Blue Team Detection

Objective

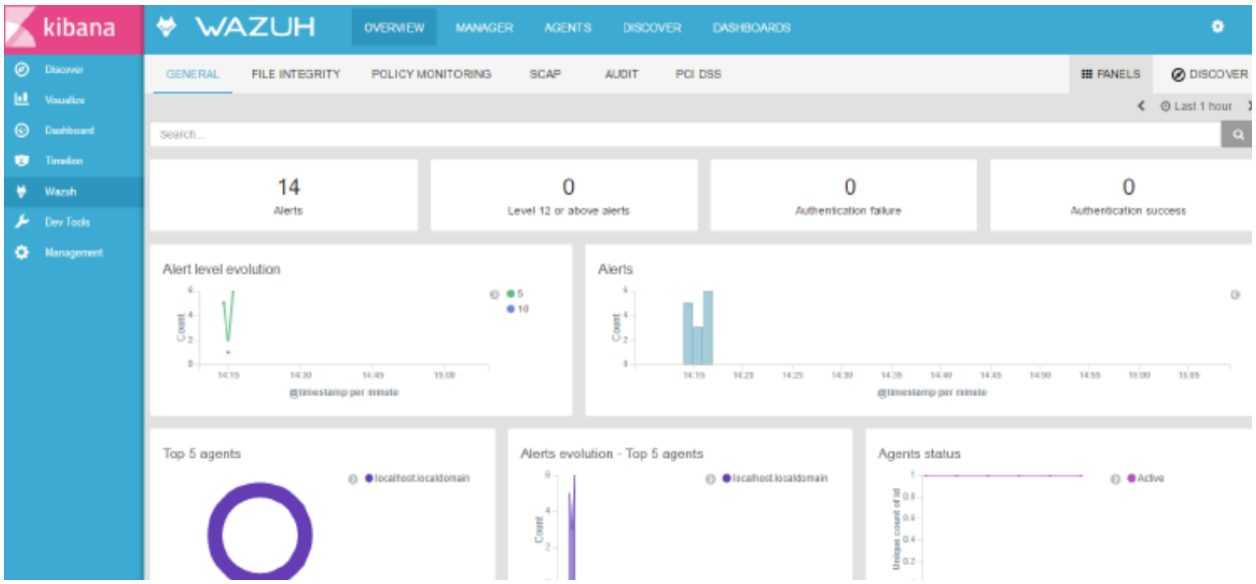
Check if defensive tools detected our attacks.

Security Tool Used

Wazuh (SIEM, Rule Engine)

Observed Alerts

Timestamp	Event	Source IP	Severity	Action Taken
Add from screenshot	Brute-force indicator	<attacker-ip>	Medium	Logged only
Add from screenshot	Suspicious remote login	Victim server	Low	No auto-response
Add from screenshot	Reverse shell behavior	Victim server	Medium	Alerted admin



Detection Outcome

⚠️ Alerts were generated but…
➡ No alerts were blocked
➡ Severity was incorrectly categorized
➡ No automated response triggered

Recommendation Table

Control	Required Improvement
SIEM correlation rules	Identify full kill-chain
Threshold alerts	Reduce false negatives
Active response	Auto-kill malicious sessions
Privilege monitoring	Detect unexpected impersonation