

Project Title: Azure Cloud Security Lab - Investigation Phase

Role: Blue Team (SOC Analyst)

Date: December 25, 2025

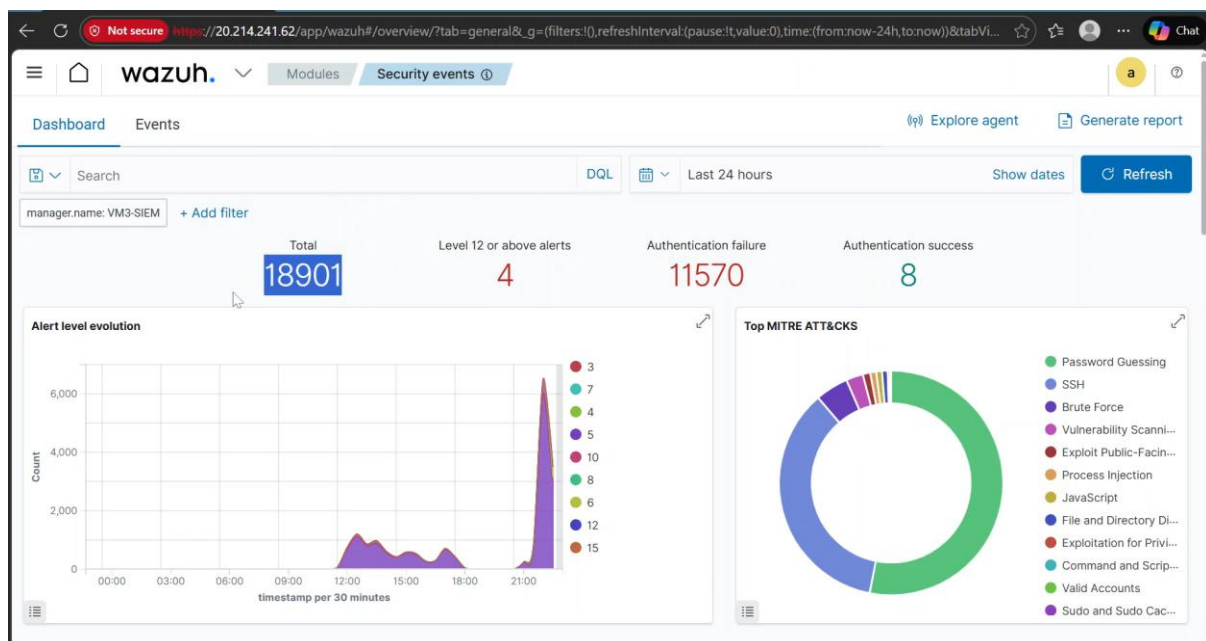
Team Members Name Involved in Blue Teaming

- 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:**



wazuh. Modules Security events ⓘ							
>	Dec 24, 2025 @ 22:06:53.808	000	VM3-SIEM	T1110.001	Credential Access	PAM: User login failed.	5 5503
>	Dec 24, 2025 @ 22:06:51.808	000	VM3-SIEM	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5 5710
>	Dec 24, 2025 @ 22:06:49.807	000	VM3-SIEM	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5 5710
>	Dec 24, 2025 @ 22:06:49.807	000	VM3-SIEM	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5 5760
>	Dec 24, 2025 @ 22:06:49.807	000	VM3-SIEM	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: Attempt to login using a non-existent user	5 5710
>	Dec 24, 2025 @ 22:06:49.807	000	VM3-SIEM	T1110.001	Credential Access	PAM: User login failed.	5 5503
>	Dec 24, 2025 @ 22:06:47.807	000	VM3-SIEM	T1110.001	Credential Access	PAM: User login failed.	5 5503

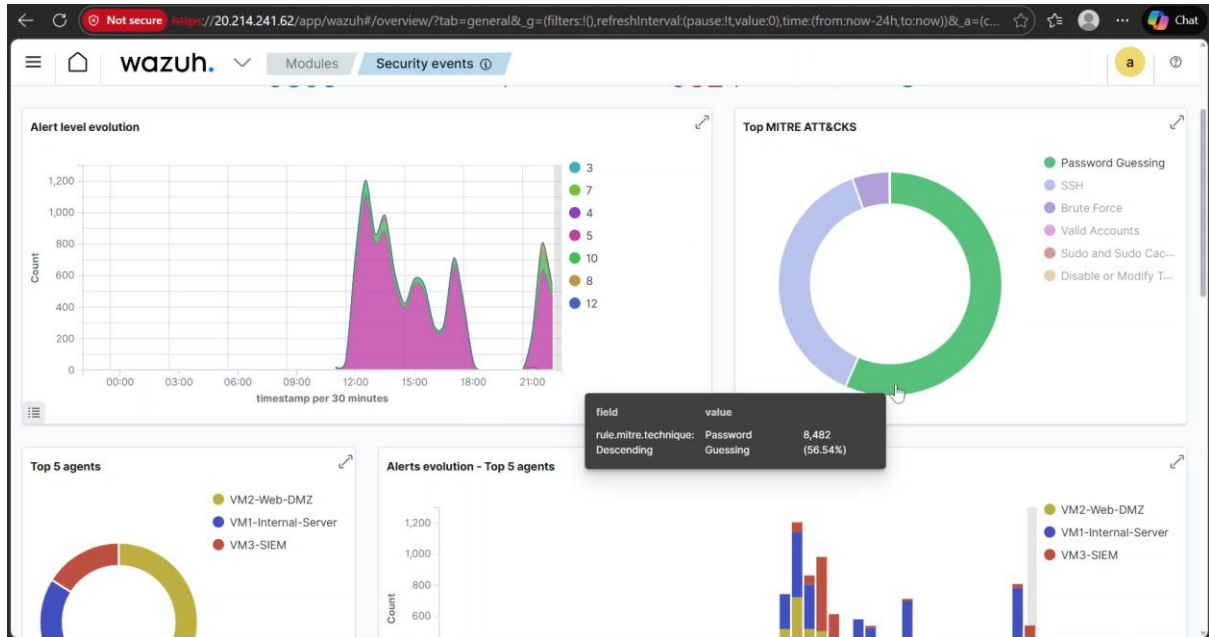
• Incident B: Web Scanner Detection

- **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:**

wazuh. Modules Security events ⓘ							
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
>	Dec 24, 2025 @ 22:41:46.616	002	VM2-Web-DMZ	T1055 T1083 T1190	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Common web attack.	6 31104
>	Dec 24, 2025 @ 22:41:46.613	002	VM2-Web-DMZ	T1055 T1083 T1190	Defense Evasion, Privilege Escalation, Discovery, Initial Access	Common web attack.	6 31104
>	Dec 24, 2025 @ 22:41:46.611	002	VM2-Web-DMZ	T1059.007	Execution	XSS (Cross Site Scripting) attempt.	6 31105
>	Dec 24, 2025 @ 22:41:46.609	002	VM2-Web-DMZ	T1059.007	Execution	XSS (Cross Site Scripting) attempt.	6 31105
>	Dec 24, 2025 @ 22:41:46.607	002	VM2-Web-DMZ	T1059.007	Execution	XSS (Cross Site Scripting) attempt.	6 31105
>	Dec 24, 2025 @ 22:41:46.605	002	VM2-Web-DMZ	T1059.007	Execution	XSS (Cross Site Scripting) attempt.	6 31105
>	Dec 24, 2025 @ 22:41:46.603	002	VM2-Web-DMZ			Web server 400 error code.	5 31101
>	Dec 24, 2025 @ 22:41:46.601	002	VM2-Web-DMZ	T1210	Lateral Movement	PHP CGI-bin vulnerability attempt.	6 31110

• 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.