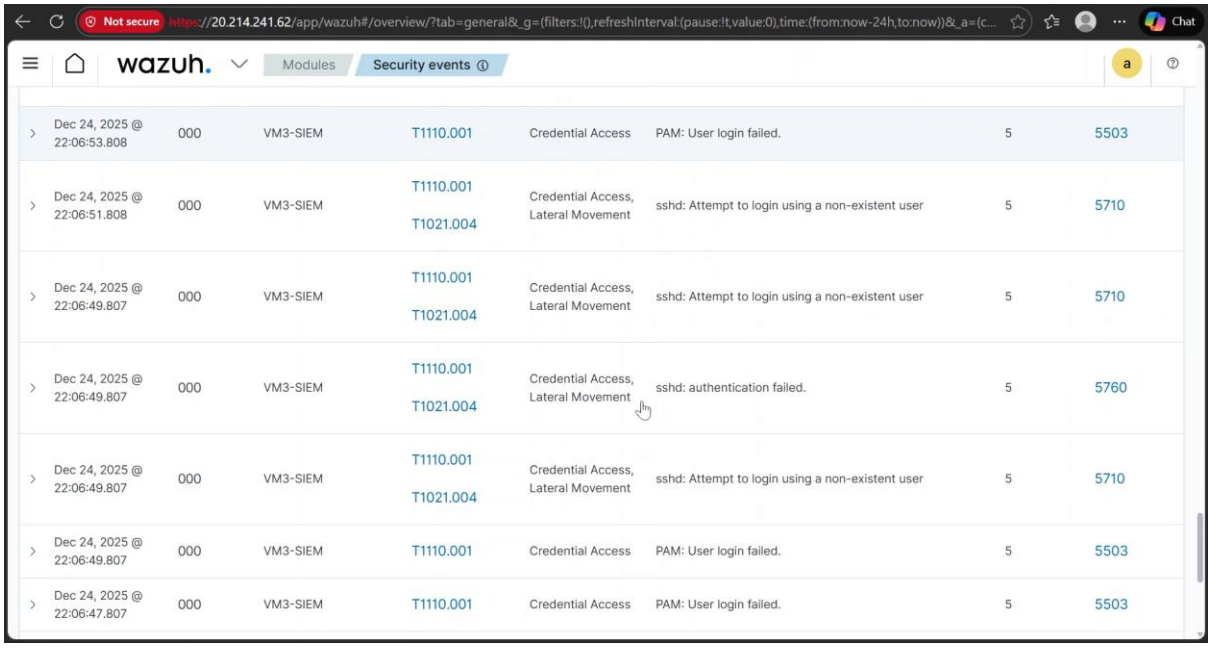
- **Suraj Madharia**
- **Yesh Nirmalkar**

1. Executive Summary The Wazuh SIEM detected multiple high-severity security events on December 24-25, indicating a successful breach of the DMZ Web Server followed by lateral movement to the Internal Network.

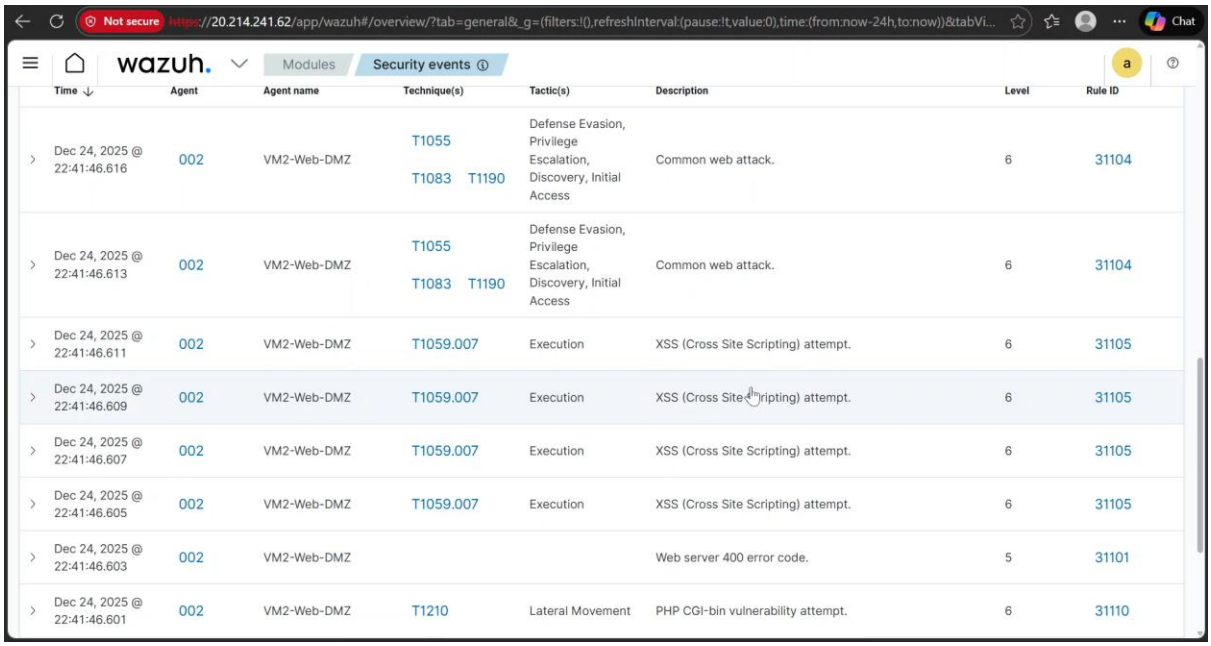
2. Incident Analysis

- **Incident A: Brute Force Detection**
    - **Observation:** A spike of over 12,000+ authentication failures was recorded on VM2.
    - **Source:** External IP (Kali Linux).
    - **SIEM Alert ID:** 5710 (Attempt to login using non-existent user).
    - **Evidence:**



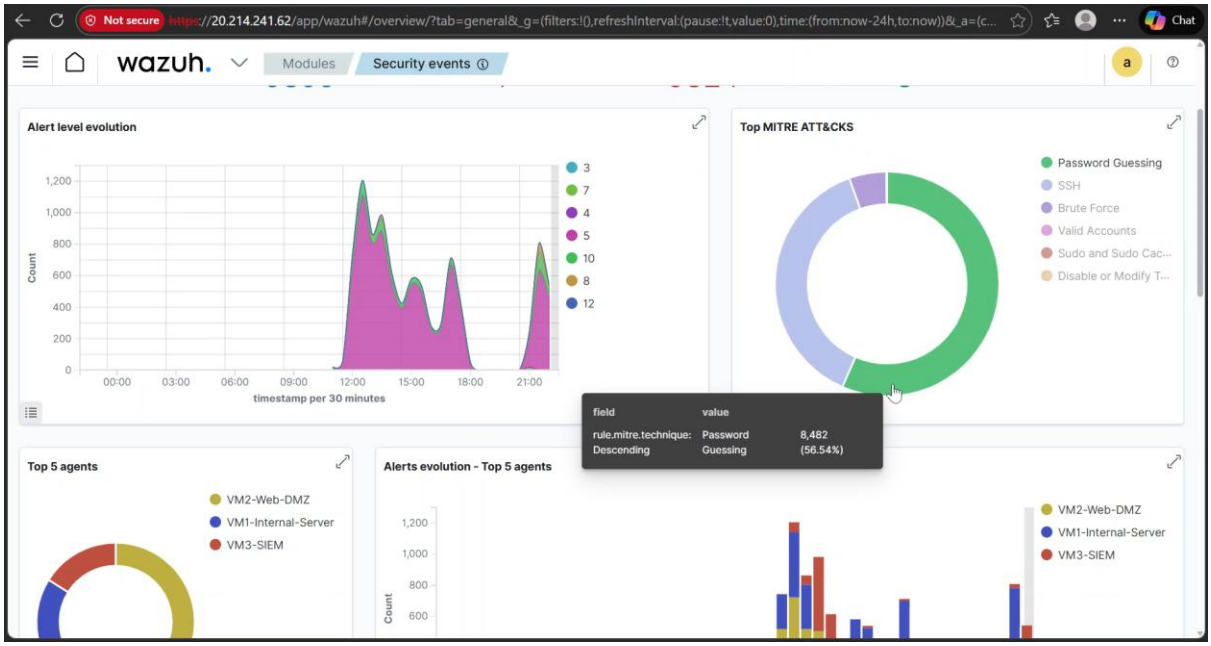


- **Incident B: Web Scanner Detection**
  - **Observation:** SIEM triggered multiple "Level 12" alerts due to rapid 404/403 error codes.
  - **Analysis:** Pattern matches known behavior of the "Nikto" vulnerability scanner.
  - **Evidence:**



- **Incident C: Insider Threat (Lateral Movement)**

- **Observation:** Valid SSH Logins detected on VM1 originating from a *Private IP address* (VM2).
- **Significance:** Indicates the attacker successfully pivoted from the DMZ to the Internal Network.
- **Evidence:**



3. Conclusion The SIEM successfully detected all phases of the attack. However, the initial brute force was successful due to weak password policies, necessitating immediate hardening.