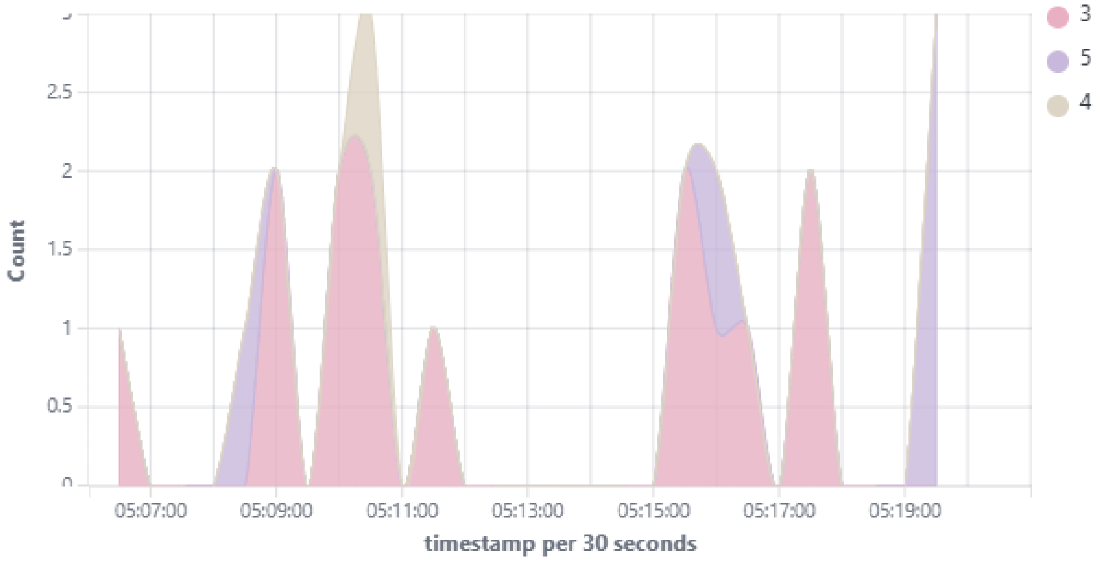
Threat hunting report

Browse through your security alerts, identifying issues and threats in your environment.

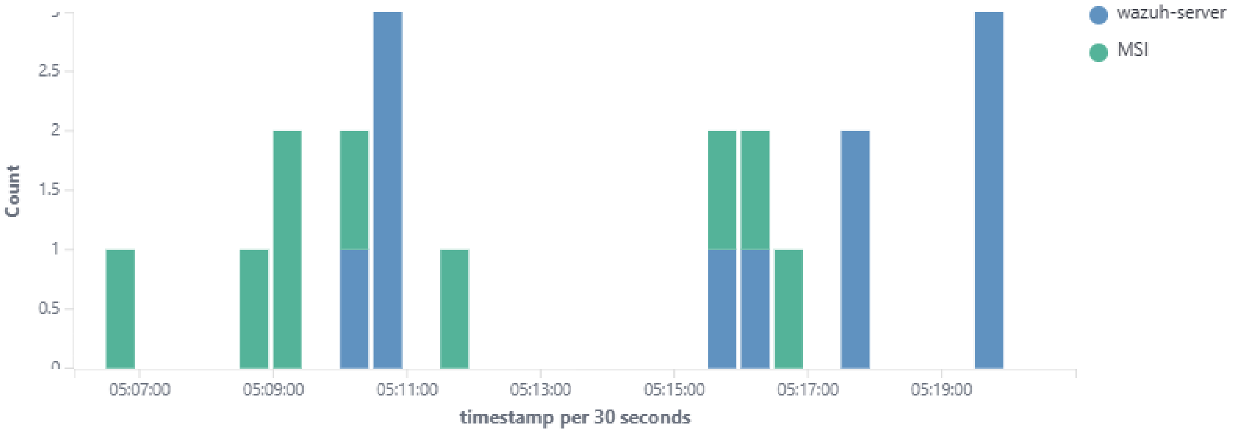
2025-10-10T05:06:05 to 2025-10-10T05:21:05

manager.name: wazuh-server

Top 10 Alert level evolution



Alerts evolution - Top 5 agents



20

- Total -

0

- Level 12 or above alerts -

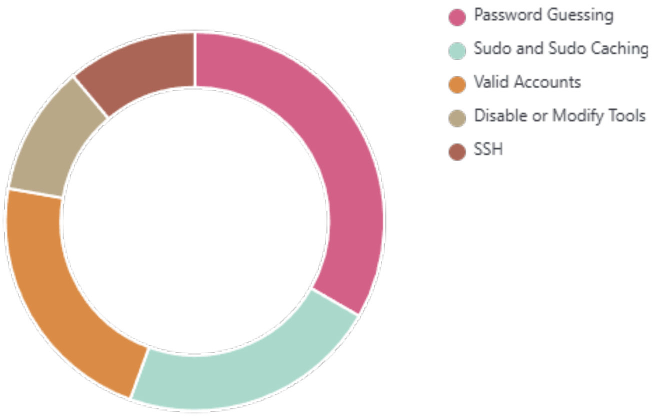
3

- Authentication failure -

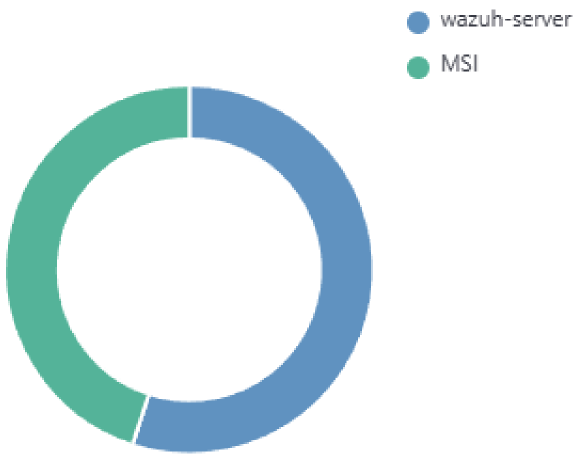
2

- Authentication success -

Top 10 MITRE ATT&CKS



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
503	Wazuh agent started.	3	3
5501	PAM: Login session opened.	3	2
5502	PAM: Login session closed.	3	2
61102	Windows System error event	5	2
61104	Service startup type was changed	3	2
502	Wazuh server started.	3	1
506	Wazuh agent stopped.	3	1
5402	Successful sudo to ROOT executed.	3	1
5403	First time user executed sudo.	4	1
5503	PAM: User login failed.	5	1
5557	unix_chkpwd: Password check failed.	5	1
5760	sshd: authentication failed.	5	1
60642	Software protection service scheduled successfully.	3	1
80730	Auditd: SELinux permission check.	3	1