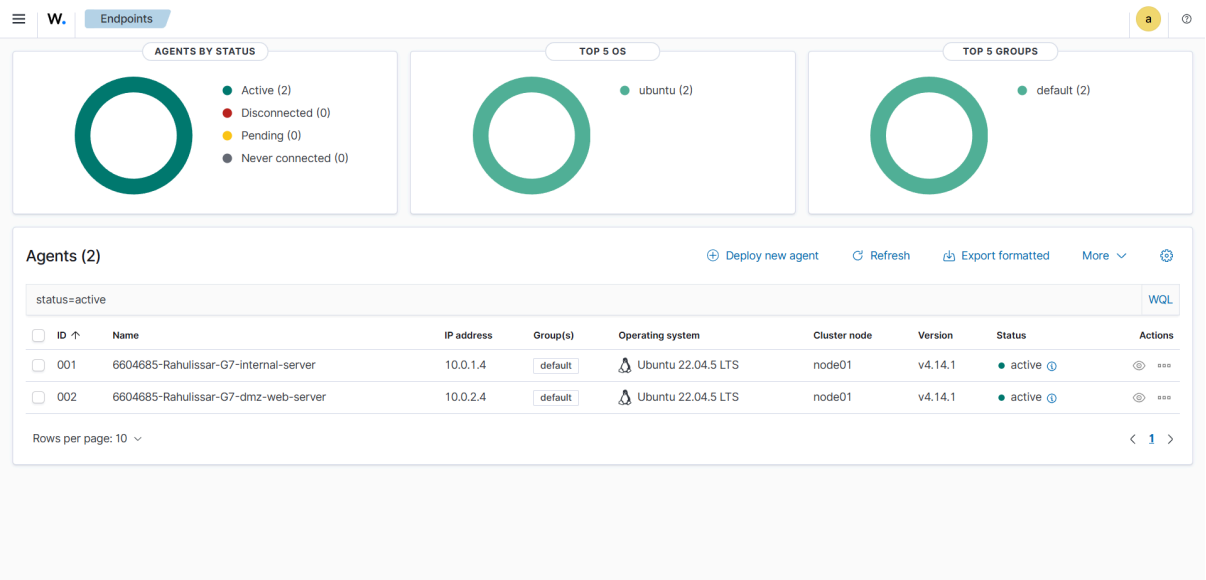
PURPOSE OF THIS REPORT

This report documents the investigation and analysis of security incidents generated during simulated attacks on the cloud-based infrastructure. The objective is to identify malicious activities using SIEM logs, analyze attack patterns, extract indicators of compromise (IOCs), determine root causes, and prepare the environment for security hardening.

SIEM Dashboard :

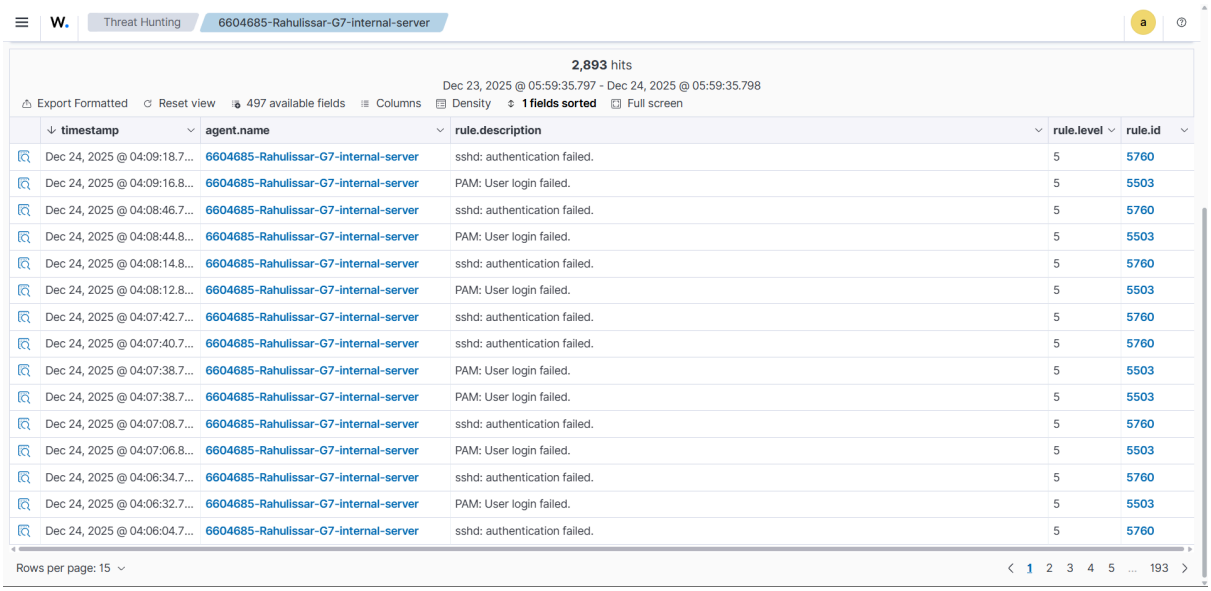


FILTERING ATTACK LOGS

SSH Brute Force Detection

In the **search bar**, apply:

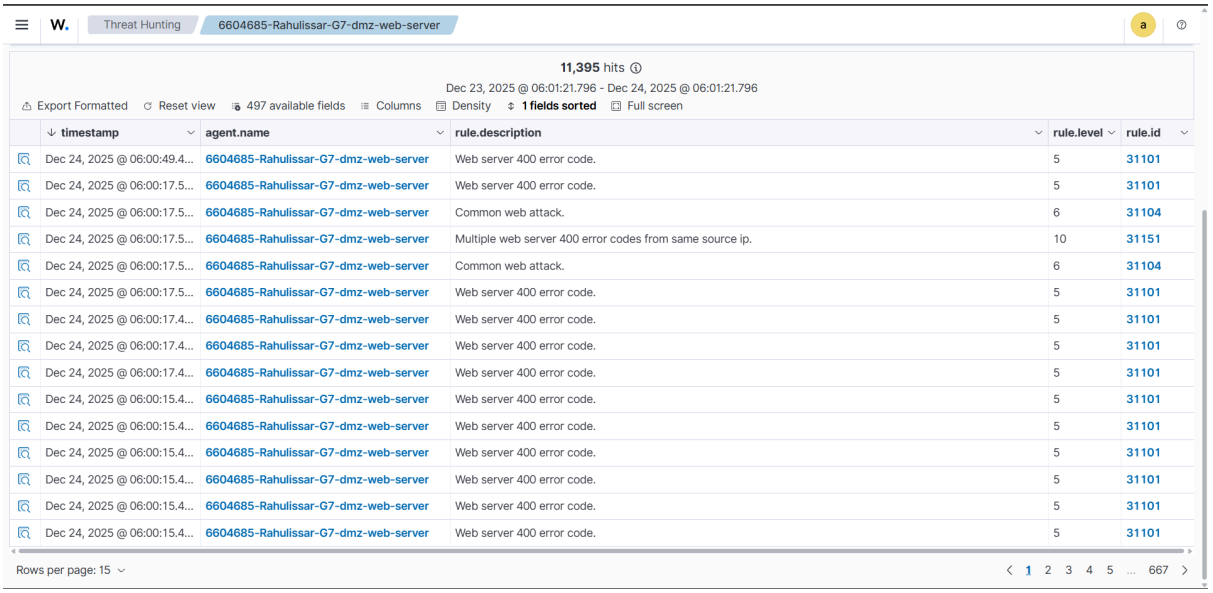
- rule.groups:authentication_failed



Web Attack Detection (VM2)

Filter:

- rule.groups:web



INCIDENT TIMELINE

Incident Overview

The following timeline represents correlated security events detected by the Wazuh SIEM during simulated attack activity against the **DMZ Web Server (VM2)** and **Internal Server (VM1)**. Events include web attack indicators, privilege escalation activity, and system-level changes.

Phase 1: Web Attack on DMZ Server (VM2)

Timestamp (UTC)	Affected Host	Event Description	Rule ID	Severity
06:00:15	DMZ Web Server	Web server returned multiple HTTP 400 error codes	31101	Level 5

06:00:15	DMZ Web Server	Repeated malformed HTTP requests detected	31101	Level 5
06:00:17	DMZ Web Server	Common web attack detected	31104	Level 6
06:00:17	DMZ Web Server	Multiple HTTP 400 errors from same source IP	31151	Level 10
06:00:49	DMZ Web Server	Continued abnormal HTTP requests detected	31101	Level 5

Analyst Interpretation

A burst of HTTP 400 responses within a very short time window indicates automated web attack activity. The presence of the “Common web attack” rule and correlation rule 31151 confirms directory enumeration or malformed request fuzzing, commonly associated with tools such as Nikto or Gobuster.

Phase 2: Privilege Escalation & System Activity (VM1 – Internal Server)

Timestamp (UTC)	Affected Host	Event Description	Rule ID	Severity
04:12:02	Internal Server	New Debian package installed	2902	Level 7
04:12:09	Internal Server	Successful sudo to ROOT executed	5402	Level 3
04:12:09	Internal Server	PAM login session opened	5501	Level 3
04:12:09	Internal Server	PAM login session closed	5502	Level 3

04:12:14	Internal Server	Repeated sudo to ROOT execution	5402	Level 3
04:12:18	Internal Server	Auditd configuration changed	80705	Level 3
04:33:18	Internal Server	Additional sudo session opened and closed	5501 / 5502	Level 3

Analyst Interpretation

Multiple successful sudo executions followed by PAM session activity indicate privilege escalation activity. The detection of an auditd configuration change further suggests administrative-level access was obtained, either by a legitimate user or following a successful compromise. These events confirm that the internal server was accessed with elevated privileges during the attack window.

ATTACK CHAIN CORRELATION

The incident timeline shows a clear attack progression. The attacker initially targeted the external-facing DMZ web server using automated web attack techniques, generating multiple HTTP 400 errors and triggering web attack correlation rules. Subsequently, privileged activity was detected on the internal server, including repeated sudo access and system configuration changes. This suggests either lateral movement or misuse of elevated credentials following initial reconnaissance.

LOG SOURCE ANALYSIS

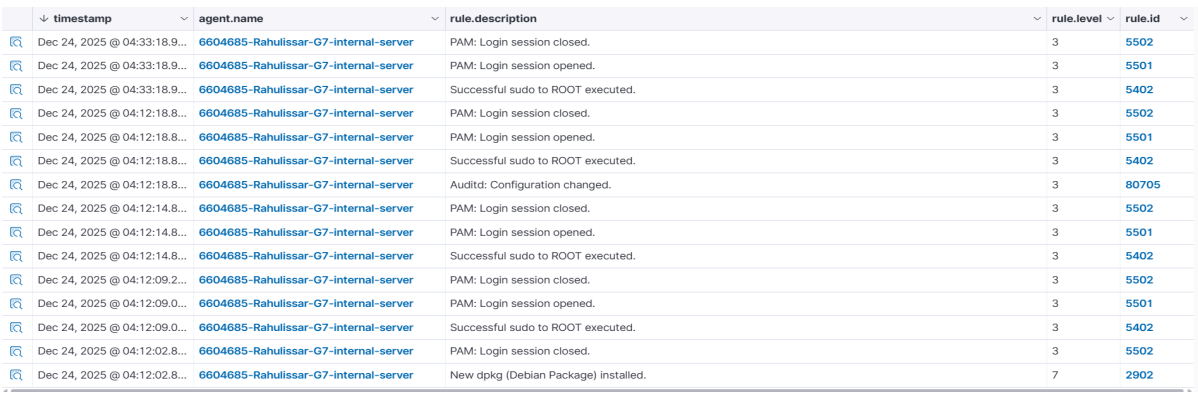
1. **Authentication Logs (`auth.log`)**

Where they come from:

- `/var/log/auth.log`

Wazuh rule example:

- `sshd: Failed password`



timestamp	agent.name	rule.description	rule.level	rule.id
Dec 24, 2025 @ 04:33:18.9...	6604685-Rahulissar-G7-internal-server	PAM: Login session closed.	3	5502
Dec 24, 2025 @ 04:33:18.9...	6604685-Rahulissar-G7-internal-server	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 04:33:18.9...	6604685-Rahulissar-G7-internal-server	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 04:12:18.8...	6604685-Rahulissar-G7-internal-server	PAM: Login session closed.	3	5502
Dec 24, 2025 @ 04:12:18.8...	6604685-Rahulissar-G7-internal-server	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 04:12:18.8...	6604685-Rahulissar-G7-internal-server	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 04:12:18.8...	6604685-Rahulissar-G7-internal-server	Auditd: Configuration changed.	3	80705
Dec 24, 2025 @ 04:12:14.8...	6604685-Rahulissar-G7-internal-server	PAM: Login session closed.	3	5502
Dec 24, 2025 @ 04:12:14.8...	6604685-Rahulissar-G7-internal-server	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 04:12:14.8...	6604685-Rahulissar-G7-internal-server	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 04:12:09.2...	6604685-Rahulissar-G7-internal-server	PAM: Login session closed.	3	5502
Dec 24, 2025 @ 04:12:09.0...	6604685-Rahulissar-G7-internal-server	PAM: Login session opened.	3	5501
Dec 24, 2025 @ 04:12:09.0...	6604685-Rahulissar-G7-internal-server	Successful sudo to ROOT executed.	3	5402
Dec 24, 2025 @ 04:12:02.8...	6604685-Rahulissar-G7-internal-server	PAM: Login session closed.	3	5502
Dec 24, 2025 @ 04:12:02.8...	6604685-Rahulissar-G7-internal-server	New dpkg (Debian Package) installed.	7	2902

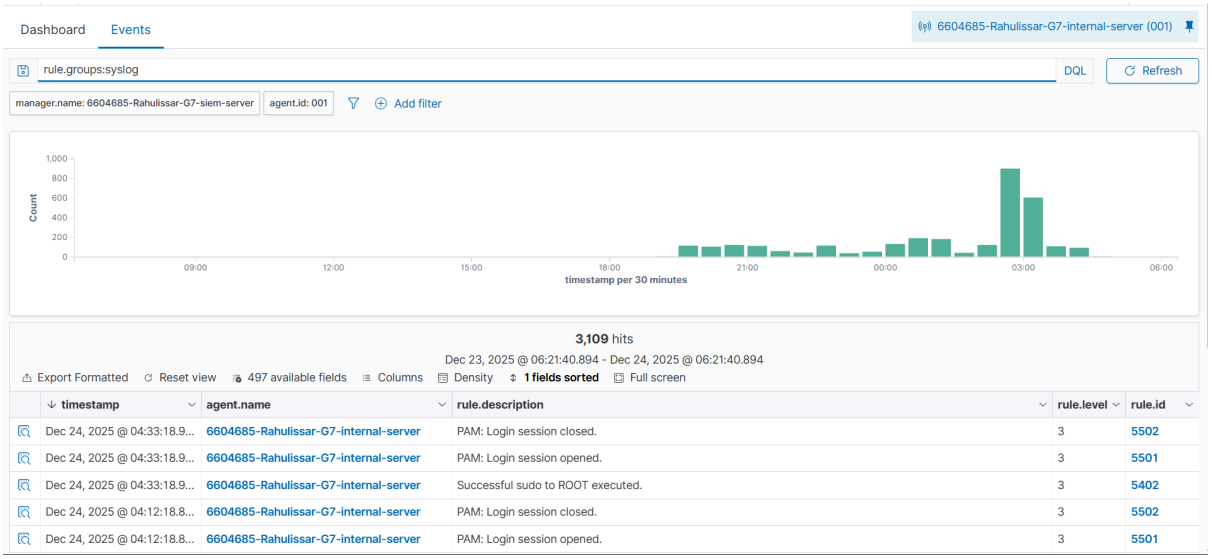
2. Syslog Analysis

Purpose:

- Service starts
- Port scans
- System activity

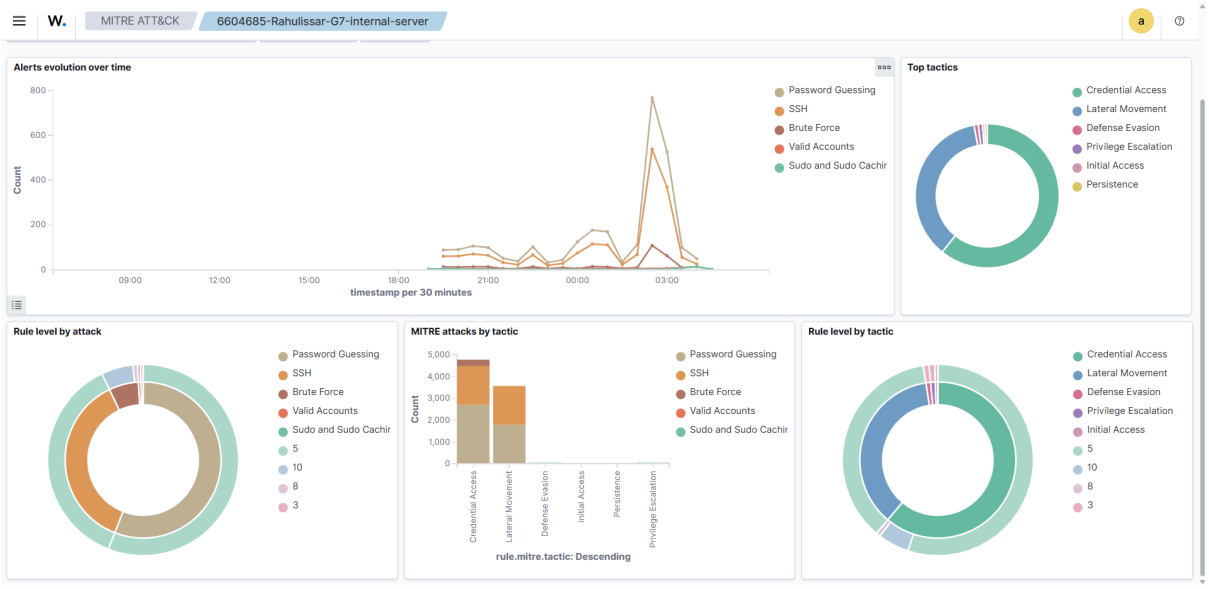
Filter:

- `rule.groups:syslog`



MITRE ATT&CK MAPPING

VM 1:



VM 2:

ROOT CAUSE ANALYSIS

The primary cause of the incidents was insecure default configurations. SSH service was publicly exposed without rate limiting or key-based authentication. The web server allowed directory enumeration. No firewall rules were applied, allowing unrestricted inbound access.